Revista del Ministerio de Trabajo y Economía Social

Derecho del trabajo

GOBIERNO DE ESPAÑA
MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL

148

2021

Revista del Ministerio de Trabajo y Economía Social

Derecho del Trabajo

DIRECTORA
Blanca Cano Sánchez
Secretaria General Técnica

SUBDIRECTOR
Luis Navas López
Subdirector General de Informes, Recursos y Publicaciones

SECRETARÍA
Subdirección General de Informes, Recursos y Publicaciones
del Ministerio de Trabajo y Economía Social
Agustín de Bethencourt, 11
28003 Madrid
Telfs: 91 363 23 05
91 363 23 05 / 03
Fax: 91 363 23 49
Correo Electrónico: proproeditorial@mites.gob.es
Internet: https://www.mites.gob.es/es/revistaministerio/

RET: 21-2.387

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita y distribuye:
Ministerio de Trabajo y Economía Social
Subdirección General de Informes,
Recursos y Publicaciones
Agustín de Bethencourt, 11. 28003 Madrid
NIPO Papel: 117-20-031-8
NIPO PDF: 117-20-033-9
ISSN Papel: 2660-4647
ISSN Electrónico: 2660-4655
Depósito legal: M-12.168-1998
Diseño cubierta: CSP
Diseño interior: C & G
Imprime: Estilo Estugraf Impresores, S.L. • Telf. 91 808 62 00

Revista del Ministerio de Trabajo y Economía Social
Derecho del Trabajo

PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA
DE LOS DERECHOS DIGITALES EN EL ÁMBITO LABORAL

SUMARIO

Journal of the Ministry of Labour and Social Economy
Labour Law

THE PROTECTION OF PERSONAL DATA AND DIGITAL RIGHTS IN THE WORKPLACE

CONTENTS

Editorial

Editorial

JOAQUÍN GARCÍA MURCIA*

1.- El cambio acelerado de la sociedad al que estamos asistiendo en los últimos tiempos, impulsado en buena medida por los constantes avances de la tecnología de la información y la comunicación, no deja de producir efectos en el ámbito particular de las relaciones de trabajo. Muchas son sus muestras y manifestaciones. Es indudable, por lo pronto, que se han incrementado notablemente las posibilidades de organización, control y supervisión del trabajo por parte del empresario, lo mismo que han crecido los riesgos de afectación a la esfera íntima o privada de la persona del trabajador. Pero no todo se mueve en esas coordenadas. También han surgido nuevas cargas y obligaciones para la empresa, al mismo tiempo que han menguado muchos de los rigores habituales del trabajo, aunque hayan aparecido otros. La instalación masiva y el uso generalizado de soportes digitales para la organización y realización del trabajo han creado, en cualquier caso, un nuevo escenario para la configuración y el desenvolvimiento de la relación laboral, con nuevos matices y horizontes en la tabla de derechos y deberes de quienes comprometen su prestación de servicios a cambio de salario y nuevas perspectivas y exigencias para el ejercicio de los clásicos poderes empresariales. Como siempre, todo ello ha supuesto también nuevas demandas para el ordenamiento jurídico, y no sólo para la acción del legislador. Como era previsible, antes de que pudiera llegar la añorada respuesta legal tuvieron que intervenir muchas veces las correspondientes instancias jurisdiccionales, que desde los primeros momentos debieron hacer frente a esta clase de problemas mediante su típica función de análisis y resolución de casos concretos. Naturalmente, esta labor de jueces y tribunales nunca ha podido apartarse de la dimensión pragmática y casuística que le es consustancial, pero en honor a la verdad también hay que reconocer que paulatinamente ha dado lugar a una nutrida doctrina que ha servido para insuflar un primer aliento jurídico en esas nuevas fronteras del mundo laboral y, a la postre, para acuñar conceptos y criterios de suma utilidad con vistas a la progresiva construcción del sistema normativo de referencia.

Ciertamente, con sus aciertos y sus defectos, la doctrina judicial y en especial la jurisprudencia emanada de los altos tribunales, han sido durante mucho tiempo no sólo el adelantado de la ley sino también el único soporte disponible en esta acuciante y complicada tarea de adaptación del entramado jurídico. De cualquier manera, el legislador ha tenido que ir haciéndose cargo de estas vicisitudes de la sociedad de nuestro tiempo de modo progresivo. Todos hemos podido ver que la pandemia covid-19 ha actuado como un imprevisto factor de aceleración de esta clase de cambios normativos, señaladamente en lo que se refiere a determinadas formas de trabajo. Pero

* Catedrático de Derecho del Trabajo y Seguridad Social. Universidad Complutense de Madrid.

el proceso de acondicionamiento legal impulsado por las transformaciones modernas del sistema social y productivo tiene raíces bastante más profundas y duraderas. Tal vez pueda decirse que nace con el cambio de siglo, aunque sus primeros pasos tengan antecedentes significativos en los tramos finales de la centuria anterior. Los casos de Francia e Italia, con sus respectivas y sucesivas reformas en el *Code du Travail* y en el *Statuto dei Lavoratori*, pueden ser buenos ejemplos de esas nuevas tendencias de la legislación laboral y social. Pero el fenómeno no puede entenderse de forma cabal si no se repara en las acciones emprendidas por las instituciones de la Unión Europea y, de manera más específica, si no se tiene en cuenta la actividad normativa registrada en el novedoso territorio del tratamiento de los datos personales. Es evidente que la incidencia de la nueva tecnología no se agota en esa concreta parcela de la vida social y comercial, y que su impacto se deja notar en muchos otros aspectos de las relaciones humanas. Sin embargo, también lo es que las exigencias de regulación engendradas por ese tipo de operaciones tienen mucho que ver con las facilidades de captación, procesamiento y transmisión de los datos personales que van de la mano del desarrollo tecnológico, y que la aprobación de normas sobre esta materia ha actuado a fin de cuentas como una especie de punta de lanza en la renovación "tecnológica" de los ordenamientos jurídicos. De hecho, las primeras normas sobre tratamiento de datos personales se referían en exclusiva a los actos de carácter "automatizado". Digna de reconocimiento es, en todo caso, la actividad desplegada por la Unión Europea a través de recomendaciones, orientaciones o documentos de similar factura en torno a la innovación tecnológica y sus múltiples consecuencias en el ámbito del empleo y las relaciones sociales.

De sobra es sabido que las primeras tomas de posición respecto del tratamiento de los datos personales no pertenecen a la Unión Europea, sino al Consejo de Europa. No obstante, cabe decir que la normativa comunitaria ha cobrado desde hace tiempo el papel de protagonista, al menos por lo que se refiere a nuestro entorno más inmediato. Tras una primera etapa cubierta por la Directiva de 1995, el Reglamento aprobado en el año 2016 ha pasado a erigirse en efecto en el centro de referencia, entre otras razones por su declarado propósito de incrementar el radio de acción y el grado de precisión de las reglas precedentes. Lo cierto es que se trata de una regulación particularmente extensa tanto en términos absolutos como en números comparativos, con nada menos que 99 artículos distribuidos en once capítulos. Su contenido, especialmente denso y abigarrado, cumple a la postre cuatro funciones básicas: la delimitación de su alcance material y su campo de juego (ámbito de aplicación, definiciones "oficiales", principios fundamentales, condiciones de uso y tratamiento de datos y derechos del interesado), la identificación de instancias y sujetos competentes (posición jurídica de responsables y delegados, obligaciones de los Estados y naturaleza de las autoridades de control), el establecimiento de mecanismos de aplicación y efectividad de sus previsiones y mandatos (códigos de conducta, operaciones de certificación, procedimientos de reclamación, infracciones y sanciones y reglas sobre coordinación y coherencia entre los sistemas nacionales), y la delimitación selectiva de "situaciones específicas de tratamiento" con vistas a su más apropiada regulación (como el "tratamiento en el ámbito laboral" o el tratamiento con fines de "investigación científica o histórica", entre otras).

2.- El Reglamento de 2016 parte desde luego del reconocimiento del derecho a la protección de datos personales en el ámbito de la Unión Europea, efectuado unos años antes, y de manera taxativa, por el artículo 8 de su Carta de Derechos Fundamentales. No describe de forma directa el alcance y contenido del derecho, pero sí se refiere, de una u otra forma, a sus dos grandes elementos, que se vierten en otras tantas facultades del interesado: la de decidir sobre el tratamiento de sus datos personales y la de reclamar información fiel, puntual y actualizada acerca de las correspondientes operaciones. El primero de esos elementos se traduce esencialmente en la exigencia de consentimiento del interesado para el tratamiento de sus datos personales, una

regla general que intensifica su potencia en el caso de datos especialmente protegidos, por ser especialmente sensibles y delicados, y que en cualquier caso cuenta con numerosas excepciones. Por su parte, el segundo de los elementos se refleja de modo principal en la concesión al interesado de un derecho de información que reviste contornos muy amplios y generales, que en determinados supuestos puede sufrir modulaciones pero que opera en todo tipo de situaciones, tanto si los datos se obtienen a través de su consentimiento como si se captan o consiguen por otros procedimientos legalmente admitidos. De cualquier forma, esos elementos nucleares vienen desgranados por la propia norma en una serie bastante nutrida de derechos más específicos, que, por así decirlo, son los que en realidad permiten al interesado el control sobre sus datos personales, aunque a veces sea con algunos matices y otras con sometimiento a determinadas condiciones. Se trata de los derechos de acceso, rectificación, supresión, oposición, limitación o portabilidad, a los que se une asimismo el particular derecho de las personas a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos, incluida la eventual elaboración y utilización de "perfiles". Son, como puede apreciarse, manifestaciones o facetas de la facultad de autodeterminación en la que, como dijo en su momento nuestro Tribunal Constitucional, se resume a fin de cuentas el contenido de este emergente y singular derecho a la protección de datos personales.

Por el momento, la Unión Europea no ha aprobado normas que específicamente atiendan la protección de datos personales en medios profesionales, a diferencia de lo que ha hecho para algún otro sector de las relaciones comerciales y económicas o en determinados ámbitos institucionales. Pero estas disposiciones generales sobre protección de datos personales tampoco han excluido el ámbito laboral o profesional de su campo de aplicación, por lo que hay que partir de su vigencia también en este terreno. Ya lo entendió así la Directiva de 1995, y así ha vuelto a suceder con el Reglamento 2016/679, que muestra mayor determinación aún en ese mismo sentido, al incluir menciones claras a ese terreno laboral en su exposición de motivos e incorporar algunos pasajes normativos que de modo explícito tienen como punto de mira esa parte de la realidad social. En realidad, el Reglamento de 2016 hace patente su proyección sobre la relación de trabajo desde su propio preámbulo, en el que se habla, como una primera aproximación, de la necesidad de conciliar el derecho de protección de datos con la libertad de empresa (apartado 4). Ciertamente, no es muy detallada esa norma comunitaria a la hora de explicar las razones por las que en esa concreta parcela de las relaciones sociales se hace necesaria la aplicación de las normas sobre tratamiento de datos personales y, en su caso, la previsión a tal efecto de determinadas reglas especializadas. Pero es obvio que en el ámbito de la relación laboral concurren suficientes razones de peso como para prestar atención al tratamiento de los datos personales y que inciden además circunstancias particulares que justifican un cuidado especial. Hay que tener en cuenta, sobre todo, que los datos relativos a la persona del trabajador, siendo sin duda datos personales dignos de protección, son en muchos casos datos sobre los que el trabajador no puede reclamar reserva plena, en la medida en que son imprescindibles para la celebración y ejecución del contrato de trabajo. El hecho de que la relación de trabajo sea de tracto sucesivo y se desarrolle a lo largo del tiempo exige, para más señas, un sistema adecuado de conservación de los datos obtenidos y manejados, hasta que pueda darse por finalizado el vínculo entre las partes. En definitiva, el Reglamento comunitario de 2016, como en su momento hizo la Directiva precedente, se hace cargo de las necesidades de regulación de las relaciones laborales y profesionales, aunque sus incursiones en ese territorio resulten a la postre bastante escuetas y limitadas.

Puede decirse, en síntesis, que el Reglamento 2016/679 aborda ese particular frente con dos tipos de previsiones. De un lado, mediante la introducción de incisos o matices en las reglas de carácter general destinados a modular o ajustar su aplicación en función de las características de la relación de trabajo o, en general, a la vista de la peculiaridad de los asuntos profesionales.

A veces son menciones explícitas y cuasi nominativas, y otras veces no se trata más que de alusiones o referencias implícitas o indirectas. En algunos casos son menciones precisas al trabajo o al trabajador, y en algunos otros supuestos se trata de previsiones dirigidas a reglas o instituciones propias del mundo del trabajo, como la seguridad y salud en el trabajo o la protección social. A veces son menciones con fines de aclaración o concreción, otras veces no entrañan más que matices o salvedades respecto de la regla general. En un esfuerzo de síntesis, todas ellas podrían ser agrupadas en dos grandes apartados. Al primer grupo podríamos incorporar aquellas previsiones normativas que, frente a la regla general, admiten el tratamiento de datos en el ámbito de la relación de trabajo aun sin consentimiento del interesado, que en este contexto es principalmente el trabajador; no se habla en estos casos del contrato de trabajo de manera expresa, pero son referencias que sin duda lo comprenden, pues ninguna duda existe, en efecto, de que es aplicable al vínculo laboral la regla que permite el tratamiento de datos personales cuando ello resulta "necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales", o cuando es "necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento". En el segundo grupo podemos incluir, por su parte, aquellas menciones que admiten la captación y tratamiento de datos que, por ser especialmente sensibles (o reveladores de aspectos muy íntimos o delicados de la persona), no pueden seguir el procedimiento ordinario; tampoco son menciones de proyección exclusiva al ámbito laboral, pero de nuevo son referencias normativas que conectan de manera muy clara con la relación de trabajo o con la faceta profesional de las personas.

El segundo rastro de la atención prestada por el Reglamento de 2016 a los asuntos laborales lo encontramos en el capítulo de las disposiciones específicas, que, en concordancia con lo ya anunciado en la exposición de motivos de la norma, reservan un hueco particular para el "tratamiento en el ámbito laboral". Condensadas en su artículo 88, estas disposiciones específicas suponen, en esencia, una habilitación a los Estados miembros de la Unión Europea para que establezcan "normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral". Según ese mismo precepto, los Estados pueden acometer esas tareas directamente, mediante la oportuna aprobación de "disposiciones legislativas", pero también pueden hacerlo, como tantas otras veces permite la propia normativa comunitaria, mediante una especie de delegación en la actividad de negociación colectiva, para que sean las representaciones colectivas de trabajadores y empresarios las encargadas en última instancia de proporcionar esa regulación especializada. En todo caso, tanto las normas estatales como los acuerdos o convenios colectivos habrán de incluir "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".

A poco que se piense sobre ello puede advertirse que la principal cuestión que plantea esa importante remisión a los ordenamientos nacionales radica en el margen de actuación con el que pueden contar los Estados miembros para llevar a cabo esa función reguladora, a la vista del nivel de protección establecido con carácter general por el propio Reglamento comunitario. En este

sentido, es importante tener en cuenta que se habla de "normas más específicas" y no de normas más protectoras, por lo que cabe pensar que el Reglamento de 2019 no prohíbe que, mediante esas normas internas, los sistemas estatales modulen o incluso rebajen en el ámbito laboral los niveles de protección general, siempre, como es lógico, que se protejan adecuadamente los derechos fundamentales afectados y los intereses legítimos en juego, como expresamente se reclama. Parece hablarse, en consecuencia, de una regulación especial que proporcione el pertinente grado de adaptación a una parcela de la realidad social que está sujeta a exigencias particulares en su configuración y en su funcionamiento. De todos modos, habrá que esperar a que haya muestras de interpretación autorizada de esas cláusulas comunitarias, a través, por ejemplo, de la intervención jurisdiccional del Tribunal de Justicia.

3.- Como es sabido, España inició su andadura en estos terrenos mediante una Ley Orgánica de 1992, bastante tiempo después de que el artículo 18.4 CE llamara al legislador para limitar "el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" y de que el Convenio número 108 del Consejo de Europa (de 1981) se adentrara en estos temas de frontera. La legislación española de 1992, dedicada específicamente al tratamiento automatizado de los datos de carácter personal, supuso una primera reacción frente a los riesgos de la nueva tecnología en las relaciones sociales, pero tal vez sirviera más como entrenamiento del sistema que como soporte estructural. Lo cierto es que la entrada en escena de la Directiva 95/46/CE condujo a la renovación de nuestra normativa interna mediante la aprobación de Ley Orgánica 15/1999, que, como marcaban las directrices comunitarias de referencia, entrañaba la extensión de este novedoso bloque legal a todo tipo de tratamiento de datos personales. El factor determinante a partir de ese momento era la existencia de datos personales "susceptibles de tratamiento", con independencia de su soporte o modo de registro. Seguramente puede decirse que la LO de 1999 albergaba suficientes mimbres como para mantener su vigencia al margen de posibles alteraciones de su entorno normativo. Sin embargo, la aprobación en el seno de la Unión Europea del Reglamento 2016/679 abrió las puertas para una nueva reconsideración del estado de nuestra legislación interna, no sólo por sus indudables innovaciones respecto de la anterior normativa comunitaria, sino también, y sobre todo, por sus numerosas llamadas y exigencias de regulación a los Estados miembros, algunas de ellas, como hemos visto, referidas a materia laboral. Fruto de esa nueva activación del poder legislativo fue la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, precedida por una primera adaptación de nuestro sistema, con sentido eminentemente logístico, a través del RDL 5/2018, de 27 de julio.

Como da a entender su propio enunciado, la LO 3/2018 cubre dos vertientes próximas pero separables de la realidad social y normativa. Por lo pronto, y acaso antes que nada, es la regulación española sobre tratamiento de datos personales, como instrumento de desarrollo y apoyo, en términos nacionales, del Reglamento UE 2016/679. En esta primera vertiente, la LO 3/2018 parte como no podía ser de otro modo de que la protección de datos personales es un "derecho fundamental de las personas físicas" que ha de ejercerse y garantizarse conforme a los principios informadores y las líneas conceptuales de dicha norma comunitaria. Con ese paradigma a la vista, la LO 3/2018 se ocupa en sus sucesivos capítulos de los "principios de protección de datos", del ejercicio de los derechos reconocidos a los interesados, de las especiales condiciones de tratamiento de determinados datos personales, de las facultades y obligaciones de los responsables, encargados y delegados de protección de datos, de la elaboración y certificación de códigos de conducta y de la transferencia internacional de datos personales. Como era de esperar, también se encarga de designar las autoridades españolas competentes en esta materia (entre las que sigue destacando la Agencia Española de Protección de Datos, junto a las pertinentes autoridades autonómicas),

de fijar el procedimiento de actuación en relación con eventuales reclamaciones relativas al tratamiento de datos y de confeccionar el régimen nacional de infracciones y sanciones en este terreno, con la clásica distinción entre infracciones leves, graves y muy graves, la descripción de los criterios de graduación de las sanciones y la previsión de publicación oficial de ciertas sanciones (las impuestas a persona jurídica por un valor superior a un millón de euros). En términos generales es traslación y complemento instrumental del reglamento 2016/679, pero también es verdad que en algunos aspectos proporciona reglas algo más minuciosas y precisas, como sucede a propósito de la exigencia de "exactitud de los datos", de los deberes de confidencialidad o de las condiciones de válida prestación del consentimiento por parte del interesado.

Esta primera parte de la LO 3/2018 es con seguridad la más convencional o previsible, por su papel institucional de norma de apoyo a esa regulación comunitaria. Al igual que esta otra, está fuera de duda que la norma española de protección de datos personales es aplicable al ámbito del trabajo asalariado y que, en consecuencia, entraña los correspondientes derechos para el interesado (el trabajador fundamentalmente) y las pertinentes obligaciones y responsabilidades tanto para el empleador como para todos aquellos que intervienen, con una u otra condición o función, en ese terreno específico. Pero no aporta una regulación especializada para las relaciones de trabajo, con independencia de que incidentalmente, o de forma implícita, aluda a ellas, o de que, como luego diremos, algunos de sus preceptos sean punto de referencia para la regulación específicamente laboral que, a propósito de los derechos digitales, también se contiene dentro de ese texto legal español. Desde esa perspectiva, la LO 3/2018 no parece que atienda debidamente las llamadas que desde varios de sus preceptos hace el Reglamento UE 2016/679 a los Estados miembros, ni parece que haya dado mucha consideración a las advertencias o peticiones que desde diversas instancias internacionales (como la OIT o el Grupo G29) o nacionales (la propia AEPD) han transmitido en más de una ocasión en ese mismo o similar sentido.

En todo caso, no cabe duda de que la parte de la LO 3/2018 dedicada a la protección de datos personales contiene numerosos preceptos especialmente relevantes para el ámbito laboral. Uno de ellos es desde luego su artículo 22, pese a no ser un precepto estrictamente dedicado a la prestación de trabajo por cuenta ajena. Como puede que se recuerde, es un precepto que se ocupa de forma general del tratamiento de datos personales "con fines de videovigilancia" o a partir de sistemas de grabación de sonidos, pero alberga una mención al "tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras" que es muy significativa desde nuestro particular punto de vista. Así las cosas, es importante saber que el artículo 22 LO 3/2018, tras permitir en principio que las personas físicas o jurídicas, sean públicas o privadas, lleven a cabo "el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones", inmediatamente impone obligaciones de supresión de datos ("en el plazo máximo de un mes desde su captación" como regla general) y de información ("colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679") que pueden tener enorme trascendencia para el correcto desenvolvimiento de las relaciones de trabajo. También son interesantes desde nuestra concreta perspectiva laboral las previsiones del artículo 24 de la LO 3/2018 acerca de los sistemas de información "de denuncias internas", que probablemente constituyan un nuevo espacio de concurrencia e incluso de confrontación de intereses entre la empresa (incluida la Administración pública y sus "empleados".

4.- Pero la LO 3/2018 fue aprovechada también para una especie de revitalización de las exigencias impuestas al legislador por el artículo 18.4 de la Constitución española. Ha servido, cuando menos, para tipificar y regular los denominados "derechos digitales", como derechos de

nuevo cuño destinados a procurar la debida atención a las personas en una sociedad presidida por el creciente protagonismo de la comunicación electrónica. En términos generales, esta segunda parte de la LO 3/2018 actúa con una triple finalidad: facilitar el acceso de todos los ciudadanos a los nuevos medios de información y comunicación, garantizar un uso razonable de los mismos y salvaguardar los derechos e intereses legítimos que pudieran verse afectados con ocasión de su implantación o su funcionamiento, con especial énfasis en el respeto de la intimidad y la vida privada de las personas. En todo caso, estas singulares previsiones de la LO 3/2018, de rabiosa actualidad como es fácil de comprender, se distribuyen a su vez en dos grandes apartados, en función de su ámbito de destino y de sus destinatarios. En gran medida son reglas que se dirigen a todos los ciudadanos y al conjunto de las relaciones sociales, pero en una parte muy considerable son reglas específicamente ligadas al ámbito de las relaciones de trabajo, incluido el sector público en sus diversos componentes (empresa pública y Administración pública).

En su dimensión más general, los preceptos de la LO 3/2018 dedicados a este espacio digital no sólo tratan de hacer posible el acceso universal a los soportes de información y comunicación que va sucesivamente proporcionando el avance de la tecnología, sino también de procurarles unas condiciones adecuadas para racionalizar su uso y para hacer frente a sus efectos nocivos o indeseados, especialmente en lo que se refiere a las personas menores de edad. Para atender uno y otro objetivo la LO 3/2018 utiliza la consabida técnica de consagración o acuñación de derechos. Así, entre las facilidades de acceso o de uso cabe citar el derecho a "la educación digital" (como nuevo ingrediente del sistema educativo en sus diferentes espacios y niveles), junto al derecho de "portabilidad" de los datos (para que, llegado el caso, y siempre en beneficio de su titular, puedan ser transmitidos entre diferentes prestadores de servicios). Por lo que se refiere a las garantías en sentido más estricto, cabe citar en esta pequeña aproximación el derecho a "la seguridad digital" (que se materializa en esencia en los correspondientes derechos de rectificación, actualización y supresión u "olvido" de datos), y el derecho a "la neutralidad en el ámbito de internet" (que comprende a su vez el derecho a no sufrir discriminación por razones económicas, sociales, geográficas o de género). Como hemos dicho, son reglas de aplicación general a la sociedad, pero no puede descartarse que algunas de ellas puedan tener asimismo cierta proyección en el contexto del trabajo asalariado, como pudiera ser el caso del especial cuidado brindado a los menores de edad en el uso de la nueva tecnología.

En cualquier caso, la LO 3/2018 contiene también un número apreciable de preceptos dedicado de modo específico al ámbito de la empresa y de la relación de trabajo. Para ello, ha incorporado una mención expresa a los derechos digitales en el Estatuto de los Trabajadores (artículo 20 *bis*) y en el Estatuto Básico de los Empleados Públicos (artículo 14.j *bis*), y ha procedido a su desarrollo directo a través de su propio articulado (artículos 87 a 91), dando lugar así, se quiera o no, a un nuevo caso de fragmentación de los bloques normativos dedicados por nuestro sistema al trabajo asalariado. Estas previsiones, que en gran medida están inspiradas a la postre en el acervo jurisprudencial (nacional y europea) acumulado en las últimas décadas, tienen como propósito principal la preservación de los derechos de intimidad y privacidad del trabajador ante el ejercicio del poder empresarial. Pese a la denominación oficial de su objeto, no vienen a reconocer exactamente "derechos digitales", como derechos de uso o acceso a técnicas o dispositivos digitales por parte de los interesados (y particularmente de los trabajadores o empleados), sino más bien a imponer límites y precauciones para el ejercicio de los poderes empresariales de ordenación y control del trabajo en este contexto de propagación en las empresas de las nuevas tecnologías. No pueden desligarse, por otra parte, de los preceptos dedicados por la propia LO 3/2018 al tratamiento de datos personales, entre otras razones porque el uso de la tecnología digital para organizar la producción y supervisar el trabajo en el ámbito de la empresa puede proporcionar, y

a menudo proporciona, una cantidad ingente de datos acerca del trabajador, incluidos los datos faciales y los que se refieren a comportamientos o hábitos de conducta. De ahí que uno de sus ingredientes principales sea la imposición al empleador de deberes de información, respecto del trabajador directamente o respecto de sus representaciones colectivas.

5.- Cuatro artículos dedica la LO 3/2018 a los llamados derechos digitales. El primero de ellos (artículo 87) contempla la hipótesis de uso por parte del trabajador "de dispositivos digitales" para la realización de su trabajo. Formalmente tiene como fin esencial la salvaguarda del derecho a la intimidad de los trabajadores, aunque también hay que reconocer que confiere al empresario importantes facultades de control y vigilancia en ese terreno. Reconoce expresamente el derecho de los trabajadores "a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador", pero habilita al empleador para "acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos". En un terreno más concreto, exige a los empleadores que establezcan "criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente", para cuya elaboración deben contar con la participación de "los representantes de los trabajadores" y sobre cuya existencia y aplicación deben dar la debida información a los trabajadores. Junto a todo ello, se ofrecen a los sujetos implicados algunas reglas sobre "el acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados", que podrá hacerse cuando "se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados". Como puede verse, el precepto trata de proteger al trabajador frente a las medidas o actuaciones del empleador, pero no hay duda de que también concede al titular de la empresa facultades muy explícitas de control y vigilancia en relación con la actividad laboral.

El segundo precepto de la LO 3/2018 referido a estas cuestiones (artículo 88) reconoce específicamente el derecho de los trabajadores "a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar". El texto legal admite diversas "modalidades de ejercicio de este derecho" en función de "la naturaleza y objeto de la relación laboral", que se habrán de sujetar a lo dispuesto por convenio colectivo o a lo acordado entre la empresa y los representantes de los trabajadores, aunque en todo caso habrán de procurar que la desconexión actúe como vía de "conciliación de la actividad laboral y la vida personal y familiar". De todos modos, el empleador queda obligado con este precepto a la elaboración de "una política interna" para sus trabajadores en la que se definan tanto "las modalidades de ejercicio del derecho a la desconexión" como "las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática", con inclusión de quienes ocupen "puestos directivos" y con particular atención a quienes trabajen "a distancia" o en su propio "domicilio", previa audiencia en todo caso de los representantes de los trabajadores. Seguramente trata el precepto sobre todo de potenciar las posibilidades de desconexión en un contexto (tecnológico) en que se corre el riesgo de que el trabajador esté pendiente sin tregua de los encargos o compromisos laborales, pero también es evidente que el legislador no ha querido dar pautas concretas o precisas sobre cómo proceder a esa desconexión del trabajo y, en consecuencia, sobre cómo ejercer el derecho. Probablemente con buen sentido, ha optado más bien por remitir esos aspectos más prácticos u operativos a la negociación colectiva (convenio colectivo o acuerdo *ad hoc* con los representantes de los trabajadores) y a las pautas de organización de la empresa (la llamada "política interna" de la empresa, que deberá ajustarse en todo

caso a lo pactado en convenio o acuerdo colectivo), que por lo demás podrían actuar de forma complementaria.

El tercer precepto de la LO 3/2018 dedicado a los derechos digitales en el campo laboral (artículo 89) consagra el "derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo". De nuevo se conjugan aquí reglas de protección del trabajador con evidentes ampliaciones o en su caso especificaciones de los poderes empresariales de dirección y control del trabajo. Según ese artículo, los empleadores pueden "tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos", siempre que ello respete las limitaciones del marco legal y que se informe a los trabajadores y en su caso a sus representantes "con carácter previo, y de forma expresa, clara y concisa". Se admite asimismo el uso empresarial de sistemas específicos de grabación de sonidos en el lugar de trabajo, pero sólo "cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo" y siempre que se respeten los principios de proporcionalidad e intervención mínima y "las garantías previstas en los apartados anteriores", con la apostilla de que habrá de procederse a la "supresión de los sonidos conservados por estos sistemas de grabación" en determinados plazos, conforme a lo establecido con carácter general por las reglas que la propia LO 3/2018 dedica a la protección de datos personales (artículo 22). El precepto contiene también una prohibición clara y tajante del uso de medios de videovigilancia "en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos", y una referencia más bien problemática a la hipótesis un tanto singular de "comisión flagrante de un acto ilícito por los trabajadores".

El cuarto precepto de la LO 3/2018 que conforma este capítulo especial (artículo 90) tiene por objeto formal el reconocimiento del derecho a la intimidad "ante la utilización de sistemas de geolocalización en el ámbito laboral", aunque tras esa primera presentación se contiene en realidad una habilitación expresa a los empleadores para "tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control", siempre que respete dos condiciones: que esas facultades se ejerzan, de nuevo, "dentro de su marco legal y con los límites inherentes al mismo", y que con carácter previo se informe de esa medida tanto a los trabajadores como a sus representantes. Una información que, según el propio precepto, no puede agotarse en la comunicación de "la existencia" de esos dispositivos, sino que ha de ampliarse a las "características" de los mismos y a los derechos "de acceso, rectificación, limitación del tratamiento y supresión" que tiene el trabajador respecto de los datos obtenidos. La información habrá de transmitirse, además, "de forma expresa, clara e inequívoca". Parece claro que la facultad empresarial de "tratar" los datos obtenidos a través de los sistemas de geolocalización encierra en sí misma la facultad de uso de tales sistemas, aunque caben dudas razonables acerca de si se trata de una posibilidad que en todo caso se brinda al empresario o más bien de un instrumento que sólo puede utilizarse en determinadas condiciones y en determinada medida, que parece lo más aceptable.

6.- A través de estos preceptos hemos podido constatar la importancia que a todos estos efectos puede revestir la negociación colectiva, como cauce de regulación bastante más apropiado que la legislación para atender con la debida precisión y mesura las circunstancias de cada sector o ámbito profesional, tanto en lo que se refiere al uso de las facultades empresariales de control y supervisión del trabajo como en lo que tiene que ver con la información que necesita el trabajador acerca de su situación en la empresa. Por ello, no extraña que la propia LO 3/2018 acuda de forma recurrente a esa peculiar fuente normativa y que añada en su artículo 91 una habilitación expresa a los convenios colectivos para que establezcan "garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salva-

guarda de derechos digitales en el ámbito laboral". Aunque esta autorización legal –que también puede entenderse por cierto como una especie de llamada o incluso como un requerimiento directo– se refiera estrictamente a los "convenios colectivos", es muy probable que deba entenderse en un sentido más amplio, esto es, como remisión general a la negociación colectiva en sus distintas manifestaciones, en cuanto procedimiento de creación de reglas de conducta o comportamiento mediante la acción conjunta y concertada de representantes de trabajadores y empresarios. De su lado, la alusión literal al establecimiento de "garantías adicionales" no debiera interpretarse tan sólo como referencia a los derechos de los trabajadores, sino, más bien, como invitación para desarrollar y completar en todos sus aspectos las medidas previstas por el legislador dentro del marco legal de referencia. Desde esa perspectiva, se supone que es de primordial interés para la autonomía colectiva tanto la descripción de las circunstancias que autorizan o sustentan la adopción de las correspondientes medidas de seguimiento y control, como la fijación de las condiciones que a tales efectos habrá de observar el empleador.

Repárese en que la alusión del artículo 91 de la LO 3/2018 a la negociación colectiva comprende también el "tratamiento de datos personales". Ello permite conectar estas habilitaciones legales con la llamada del artículo 88 del Reglamento UE 2016/679 a los ordenamientos nacionales para garantizar la protección de derechos y libertades en el ámbito laboral y, en definitiva, para adaptar la regulación de protección de datos personales a las singulares características de la relación de trabajo. Como se recordará, dentro de esa previsión general se incluye una referencia específica a la negociación colectiva, que también aparece con ocasión del tratamiento de datos especialmente sensibles (en el artículo 9 del Reglamento). En este terreno más preciso el convenio colectivo puede actuar como vía de autorización del tratamiento de datos personales por entenderlo necesario para el cumplimiento de obligaciones o el ejercicio de derechos (art.9), mientras que en el radio de acción de aquella otra regla, de contornos bastante más amplios, la alusión a los productos de la negociación colectiva se conecta en general con la elaboración de "especificaciones" para el "tratamiento en el ámbito laboral". Desde luego, todas estas llamadas a la negociación colectiva parecen oportunas y razonables, por la mayor proximidad de esta vía de regulación al terreno profesional y por su mayor capacidad de entronque con los intereses de las partes. Esperemos que se aprovechen, aunque desde la perspectiva española la entrada de la negociación colectiva en todas estas materias y, en particular, la asunción por el convenio colectivo de funciones de traslación de reglas de derecho comunitario, tal vez constituyan en mayor medida un reto para el futuro que una probabilidad de efectos más o menos inmediatos.

7.- El avance de nuestro sistema normativo en lo que toca a la protección de los datos personales y el uso de las nuevas tecnologías en el medio laboral ha sido considerable. La jurisprudencia, por su parte, ha seguido jugando un papel muy destacado en la interpretación de las reglas legales y convencionales y en la solución de sus muchos problemas de aplicación. Pero sigue siendo imprescindible el concurso de la doctrina científica, por su insustituible tarea de racionalización de los mandatos normativos a la vista del correspondiente acervo conceptual y de las aportaciones de los tribunales. No puede sorprender que la bibliografía española sobre todos estos asuntos haya alcanzado proporciones verdaderamente notables. Con todo, la prestigiosa Revista del Ministerio de Trabajo y Economía Social no podía quedar al margen de este particular campo de operaciones. Su número 148 viene precisamente a revisitar desde el punto de vista doctrinal todo este flanco del ordenamiento jurídico español. Como habrá podido advertir el lector, la lista de estudios que ahora se presentan cubre prácticamente todo el posible recorrido dentro de este denso e interesante espacio normativo y jurisprudencial, desde la aproximación a su marco general (*Antonio Troncoso Reigada)* al papel de la negociación colectiva (*Yolanda R. Quintanilla Navarro*), pasando por el derecho a la protección de datos personales (*Juan José Fernández Domínguez*), su contenido y sus elementos principales (*María Belén Cardona Rubert*), los problemas de recogida

y tratamiento de datos personales en el contexto del contrato de trabajo (*Alberto Cámara Botía*), la especialidad de ciertas categorías de datos personales (Ángel Luís de Val Tena), la importancia de la protección de datos personales en los procesos de selección de trabajadores (*Olga García Coca*), el sistema de denuncias internas (*María del Rosario Cristóbal Roncero*), el uso de dispositivos digitales en el ámbito laboral (*Federico Navarro Nieto*), los dispositivos de videovigilancia y de grabación de sonidos (*Jesús Lahera Forteza*), la utilización de sistemas de geolocalización (*Iván A. Rodríguez Cardo*), el derecho a la desconexión digital (*Carolina San Martín Mazzucconi*), la protección de datos personales y garantía de derechos digitales en el empleo público (*Ferrán Camas Roda*), las implicaciones del registro de la jornada de trabajo con la protección de datos personales (*Ana Belén Muñoz Ruíz*), o la gestión y aplicación empresarial de las exigencias impuestas por las normas sobre protección de datos personales (*Eva María Blázquez Agudo*). Todas las personas que amablemente han colaborado en este número monográfico proceden del medio universitario, con todo el bagaje científico y conceptual que ello reporta, pero todas ellas acumulan también, por unas u otras vías, suficiente experiencia práctica como para hacerse cargo de los problemas de aplicación real y efectiva de este peculiar conglomerado jurídico. Su proceso de formación y su trayectoria académica, caracterizados por los elementos comunes de seriedad y solvencia profesional, revisten también la variedad necesaria para que sus aportaciones ofrezcan riqueza y y diversidad de opinión. A todas ellas nuestro más sincero agradecimiento.

Estudios

El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre

The legal framework for the protection of personal data: EU regulation 2016/679 and organic law 3/2018 of 5 december

ANTONIO TRONCOSO REIGADA*

1. EL NUEVO MARCO JURÍDICO EUROPEO: EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES

El enorme desarrollo de las tecnologías de la información y la comunicación en los últimos años permite fácilmente considerar que nuestros datos personales son *res in commercio*, no *res extra commercium,* una distinción que tiene en cuenta el criterio de la posibilidad o imposibilidad legal de que una cosa sea objeto de negocio jurídico, y que partía de la clásica división que hacía GAYO entre *res in patrimonio* y *res extra patrimonium,* que valoraba el hecho de que una cosa esté comprendida o no en el patrimonio de una persona[1]. Admitir la posibilidad de comerciar con nuestros datos personales conlleva también aceptar que sea legítimo intercambiar datos personales por medicamentos, por servicios sanitarios o por un descuento en una póliza de seguro o, incluso para conseguir un trabajo o mantenerlo. Este planteamiento, que sitúa la protección de datos personales en la esfera del derecho de propiedad –los datos personales como una *quasi* propiedad[2]–, y que se manifiesta en convertir el consentimiento del interesado en el principio jurídico fundamental, genera una enorme brecha, no sólo social sino de derechos, entre los pobres que comercian con sus datos personales y los ricos, que no se ven obligados a compartir sus datos personales. Este planteamiento convierte la privacidad en un lujo y condena a los pobres a no tener privacidad. Este mismo planteamiento trasladado al ámbito del trabajo diferencia entre los trabajadores que se ven resignados a trabajar sin privacidad y los empleadores, ahonda el desequilibrio existente en las relaciones laborales y condena a los trabajadores a no tener privacidad.

No obstante, hay que recordar que los derechos fundamentales, también el derecho a la protección de los datos personales, y, en especial, los derechos de los trabajadores han surgido para proteger a los más débiles en el ámbito de las relaciones laborales. El derecho

* Catedrático de Derecho Constitucional.

[1] Cfr. IGLESIAS, JUAN, *Derecho Romano. Instituciones de Derecho Privado,* 8ª ed., Ariel, Barcelona, 1983, pp. 238-239.

[2] ESSER consideraba que la expresión *quasi*, siguiendo tanto a juristas romanos como a aquellos del ámbito del *Common Law*, era manifestación de una analogía. Cfr. ESSER, JOSEF, *Principio y norma en la elaboración jurisprudencial del derecho privado*, Bosch, Barcelona, 1961, pp. 294-296.

a la protección de datos personales no tiene en el consentimiento del interesado –del trabajador– su principio jurídico fundamental pues es mucho más que un derecho a la autodeterminación informativa y obliga a respetar otros principios y derechos de protección de datos, en especial el principio de calidad y proporcionalidad. Es necesario en todo caso continuar el desarrollo normativo del derecho fundamental a la protección de datos personales para poder disponer de un marco jurídico que garantice a las personas –en este caso, a los trabajadores– el control sobre sus datos personales sometidos a tratamiento.

Por ello, la Unión Europea aprobó el 27 de abril de 2016 el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos –Reglamento General de Protección de Datos Personales, en adelante RGPD–[3]. Con anterioridad, la Comisión había elaborado durante los años 2010 y 2011[4] y aprobado en enero de 2012 una Propuesta de Reglamento y una Propuesta de Directiva de protección de datos personales para el ámbito policial y judicial, que fueron sometidas a un amplio debate en las instituciones europeas en el que participó un amplio número de expertos y de entidades afectadas[5]. El Reglamento General de Protección de Datos personales, junto con la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la libre circulación de dichos datos conforman este nuevo marco normativo europeo sobre protección de datos personales.

Pues bien, este Reglamento General de protección de datos personales afecta intensamente al ámbito del trabajo, donde se producen frecuentes tratamientos de datos personales para el desarrollo y control del cumplimiento de la relación laboral como los producidos en relación con los recursos humanos, las nóminas o la vigilancia de la salud y donde se manejan también categorías especiales de datos personales, que suponen una injerencia clara sobre los derechos de los trabajadores. Por ello, el derecho fundamental a la protección de datos personales representa un importante límite al ejercicio de la libertad de empresa[6]. Como señaló tempranamente el Tribunal Constitucional en la Sentencia 99/1994, de

[3] DOUE 4 de mayo de 2016. Cfr. recientemente RALLO, ARTEMI (Dir.), *Tratado de Protección de Datos*, Tirant lo blanch, Valencia 2019; GARCÍA MAHAMUT, ROSARIO y TOMÁS MALLÉN, BEATRIZ (Ed.), *El Reglamento General de Protección de Datos Un enfoque nacional y comparado. Especial referencia a la LO 3/2018*, Tirant lo Blanch, Valencia, 2019; ARENAS RAMIRO, MÓNICA y ORTEGA GIMÉNEZ, ALFONSO, *Protección de Datos*, Sepin, Madrid, 2019, LÓPEZ CALVO, JOSÉ (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Wolters Kluwer, Madrid, 2018; DELGADO CARRAVILLA, ENRIQUE y PUYOL MONTERO, JAVIER, *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018; PUYOL MONTERO, JAVIER, *Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018; *Protección de datos. Aplicación del RGPD*, Francis Lefebvre, Madrid, 2018; PIÑAR MAÑAS, JOSÉ LUIS (Dir.), *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, Reus, Madrid, 2016.

[4] La Comisión aprobó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que es considerada el origen de la reforma del marco europeo en esta materia.

[5] Sobre el proceso hacia un nuevo marco normativo europeo de protección de datos personales y las propuestas de Reglamento y Directiva aprobadas por la Comisión, cfr. LOMBARTE, ARTEMI, «Hacia un sistema europeo de protección de datos: las claves de la reforma», *RDP*, núm. 85, 2012, pp. 15-56; TRONCOSO REIGADA, ANTONIO, «Hacia un nuevo marco jurídico europeo de protección de datos personales», *REDE*, núm. 43, 2012, pp. 25-184, RALLO LOMBARTE, ARTEMI y GARCÍA MAHAMUT, ROSARIO (ed.), *Hacia un derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.

[6] Cfr. TASCÓN LÓPEZ, RODRIGO, *El tratamiento por la empresa de datos personales de los trabajadores*, Civitas, Madrid, 2005. Sobre la protección de datos personales en el ámbito laboral, cfr. TRONCOSO REIGADA, ANTONIO, *La protección de datos personales. En busca del equilibro*, Tirant lo Blanch, Valencia, 2010, pp. 1563-1611.

11 de abril –F. J. 7º–, "la relación laboral, en cuanto tiene como efecto típico la sumisión de ciertos aspectos de la actividad humana a los poderes empresariales, es un marco que ha de tomarse en forzosa consideración a la hora de valorar hasta qué punto ha de producirse la coordinación entre el interés del trabajador y el de la empresa que pueda colisionar con él. […] Descartado que la restricción del derecho fundamental viniera impuesta por la naturaleza misma de las tareas expresamente contratadas, no bastaría con la sola afirmación del interés empresarial, dada la posición prevalente que alcanzan los derechos fundamentales en nuestro ordenamiento"[7].

La aprobación por parte de la Unión Europea del Reglamento General de Protección de Datos, que deroga la Directiva 95/46/CE, está encaminada a alcanzar cuatro grandes objetivos[8]:

El primer objetivo del Reglamento General de Protección de Datos es adaptar el derecho derivado institucional de la Unión Europea sobre el derecho fundamental a la protección de datos personales a los enormes avances producidos en las tecnologías de la información y la comunicación desde la aprobación de la Directiva 95/46/CE[9], que no fue capaz de regular ni tampoco de entrever esta nueva realidad de Internet. La rapidez y la universalización de Internet a mediados de los noventa del siglo pasado ha permitido la efectividad de los buscadores –Yahoo aparece en 1995–, las redes sociales –LinkedIn y My Space surgen en 2003–, la computación en nube –2006–, el *Big Data* –2006–, el Internet de las cosas –2008–, la inteligencia artificial, el *Blockchain* –que nace en el 2008 de la mano del *Bitcoin* o mejor al revés–, el *Machine Learning*, etc[10]. Si bien la Directiva 95/46/CE, al igual que el Convenio 108 del Consejo de Europa, es técnicamente una buena norma, no ha podido regular el desarrollo de las tecnologías de la información y no ha sido capaz de dar respuesta a los conflictos jurídicos que se han producido en los últimos años, forzando a los Tribunales a resolver sin una norma jurídica previa, lo que ha abocado a que muchas de sus resoluciones no tuvieran acomodo en un parámetro normativo previo sino que fueran un ejemplo de creación del derecho por unos órganos judi-

[7] Es especialmente aplicable en este ámbito el principio de proporcionalidad: "Los requerimientos organizativos de la empresa que pudieran llegar a ser aptos para restringir el ejercicio de aquellos (al margen de los conectados de forma necesaria con el objeto mismo del contrato) deben venir especialmente cualificados por razones de necesidad, de tal suerte que se hace preciso acreditar –por parte de quien pretende aquel efecto– que no es posible de otra forma alcanzar el legítimo objetivo perseguido, porque no existe medio razonable para lograr una adecuación entre el interés del trabajador y el de la organización en que se integra. […]. Una complejidad especial en cuanto que no basta con que la orden sea, *prima facie*, legítima; es preciso acreditar una racionalidad específica en la que la restricción del derecho del trabajador, no instrumental para el efectivo desarrollo de su tarea, sea, verdaderamente, la única solución apreciable para el logro del legítimo interés empresarial" –STC 99/1994, de 11 de abril –F. J. 7º–.

[8] Una primera aproximación a esta cuestión la hemos realizado en "Autoridades de control independientes", PIÑAR MAÑAS, JOSÉ LUIS (Dir.), *Reglamento General de Protección de Datos, cit.* pp. 461-464.

[9] Cfr. HEREDERO HIGUERAS, MANUEL, *La Directiva Comunitaria de Protección de los Datos de Carácter Personal,* Aranzadi, Pamplona, 1997.

[10] Las fechas de comienzo de las tecnologías son muy difusas en general, aunque hay excepciones. Existe una gran distancia temporal entre las primeras definiciones teóricas, los primeros desarrollos y la implantación de un producto en el mercado. El término *Big Data*, que hace referencia al análisis de grandes volúmenes de información de fuentes heterogéneas no estructuradas y a gran velocidad, se empieza a usar en los años 90 del siglo pasado, aunque es en 2006 cuando se populariza de la mano de Google, si bien había estudios, prototipos y quizás alguna *startup* antes. El *cloud*, aunque se difunde en la primera década del siglo XXI, empieza a pergeñarse ya a finales de los 80, apareciendo en 1995-96 las primeras empresas de esa tecnología. En 1956 se celebra el primer *workshop* universitario sobre inteligencia artificial; comienza a investigarse esta cuestión en el decenio de 1960, pero no es hasta finales de los 80 o principios de los 90 cuando adquiere carta de naturaleza, con los primeros sistemas expertos. Los primeros estudios sobre *Machine Learning* son de 1959 y florece como estudio independiente en los años 90 del siglo pasado. El *Machine Learning* estaba en los años 60 unido a la inteligencia artificial aunque luego se segrega. Algo semejante ocurre con las redes neuronales. Agradezco a Luis de Salvador Carrasco, Coordinador de Evaluación y Estudios Tecnológico de la AEPD, y a Arturo Ribagorda, Catedrático de Informática de la Universidad Carlos III de Madrid, sus aclaraciones en este punto.

ciales no especializados, convirtiendo muchas resoluciones judiciales en un caso fortuito. Era necesario que el legislador europeo y nacional reflexionase sobre los bienes jurídicos en conflicto, también en el ámbito de las relaciones laborales, y diera un criterio sobre los derechos que deben prevalecer, teniendo en cuenta el principio de proporcionalidad.

Este enorme impulso de las tecnologías de la información y la comunicación en los últimos años, que nos ha abierto posiblemente las puertas a una nueva era, ha supuesto una decisiva contribución al avance en el mundo empresarial y en las Administraciones Públicas, en el funcionamiento de los servicios públicos y del mercado de trabajo y en las relaciones laborales y funcionariales. Sin embargo, el desarrollo y la generalización de las tecnologías de la información y de las comunicaciones, que se ha hecho especialmente visible en el ámbito laboral –video vigilancia, geolocalización, biometría, etc.–, ha supuesto un incremento exponencial de los tratamientos de datos personales de los trabajadores, lo que ha dado lugar a la aparición masiva de nuevos riesgos tanto sobre el derecho fundamental a la protección de datos personales de los trabajadores, considerado como derecho autónomo, como sobre otros derechos fundamentales de los trabajadores de los que la protección de datos personales es en muchas ocasiones una garantía institucional o de instituto[11]. Esto ha obligado a modificar el marco normativo de la Unión Europea en esta materia. De manera semejante ha reaccionado el Consejo de Europa. Así, el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ha sido reformado en la misma dirección que el derecho derivado institucional de la Unión Europea por el Protocolo por el que se modifica el Convenio –el llamado "Convenio 108 +"–, acordado durante la 128ª sesión del Comité de Ministros del Consejo de Europa en Elsinore, Dinamarca, los días 17 y 18 de mayo de 2018[12].

El segundo objetivo del Reglamento General de Protección de Datos es garantizar el derecho fundamental a la protección de datos personales, mejorando la definición de su contenido, de sus facultades y de sus límites. Por ello, el RGPD avanza en el desarrollo de los principios de protección de datos personales y de los derechos de las personas en este ámbito, al mismo tiempo que ofrece una nueva configuración de las obligaciones de los responsables y de los encargados del tratamiento de datos personales y del papel de las autoridades de control. Todo ello va encaminado a que las personas tengan un mayor "poder de disposición y control" sobre sus datos personales sometidos a tratamiento, también en relación con los tratamientos transfronterizos, lo que "faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso" –STC 292/2000, de 30 de noviembre, F. J. 7º–.

La posición adoptada en el RGPD ha sido especialmente acertada en este ámbito. Si como hemos señalado antes, el incremento de los tratamientos de datos personales derivado del proceso tecnológico ha elevado los riesgos para la privacidad, el legislador europeo no se ha planteado limitar el recurso a las nuevas tecnologías e impedir las ventajas que éstas aportan a la empresa privada y a la Administración Pública sino que ha puesto el acento en que el progreso tecnológico imparable vaya acompasado a un proceso de fortalecimiento de

[11] Incluso en nuestro país ha dado lugar al reconocimiento de nuevos derechos digitales de los trabajadores independientes del derecho a la protección de datos personales, como después señalaremos, como el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral o el derecho a la desconexión digital en el ámbito laboral, que se encuentra regulados en el Título X de la LO 3/2018, de 5 de diciembre.

[12] El texto consolidado del Convenio 108 modernizado está disponible en la siguiente dirección: https://rm.coe.int/16808ade9d

las garantías del derecho a la protección de datos personales, que permitan a las personas un mayor control sobre sus datos personales sometidos a tratamiento. Por ese motivo el RGPD, como señala el art. 1, que define su objeto, establece "las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales" y "protege los derechos y libertades fundamentales de las personas físicas, en particular, su derecho a la protección de datos personales" –art. 1.1 y 1.2–.

El RGPD fortalece el control de las personas sobre sus datos personales, mejorando la regulación de los principios relativos al tratamiento de datos personales y de los derechos de las personas en este ámbito. Si bien, como señala el Considerando 9 del RGPD, los "principios de la Directiva 95/46/CE siguen siendo válidos", el RGPD hace un esfuerzo de concreción, definición y desarrollo de los principios ya incluidos en la Directiva. Así, el RGPD, al regular los principios relativos al tratamiento, junto con el principio de licitud y lealtad, proclama el principio de transparencia de los tratamientos –art. 5.1.a) RGPD–, que se concreta en la ampliación de la información al interesado –arts. 12-14 RGPD– y del derecho de acceso –art. 15 RGPD–. Igualmente se proclama como principios el de "minimización de datos", de forma que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" –art. 5.1.c) RGPD–, el de "limitación del plazo de conservación", en virtud del cual los datos serán "mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales –art. 5.1.e) RGPD– y el responsabilidad proactiva –art. 5.2 RGPD–, que más adelante analizaremos. Igualmente, el RGPD fortalece los derechos del interesado, desarrollando el contenido de las facultades tradicionales y añadiendo nuevos derechos, de forma que ya no se puede hablar más de derechos *arco*. La información al interesado no es sólo un principio sino que es un derecho y se incorpora una información adicional al interesado que no se encontraba en la Directiva, como la relativa a la base jurídica del tratamiento, al delegado de protección de datos, al plazo de conservación de los datos, al derecho a retirar el consentimiento o al derecho a presentar una reclamación a la autoridad de control, incorporando el uso de iconos o la información por capas para garantizar que el incremento de la información al interesado no perjudique la transparencia del tratamiento de datos –art. 12 RGPD–. Igualmente se amplía el contenido del derecho de acceso del interesado con la información del plazo previsto de conservación de los datos o la existencia de un derecho a solicitar del responsable información sobre el ejercicio de los derechos que asisten al interesado, entre otros –art. 15 RGPD–. También se fortalece la regulación del derecho de rectificación –art. 16 RGPD–, del derecho de supresión o derecho al olvido –art. 17 RGPD–, del derecho de oposición –art. 21 RGPD– o del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles –art. 22 RGPD–, al mismo tiempo que se reconocen nuevos derechos al interesado que no se encontraban en la Directiva 95/46/CE ni en la LOPD como el derecho a la limitación del tratamiento –art. 18 RGPD– o el derecho a la portabilidad de los datos –art. 20 RGPD–.

Por consiguiente, el RGPD, al desarrollar los principios y los derechos de protección de datos en un norma obligatoria en todos sus elementos y directamente aplicable y al mejorar su implementación a través de las autoridades de control, pretende fortalecer el control de las personas sobre sus datos personales sometidos a tratamiento y garantizar un nivel equivalente de protección de los datos personales en la Unión Europea[13].

El tercer objetivo del Reglamento General de Protección de Datos Personales es contri-

[13] Como señala la Exposición de Motivos de la LOPDGDD –apdo. III–, "la transposición de la Directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos".

buir a la creación de un mercado digital europeo que favorezca el crecimiento de la actividad económica y mejore la competitividad de las empresas europeas, lo que requiere la adopción de decisiones encaminadas a facilitar la libre circulación de datos personales en la Unión Europea. No hay que olvidar que la decisión de promover la elaboración de un nuevo RGPD se adopta en un contexto de fuerte crisis económica. Por ese motivo, el objeto de este RGPD no es sólo la protección de las personas físicas en lo que respecta al tratamiento de datos personales sino que, al igual que hacia la Directiva 95/46/CE, es un Reglamento que regula *la libre circulación de estos datos*. Así, como señala su propio título y el art. 1, el Reglamento no sólo "establece […] las normas relativas a la libre circulación de […] datos" –apdo. 1– sino que tiene como objeto que "la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales" –apdo. 3–.

El nuevo marco normativo europeo sobre protección de datos personales tiene como objetivo favorecer la libre circulación de datos personales en la Unión Europea. Esto es así no sólo en relación con el Reglamento General de Protección de Datos sino también con la Directiva 2016/680, del Parlamento Europeo y del Consejo, del 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, que supone un importante avance en la regulación de la protección de datos personales en un ámbito como el policial y el judicial que hasta el Tratado de Lisboa se movía en los terrenos de la cooperación y no de la integración. Como señala su artículo 1.2 –"Objeto y objetivos"–, "de conformidad con la presente Directiva, los Estados miembros deberán: a) proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y b) garantizar que el intercambio de datos personales por parte de las autoridades competentes en el interior de la Unión, en caso de que el Derecho de la Unión o del Estado miembro exijan dicho intercambio, no quede restringido ni prohibido por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales". De esta forma, la nueva Directiva, al mismo tiempo que pretende llevar a cabo una primera armonización normativa en protección de datos personales en un ámbito que hasta ahora pertenecía a la soberanía de los Estados y que estaba regulado por la Decisión Marco 2008/977/JAI del Consejo, tiene también la voluntad decidida de facilitar la compartición de información policial y judicial, mejorando la eficacia policial ante un desafío terrorista que no tiene en cuenta las fronteras nacionales y cuyos autores se mueven libremente en el espacio *Schengen*. Por tanto, la libre circulación de datos personales para favorecer el mercado digital y para permitir el intercambio de información policial y judicial es una razón poderosa que ha movido a la Unión Europea a impulsar este nuevo marco normativo europeo al mismo nivel –al menos– que la tutela del derecho fundamental a la protección de datos personales.

Para lograr este objeto de favorecer la libre circulación de los datos, la Unión Europea ha establecido una regulación común de protección de datos personales, a través de la aprobación de una norma de derecho derivado institucional como es el Reglamento, que a diferencia de la Directiva 95/46/CE, es obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro, lo que permite superar la fragmentación de las legislaciones de protección de datos existente en los diferentes países de la Unión Europea durante el periodo de vigencia de esa Directiva[14]. Exis-

[14] Como señala la Exposición de Motivos de la LOPDGDD –apdo. III–, "el RGPD pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE".

tía un convencimiento en la industria y en los mercados de que la diferente transposición de la Directiva 95/46/CE por los Estados miembros había dificultado la comercialización de productos y servicios y el desarrollo de políticas de privacidad paneuropeas, al obligar a las empresas adaptar sus productos a las distintas extensiones normativas nacionales. Esta situación, además de suponer un incremento de costes, representaba un límite a la competencia y al funcionamiento del mercado interior en la Unión Europea, encontrándose muchas empresas europeas en una situación de desventaja en el mercado. La legislación nacional de protección de datos personales que transponía de forma diferente la Directiva 95/46/CE había dificultado el cumplimiento de uno de los objetivos de la Unión Europea que era la creación de un espacio único europeo de personas, mercancías y capitales[15]. Por ello, la aprobación del RGPD, que establece normas comunes de protección de datos personales y que mejora sustancialmente la armonización normativa en este punto, favorece la competitividad de sus empresas y la investigación, lo que permite la creación en Europa de un sector empresarial fuerte también en el ámbito de la economía digital, que pueda competir con otros ámbitos geográficos fuera de la Unión Europea como EE.UU. y Asia-Pacífico.

En esta dirección hay que subrayar que la Comisión Europea está elaborando una comunicación sobre "Una estrategia europea para los datos" que pretende aprobar en este año 2020, donde se plantea la creación de un espacio único para los datos mediante la agrupación e interconexión de las plataformas virtuales, públicas y privadas, de almacenaje de los veintisiete Estados miembros. Con esta medida, la Comisión Europea quiere tener el control sobre la materia prima por excelencia del siglo XXI, los datos de sus ciudadanos, compitiendo con EE.UU. y China. Los datos no son algo que atañe únicamente al sector tecnológico sino que presentan una dimensión que afecta a todo el crecimiento económico: "los datos están en el centro de la transformación digital y son esenciales para la innovación". Si el origen de la Unión Europea está en el establecimiento de un mercado común de carbón y del acero –la llamada Comunidad Europea del Carbón y del Acero (CECA)– y de la energía atómica –la Comunidad Europea de la Energía Atómica (Euratom)–, la Unión Europea pretende de la creación de un "espacio común europeo" de datos para sectores clave como industria, las finanzas, la salud o la contratación pública. Además, la Unión Europea, a diferencia de otros modelos existentes en EEUU y en China, pretende también entrar en este ámbito de la economía digital siguiendo un modelo europeo, que es más garantista para los derechos fundamentales y, en especial, para la protección de los datos personales, al mismo tiempo que adopta decisiones que salvaguardan su soberanía en el actual contexto geopolítico. La dependencia de proveedores no europeos para el almacenamiento y procesamiento de la información de ciudadanos europeos entraña riesgos tanto para los derechos de los ciudadanos europeos como para la soberanía de los Estados y la posición de la Unión Europea[16].

[15] Las divergencias en la protección de los datos personales entre los Estados miembros de la Unión Europea obedecía a diversas causas: el propio margen de maniobra que dejada la Directiva, el incumplimiento de las exigencias de la Directiva en su transposición por la legislación de los Estados miembros y los déficits de *enforcement* en la aplicación de la normativa de protección de datos personales por los diferentes Estados. Esta cuestión la hemos analizado más ampliamente en "Hacia un marco jurídico europeo", *cit.* pp. 53-68.

[16] La Comisión Europea ha planteado recientemente una inversión de 1.600 millones de euros para la creación de una gran nube, agrupando las nubes de los países y compartiendo datos en sectores clave. La Comisión Europea no puede esperar más para entrar en la economía de los datos. Existe una importante dependencia tecnológica de las compañías de la Unión Europeo respecto de Google, Microsoft, Amazon o Huawei. En la actualidad, solo el 4% de los datos del continente están albergados en proveedores europeos. La Unión Europea se ha fijado como objetivo que en 2030 "la proporción de datos almacenados y procesados y el tamaño de la economía que generan se corresponda al menos con el peso de la UE en el mundo, que en 2018 era de cerca del 16,5%". Cfr. *El País*, 4 de febrero de 2020. También existe en EEUU una preocupación acerca de la dependencia tecnológica de China y cómo afecta ésta a la seguridad nacional.

Además, la Unión Europea ha regulado acertadamente el ámbito territorial de aplicación del RGPD, en relación a la problemática de jurisdicción y de ley aplicable que plantean los proveedores de servicios de tratamiento de datos radicados fuera de la Unión Europea. El RGPD establece una clara orientación hacia las personas, lo que obliga al responsable o al encargado que no se encuentre establecido en la Unión a aplicar el RGPD al tratamiento de datos personales de interesados que residan en la Unión cuando las actividades de tratamiento estén relacionadas con oferta de bienes o servicios a ciudadanos europeos o el control de su comportamiento en la medida en que tenga lugar en la Unión –art. 3.2–.

Otra vía para favorecer la libre circulación de los datos personales no sólo dentro del ámbito de la Unión Europea sino también fuera de él es la utilización que hace el RGPD de algunos elementos de autorregulación como los códigos de conducta –arts. 40-41 RGPD– y los mecanismos de certificación –arts. 42-43 RGPD– para facilitar las transferencias internacionales de datos personales. Así, el RGPD prevé la licitud de las transferencias de datos personales a terceros países y a organizaciones internacionales si existen garantías adecuadas recogidas en normas corporativas vinculantes, en códigos de conducta o mecanismos de certificación –art. 46.2.b), e) y f)–. Esta previsión permite a las empresas europeas intercambiar datos personales dentro y fuera de la Unión Europea y competir en mercados distintos del europeo. Esta apuesta decidida del legislador europeo por las herramientas de autorregulación supone una clara aproximación al modelo norteamericano de protección de datos –se trata de un RGPD *pre Brexit*–, lo que también favorece el diálogo económico trasatlántico y con otras regiones, ampliando las posibilidades de crecimiento económico y de creación de empleo. Por tanto, tanto la mayor armonización europea en el ámbito de la protección de datos producida por la sustitución de la Directiva 95/46/CE por el RGPD como la introducción en este último de elementos procedentes de la autorregulación son dos instrumentos que, aunque aparentemente pueden parecer contradictorios –no lo son en realidad–, favorecen la libre circulación de los datos personales en la Unión Europea y fuera de ella[17].

El cuarto objetivo del RGPD es hacer más sencillo a los responsables y encargados de tratamiento el cumplimiento de la normativa de protección de datos, incrementando al mismo tiempo su responsabilidad –la *accountability*–[18] y, en general, el respeto a este derecho fundamental. Esto lo hace el legislador europeo: primero, suprimiendo algunas obligaciones de los responsables y encargados de tratamiento que eran consideradas burocráticas y poco útiles para la tutela del derecho fundamental; segundo, estableciendo unas obligaciones específicas a categorías concretas de responsables y encargados de tratamiento –y no a todos ellos de manera indiferenciada–; y tercero, añadiendo nuevas obligaciones de los responsables y encargados de tratamiento menos formales y más efectivas para la protección de datos personales.

Así, en primer lugar, el RGPD supone la supresión o la flexibilización de algunas exigencias recogidas en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –LOPD– como la obligación que tenían todos los responsables de notificación de todos los tratamientos de datos personales a la autoridad de control –arts. 26 y 39.2 LOPD– lo que permitía la existencia de un derecho a la consulta al Registro General de Protección de Datos –art. 14 LOPD– y que ha sido sustituida por un registro de las actividades de tratamiento –art. 30 RGPD–, que es una medida de carácter interno. También han desaparecido algunas autorizaciones administrativas para las transferencias internacionales de da-

[17] El estudio de la autorregulación en la Propuesta de Reglamento de la Comisión y la necesidad de unos estándares internacionales de protección de datos personales y de un equilibrio entre las diferentes visiones sobre la protección de datos personales a nivel internacional la hemos analizado en "Hacia un nuevo marco jurídico europeo", *cit.* pp. 41-53.

[18] *Ibidem* pp. 93-94 y pp. 178-179 y "Autoridades de control independientes", *cit.* pp. 463-464.

tos –arts. 33-34 LOPD–, al ampliar los instrumentos de garantía que no requieren autorización –arts. 46 a 49 RGPD– o se ha suprimido la obligación de cumplir un listado muy amplio de medidas de seguridad de carácter organizativo o técnico aprobadas por vía reglamentaria –art. 9.2 y 3 LOPD–. De esta forma, el Reglamento trata de desburocratizar la protección de datos personales, que en muchas ocasiones se había convertido para muchas empresas en un cumplimiento formal y vacío de algunas exigencias que se encomendaba a las gestorías y que se materializaba en la notificación de un tratamiento, en la existencia de un documento de seguridad estándar no adaptado a la organización o en la inclusión de unas cláusulas informativas genéricas.

En segundo lugar, el RGPD ha evitado establecer el mismo catálogo de obligaciones generales para cualquier clase de responsable o encargado del tratamiento sino que ha fijado algunas obligaciones específicas a determinadas categorías de responsables y encargados de tratamiento, teniendo en cuenta la naturaleza de los tratamientos y los riesgos para los derechos de las personas. Así, si la obligación de notificación de todos los tratamientos a la autoridad de control era visto por las pequeñas y medianas empresas como una carga burocrática, el registro de actividades de tratamiento –que es la nueva obligación del RGPD que sustituye a la notificación– no se aplica a las empresas u organizaciones que empleen menos de doscientas cincuenta personas –art. 30.5 RGPD–[19]. La obligación de realizar una evaluación de impacto en la protección de datos sólo es aplicable a los responsables de aquellos tratamientos que por su naturaleza, alcance, contexto o fines, sea probable que entrañen un alto riesgo para los derechos y libertades de las personas físicas, como es el caso de la evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente, el tratamiento a gran escala de las categorías especiales de datos personales o relativos a condenas e infracciones penales o la observación sistemática a gran escala de una zona de acceso público –art. 35.1 y 3 RGPD–. Igualmente la obligación de designar un delegado de protección de datos no es general para todos los responsables y encargados de tratamiento sino sólo cuando el tratamiento lo lleve a cabo una autoridad u organismo público –excepto los tribunales en el ejercicio de la función jurisdiccional–, cuando las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales o de datos relativos a condenas o infracciones penales –art. 37.1 RGPD–, sin perjuicio de lo previsto en el art. 34 de la Ley Orgánica 3/2018, de 5 de diciembre. Tanto la supresión de algunas obligaciones como el establecimiento de otras sólo para categorías concretas de responsables y encargados de tratamiento, poniendo el acento en dónde está realmente el riesgo y no en todas las pymes, ha simplificado en términos generales las obligaciones de estos, en línea con la posición británica en el proceso de negociación del Reglamento, que buscaba que el nuevo marco normativa europeo no sobrecargase –*not overburden*– a las empresas y permitiera el desarrollo y la innovación, lo que ha sido valorado de manera positiva[20].

En tercer lugar, el RGPD introduce algunas nuevas obligaciones del responsable y del encargado como la evaluación de impacto

[19] "A menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional o incluya categorías especiales de datos personales o datos relativos a condenas o infracciones penales".

[20] La memoria económica de la Comisión cuantificaba que la reducción de las cargas administrativas para las empresas suponía un ahorro de 2.300 millones de euros anuales.

relativa a la protección de datos –art. 35–, el delegado de protección datos –art. 37-39– y la protección de datos en el diseño o por defecto –art. 25– que son obligaciones de carácter menos formal y burocrático pero mucho más efectivas para el cumplimiento del derecho a la protección de datos personales y que reflejan mejor el principio de responsabilidad proactiva –arts. 5.2 y 24 RGPD– y la *accountability*. De esta forma, el RGPD no se limita a suprimir algunas exigencias de la normativa de protección de datos que podían ser consideradas formales o propio de las gestorías sino que introduce nuevas garantías para la protección de datos personales que provienen en muchas ocasiones de la cultura jurídica anglosajona y del ámbito de la autorregulación[21]. La introducción de la *privacy impact assesment*, de la *privacy by design*, de la *privacy by default* y del *data protection officer* nos aproximan al modelo anglosajón de protección de datos. Estas nuevas medidas como la responsabilidad proactiva o las evaluaciones de impacto en la protección de datos personales no pueden ser llevadas a cabo por una gestoría –no se trata del cumplimiento formal de una serie de trámites– sino por una persona con unos conocimientos especializados del Derecho y la práctica en materia de protección de datos –art. 37.5 RGPD–.

El RGPD fue publicado el 4 de mayo de 2016 y, en virtud de la previsión contenida en el art. 99.1, entró en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*. Sin embargo, el RGPD estableció un plazo de dos años a partir de la fecha de la entrada en vigor para el inicio de su aplicación –art. 99.2–. Por tanto, es una norma que había entrado en vigor pero que no era aplicable hasta pasados dos años, plazo que finalizó el 25 de mayo de 2018. Esta *vacatio legis* de dos años en su entrada en aplicación se debió principalmente a que, siendo el derecho un importante instrumento de ingeniería social, la realidad no cambia sólo porque el derecho cambie. Era necesario un periodo de conocimiento y de adaptación tanto de las Administraciones Públicas como de las empresas privadas al nuevo derecho derivado institucional de la Unión Europea. El RGPD introduce no sólo un gran número de novedades en relación con la Directiva 95/46/CE y con la legislación vigente en los Estados miembros sino que supone, en gran medida, un cambio de enfoque. Como señala la Exposición de Motivos de la LOPDGDD, el RGPD "supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa" –apdo. III–. Era necesario un tiempo para adecuar los ordenamientos jurídicos de los Estados miembros a los cambios establecidos en el RGPD.

2. LA NECESIDAD DE UNA LEY NACIONAL PARA APLICAR EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS: EL MARGEN DE MANIOBRA DE LOS ESTADOS PARA COMPLETAR EL MARCO NORMATIVO

La Unión Europea, como ya hemos analizado en otro momento, ha optado que sea un Reglamento la norma de derecho derivado institucional para aprobar la normativa de la Unión Europea relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los datos. El RGPD, a diferencia de esta Directiva, es obligatorio en todos sus elementos y directamente aplicable, habiéndose producido su recepción en el derecho interno desde su entrada en vigor, por lo que no requiere ninguna norma nacional de transposición.

Esto diferencia al RGPD no sólo de la Directiva 95/46/CE sino también de la otra norma de derecho derivado institucional que fue aprobada a la vez por la Unión Europea para conformar el nuevo marco normativo europeo de protección de datos personales: la Directi-

[21] Hemos analizado la diferencia entre el modelo europeo y americano de protección de datos en "Hacia un nuevo marco jurídico europeo", *cit.* pp. 50-53 y 180-184.

va (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos[22]. El art. 63.1 de esta Directiva señala que "los Estados miembros adoptarán y publicarán, a más tardar el 6 de mayo de 2018, las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva" y "aplicarán dichas disposiciones a partir del 6 de mayo de 2018". En la actualidad, el Ministerio del Interior ha asumido la elaboración del anteproyecto de ley para la transposición de la Directiva (UE) 2016/680, habiendo solicitado el Ministerio de Justicia que se excluyera de este anteproyecto de Ley los tratamientos de datos personales del ámbito jurisdiccional. El Ministerio de Justicia está trabajando sobre la modificación de la LOPJ que mejore los arts. 230 y ss de la LOPD y, en su caso, las leyes procesales para adaptarlas tanto al RGPD como a la Directiva (UE) 2016/680, lógicamente, también a la nueva Ley Orgánica 3/2018, de 5 de diciembre, ya que la LOPJ sigue refiriéndose a la LOPD. En todo caso, el Estado español ha incumplido el plazo de transposición de la Directiva (UE) 2016/680 establecido por la Unión Europea.

Si el RGPD es una norma obligatoria en todos sus elementos y directamente aplicable, que no requiere una norma nacional de transposición, es necesario preguntarse qué sentido tiene la aprobación en nuestro país de una nueva Ley Orgánica de Protección de Datos Personales. Hay que recordar que la Unión Europea eligió el Reglamento como norma de derecho derivado institucional en detrimento de aprobar otra Directiva como la 95/46/CE justamente porque trataba de mejorar la armonización normativa en este ámbito de la protección de datos personales, reduciendo las divergencias existentes entre las legislaciones de los Estado miembros que permitía la Directiva 95/46/CE y que daba lugar a una fragmentación normativa que perjudicaba el funcionamiento adecuado del mercado interior.

Son dos las razones que justifican la aprobación de una ley nacional de protección de datos personales.

La primera razón es que el RGPD desplaza la normativa interna que sea incompatible con éste por el principio de primacía y el efecto directo del Derecho europeo, lo que afecta especialmente a la Ley Orgánica 15/1999, de 13, de Protección de Datos de Carácter Personal (LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre. Sin embargo, el RGPD no deroga las normas nacionales incompatibles porque la primacía del derecho europeo no es supremacía y no afecta a la validez de las normas internas[23]. Le corresponde a la Ley nacional, *por razones de seguridad jurídica*, la labor de depurar el ordenamiento jurídico interno, derogando los preceptos de la LOPD que sean incompatibles con el RGPD. Esto evita a los responsables de tratamiento o las autoridades de control situaciones de incertidumbre que les obliguen a interpretar en cada caso si un precepto de la LOPD debe ser o no inaplicado por haber quedado desplazado al estar en contradicción con el RGPD, aplicando lo previsto en esta norma o que el juez nacional se plantee la necesidad o no de presentar una cuestión prejudicial antes de inaplicar la ley interna. De esta forma, no deben mantenerse en el ordenamiento jurídico interno normas nacionales contrarias al RGPD aunque los poderes públicos procedan a la inaplicación. Lo mismo cabe decir de la legislación autonómica de protección de datos personales. Por las mismas razones, es necesario también derogar ex-

[22] Esta Directiva deroga la Decisión Marco 2008/977/JAI del Consejo.

[23] Sobre las relaciones entre el Derecho constitucional nacional y el derecho de la Unión Europea, cfr. GORDILLO PÉREZ, LUIS IGNACIO, *Constitución y ordenamientos supranacionales*, CEPC, Madrid, pp. 35-99.

presamente los preceptos de las leyes laborales incompatibles con lo previsto en el RGPD. También le corresponde al Gobierno derogar la normativa reglamentaria incompatible con el Derecho de la Unión Europea, en especial el Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre[24].

La segunda razón es que el RGPD, a pesar de tener un alto nivel de detalle y de especificación –tiene 99 artículos y 173 considerandos–, a diferencia de otros Reglamentos de la Unión Europea, deja un *margen de maniobra a los Estados*. En ocasiones, la intervención legislativa de los Estados puede ser no sólo procedente sino incluso necesaria para el *desarrollo o complemento* de un Reglamento de la Unión Europea. Los Reglamentos, "pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de "desarrollo" o complemento del Derecho de la Unión Europea"[25]. El RGPD, aunque pueda parecer extraño, está llamando de alguna manera a la intervención legislativa de los Estados miembros para que concrete algunos ámbitos dejados a la decisión de los Estados. Así, el RGPD permite que sus disposiciones sean especificadas o restringidas por el Derecho de los Estados miembros, "conteniendo un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias". Como ya adelantamos en relación con su proceso de negociación, se pasa de una Directiva que era flexible en lo formal a un Reglamento que es flexible en lo material y que permite un margen de maniobra al legislador nacional[26].

Por tanto, les corresponde a las Cortes Generales a través de la función legislativa y también al Gobierno, a través del desarrollo reglamentario de la ley nacional, la actividad de complementar y aplicar el RGPD, en virtud del principio de cooperación leal que obliga a los Estados miembros a adoptar "todas las medidas generales o particulares apropiadas para asegurar el cumplimiento de las obligaciones derivadas de los Tratados o resultantes de los actos de las instituciones de la Unión" –art. 4.3 TUE–. Esta obligación es también trasladable a los legisladores y gobiernos autonómicos, dentro de la distribución constitucional de competencias y del respeto al principio de autonomía institucional. No se trata de incorporar el RGPD al derecho interno –porque no requiere transposición– pero sí de aplicarlo. Esta actividad de desarrollo normativo tiene que respetar lógicamente el RGPD que es obligatorio en todos sus elementos. Esto significaba que el legislador nacional –también el Gobierno– ha tenido limitadas las materias de decisión política en un ámbito que supone el desarrollo de un derecho fundamental, lo que afecta al principio democrático.

El RGPD deja expresamente cierto margen a los Estados miembros para hacer *previsiones normativas cuando el tratamiento de datos personales afecta a derechos constitucionales* algo que se evidencia especialmente en el Capítulo IX dedicado a las "Disposiciones

[24] Como señala la Exposición de Motivos de la LOPDGDD –apdo. III–, "hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, [...] para la depuración del ordenamiento nacional. [...] Así, el principio de seguridad jurídica [...] en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada "mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse" (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia)".

[25] *Ibidem* apdo. III.

[26] Esta cuestión la habíamos adelantado en relación con la Propuesta de Reglamento en "Hacia un nuevo marco jurídico europeo", *cit.* p. 176.

relativas a situaciones específicas de tratamiento". En relación con la libertad de expresión y de información, el RGPD establece que "los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del […] Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria", por lo que los Estados miembros establecerán exenciones y excepciones a los principios, a los derechos de los interesados, a las obligaciones de los responsables y de los encargados, a las funciones de las autoridades de control y a los mecanismos de cooperación y coherencia "si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información" –art. 85 RGPD–. Especial mención en relación con los derechos de los trabajadores merece la referencia que el RGPD hace al "Tratamiento en el ámbito laboral" –art. 88– que faculta expresamente a los Estados miembros, a través de disposiciones legislativas, que deben ser notificadas a la Comisión, o de convenios colectivos, a "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 la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral". En todo caso, el legislador europeo obliga a que las normas nacionales incluyan "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". Igualmente, en relación con el derecho de acceso del público a documentos oficiales, el RGPD autoriza que de conformidad no sólo con el Derecho de la Unión sino también con el Derecho de los Estados miembros, "los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad […] a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales" –art. 86–. En relación con la libertad religiosa el RGPD tiene en cuenta la existencia en el momento de su entrada en vigor de normas vigentes en los Estados miembros relativas a la protección de datos personales en iglesias, asociaciones o comunidades de fieles que seguirán aplicándose siempre que sean conformes con el Reglamento, sin perjuicio de que añade que estos tratamientos deben estar sujetos al control de una autoridad de control independiente –art. 91–. También el RGPD deja espacio a los Estados en relación a los derechos de los menores –cuándo se considera que el menor es maduro– y el libre desarrollo de su personalidad. Así, al regular las condiciones aplicables al consentimiento del niño en los servicios de la sociedad de la información –art. 8– establece que se considera lícito el tratamiento de los datos personales de un niño cuando tenga como mínimo 16 años, si bien "los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años".

También el RGPD deja cierto margen a los Estados miembros para hacer *previsiones normativas, fijando de manera más precisa requisitos y otras medidas adicionales que garanticen un tratamiento lícito y equitativo, en determinados* ámbitos específicos. En relación con el tratamiento del número nacional de identificación, el RGPD establece que si bien éste se utilizará únicamente con las garantías

adecuadas para los derechos y libertades del interesado establecidas en el mismo Reglamento, también prevé que los Estados miembros "podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general" –art. 87–. Igualmente, en relación con los tratamientos con fines de archivo público o de investigación científica o histórica o estadísticos, el RGPD establece que estos tratamientos están sujetos a las garantías establecidas en el Reglamento para asegurar el principio de minimización de datos personales, que es consecuencia del principio de proporcionalidad y de la aplicación del subjuicio de necesidad, lo que puede incluir la seudonimización o la anonimización. Además también prevé que no sólo el Derecho de la Unión sino también el de los Estados miembros podrá establecer excepciones en estos tratamientos al derecho de acceso –art. 15 RGPD–, al derecho de rectificación –art. 16 RGPD–, al derecho a la limitación del tratamiento –art. 18 RGPD–, a la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento –art. 19 RGPD–, al derecho a la portabilidad de los datos –art. 20 RGPD–[27] y al derecho de oposición –art. 21 RGPD–[28], "siempre que sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines" –art. 89 RGPD–. Hay que recordar que el RGPD establece una obligación a los Estados miembros a este respecto. El Considerando 156 del RGPD señala que "los Estados miembros *deben establecer garantías adecuadas* para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos"[29].

Además, el RGPD prevé la *colaboración de las leyes de los Estados al regular los principios y derechos de protección de datos personales*. Así, en relación con la licitud del tratamiento, el RGPD establece que el tratamiento será lícito cuando sea "necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento" –art. 6.1.c)– o cuando sea "necesario para el cumplimiento de una misión realizada en interés público[30];

[27] Las excepciones a la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento o al derecho a la portabilidad de los datos sólo se aplican a los tratamientos de datos personales con fines de archivo en interés público –art. 89.3 RGPD–.

[28] También es posible la excepción del derecho de supresión, como señala el art. 17.3.c) RGPD, cuando el tratamiento es necesario "por razones de interés público en el ámbito de la salud pública" de conformidad con el art. 9.2.h) e i) y 9.3 RGPD y cuando el tratamiento sea necesario "con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el art. 89.1, en la medida en que el derecho de supresión pueda hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento" –art. 17.3.d)–. Cfr. también el Considerando 65 del RGPD. En relación con el derecho de oposición, hay que recordar que el art. 21.6 RGPD establece que "cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el art. 89.1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernen, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público".

[29] Señala el Considerando 156 RGPD: "Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad".

[30] El RGPD establece que los Estados miembros tienen un margen de maniobra para definir por Ley la existencia de un *interés público* que justifica la licitud del tratamiento sin consentimiento –art. 6.1.e)–. En cambio, los Estados miembros no disponen de ese mismo margen de maniobra para concretar por Ley cuáles son los *intereses legítimos –privados–* que puede perseguir el responsable del tratamiento o un tercero y cuya satisfacción justifica la legitimidad del tratamiento de datos personales sin consentimiento, una previsión que se encuentra en el art. 6.1.f) RGPD, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos

o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" –art. 6.1.e)–, estableciéndose además que la base jurídica del tratamiento en ambos casos no es solo el Derecho de la Unión sino también "el Derecho de los Estados miembros que se aplique al responsable del tratamiento" –art. 6.3.b)–[31]. Es importante subrayar que el RGPD atribuye una importante función a la base jurídica –también recogida en el Derecho de los Estados miembros–, que determinará la finalidad del tratamiento o que el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además, también el Derecho de los Estados miembros –no sólo el Derecho de la Unión– podrá contener disposiciones específicas para adaptar la aplicación de Reglamento como las relativas entre otras a "las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento" reguladas en el Capítulo IX. En todo caso, los Estados miembros no tienen una absoluta libertad sino que el Derecho de la Unión de los Estados miembros "cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido" –art. 6.3 RGPD–. Además, el art. 6.2 RGPD establece expresamente que los Estados miembros –en este caso, no la Unión Europea– "podrán *mantener o introducir disposiciones más específicas* a fin de adaptar la aplicación de las normas del presente Reglamento" con respecto al tratamiento en cumplimiento de una obligación legal aplicable al responsable del tratamiento o para el cumplimiento de una misión realizada en interés público o en ejercicio de poderes públicos conferidos al responsable del tratamiento, "*fijando de manera más precisa requisitos específicos de tratamiento y otras medidas* que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento", como las mencionadas en el Capítulo IX.

También el RGPD deja margen de maniobra a los Estados en la regulación del "Tratamiento de categorías especiales de datos personales" –art. 9–[32], que tiene un régimen

personales, en particular cuando el interesado sea un niño. Como hemos señalado en otra ocasión, "esto es algo a lo que debe prestar una atención especial el legislador español para no volver a las andadas, circunscribiendo los intereses legítimos sólo a unos concretos tratamientos de datos personales. Otra cosa distinta es que las autoridades de control puedan ayudar a los responsables, categorizando supuestos que presumiblemente –*iuris tantum*– puedan representar un interés legítimo del responsable que sirva como criterio de licitud del tratamiento sin consentimiento sin perjuicio de la necesidad de llevar a cabo una valoración en el caso concreto. Hay que tener en cuenta que la actividad de ponderación que el art. 6.1.f) RGPD –y anteriormente el art. 7.f) de la Directiva 95/46/CE– asigna al responsable del tratamiento implica la realización por parte de éste de un juicio de proporcionalidad, algo más propio de los órganos jurisdiccionales, que supera el principio de responsabilidad proactiva –*accountability*– que el RGPD atribuye al responsable –art. 2.2 y 2". Esta es una cuestión que hemos analizado en «Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y garantía de los Derechos digitales", *Revista de Derecho y Genoma Humano*, núm. 49, 2018, p. 225.

[31] Así, el Considerando 10 del RGPD señala que "en lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento".

[32] Como señala el Considerando 10 del RGPD "junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamien-

jurídico de legitimación de los tratamientos distinto al de las categorías generales de datos personales –art. 6– y que parte de la prohibición de los tratamientos y de la presunción *iuris tantum* presente en el apartado primero del art. 9 de su ilegitimidad, salvo los supuestos tasados recogidos en el apartado segundo. Así, hay que reseñar que el consentimiento explícito del interesado como supuesto que justifica el tratamiento de categorías especiales de datos personales no es suficiente cuando tanto el Derecho de la Unión como el Derecho de los Estados miembros establezca que la prohibición del tratamiento no puede ser levantada por el interesado –art. 9.2.a)–.

Pues bien, por una parte, el RGPD prevé la participación del Derecho de los Estados miembros en la delimitación de los supuestos tasados del art. 9.2 RGPD. El RGPD contiene una remisión expresa a la legislación laboral de los Estados miembros al considerar legítimo el tratamiento de categorías especiales de datos personales cuando "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" –art. 9.2.b)–. Asimismo, el RGPD reputa como legítimo el tratamiento de categorías especiales de datos personales cuando "es necesario por razones de un interés público esencial" no sólo sobre la base del Derecho de la Unión sino también sobre la base del Derecho de los Estados miembros, "que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" –art. 9.2.g)–. El RGPD contiene una especial remisión al Derecho de los Estados miembros para la legitimación de los tratamientos de categorías especiales de datos personales con finalidad de atención sanitaria, de salud pública y de investigación. Así, el Derecho de los Estados miembros –y no sólo el Derecho de la Unión– puede establecer que el tratamiento de categorías especiales de datos personales es necesario "para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social" –art. 9.2.h)–[33], debiendo fijar también que el tratamiento lo realiza un profesional sujeto al secreto profesional o bajo su responsabilidad o cualquier otra persona sujeta a la obligación de secreto, teniendo un papel relevante en este último aspecto el Derecho de los Estados miembros o las normas establecidas por los organismos nacionales competentes –art. 9.3–[34]; que el tratamiento de categorías especiales de datos personales es necesario "por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los me-

to, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito".

[33] También puede hacerse "en virtud de un contrato con un profesional sanitario", teniendo en cuenta las condiciones y garantías establecidas en el art. 9.3 RGPD.

[34] De hecho, la regulación del art. 9.2.h) RGPD recuerda el margen de maniobra que ofrecía el art. 8.3 de la Directiva 95/46/CE, que establecía que la prohibición de tratamiento de categorías especiales de datos personales "no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto". Este precepto fue traspuesto casi literalmente por el art. 7.6 LOPD que omitía únicamente que la sujeción al secreto profesional del profesional sanitario estuviera prevista en la legislación nacional o en las normas establecidas por las autoridades competentes.

dicamentos o productos sanitarios", debiendo establecerse en la base jurídica –el Derecho de la Unión o de los Estados miembros– las medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en especial el secreto profesional –art. 9.2.i)–; o que el tratamiento de categorías especiales de datos personales es necesario "con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos", teniendo en cuenta lo establecido en el art. 89 RGPD, debiendo establecerse en la base jurídica –de nuevo, no sólo el Derecho de la Unión sino también el de los Estados miembros–, que el tratamiento "debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" –art. 9.2.j)–.

Por otra parte, el RGPD permite a los Estados miembros "mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud" –art. 9.4–. Esto significa que el RGPD deja un margen de maniobra a los Estados miembros en los tratamientos de determinadas categorías especiales de datos personales, como los biométricos, cuyo tratamiento es especialmente considerado sospechoso por los países pertenecientes al antiguo bloque del este, o los datos genéticos o de salud, lo que atribuye a los Estados un espacio para la regulación en el ámbito de la atención sanitaria y la investigación sanitaria que aleja al RGPD del cumplimiento del objetivo de armonización[35]. Por tanto, en ocasiones, el RGPD está llamando al legislador de los Estados miembros para que concrete las garantías adicionales, las limitaciones o las excepciones a estos tratamientos de categorías especiales de datos personales.

No obstante, esta llamada que el RGPD hace al legislador de los Estados miembros para que concrete las garantías relativas a estos tratamientos, las condiciones adicionales, las limitaciones e inclusive las excepciones no puede servir para suprimir o para desnaturalizar las previsiones contenidas en el RGPD. Este margen maniobra que el RGPD concede a los Estados no debe hacer olvidar que, como señala el Considerando 10, "para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea"[36]. Llegados a este punto hay que reconocer la dificultad que supone la coexistencia de una voluntad de establecer en la Unión Europea un nivel uniforme y elevado en la protección de datos personales y el reconocimiento al mismo tiempo de un margen de maniobra a los Estados en distintos ámbitos.

En cambio, uno de los ámbitos donde el RGPD supone una mayor alteración del marco jurídico en protección de datos personales existente hasta ahora y, más en concreto, del margen de maniobra de los Estados, en este caso, reduciéndolo o suprimiéndolo, es el de la seguridad de los datos. El RGPD considera la

[35] ÁLVAREZ RIGAUDAS considera que esta previsión es desafortunada porque "cualquier fragmentación del mercado interior incidirá negativamente (como ya demuestra la normativa presente) en el desarrollo de la investigación científica en la Unión Europea". Cfr. ÁLVAREZ RIGAUDAS, CECILIA, "Tratamiento de datos de salud", en PIÑAR MAÑAS, JOSÉ LUIS, *El Reglamento General de Protección de Datos*, *cit.* p. 178.

[36] En esta dirección, el Considerando 53 del RGPD, después de señalar que los Estados miembros están facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, también señala que "no obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos".

seguridad de los datos tanto un principio relativo al tratamiento como una obligación del responsable y del encargado. Así, por una parte, el RGPD proclama entre los principios relativos al tratamiento el principio de "integridad y confidencialidad", en virtud del cual "los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas" –art. 5.1.f)–; por otra parte, el RGPD regula en el Capítulo IV al responsable y al encargado del tratamiento, situando la seguridad de los datos tanto entre las obligaciones generales contenidas en la Sección 1º como entre las obligaciones específicas incluidas en la Sección 2º, titulada "Seguridad de los datos personales".

Como hemos señalado antes, el responsable del tratamiento tiene una "responsabilidad proactiva" por la que el "responsable del tratamiento será responsable del cumplimiento de [los principios relativos al tratamiento] y capaz de demostrarlo" –art. 5.2 RGPD–. Este principio de responsabilidad proactiva se manifiesta en el cumplimiento de unas obligaciones generales del responsable y del encargado del tratamiento, entre las que se encuentra la seguridad de los datos. Así, el RGPD establece que "teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento es conforme con el […] Reglamento" –art. 24.1–. De manera específica el RGPD aborda en el art. 32 la seguridad del tratamiento como obligación del responsable y del encargado del tratamiento. Señala en el apartado 1 que "teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"[37]. Por tanto, el RGPD obliga al responsable a llevar a cabo un análisis de riesgos, que valore, por una parte, la naturaleza, el ámbito, el contexto y los fines del tratamiento, y, por otra parte, los riesgos para los derechos de las personas que pueden provenir del tratamiento de datos, tanto la gravedad de los riesgos como su probabilidad. El art. 32.2 RGPD precisa aún más cuales son los riesgos que presenta el tratamiento y que hay que tener en cuenta al evaluar el nivel de seguridad: "la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

A partir de este análisis de riesgos, el responsable y el encargado del tratamiento deben aplicar las medidas técnicas y organizativas apropiadas, valorando también el estado de la técnica y los costes de aplicación. Estas medidas no son solo para garantizar que el tratamiento de datos personales cumple el Reglamento –esto es insuficiente– sino también para "poder demostrarlo" –art. 24.1 RGPD–. Además, el Reglamento establece un mayor dinamismo y fluidez en el análisis del cumplimiento de las medidas al señalar que "dichas medidas se revisarán y actualizarán cuando sea necesario".

Hay que subrayar, llegados a este punto, que el RGPD contiene muy pocas obligaciones concretas al responsable y al encargado en relación con la seguridad del tratamiento. Realmente el RGPD sólo explicita dos obligaciones que se aplican a supuestos concretos: la "no-

[37] Cfr. I. González Ubierna, "Seguridad del tratamiento", en J. López Calvo (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, *cit.* pp. 453-459; M. Carpio Cámara, "Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad", en J. L. Piñar Mañas (Dir.), *Reglamento general de protección de datos*, *cit.* pp. 335-348.

tificación de una violación de la seguridad de los datos personales a la autoridad de control" –art. 33– y la "comunicación de una violación de la seguridad de los datos personales al interesado" –art. 34–.

Esto significa que las medidas técnicas y organizativas que se van a implementar en cada tratamiento no van a provenir inicialmente de la norma sino que van a ser consecuencia de ese análisis de riesgos que lleve a cabo el responsable y el encargado del tratamiento. En todo caso, el RGPD, después de señalar que el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, menciona expresamente dos medidas de seguridad como son "la seudonimización y el cifrado de datos personales" –art. 32.1.a)–, que son las únicas medidas de seguridad técnicas que se incorporan al Reglamento lo que dice mucho de su importancia, si bien el RGPD no fija a que tratamientos se deben aplicar. Además, el RGPD señala que el responsable y el encargado deben aplicar medidas técnicas y organizativas que incluyan: "la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento" –art. 32.1.b)–; "la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico" –art. 32.1.c)–; "un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento" –art. 32.1.d)–. Además, el RGPD también establece que "el responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros" –art. 32.4–. Cómo se puede comprobar, a excepción de la mención a la seudonimización y al cifrado, el RGPD no contiene una mención de las concretas medidas técnicas y organizativas que deben implementarse sino únicamente contiene los fines de estas medidas: garantizar la integridad de los datos –evitando su destrucción, pérdida o alteración–, garantizar la disponibilidad de los datos, garantizar la confidencialidad de los datos–evitando el acceso no autorizado o ilícito– y garantizar la resiliencia –capacidad para seguir cumpliendo sus funciones en situaciones de riesgo–.

El RGPD no autoriza ni a la Comisión ni a los Estados miembros a establecer las medidas técnicas y organizativas para la seguridad de los tratamientos. El RGPD no deja margen de maniobra a los Estados en el ámbito de la seguridad, sin perjuicio del ya reseñado relativo a la licitud de los tratamientos, a las situaciones específicas de tratamiento recogidas en el Capítulo IX y a las categorías especiales de datos personales que pueden implicar requisitos adicionales relativos a la seguridad y a la confidencialidad[38]. Esta ausencia de margen de maniobra a la Comisión y a los Estados contrasta con el espacio que el RGPD sí ofrece a la autorregulación en el ámbito de la seguridad del tratamiento. Así, dentro de las obligaciones generales del responsable del tratamiento se establece que "las oportunas

[38] Únicamente el RGPD, como hemos señalado antes, al regular la licitud de los tratamientos para el cumplimiento de una obligación legal o de una misión de interés público o en el ejercicio de los poderes públicos así como en relación con situaciones específicas de tratamiento contempladas en el Capítulo IX, permite a los Estados introducir disposiciones más específicas para adaptar la aplicación del Reglamento y para fijar de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo –art. 6.2 y 3–. Igualmente, también como ya hemos indicado, el RGPD reconoce un cierto margen de maniobra a los Estados en relación con el tratamiento de categorías especiales de datos personales que permite a los Estados miembros introducir condiciones adicionales –art. 9.4–. Asimismo, el Derecho de los Estados miembros puede establecer medidas adecuadas y específicas para proteger los derechos fundamentales del interesado en los tratamientos por razones de un interés público esencial, en los tratamientos en el ámbito de la salud pública y en los tratamientos con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos –art. 9.2.g), i) y j)–.

políticas de protección de datos" que adopten serán medidas técnicas y organizativas para garantizar y poder demostrar el cumplimiento de la normativa, cuando sean proporcionadas con las actividades del tratamiento –art. 24.2 RGPD–. Igualmente se establece expresamente que la adhesión a los códigos de conducta y los mecanismos de certificación, regulados en los arts. 40 y 42 RGPD respectivamente, son "elementos para poder demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento" –art. 24.3 RGPD–. Esta apuesta por la autorregulación se reitera expresamente en el art. 32 RGPD, dedicado a la seguridad del tratamiento donde se establece que la adhesión a un código de conducta o a un mecanismo de certificación "podrá servir de elemento para demostrar" que se adoptan las medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado y que, por tanto, se cumplen los requisitos recogidos en el art. 32.1 –art. 32.3–.

La regulación que hace el RGPD de la seguridad del tratamiento se aparta radicalmente del modelo de normativa de protección de datos personales que era de aplicación hasta ahora en nuestro país y que respondía a un modelo jurídico continental. Como es sabido, la Directiva 95/46/CE señalaba que "los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales". Estas medidas "deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse" –art. 17.1–. La Directiva 95/46/CE dejaba esta cuestión en manos de los Estados miembros si bien no precisaba si le correspondía a los Estados la determinación del listado de las medidas técnicas y organizativas para la seguridad de los tratamientos –correspondiéndole al responsable su aplicación al caso concreto– o si la determinación de las medidas de seguridad era una cuestión que debía decidir el responsable del tratamiento después de una evaluación de los riesgos[39]. El TJUE, en la Sentencia de 30 mayo 2013, *caso Worten* (asunto C-342/12), que resolvía una cuestión prejudicial en relación con el art. 17.1 de la Directiva 95/46/CE, señaló que la Directiva "no impone a los Estados miembros, salvo cuando tienen la condición de responsables del tratamiento, la adopción de estas medidas técnicas y de organización, dado que la obligación de adoptarlas incumbe únicamente al responsable del tratamiento, que en el presente caso es el empresario. Sin embargo, la misma disposición sí exige a los Estados miembros la adopción de una disposición de Derecho interno que establezca esta obligación" –apdo. 25–. Por tanto, en aplicación de la Directiva 95/46/CE los Estados no estaban obligados a imponer las concretas medidas de seguridad a los responsables salvo para sus propios tratamientos, pero sí tenían que aprobar una legislación que transpusiera la Directiva obligando al responsable a adoptar estas medidas para garantizar un nivel de seguridad adecuado.

En cambio, la LOPD no se limitó a transponer este precepto de la Directiva, reproduciéndolo a través de un mandato genérico de que "el responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su

[39] La mayoría de los Estados habían optado por una formulación similar a la prevista en el art. 17 de la Directiva, imponiendo únicamente a los responsables del tratamiento la obligación de aplicar medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, pérdida accidental, difusión y acceso no autorizado y señalando que estas medidas debían garantizar un nivel de seguridad adecuado en relación con los riesgos y la naturaleza del tratamiento, pero sin establecer unas concretas medidas de seguridad.

alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural" –art. 9.1– LOPD–[40]. El legislador español dio un paso más al añadir que "no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas" –art. 9.2–, completando que "reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley [Datos especialmente protegidos]" –art. 9.3–. Por tanto, la LOPD establecía que una norma reglamentaria fijaría las condiciones relativas a la integridad y a la seguridad que deben reunir los ficheros y los centros de tratamiento, locales, equipos, sistemas y programas y, específicamente, en relación con los datos especialmente protegidos del art. 7 LOPD[41]. Incluso la LOPD calificaba como infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen" –art. 44.3.h)–.

Por tanto, la LOPD, a diferencia de la legislación de otros países, no se limitaba a señalar que el cumplimiento del principio de seguridad de los tratamientos era una obligación genérica del responsable y del encargado sino que lo vinculaba a la adopción de unas medidas técnicas y organizativas concretas aprobadas en la normativa. Desde un planteamiento exigente con la calidad de la ley, la seguridad de los datos no podía ser algo indeterminado sino que debía presentar la certeza suficiente que evitase la incertidumbre sobre su modo de aplicación efectiva[42]. La normativa de seguridad de los tratamientos de datos personales –tanto la de 1999 como la de 2007– estableció la existencia de tres niveles de seguridad –básico, medio y alto–, a cada uno de los cuales le correspondían un listado de medidas de seguridad, y estos niveles de seguridad se aplicaban teniendo en cuenta la tipología de datos, "la naturaleza de la información tratada, en relación con la mayor o menor nece-

[40] El Tribunal Constitucional se había pronunciado en la Sentencia 17/2013, de 31 de enero, sobre la importancia de la seguridad de los datos como garantía de la confidencialidad, señalando que el principio de proporcionalidad aplicable a la limitación de un derecho fundamental exige "la necesidad de motivar y justificar expresamente tanto la concreta atribución de la condición de usuario para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos accesos de que se trate, evitando [...] que se produzca tanto un uso torticero de dicha facultad como accesos indiscriminados o masivos" –F. J. 9º–.

[41] La normativa que desarrolló esta previsión legal del art. 9.2 y 3 LOPD fue primero el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, aprobado por el Real Decreto 994/1999, de 11 de junio, y después el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, que regulaba en su Título VIII "las medidas de seguridad en el tratamiento de datos de carácter personal" –y derogaba el Real Decreto anterior–.

[42] El Magistrado Pérez Tremps, en su voto particular a la STC 17/2013, de 31 de enero –F. J. 3º–, ha subrayado que las exigencias de la calidad de la ley obligan a ésta no sólo a respetar el principio de proporcionalidad sino a "la necesidad de que se regulen las instituciones o medidas limitativas de derechos fundamentales con un grado de determinación y certeza suficiente para evitar que se genere grave inseguridad o incertidumbre sobre su modo de aplicación efectiva", señalando las "profundas indeterminaciones" en relación con las garantías del acceso: "aunque la norma prevé que el acceso se realizará con las «máximas medidas de seguridad», éstas no se concretan, más allá de que quedará constancia de cada acceso, de la identidad del accedente, de la fecha y hora del acceso y de los datos consultados. La posición de la mayoría afirma que el acceso, y la motivación que lo inspira, estará sujeta a control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional contencioso-administrativo, y entiende que habrá de evitarse que se produzca un uso torticero de la facultad de acceso, así como un acceso indiscriminado o masivo. Todas estas previsiones, no obstante, resultan excesivamente indeterminadas e insuficientes. Por dar sólo un ejemplo, no se contempla que el propio afectado pueda conocer que se ha producido el acceso y, en consecuencia, queda indefenso respecto de una medida limitativa de un derecho fundamental ante la que no puede protegerse plenamente en caso de un eventual acceso indebido en su información padronal".

sidad de garantizar la confidencialidad y la integridad de la información"[43], haciendo una especial consideración, además, a los datos especialmente protegidos. La normativa española no dejaba la determinación de las medidas de seguridad en manos del responsable del tratamiento a partir de la evaluación de riesgos sino que esta se encontraba fijada de manera rigurosa por la normativa, sin dejar margen de apreciación alguno al responsable del tratamiento[44]. Sin embargo, esta no era la posición preferida por la Comisión Europea. Para la Comisión Europea, el hecho de que España aprobara una regulación que con gran nivel de detalle establecía las medidas de seguridad técnicas y organizativas que debían ser implantadas por los responsables y encargados del tratamiento contribuía a generar un alto nivel de divergencia en relación con la seguridad de los tratamientos en la Unión Europea. En cambio, Holanda había aprobado unas medidas de seguridad que, sin embargo, no eran vinculantes para los responsables de ficheros aunque eran usadas como un importante elemento de autorregulación[45]. Esta es la posición que se materializó en el RGPD que no concede a los Estados un margen de maniobra para llevar a cabo un desarrollo normativo en el ámbito de la seguridad de los tratamientos de datos personales.

El RGPD únicamente concede a las autoridades de control la capacidad de emitir directrices, recomendaciones y buenas prácticas en materia de seguridad, que configuren no unas normas imperativas sino una suerte de *soft law* en este ámbito. De esta forma, se facilitan unas directrices en materia de seguridad, que suponen, de alguna manera, una alternativa a la adhesión a un código de conducta y, en definitiva, a la privatización de la normativa. Así, el RGPD ha tenido en cuenta la importancia de la seguridad del tratamiento al definir las funciones del Comité Europeo de Protección de Datos –art. 70–. Así, le corresponde a este Comité supervisar y garantizar la aplicación coherente del RGPD y asesorar a la Comisión sobre cualquier cuestión relativa a la protección de datos personales en la Unión Europea –art. 70.1.a) y b) RGPD–, lo que también alcanza la seguridad del tratamiento. En especial, el Comité examinará "cualquier cuestión relativa a la aplicación del Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del Reglamento" –art. 70.1.e) RGPD–. En especial, le corresponde al Comité Europeo emitir *directrices, recomendaciones y buenas prácticas* "a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales" –art. 70.1.g)– y "con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas" –art. 70.1.h RGPD–.

Como hemos señalado tempranamente, el RGPD "se aleja de un modelo de seguridad basado en que el responsable aplique unas normas predeterminadas decididas por la Administración. El Reglamento no sólo desplaza las normativas nacionales en materia de seguridad e impide que los Estados nacionales dicten una normativa en materia de seguridad, sino que tampoco permite que esa materia sea objeto de actos de delegación y aplicación por parte de la Comisión. El Reglamento no establece unas medidas específicas sino que deja en manos de los responsables del tratamiento

[43] Cfr. el art. 3 del Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal, aprobado por el Real Decreto 994/1999, de 11 de junio.

[44] La Exposición de Motivos del Real Decreto 1720/2007, de 21 de diciembre, establece que el Reglamento "trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso" –III–.

[45] Cfr. *Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE),* Bruselas, 15.5.2003 COM (2003) 265 –http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm–; *Analysis and impact study on the implementation of Directive EC 95/46 in Member States*, http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm

la adopción de las medidas técnicas y organizativas apropiadas al caso concreto, si bien es posible que las autoridades de control elaboren y den publicidad a protocolos, parámetros o indicadores de seguridad". De esta forma, "el Reglamento se aleja de un modelo jurídico de Derecho continental europeo, que proviene del Derecho romano y que se caracteriza por una amplia regulación y una predeterminación de la solución jurídica, para acercarse más a un modelo de *Common Law*, que se caracteriza por una mayor desregulación y que tiene en cuenta la valoración del caso concreto. Esto se pone de manifiesto especialmente en las medidas de seguridad de los tratamientos. Evidentemente, la introducción de elementos de la cultura jurídica anglosajona, como la autorregulación, la desregulación y la *accountability*, si bien aporta una mayor flexibilidad a la hora de buscar soluciones al caso concreto y de adaptarse a los futuros cambios tecnológicos, también supone una mayor inseguridad jurídica para aquellos responsables acostumbrados a la detallada y extensa regulación característica del modelo jurídico continental"[46].

3. LA LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

Las razones antes expuestas llevaron al Gobierno a elaborar un anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal. El Consejo de Ministros aprobó finalmente el 10 de noviembre de 2017 el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal –PLOPD–. Teniendo en cuenta que el RGPD, aprobado por el Parlamento Europeo y por el Consejo el 27 de abril de 2016, fue publicado el 4 de mayo de 2016, entró en vigor el 25 de mayo de 2016 y era aplicable a partir del 25 de mayo de 2018, hay que poner de manifiesto que el Gobierno apuró excesivamente el plazo de *vacatio legis* para ejercer la iniciativa legislativa que permitiera adaptar la legislación interna que había transpuesto la ya derogada Directiva 95/46/CE al nuevo derecho derivado institucional de la Unión Europea. Esto se evidencia aún más teniendo en cuenta que la Propuesta de Reglamento es aprobada por la Comisión en enero de 2012 y tuvo una tramitación muy lenta en las instituciones europeas, interviniendo el Gobierno en el procedimiento legislativo por lo que había dispuesto de la información y del tiempo suficiente para haber elaborado con anterioridad el anteproyecto.

El retraso en la tramitación parlamentaria del proyecto de ley en las Cortes Generales y en la consiguiente aprobación de la Ley Orgánica, posiblemente afectado por la moción de censura y el cambio de gobierno, hizo que se llegara al 25 de mayo de 2018, fecha del inicio de la aplicación del RGPD, sin haberse aprobado antes la nueva LOPD. Esto obligó al Consejo de Ministros a aprobar el 27 de julio de 2018 un Real Decreto Ley con medidas urgentes para adaptar el Derecho español al Reglamento General de Protección de Datos.

El PLOPD fue objeto de importantes enmiendas en su tramitación en el Congreso de los Diputados. En especial hay que mencionar las enmiendas del Grupo Parlamentario Socialista relativas a los llamados derechos digitales. A finales de septiembre de 2018 se elaboró en el Congreso de los Diputados el Informe definitivo de la Ponencia sobre el Proyecto de Ley Orgánica, que incorporaba estas enmiendas y que pasó a denominarse de Protección de Datos Personales y garantía de los derechos digitales –PLOPDGDD–[47]. El 23 de

[46] Cfr. A. TRONCOSO REIGADA, "Autoridades de control independientes", *cit.* pp. 468-469.

[47] El dictamen de la Comisión de Justicia fue el 9 de octubre y después pasó al Pleno del Congreso. El 18 de octubre se aprobó por unanimidad en el Pleno del Congreso de los Diputados el Dictamen de la Comisión sobre el Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Cfr. el debate y votación en el Diario de Sesiones de ese día.http://www.congreso.es/portal/page/portal/Congreso/PopUpCGI?CMD=VERLST&BASE=pu12&DOCS=1-1&QUERY=%28DSCD-12-PL-157.CODI.%29#(P%C3%A1gina38).

octubre de 2018 el texto aprobado por el Pleno del Congreso tuvo entrada en el Senado y se remitió a la Comisión de Justicia, abriéndose el plazo para presentar enmiendas y propuestas de veto hasta el 5 de noviembre. El 15 de noviembre de 2018 se debatió en la Comisión de Justicia del Senado las enmiendas al Proyecto de Ley Orgánica que finalmente no fueron aceptadas. Finalmente el Senado aprobó el 21 de noviembre de 2018 la Ley Orgánica de Protección de Datos de Carácter Personal y garantía de los derechos digitales, al haber aceptado sin introducir enmiendas el Proyecto de Ley Orgánica debatido y aprobado por el Congreso de los Diputados, quedando finalizada, de esta forma, la tramitación legislativa. Finalmente el 6 de diciembre se publicó en el BOE la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales –LOPDGDD–, coincidiendo con el 40º Aniversario de la Constitución Española de 1978.

El objeto de esta Ley Orgánica es "*adaptar el ordenamiento jurídico español* al RGPD, y *completar sus disposiciones*" –art. 1.a) primer párrafo de la LOPDGDD–. El RGPD adapta el ordenamiento jurídico español al RGPD al derogar no sólo la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos personales sino también "cuantas disposiciones de igual o inferior rango contradigan, se opongan o resulten incompatibles" con lo dispuesto en el RGPD y en esta Ley Orgánica –Disposición derogatoria única LOPDGDD–. Estas normas internas incompatibles con el RGPD no quedan únicamente desplazadas sino derogadas, lo que lleva a cabo la LOPDGDD que tiene como razón última garantizar el principio de seguridad jurídica[48]. De esta forma, la referencia a la adaptación del ordenamiento jurídico español contenida en el art. 1.a) LOPDGDD tiene que ser interpretada como una depuración del ordenamiento jurídico interno. Además, el objeto de esta Ley Orgánica es completar las disposiciones del RGPD. La LOPDGDD no trata sólo de adecuar la legislación española al RGPD sino también de aprovechar el margen de maniobra que el RGPD confiere a los Estados miembros para interpretar, especificar y, en ocasiones, restringir sus previsiones normativas. Por último, la LOPDGDD reitera en ocasiones previsiones contenidas en el RGPD para facilitar la integración de ambas normas, su coherencia y su comprensión. Como señala la Exposición de Motivos de la LOPDGDD –apdo. III–, el principio de seguridad jurídica, "en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos". Así, apartándose del principio general del Derecho de la Unión Europea, el Considerando 8 del RGPD señala que cuando las normas del RGPD deban ser especificadas o restringidas por el Derecho de los Estados miembros, "estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del […] Reglamento".

Por consiguiente, el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el RGPD y a la LOPDGDD –art. 1.a), segundo párrafo de la LOPDGDD–. El marco normativo en nuestro país sobre protección de datos personales está formado tanto por el RGPD como por la LOPDGDD, así como por el resto de la normativa relativa a protección de datos personales, de ámbito estatal y autonómico y de rango legal y reglamentario en lo que no se opongan a lo establecido en ellas. Hay que señalar que las enmiendas introducidas al PLOPD fueron más sensibles a

[48] Como señala su Exposición de Motivos, la adaptación al RGPD "requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica" –apdo. III–.

las competencias de las Comunidades Autónomas en este ámbito[49]. A este marco normativo hay que añadir la legislación específica mencionada en el art. 2 LOPDGDD. Los tratamientos de datos personales sometidos a la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la libre circulación de dichos datos, se regirán por la futura normativa de trasposición y, entre tanto, por la LOPD–[50].

En todo caso, hay que señalar que el objeto de la LOPDGDD no es sólo adaptar el ordenamiento jurídico español al RGPD, y completar sus disposiciones. El art. 1.b) LOPDGDD establece que la ley orgánica también tiene por objeto "garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el art. 18.4 de la Constitución", una previsión que se incorporó en la tramitación legislativa y que no se encontraba en el proyecto de Ley aprobado en el Consejo de Ministros. Las Cortes Generales, a través del trámite de enmiendas, quisieron subrayar la importancia de garantizar en esta Ley el pleno ejercicio de los derechos fundamentales en Internet, algo que se plantea como la antesala de un futura reforma constitucional que reconozca y dé rango constitucional a los derechos digitales de los ciudadanos y que actualice la Constitución a la era digital[51].

De esta forma, el objeto de la LOPDGDD va más allá que el objeto del RGPD, que era establecer las normas relativas a la protección de las personas físicas en lo que respecta al *tratamiento de los datos personales* y las normas relativas a la libre circulación de tales datos, proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su *derecho a la protección de los datos personales* y evitar que la libre circulación de los datos personales en la Unión sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al *tratamiento de datos personales* –art. 1 RGPD–. La LOPDGDD, a diferencia del RGPD, tiene un objeto más amplio porque trata de garantizar los derechos digitales de la ciudadanía más allá del derecho fundamental a la protección de datos personales[52].

[49] Como señala la Exposición de Motivos de la LOPDGDD, "las Comunidades Autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía" –apdo. IV, incorporado en la tramitación parlamentaria–.

[50] El art. 2.2.d) RGPD excluye de su ámbito de aplicación estos tratamientos, lo que se traslada al art. 2.2.a) LOPDGDD. Estos tratamientos se regirán en el futuro por la normativa que transponga la Directiva (UE) 2016/680. Mientras que no se apruebe esta normativa de trasposición, la Disposición adicional decimocuarta de la LOPDGDD establece que "las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la LOPD, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas". La Disposición transitoria cuarta de la LOPDGDD establece que los tratamientos sometidos a la Directiva (UE) 2016/680 continuarán rigiéndose por la LOPD, en particular el art. 22 y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva. En coherencia, la Disposición derogatoria única de la LOPDGDD deroga la LOPD "sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta".

[51] Llama la atención que se haya incluido en la Exposición de Motivos de la LOPDGDD una apuesta por la reforma constitucional: "Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea" –apdo. IV, incorporado en el trámite de enmiendas–.

[52] Sin embargo, el hecho de que el art. 1.b) LOPDGDD prevea garantizar los derechos digitales de la ciudadanía "conforme al mandato establecido en el art. 18.4 de la Constitución", que hace referencia a que la ley limitará el uso de la *informática* presupone la existencia de un tratamiento automatizado.

Lógicamente esta diferencia también aparece en el "Ámbito de aplicación material". Así, el RGPD "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero" –art. 2.1–. Esto significa que hay dos elementos que son esenciales para que se dé el objeto del RGPD y para la delimitación de su ámbito de aplicación material: que exista un tratamiento y que este se sustancie sobre datos personales. Tradicionalmente la normativa de protección de datos personales ha exigido para que sea de aplicación el derecho fundamental a la protección de datos personales que se den estos dos elementos que delimitan su objeto y su ámbito de aplicación[53]. En cambio, la LOPDGDD al regular su ámbito de aplicación en el art. 2.1, si bien ha recogido textualmente en una parte la redacción del art. 2.1 RGPD "Ámbito de aplicación", señala claramente que su ámbito de aplicación no se circunscribe a los tratamientos de datos personales en el caso del Título X "Garantía de los derechos digitales", salvo los artículos 89 al 94 para los que sí se exige el tratamiento de datos personales. Por tanto, la LOPDGDD no sólo tiene como único ámbito de aplicación material los tratamientos de datos personales –este es el ámbito de aplicación material de los Títulos I a IX y de los artículos 89 a 94–, sino que se extiende también a los derechos digitales de la ciudadanía, sin que se exija en este caso un tratamiento de datos personales. Por tanto, no se aplica la exigencia de que exista un tratamiento de datos personales a los derechos en la era digital –art. 79–, al derecho a la neutralidad de Internet –art. 80–, al derecho al acceso universal a Internet –art. 81–, al derecho a la seguridad digital –art. 82–, al derecho a la educación digital –art. 83–, a la protección de los menores en Internet –art. 84–, al derecho a la rectificación en Internet –art. 85–, al derecho a la actualización de informaciones en medios de comunicación digitales –art. 86–, al derecho a la portabilidad en servicios de redes sociales y servicios equivalentes –art. 95–, al derecho al testamento digital –art. 96– y a las políticas de impulso de los derechos digitales –art. 97–. En relación con la regulación de los derechos en el ámbito laboral, no se exige la existencia de tratamiento de datos personales al derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral –art. 87– y al derecho a la desconexión digital en el ámbito laboral –art. 88–. En cambio, la regulación del ámbito de aplicación material requiere la existencia de un tratamiento de datos personales en relación con el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo –art. 89–, el derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral –art. 90– y en relación con los derechos digitales en la negociación colectiva –art. 91–.

El carácter más amplio de la LOPDGDD en relación con el RGPD se pone de manifiesto en el propio título. Si el Reglamento es "relativo a la protección de las personas físicas en lo que respeta al *tratamiento de datos personales* y a la libre circulación de estos, la Ley Orgánica 3/2018, de 5 de diciembre no es sólo de Protección de Datos Personales sino también de *garantía de los derechos digitales*.

Como hemos señalado antes, el RGPD confiere a los Estados miembros un margen de maniobra para completar sus disposiciones, interpretando, especificando y, en ocasiones, restringiendo sus previsiones normativas.

[53] La Directiva 95/46/CE, establece como objeto "la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales" –art. 1.1– y como ámbito de aplicación el "tratamiento total o parcialmente automatizado de datos personales, así como [e]l tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero". También la LOPD señalaba que "la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar" –art. 1– y que será "de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento" –art. 2.1 LOPD–.

En general, la LOPDGDD ha aprovechado el margen de maniobra que el RGPD ha dado a los Estados.

Así, la Exposición de Motivos –apdo. V– señala que esta LOPDGDD contiene "*las posibles habilitaciones legales* para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal". Como ejemplos de habilitaciones legales, la Exposición de Motivos refiere la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, que regula la base de datos central de información de riesgos del Banco de España o la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, que regula los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones.

Añade la Exposición de Motivos que "se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y sólo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley". La LOPDGDD, siguiendo al RGPD, atribuye una importante función a la base jurídica del tratamiento cuando es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, lo que refuerza el principio de legalidad administrativa en este ámbito y el sometimiento pleno de la Administración Pública a la Ley y al Derecho –art. 103.1 CE–.

En esta dirección, el art. 8.1 LOPDGDD **–"**Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos"–, después de afirmar que el tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del RGPD cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, establece que ésta Ley "podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679". El art. 8.2 LOPDGDD reitera que "el tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley". Llegados a este punto se evidencia que la LOPDGDD refuerza el principio de reserva de Ley en esta materia.

Igualmente, la LOPDGDD aprovecha la habilitación normativa que el RGPD concede a los Estados miembros para interpretar, especificar y, en ocasiones, restringir sus previsiones en relación con los tratamientos de categorías especiales de datos personales.

Esto se pone de manifiesto en el primer supuesto que legitima el tratamiento de categorías especiales de datos personales, que es que el interesado haya dado "su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados" –art. 9.2.a)–. Así, el RGPD establece que si bien el interesado puede dar su consentimiento explícito para el tratamiento de estas categorías especiales de datos personales, también permite que el Derecho de los Estados

miembros establezca que la prohibición de tratamiento de las categorías especiales de datos personales no puede ser ni siquiera levantada con el consentimiento explícito del interesado –art. 9.2.a), *in fine*–. De esta forma, el RGPD deja un margen de maniobra a los Estados en un ámbito que puede afectar a los derechos fundamentales, especialmente, a la libertad ideológica, religiosa y sindical y a la prohibición de discriminación por raza o por orientación sexual. Este margen ha permitido que la LOPDGDD, al regular las categorías especiales de datos personales, establezca que, en virtud de esta previsión del RGPD y "a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico" –art. 9.1–.

Por tanto, el consentimiento explícito del interesado no es suficiente para legitimar los tratamientos de algunas categorías especiales de datos personales si estos tratamientos tienen como finalidad principal –no meramente accesoria– identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. Como señala la Exposición de Motivos –apartado V–, "se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el RGPD. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de "listas negras" de sindicalistas". De esta forma, si el RGPD permite mejorar la protección de las categorías especiales de datos personales en relación con el recurso al consentimiento explícito como supuesto de legitimación, el legislador español ha optado por fortalecer la protección de aquellas categorías especiales de datos personales cuyo tratamiento puede dar lugar a una vulneración de la libertad ideológica y religiosa –art. 16 CE–, de la libertad sindical –art. 28 CE– y de la prohibición de discriminación –art. 14 CE–. Hay que recordar que el art. 16 CE no sólo garantiza la libertad ideológica, religiosa y de culto sino que establece expresamente en el apartado 2 que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias".

Es interesante señalar que este planteamiento del RGPD proviene de la Directiva 95/46/CE, que establecía asimismo que el consentimiento explícito del interesado podía legitimar el tratamiento de categorías especiales de datos personales, "salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición […] no pueda levantarse con el consentimiento del interesado" –art. 8.2.a)–. Por ese motivo, es interesante comparar cómo la LOPDGDD ha completado la habilitación normativa prevista en el RGPD, con la forma en que la LOPD traspuso la Directiva 95/46/CE en este punto. Pues bien, la LOPD optó por hacer una regulación que continuaba con la previsión contenida en el art. 7 de la LORTAD, que era anterior a la Directiva, y no tuvo en cuenta el art. 8 de la Directiva, pues no se limitó a señalar que el solo consentimiento explícito del afectado no bastará para levantar la prohibición del tratamiento de categorías especiales de datos personales. El art. 7 de la LOPD, reiterando lo que señalaba la LORTAD, después de recordar la previsión contenida en el art. 16.2 CE de que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias", establecía dos garantías cuando se proceda a recabar el consentimiento del interesado para el tratamiento de sus datos de ideología, religión o creencias: la primera garantía era relativa al principio de información al interesado, de forma que cuando se proceda a recabar el consentimiento al interesado para el tratamiento de estos datos, se le advertirá expresamente de su derecho a no prestarlo –art. 7.1–; la segunda garantía era una exigencia relativa al consentimiento, no siendo suficiente que sea expreso sino que también escrito –art. 7.2–[54].

[54] La Agencia Española de Protección de Datos había señalado que "el régimen establecido en el artículo 7.2 [la exi-

Al tratarse de una Directiva, el Estado tenía un mayor margen de maniobra para establecer una exigencia adicional de consentimiento expreso y escrito en algunos tratamientos de datos que revelen la ideología, afiliación sindical, religión y creencias al afectar a la libertad ideológica y religiosa y a la libertad sindical reconocidas en los arts. 16 y 28 CE[55]. Por tanto, la manera en que la LOPD garantizaba efectivamente que nadie era obligado a declarar sobre su ideología, religión o creencias y, por tanto, que se respetaba la libertad ideológica y religiosa era introducir en los tratamientos de ideología, afiliación sindical, religión o creencias estas dos exigencias adicionales de información y de consentimiento del interesado.

Este planteamiento previsto en la LOPD inicialmente no parecía trasladable fácilmente al margen de maniobra que tiene la LOPDGDD para completar las previsiones contenidas en el RGPD. Por una parte, el RGPD no deja espacio a los Estados para incorporar una información adicional a la que de forma extensa ya se encuentra contenida en el art. 13 cuando los datos personales se obtengan del interesado. Sin embargo, parece que un tratamiento leal y transparente de datos de ideología, religión o creencias debería tener en cuenta la previsión constitucional del art. 16.2 CE de que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias", lo que implica la advertencia al interesado de su derecho a no prestar su consentimiento cuando se pretenda recabarlo. Por otra parte, en relación con el consentimiento y como hemos señalado en otro momento[56], "de una lectura del tenor literal del art. 9.2.a) *in fine* no parece claro o no se deduce que el RGPD autorice a los Estados a endurecer la forma de prestación del consentimiento y exigir que sea escrito para una clase o para todas las categorías especiales de datos personales. Esto pudo establecerse en el ámbito de una Directiva que es una norma de fines y no tanto en el de un Reglamento que es obligatorio en todos sus elementos y que tiene como uno de sus objetivos clarificar la regla del consentimiento como criterio de licitud de los tratamientos, superando la divergencia existente en Europa en este aspecto. Ahora bien, si el RGPD permite a los Estados miembros excepcionar el consentimiento explícito como supuesto de licitud para el tratamiento de categorías especiales de datos personales, también puede haber permitido endurecer el régimen jurídico de la prestación del consentimiento exigiendo un consentimiento expreso y escrito bajo el principio jurídico de *qui potest plus, potest minus* –quien puede lo más, puede lo menos–. En todo caso, el mayor rigor en el consentimiento o en la información al interesado no es una exigencia constitucional del art. 16.2 CE que se limita afirmar que "nadie podrá ser obligado a declarar sobre su ideología, religión o creencias" por lo que la previsión del art. 9.2.a) del RGPD no entra en contradicción con la CE.

Pues bien, la LOPDGDD al regular el tratamiento de las categorías especiales de datos personales basado en el consentimiento del afectado –art. 9.1– no incluye el requisito del consentimiento expreso y escrito para el tratamiento de los datos de opiniones políticas, convicciones religiosas o filosóficas o afiliación sindical que antes estaba presente en el art. 7.2 LOPD. Esto es lo que puede parecer a simple vista. Sin embargo, la Disposición final undécima. Dos de

gencia de un consentimiento expreso y escrito] parece traer su causa directa de lo dispuesto en el artículo 7.1 de la propia Ley Orgánica que establece que "de acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias". Cfr. el Informe de la AEPD, de 4 de agosto de 2009, publicado en su web, p. 20.

[55] La LOPD diferenciaba, dentro de estas categorías especiales de datos personales, los datos de ideología, afiliación sindical, religión o creencias cuyo tratamiento requería no sólo un consentimiento expreso sino expreso y escrito –art. 7.2– y los datos de origen racial, salud y vida sexual cuyo tratamiento requería consentimiento expreso –art. 7.3–, que era el previsto inicialmente en el art. 8.2.a) de la Directiva 95/46/CE para las categorías especiales de datos personales.

[56] Esta cuestión la hemos analizado en «Investigación, salud pública y asistencia sanitaria", *cit.* pp. 230-231.

la LOPDGDD, que modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en relación con el ejercicio del derecho de acceso cuando la información solicitada tuviera datos especialmente protegidos, redacta de nuevo el art. 15.1, primer párrafo, suprimiendo la mención al art. 7 LOPD pero manteniendo la regla del consentimiento expreso y escrito. Así, se establece que "si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el *consentimiento expreso y por escrito del afectado*, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso". Esto lleva a la situación paradójica de que sea suficiente el consentimiento expreso para el tratamiento o la cesión por un tercero de datos de opiniones políticas, convicciones religiosas o filosóficas o afiliación sindical pero para el ejercicio de un derecho de acceso a información administrativa en la que se contuviera esta clase de datos sería necesario el consentimiento expreso y escrito. Esto no parece ser algo buscado de propósito sino un problema de técnica legislativa característico de la modificación de los proyectos de ley en el trámite de enmiendas".

Además, la LOPDGDD también ha aprovechado el margen de maniobra que el art. 9.2 RGPD atribuye a los Estados miembros en el ámbito de los tratamientos de categorías especiales de datos personales para interpretar, especificar o restringir sus previsiones en relación con otros supuestos de legitimación del tratamiento. Este es el caso de los tratamientos de categorías especiales de datos por razones de interés público esencial –g)–, para fines de medicina preventiva o laboral, diagnóstico médico, prestación de asistencia o gestión de los sistemas y servicios de asistencia sanitaria y social –h)– y en el ámbito de la salud pública o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios –i)–[57]. El art. 9.2 LOPDGDD señala que estos tratamientos "deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte" –art. 9.2 LOPDGDD–[58]. Como hemos señalado antes, el art. 9.2 RGPD establece la participación de los Estados miembros en la delimitación de estos supuestos tasados de legitimación del tratamiento de categorías especiales de datos personales, aportando también la base jurídica. En todo caso, el art. 9.2 LOPDGDD establece expresamente que debe ser una Ley la que establezca los requisitos adicionales de seguridad y confidencialidad. De nuevo se observa, como señala la Exposición de Motivos de la LOPDGDD[59], en este caso en relación con el tratamiento de categorías especiales de datos personales, que "el artículo 9.2 LOPDGDD consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el RGPD".

La remisión a las habilitaciones legales para el tratamiento de categorías especiales de datos personales, como señala la Exposición de Motivos de la LOPDGDD, "no sólo alcanza a las disposiciones que pudieran

[57] Llama la atención la omisión en el art. 9.2 LOPDGDD de la referencia a los tratamientos con fines investigación científica sanitaria, que se encuentran previstos en el art. 9.2.j) RGPD y que después sí se encuentran mencionados en la Disposición adicional decimoséptima LOPDGDD que también se realizan sobre la base del Derecho de los Estados miembros.

[58] El art. 9.2 LOPDGDD *in fine* hace una mención específica a los tratamientos de datos de salud en la gestión de los sistemas y servicios de asistencia sanitaria y social *público y privada* o al contrato *de seguro*, por lo que incluye en el mismo precepto una referencia a la actividad aseguradora, que es un tratamiento por razones de interés público del art. 9.2.g) RGPD, y la gestión de la asistencia sanitaria y social, que se encuadraría en el art. 9.2.h) RGPD.

[59] Esta referencia dentro del apdo. V de la Exposición de Motivos se incluyó en la tramitación parlamentaria.

adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes". Así, la Disposición adicional decimoséptima de la LOPDGDD, incorporada también como enmienda en la tramitación parlamentaria, incluye supuestos de licitud del tratamiento de los datos de salud y de los datos genéticos que están ya regulados en la legislación sanitaria y aseguradora y que, por tanto, se encuentran amparados en los apartados g), h), i) y j) del art. 9.2 RGPD[60], lo que aporta una mayor seguridad jurídica en un ámbito como el de los tratamientos de categorías especiales de datos personales, donde existe una presunción de ilegitimidad salvo unos supuestos tasados, entre los que no se incluye la satisfacción de un interés legítimo perseguido por el responsable del tratamiento.

Así, la remisión que hace el RGPD al Derecho de los Estados miembros para regular los tratamientos de categorías especiales de datos personales "por razones de un interés público esencial", "que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" –art. 9.2.g)– hay que entenderla en nuestro país referida a la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras –Disposición adicional decimoséptima 1.h) LOPDGDD–. Este reconocimiento expreso que ha hecho el legislador de que los tratamientos de datos de salud y de datos genéticos regulados por la Ley 20/2015, de 14 de julio, se encuentran amparados en el art. 9.2.g) RGPD ha sido importante para el sector asegurador que siempre ha defendido que estos tratamientos son necesarios por razones de un interés público esencial y tienen cabida como supuesto de legitimación del tratamiento de las categorías especiales de datos personales.

De igual forma, la remisión que hace el art. 9.2.h) RGPD al Derecho de los Estados miembros para regular los tratamientos de categorías especiales de datos personales "para fines de medicina preventiva o laboral" y de "evaluación de la capacidad laboral del trabajador" debe entenderse referida en nuestro país a la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales; la relativa a los fines de "diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social" debe entenderse realizada a la Ley 14/1986, de 25 de abril, General de Sanidad, a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, a la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud y al texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre" –Disposición adicional decimoséptima 1.a), b), c), d), y j) LOPDGDD–. Asimismo, la remisión que hace el art. 9.3 RGPD al Derecho de los Estados miembros para determinar qué profesionales o personas están sujetos a secreto profesional hay que entenderla realizada a la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias –Disposición adicional decimoséptima.1.e) LOPDGDD–. Igualmente la remisión que hace el art. 9.2.i) RGPD al Derecho de los Estados miembros para regular los tratamientos de categorías especiales de datos personales "por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios",

[60] La Disposición adicional decimoséptima LOPDGDD, a diferencia de la previsión contenida en el art. 9.2 RGDUE –y anteriormente en los arts. 8.2 de la Directiva 95/46/CE y 7.6 LOPD–, no permite el tratamiento de todas las categorías especiales para los fines descritos en los letras g), h), i) y j) del artículo 9.2 RGPD sino sólo los tratamientos de datos de salud y genéticos.

estableciendo las medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en especial el secreto profesional hay que entenderlas referidas en nuestro país a la Ley 33/2011, de 4 de octubre, General de Salud Pública y al texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio –Disposición adicional decimoséptima 1.g) e i) LOPDGDD–. Por último, la remisión que hace el art. 9.2.j) RGPD al Derecho de los Estados miembros para regular los tratamientos de categorías especiales de datos personales "con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos", que "debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado", debe entenderse realizada en nuestro país a la Ley 14/2007, de 3 de julio, de Investigación biomédica –Disposición adicional decimoséptima 1.f) LOPDGDD–.

Esta legislación conforma por expresa mención del legislador el marco normativo sobre protección de datos en relación con los tratamientos de datos de salud. La Exposición de Motivos de la LOPDGDD señala claramente que "el Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes" –apdo. V–. Además, esta remisión que hace la Disposición Adicional decimoséptima de la LOPDGDD a un conjunto de leyes no debe ser entendido como *numerus clausus:* por una parte porque hay leyes ya aprobadas que contienen habilitaciones legales para el tratamiento de datos de salud como la legislación de tráfico y seguridad vial o la Ley de protección de la salud del deportista; por otra parte, porque habrá otras posibles leyes que se aprueben en el futuro; y, por último, porque la Disposición adicional decimoséptima LOPDGDD no contiene una referencia a las Leyes autonómicas sobre esta materia que también conforman el marco normativo en el ordenamiento jurídico autonómico.

La Exposición de Motivos de la LOPDGDD señala también que el Reglamento general de protección de datos permite llevar a cabo una "interpretación extensiva" de las habilitaciones legales, "en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, la disposición final décima introduce una serie de artículos en la Ley 14/1986, de 25 de abril, General de Sanidad, encaminados a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos" –apdo. V–.

Pues bien, la LOPDGDD ha aprovechado el margen de maniobra que ofrecía el RGPD para regular en la Disposición adicional decimoséptima los "Tratamientos de datos de salud", haciendo una interpretación extensiva de las habilitaciones previstas en el RGPD para la investigación sanitaria. Inicialmente se podía afirmar que la aprobación del RGPD facilitaba la investigación sanitaria, especialmente en nuestro país que tenía un marco jurídico muy restrictivo en este ámbito, sin perjuicio de que el Reglamento pudiera haber sido más preciso. Sin embargo, aprobado el RGPD se había discutido en algunos foros si esta cuestión había quedado suficientemente clara en el RGPD y si suponía realmente un cambio en el régimen jurídico vigente de la investigación sanitaria en nuestro país. Pues bien, el proyecto de Ley Orgánica aprobado por el Consejo de Ministro no se refería a esta cuestión. Fueron las enmiendas al PLOPD de los Grupos Parlamentarios, que fueron sensibles al planteamiento de los grupos de investigación y de la industria, los que permitieron incorporar al Proyecto de Ley Orgánica una nueva Disposición adicional decimoséptima, que lleva por título "Tratamientos de datos de salud" y que aporta una mayor seguridad

jurídica en este ámbito, desarrollando lo previsto en el art. 9.2.a) g), h), i) y j) RGPD, que regula los tratamientos de categorías especiales de datos personales con consentimiento explícito y sin consentimiento explícito por razones de interés público, atención sanitaria, salud pública e investigación sanitaria y en el art. 89 RGPD, que regula las garantías de los tratamientos con fines de investigación científica que pueden desarrollarse sin consentimiento del interesado, que deben tener en cuenta en especial el principio de minimización de los datos personales, en especial, la seudonimización.

Pues bien, la Disposición adicional decimoséptima LOPDGDD en su apartado segundo regula de manera específica los supuestos de legitimación del tratamiento de los datos de salud y genéticos para fines de investigación en salud, completando y desarrollando lo previsto en el RGPD, añadiendo las garantías de los derechos de protección de datos personales aplicables a los tratamientos con estas finalidades que exigen implementar determinadas medidas técnicas y organizativas y estableciendo excepciones a los derechos de protección de datos. Así, si el art. 9.2.a) RGPD establece que el primer supuesto de licitud del tratamiento de categorías especiales de datos personales es el consentimiento explícito del interesado para uno o más de los fines especificados, la Disposición adicional decimoséptima.2.a) LOPDGDD no se limita a reiterar que "el interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica", sino que añade que "tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora". De esta forma, la LOPDGDD completa lo previsto en el RGPD, interpretando el consentimiento explícito para uno o más fines especificados, en el caso de la investigación en salud y biomédica, como un consentimiento no para una concreta investigación sino para áreas generales vinculadas a especialidades médicas e investigadoras. Esta interpretación del consentimiento para la investigación en salud comprensivo de áreas generales vinculadas a especialidades médicas e investigadoras no se aplica *ex nunc* –desde ahora– sino *ex tunc,* –desde entonces, desde el momento en que se prestó ese consentimiento–. En esta dirección, la Disposición adicional decimoséptima en su apartado 2.c) LOPDGDD establece que "se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial". Esta previsión facilita que un consentimiento explícito previo prestado para una investigación concreta pueda, *a posteriori,* permitir la licitud de tratamientos con fines de investigación en salud relacionados con el área en la que se integró el estudio inicial para el cual se prestó el consentimiento. Estas finalidades posteriores se consideran compatibles con la finalidad de la investigación inicial[61]. Para poder aplicar esta previsión de reutilización con fines de investigación en salud y biomédica a los datos personales recogidos lícitamente con anterioridad a la entrada en vigor de la LOPDGDD, la Disposición transitoria sexta establece que se considera lícita y compatible cuando los datos personales "se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento" o cuando, "habiéndose obtenido el consentimiento para una fi-

[61] Esta interpretación amplia de las finalidades compatibles en el ámbito de la investigación biomédica es también consecuencia de la excepción del principio de "limitación del plazo de conservación", que permite que los datos personales se conserven durante periodos más largos del tiempo necesario para los fines del tratamiento inicial siempre que se traten con fines de investigación científica –art. 5.1.e) RGPD–. De esta forma, la conservación de los datos personales obtenidos con el consentimiento para una finalidad concreta de investigación permite su reutilización para finalidades o áreas de investigación relacionadas con el área en la que se integraba científicamente el estudio inicial.

nalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial". En todo caso, la Disposición adicional decimosétima 2.c) LOPDGDD completa la regulación prevista en el RGPD, estableciendo dos garantías adicionales para los tratamientos de datos de salud o de datos genéticos, cuando el consentimiento inicial para una finalidad concreta se utilice para finalidades o áreas de investigación relacionadas con el área en la que se integra científicamente el estudio inicial. La primera garantía adicional es relativa a la información al interesado, que completa lo previsto en el art. 13 RGPD que ya regula la información que debe facilitarse al interesado cuando los datos personales se obtengan de éste pero el responsable proyecte un tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron. Pues bien, el apartado 2.c), segundo párrafo de la Disposición adicional decimoséptima señala que "en tales casos, los responsables deberán publicar la información establecida por el artículo 13 del RGPD, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato". La segunda garantía, también prevista en la Ley de Investigación Biomédica, es que este tratamiento de datos de salud o datos genéticos *a posteriori* para finalidades o áreas de investigación relacionadas con el área en la que se integraba científicamente el estudio inicial requerirá informe previo favorable del comité de ética de la investigación.

Igualmente, la Disposición adicional decimoséptima.2.b) LOPDGDD también desarrolla las habilitaciones previstas en el art. 9.2.i) y j) del RGPD relación con los tratamientos de datos de salud y de datos genéticos por razones de interés público en el ámbito de la salud pública y con fines de investigación científica al establecer que "las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública".

Mención especial merece la Disposición adicional decimoséptima 2.d) LOPDGDD, que desarrolla las previsiones contenidas en el art. 9.2.j) RGPD y en el art. 89 RGPD, añadiendo algunas garantías adicionales e implementando medidas en relación con los tratamientos de datos de salud y de datos genéticos para la investigación en salud y biomédica sin consentimiento del interesado. Si el art. 9.2.j) RGPD establece que estos tratamientos deben realizarse también sobre la base del Derecho de los Estados miembros, que "debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" y el art. 89 RGPD prevé como garantía el principio de minimización y la seudonimización, la Disposición adicional decimoséptima 2.d) LOPDGDD considera lícito el tratamiento de datos de salud y datos genéticos seudonimizados sin consentimiento del interesado con fines de investigación en salud y en particular biomédica. Por tanto, se establece la seudonimización como principal garantía para los tratamientos de datos de salud y genéticos sin consentimiento del interesado con fines de investigación. Además, la LOPDGDD establece otras medidas y garantías adicionales que son específicas para los tratamientos de datos seudonimizados con fines de investigación. La primera es una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. De esta forma, la LOPDGDD no establece únicamente como garantía que los datos estén seudonimizados sino que quien realice la seudonimización y conserve la información adicional que permite la reidentificación no sea el propio equipo investigador. La segunda garantía adicional es

que los miembros del equipo de investigación sólo puedan acceder a los datos seudonimizados si existe "un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación" y si se adoptan "medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados"[62]. La tercera garantía adicional, presente en este caso en la Disposición adicional decimoséptima 2.g) LOPDGDD, es que el uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica sea sometido al informe previo del comité de ética de la investigación o, en su defecto, del delegado de protección de datos o de un experto en esta materia.

La Disposición adicional decimoséptima apartado 2.f) de la LOPDGDD completa lo previsto en el art. 89.1 RGPD, añadiendo otras garantías adicionales para la investigación en salud pública y biomédica como realizar una evaluación de impacto que incluya –esta es la novedad– "de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos" y someter la investigación científica "a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica".

Finalmente la Disposición adicional decimoséptima.2.e) LOPDGDD completa el RGPD al regular las excepciones a los derechos de acceso, rectificación, limitación del tratamiento y oposición contempladas en el art. 89.2 RGPD cuando se traten datos personales con fines de investigación en salud y biomédica. Así podrán excepcionarse esos derechos cuando "se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados" o cuando "se refiera a los resultados de la investigación"[63].

En relación con la seguridad de los tratamientos ya hemos señalado antes que el RGPD no concede a los Estados miembros un margen de maniobra para aprobar las medidas técnicas y organizativas para la seguridad de todos los tratamientos de datos personales, como sí ocurría en el ordenamiento jurídico español sino que esto es una decisión que le corresponde ahora al responsable del tratamiento que debe aplicar en cada caso las medidas técnicas y organizativas apropiadas a partir de una evaluación de riesgos. No obstante, el RGPD sí permite la introducción de requisitos adicionales relativos a la seguridad y a la confidencialidad en lo relativo a la licitud de algunos tratamientos, en situaciones específicas de tratamiento recogidas en el Capítulo IX y en relación con las categorías especiales de datos personales. Por ese motivo, la Exposición de Motivos de la LOPDGDD señala que "se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras". Esto se aplica en los tratamientos derivados del ejercicio de potestades públicas y de misiones realizadas en interés público, en los tratamientos que son necesarios para el cumplimiento de una obligación legal, en las situaciones específicas de tratamiento descritas en el Capítulo IX del RGPD y en los tratamientos de categorías especiales de datos personales. Por ese motivo, el art. 8.1 LOPDGDD, antes citado, dedicado a los "Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos", establece que la Ley "podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras

[62] La Disposición Adicional decimoséptima 2.d).2º.II LOPDGDD autoriza únicamente a la reidentificación de los datos en su origen "cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria", al prevalecer el derecho a la vida sobre el derecho a la protección de datos personales en caso de conflicto.

[63] También podrá excepcionarse el ejercicio de los derechos cuando "la investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley".

establecidas en el capítulo IV del Reglamento (UE) 2016/679".

La LOPDGDD contiene determinadas exigencias en materia de seguridad de los tratamientos de datos personales que realizan los poderes públicos, que se encuentran recogidas en la Disposición adicional primera, titulada "Medidas de seguridad en el ámbito del sector público". Esta establece expresamente en su apartado primero que "el Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales, para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679". Por tanto, a partir del inicio de la aplicación del RGPD, el Esquema Nacional de Seguridad sigue siendo aplicable a las Administraciones públicas si bien su contenido deberá adecuarse al Reglamento. Además, su apartado 2, incorporado a través de una enmienda parlamentaria, señala que determinadas categorías de responsables o encargados del tratamiento "deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad". Estas categorías de responsables o encargados son las recogidas en el art. 77.1 LOPDGDD: los órganos constitucionales o con relevancia constitucional y las instituciones de las Comunidades Autónomas análogas a los mismos, los órganos jurisdiccionales, la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local, los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, las autoridades administrativas independientes, el Banco de España, las Corporaciones de Derecho Público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, las fundaciones del sector público, las Universidades Públicas, los consorcios y los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales[64].

La LOPDGDD no sólo obligar aplicar el Esquema Nacional de Seguridad a los órganos constitucionales y estatutarios, al Poder Judicial, al Poder Ejecutivo –a la Administración General e Institucional de los diferentes niveles territoriales, a la Administración Corporativa, a las Administraciones Independientes– y al Poder Legislativo, sino que pretende que este Esquema Nacional de Seguridad sea también aplicable a las empresas y fundaciones vinculadas a las Administraciones Públicas sujetas al Derecho privado, e incluso a empresas privadas que presten servicio para las Administraciones Públicas. Así, a partir de la redacción del precepto introducida en virtud de enmienda parlamentaria, la LOPDGDD anima a estas categorías de responsables o encargados a "impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado. En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad" –Disposición adicional primera. 2–.

Como hemos señalado antes, el RGPD no permite a los Estados miembros desarrollar reglamentariamente el principio de seguridad, aprobando medidas de seguridad técnicas y organizativas por lo que las medidas de seguridad reguladas en el Real Decreto 1720/2007 de 21 de diciembre, han sido desplazadas y como obligación jurídica para el responsable resultaban inaplicables desde el inicio de aplicación del RGPD[65], si bien sí es

[64] Cfr. los arts. 17.3, 27 y Disposición adicional segunda de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que obliga a las Administraciones Públicas a cumplir las medidas de seguridad previstas en el Esquema Nacional de Seguridad.

[65] En todo caso estas medidas de seguridad previstas reglamentariamente podrán ser indicativas, incluso a nuestro

posible que las autoridades de control emitan directrices, recomendaciones y buenas prácticas en materia de seguridad. La LOPDGDD quiere facilitar que los responsables de tratamiento, especialmente aquellos que puedan disponer de menos medios, puedan tener unas orientaciones y guías sobre el cumplimiento de las Disposiciones aplicables a tratamientos concretos –Título IV–, también en lo relativo a la seguridad de los tratamientos. Por ello, la Disposición adicional decimoctava de la LOPDGDD, denominada "Criterios de seguridad" establece que "la Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del RGPD"[66] y el Título V de esta ley orgánica", dedicado a las obligaciones del responsable y del encargado del tratamiento. Lógicamente, esto debe hacerse en coordinación con el Comité Europeo de Protección de Datos a través de los mecanismos de cooperación y coherencia establecidos en el RGPD.

Por último, como hemos señalado antes, la LOPDGDD, a diferencia del RGPD, incluye en el Título X la "Garantía de los derechos digitales". La Exposición de Motivos de la LOPDGDD señala que "en particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital […]". Pues bien, en este contexto de inflación de los derechos digitales y en línea con el tenor general de una Ley que se denomina de "Garantía de los derechos digitales", la LOPDGDD reconoce el "derecho a la seguridad digital" –art. 82–, que, como ya hemos señalado antes cae fuera del ámbito de aplicación material del RGPD –art. 2.1 RGPD y art. 2.1 LOPDGDD–. Así, se establece que "los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos"[67]. Llama la atención que el principio de seguridad de los tratamientos recogido en el art. 9 LOPD y en el RGPD se convierta en un derecho a la seguridad únicamente en relación con las comunicaciones que los usuarios transmitan y reciban a través de Internet y no sea un derecho a la seguridad en los tratamientos de datos personales en general[68]. La LOPDGDD también establece que "los proveedores de servicios de Internet informarán a los usuarios

juicio en un futuro próximo la mera aplicación de estas medidas acredita que el responsable del tratamiento garantiza un nivel de seguridad adecuado al riesgo –si estas medidas eran adecuadas hasta ahora, lo normal es que lo sigan siendo–. De hecho, lo razonable es que estas medidas de seguridad se incorporen a los códigos de conducta que se aprueben en virtud del art. 40 RGPD. Cfr. A. TRONCOSO REIGADA, "Autoridades de control independientes", *cit.* pp. 468-469.

[66] Se trata de un error ya que se refiere al Capítulo IV del RGPDUE, que está dedicado a las obligaciones de responsable y del encargado del tratamiento, entre las que se encuentra la seguridad del tratamiento.

[67] Otros textos legislativos ya habían puesto de manifiesto que la seguridad de la información personal no sólo es un principio de protección de datos que debe respetar el responsable del tratamiento sino que tambien que es un derecho de las personas. La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, también reconoce entre los derechos de las personas en sus relaciones con las Administraciones Públicas "la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas" –art. 13.h)–. La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, ya derogada, reconoció como un derecho de los ciudadanos "la garantía de la seguridad y la confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas" –art. 6.2.i)–. Igualmente, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica señala que el paciente "tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad" –art. 19–.

[68] Hay que recordar que también la Directiva 95/46/CE hizo especial hincapié en la seguridad en la transmisión de datos dentro de una red –art. 17.1–.

de sus derechos", sin precisar bien si informarán de todos sus derechos de protección de datos personales o de su derecho a la seguridad digital –art. 82–. Finalmente se reconoce el derecho a la educación digital en virtud del cual "los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y *seguridad de los medios digitales* y en la garantía de los derechos fundamentales en Internet" –art. 83.3–[69].

[69] Sin embargo, sí parece un poco desmedida la Disposición final octava de la LOPDGDD, que modifica el art. 46.2 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades para añadir un nuevo apartado l). Este artículo regula los derechos y deberes de los estudiantes así como la igualdad de oportunidades y no discriminación en el acceso a la universidad, el asesoramiento y asistencia por parte de profesores, la representación de los alumnos en los órganos de gobierno, la libertad de expresión, de reunión y de asociación en el ámbito universitario, la garantía de sus derechos a través de la actuación del defensor universitario, a lo que ahora se añade la "formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet".

RESUMEN El Reglamento General de Protección de Datos Personales de la Unión Europea (RGPD), que junto con la Directiva 2016/680, conforma el nuevo marco europeo de protección de datos personales, afecta intensamente al ámbito del trabajo. El desarrollo y la generalización de las TIC en el ámbito laboral –video vigilancia, geolocalización, biometría, etc.– para el desarrollo y control del cumplimiento de la relación laboral ha supuesto un incremento exponencial de los tratamientos de datos personales de los trabajadores, lo que ha dado lugar a la aparición masiva de nuevos riesgos que suponen una injerencia clara sobre el derecho fundamental a la protección de datos personales de los trabajadores, considerado como derecho autónomo, así como sobre otros derechos fundamentales de los trabajadores de los que la protección de datos personales es una garantía institucional o de instituto

Este RGPD pretende adaptar la normativa europea a los avances producidos en las tecnologías de la información y la comunicación desde la Directiva 95/46/CE. Además, garantiza el control de las personas sobre sus datos personales sometidos a tratamiento, mejorando la regulación de los principios relativos al tratamiento de datos personales, fortaleciendo los derechos del interesado –desarrollando el contenido de las facultades tradicionales y añadiendo nuevos derechos–, ofreciendo una nueva configuración de las obligaciones de los responsables y de los encargados del tratamiento y fortaleciendo a las autoridades de control. Al mismo tiempo, el RGPD garantiza un nivel equivalente de protección de los datos personales en la Unión Europea al desarrollar los principios y los derechos de protección de datos en un norma obligatoria en todos sus elementos y directamente aplicable. Igualmente, el RGPD quiere contribuir a la creación de un mercado digital europeo que favorezca el crecimiento de la actividad económica y mejore la competitividad de las empresas europeas, lo que requiere la adopción de decisiones encaminadas a facilitar la libre circulación de datos personales en la Unión Europea. El RGPD pretende también hacer más sencillo a los responsables y encargados de tratamiento el cumplimiento de la normativa de protección de datos, incrementando al mismo tiempo su responsabilidad –la *accountability*– y, en general, el respeto a este derecho fundamental. Esto supone la supresión o la flexibilización de algunas exigencias formales, la fijación de obligaciones específicas a determinadas categorías de responsables y encargados de tratamiento y la apuesta decidida por la autorregulación.

Si el RGPD es una norma obligatoria en todos sus elementos y directamente aplicable, que no requiere una norma nacional de transposición, es necesario preguntarse qué sentido tiene la aprobación en nuestro país de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales –LOPDGDD–. Le corresponde a la LOPDGDD la adaptación del ordenamiento jurídico español al RGPD, lo que tiene que ser interpretado como una depuración del ordenamiento jurídico interno –la derogación de los preceptos de la LOPD incompatibles con el RGPD– por razones de seguridad jurídica. Además, la LOPDGDD tiene como finalidad completar las disposiciones del RGPD. El RGPD, a pesar de tener un alto nivel de detalle y de especificación, deja un margen de maniobra a los Estados para interpretar, especificar y, en ocasiones, restringir sus previsiones normativas cuando el tratamiento de datos personales afecta a derechos constitucionales como la libertad de expresión y de información, los derechos de los trabajadores, el derecho de acceso del público a documentos oficiales o los derechos de los menores. También el RGPD autoriza a los Estados miembros para hacer previsiones normativas, fijando de manera más precisa requisitos y otras medidas adicionales que garanticen un tratamiento lícito y equitativo, en determinados ámbitos específicos como los tratamientos con fines de archivo público o de investigación científica o histórica o estadísticos. Además, el RGPD prevé la colaboración de las leyes de los Estados al regular

la licitud de los tratamientos de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos o para el tratamiento de categorías especiales de datos personales. La LOPDGDD aprovecha las habilitaciones normativas que el RGPD concede a los Estados miembros. La LOPDGDD, siguiendo al RGPD que atribuye una importante función a la base jurídica del tratamiento, refuerza el principio de legalidad administrativa en este ámbito y el sometimiento pleno de la Administración Pública a la Ley y al Derecho. Especialmente la LOPDGDD ha aprovechado el margen de maniobra que ofrecía el RGPD para llevar a cabo una interpretación extensiva de las habilitaciones previstas en el RGPD para la investigación en salud y biomédica, completando y desarrollando lo previsto en el RGPD y añadiendo garantías de los derechos de protección de datos personales aplicables a los tratamientos con estas finalidades sin consentimiento explícito del interesado. Por último, la LOPDGDD tiene por objeto "garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el art. 18.4 de la Constitución", lo que supone el reconocimiento de derechos digitales en la mayoría de los casos fuera del ámbito de aplicación material del RGPD.

Hay que reconocer la dificultad que supone la coexistencia de una voluntad de establecer en la Unión Europea un nivel uniforme y elevado en la protección de datos personales y el reconocimiento al mismo tiempo de un margen de maniobra a los Estados en distintos ámbitos. En cambio, uno de los ámbitos donde el RGPD supone una mayor alteración del marco jurídico en protección de datos personales existente hasta ahora y, más en concreto, del margen de maniobra de los Estados, en este caso, reduciéndolo o suprimiéndolo, es el de la seguridad de los datos. El RGPD contiene muy pocas obligaciones concretas al responsable y al encargado en relación con la seguridad del tratamiento. Esto significa que las medidas técnicas y organizativas que se van a implementar en cada tratamiento no van a provenir inicialmente de la norma sino que van a ser consecuencia de ese análisis de riesgos que lleve a cabo el responsable y el encargado del tratamiento. La regulación que hace el RGPD de la seguridad del tratamiento se aparta radicalmente del modelo de normativa de protección de datos personales que era de aplicación hasta ahora en nuestro país donde la seguridad de los tratamientos se vinculaba al cumplimiento de unas medidas técnicas y organizativas concretas aprobadas en la normativa y que respondía a un modelo jurídico continental y evidencia la apuesta del RGPD por la desregulación y por la autorregulación y la aproximación a un modelo de protección de datos anglosajón.

Por consiguiente, el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el RGPD y a la LOPDGDD. El marco normativo en nuestro país sobre protección de datos personales está formado tanto por el RGPD como por la LOPDGDD, así como las Leyes autonómicas sobre esta materia que también conforman el marco normativo en el ordenamiento jurídico autonómico.

Palabras clave: Reglamento General de Protección de Datos; Ley Orgánica de Protección de Datos; licitud de los tratamientos; seguridad de los tratamientos; investigación biomédica.

ABSTRACT The General Regulation on the Protection of Personal Data of the European Union (RGPD), which together with Directive 2016/680, forms the new European framework for the protection of personal data, intensely affects the area of labour relations. The development and generalisation of ICTs in the field of employment –video surveillance, geolocalisation, biometrics, etc.– for the development and control of compliance with the employment relationship has meant an exponential increase in the processing of workers' personal data, which has led to the massive appearance of new risks that represent a clear interference in the fundamental right to the protection of workers' personal data, considered as an autonomous right, as well as in other fundamental rights of workers for which the protection of personal data is an institutional or institutional guarantee.

This RGPD aims to adapt the European regulations to the advances produced in the information and communication technologies since the Directive 95/46/CE. Furthermore, it guarantees the control of persons over their personal data submitted to processing, improving the regulation of the principles relating to the processing of personal data, strengthening the rights of the data subject – developing the content of the traditional powers and adding new rights –, offering a new configuration of the obligations of those responsible for and in charge of the processing and strengthening the control authorities. At the same time, the RGPD ensures an equivalent level of protection of personal data in the European Union by developing data protection principles and rights into a standard which is binding in its entirety and directly applicable. Likewise, the RGPD wants to contribute to the creation of a European digital market that favours the growth of economic activity and improves the competitiveness of European companies, which requires the adoption of decisions aimed at facilitating the free circulation of personal data in the European Union. The RGPD also intends to make it easier for data controllers and processors to comply with data protection regulations, while increasing their responsibility – accountability – and, in general, respect for this fundamental right. This implies the suppression or the relaxation of certain formal requirements, the establishment of specific obligations for certain categories of data controllers and processors and the decisive support for self-regulation.

If the RGPD is an obligatory norm in all its elements and directly applicable, which does not require a national transposition norm, it is necessary to ask what is the sense of the approval in our country of the Organic Law 3/2018, of December 5, of Protection of Personal Data and guarantee of the digital rights –LOPDGDD–. The LOPDGDD is responsible for adapting the Spanish legal system to the RGPD, which must be interpreted as a purge of the internal legal system – the derogation of the precepts of the LOPD that are incompatible with the RGPD – for reasons of legal certainty. Furthermore, the LOPDGDD is intended to supplement the provisions of the RGPD. The RGPD, in spite of having a high level of detail and specification, leaves a margin of maneuver to the States to interpret, specify and, sometimes, restrict its normative previsions when the processing of personal data affects constitutional rights such as the freedom of expression and information, the rights of workers, the right of public access to official documents or the rights of minors. The RGPD also authorises Member States to make regulatory provisions, laying down more precise requirements and other additional measures to ensure lawful and fair processing, in certain specific areas such as processing for the purposes of public archiving or scientific or historical research or statistics. Furthermore, the RGPD provides for the cooperation of Member States' laws in regulating the lawfulness of processing of personal data for the fulfilment of a legal obligation, for the performance of a task carried out in the public interest or in the exercise of public authority, or for the processing of special categories of personal data. The LOPDGDD takes advantage of the regulatory powers conferred on Member States by the RGPD. The LOPDGDD, following the RGPD which attributes an important function to the legal basis of the processing, reinforces the principle of administrative legality in this field and the full submission of

the public administration to the law. In particular, the LOPDGDD has taken advantage of the margin of manoeuvre offered by the RGPD to carry out an extensive interpretation of the authorisations provided for in the RGPD for health and biomedical research, completing and developing what is provided for in the RGPD and adding guarantees of the rights of personal data protection applicable to processing for these purposes without the explicit consent of the data subject. Finally, the LOPDGDD aims to "guarantee the digital rights of citizens in accordance with the mandate established in article 18.4 of the Constitution", which implies the recognition of digital rights in most cases outside the material scope of the RGPD.

We must recognise the difficulty of the coexistence of a desire to establish a uniform and high level of protection of personal data in the European Union and at the same time recognise the scope for manoeuvre of the States in different areas. On the other hand, one of the areas in which the RGPD means a greater alteration of the legal framework in the protection of personal data that has existed until now and, more specifically, of the scope for manoeuvre of the States, in this case, reducing it or removing it, is that of data security. The RGPD contains very few specific obligations for the data controller and processor with regard to security of processing. This means that the technical and organisational measures to be implemented for each processing operation will not initially derive from the regulation but will be the consequence of that risk analysis carried out by the controller and processor. The regulation that the RGPD makes of the security of the processing differs radically from the model of regulation of protection of personal data that was applicable until now in our country where the security of the processing was related to the fulfillment of some specific technical and organizational measures approved in the regulation and that responded to a continental legal model and it evidences the support of the RGPD for the deregulation and for the self-regulation and the approach to an Anglo-Saxon model of data protection.

Consequently, the fundamental right of natural persons to the protection of personal data, protected by Article 18.4 of the Constitution, will be implemented in accordance with the provisions of the RGPD and the LOPDGDD. The regulatory framework in our country on the protection of personal data is formed by both the RGPD and the LOPDGDD, as well as by the Autonomous Laws on this matter which also form the regulatory framework in the autonomous legal system.

Keywords: General Data Protection Regulations; Organic Law on Data Protection; lawfulness of processing; security of processing; biomedical research.

El derecho a la protección de datos personales: configuración y relación con otros derechos de la persona*

Right to personal data protection: configuration and relationship with other fundamental rights

JUAN JOSÉ FERNÁNDEZ DOMÍNGUEZ**

1. INTRODUCCIÓN

Pocos podían esperar que, cuando allá por la década de los 70 del siglo pasado comenzaron a surgir leyes destinadas a proteger la intimidad o privacidad de las personas frente al peligro derivado de la falta de control sobre el uso y destino de sus datos, se estuviera asistiendo al proceso de cimentación de un derecho fundamental que, pese a ese origen relativamente reciente, ha cobrado una importancia y dimensiones inusitadas. Lo ha hecho alentado, sobre todo, por la explosión tecnológica y la intensificación de las relaciones económicas, sociales, institucionales y culturales a una escala global, capaz de modificar de manera sustancial las pautas de comportamiento y relaciones humanas.

Apenas medio siglo después cabrá constatar cómo aquel brote surgido de normas estatales adquiere la dimensión supranacional exigida para su eficacia y, bifurcándose en dos grandes alternativas a nivel mundial, cobra una nueva dimensión como derecho autónomo en el continente europeo.

Analizar su configuración actual y la relación que mantiene con el resto de los derechos fundamentales supone, por ende, asumir de partida una doble limitación: en primer lugar, que el análisis se asienta sobre la base del modelo europeo, donde la protección de datos ha alcanzado ese espacio de autonomía del que carece en otros sistemas; en segundo término, que únicamente cabrá ofrecer el resultado de la decantación histórica hasta cuanto ofrece la imagen fija de su realidad actual, conscientes de que la evolución dista de haber culminado.

Desde el primero de los planos, importará fijar la atención en que la protección de datos no surgió como un derecho diferenciado, y en el ámbito anglosajón –y, por "contaminación cultural", en muchos otros rincones del mundo[1]– la opción sigue quedando situada en un marco estrictamente relacionado con la priva-

* Este ensayo ha sido realizado en el marco del Proyecto de Investigación del Ministerio de Economía, Industria y Competitividad titulado *Nuevos lugares, distintos tiempos y modos diversos de trabajar. Innovación tecnológica y cambios en el ordenamiento social*, DER2017-821792-C3-1.R.

** Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de León.

[1] Baste la extensa reflexión que, centrada en el África Subsahariana, pero con paralela exposición de la extensión del patrón americano a la Región Asia-Pacífico o la Liga de Estados Árabes, realiza MUKULILO, A.B., *Protection of personal data in Sub-Saharan Africa*, Tesis Doctoral, Bremen Universität, 2012, pp. 216 y ss., en http://elib.suub.uni-bremen.de/edocs/00102854-1.pdf.

cidad[2]. Lejos, por tanto, de ese nuevo derecho que aflora de un marco multinivel donde se mezclan e interactúan normas nacionales y europeas para, a través de una transformación en los elementos que lo hacen reconocible, así como en el sistema de garantías que lo ampara[3], alumbrar un nuevo fundamento que lo desplaza desde el ámbito estatal al supranacional, "y, sobre este último anclaje, lleva a normativizar un derecho fundamental homogéneo en toda la Unión Europea"; es decir, con una patente alteración del sistema de fuentes, "al producirse la abducción de un derecho constitucional convertido en un derecho fundamentalmente europeo"[4].

De atender al segundo de los elementos, que al tiempo constituye también una seña de identidad característica, cabrá compartir la idea de quien lo presenta como "un derecho de cierta complejidad y con perfiles un tanto borrosos, no solo por lo que atañe a su contenido o alcance, que por razones fáciles de comprender se encuentra aún en fase de identificación y construcción, sino también porque está llamado a operar en terrenos de juego abiertos a otros muchos protagonistas"[5].

En la confluencia de ambos factores procederá situar el objeto de la presente reflexión, como tránsito paulatino hacia esa homogeneidad no completa que supone el diseño de un soporte europeo, llamado a convivir e integrar las tradiciones constitucionales con que los Estados han ido forjando progresivamente sus rasgos definitorios. A la par, con la precaución de medir con tiento sus contornos, bajo el riesgo de distorsionar la imagen que de él pueda proyectarse, conforme ocurre cuando metafóricamente viene a ser identificado como "un agujero negro que lo absorbe todo y no deja escapar nada de su entorno"[6]; en parecido sentido, si se considera que su fuerza arrolladora estaría en disposición de ocupar los espacios de la privacidad, imponiendo unos principios de actuación mucho más exigentes y rigurosos de los que hasta este momento habían venido sirviendo para limitar el derecho a la intimidad, a la cual se terminaría "comiendo"[7].

He ahí, por tanto, el reto de la aproximación a un derecho de perfiles inacabados, cuya proyección no puede descartar en un futuro próximo la novedad de aspectos que a día de hoy resultarían sorpresivos, por imposibles de adivinar siquiera[8].

---

[2] Sobre los elementos diferenciales en el origen de uno y otro modelo de protección, los factores y elementos de evolución comunes y, sin embargo, la distancia importante que los separa a día de hoy, DAVIS, S.: "Is there a right to privacy?", *Pacific Philosophical Quarterly*, Vol. 90, núm. 4, 2009, pp. 450-475.

[3] Los datos de tal transformación con el necesario detalle en MARTÍNEZ LÓPEZ-SÁEZ, M.: *Una revisión del derecho fundamental a la protección de datos de carácter personal*, Valencia (Tirant lo Blanch), 2018, Parte II, Capítulos III y IV.

[4] RALLO LOMBARTE, A.: "El nuevo derecho de protección de datos", *Revista Española de Derecho Constitucional*, núm. 116, 2019, pp. 48 y 49.

[5] En este último aspecto se añade que, "si se ha llegado a la convicción de que hay que reconocer de manera clara y terminante un derecho a la protección de datos personales es sencillamente porque en muchos ámbitos de la vida, y por razones de muy diversa índole, es necesario el uso de esa clase de datos. En suma: hay que proteger unos datos que muchas veces son de manejo inexcusable para el desenvolvimiento de las relaciones sociales y jurídicas", GARCÍA MURCIA, J.: "La protección de datos personales en el ámbito laboral: una sucinta reseña jurisprudencial a partir de cinco sentencias del Tribunal Supremo", *Revista Galega de Dereito Social*, 2ª etapa, núm. 5, 2018, p. 10.

[6] Por consiguiente, con un potencial sin fronteras, que si bien ha permanecido larvado durante un largo período de tiempo, la utilización de un concepto amplio de las nociones de datos personales y tratamiento lleva a que cualquier acto de comunicación asentado en medios automáticos, como las telecomunicaciones, el correo electrónico o las redes sociales, si relativo a una persona física, "constituya una referencia putativa tal de este derecho fundamental que requiere justificación", CÓRDOBA CASTROVERDE, D. y DÍEZ-PICAZO GIMÉNEZ, L.M.: "Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico", en AA.VV.: *El derecho a la privacidad en un nuevo entorno tecnológico. XX Jornadas de la Asociación de Letrados del Tribunal Constitucional*, Madrid (Centro de Estudios Políticos y Constitucionales), 2016, pp. 99 y ss.

[7] GARCÍA-PERROTE ESCARTÍN, I. y MERCADER UGUINA, J.R.: "La protección de datos se come a la intimidad: la doctrina de la sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017 (caso Barbulescu v. Rumania; nº 61496/08; Gran Sala)", *Información Laboral*, núm. 10, 2017, BIB 2017/13275.

[8] GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I.D.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216, 2019, p. 22.

2. LA RAÍZ DEL DERECHO: DE LAS PRIMERAS NORMAS Y EL ENTRONQUE CONSTITUCIONAL DE LA PROTECCIÓN DE DATOS

Intentar aquilatar el contenido y función relacional del derecho a la protección de datos exige conocer bien su origen, la fuente de donde surge y a partir de la cual toma un determinado sentido: primero, a nivel nacional; más tarde, como parte del patrimonio jurídico europeo.

2.1. Las leyes nacionales de protección de datos y el entronque constitucional con los derechos de la personalidad y los valores superiores del ordenamiento

En el contexto del proceso de informatización de los Länder alemanes, y dentro de los planes que al efecto se diseñaron, vieron la luz distintas regulaciones administrativas, a modo de reglamentos internos de gestión, que recogían las actividades básicas y sistemas de gobierno y financiación de cuanto derivaba de ese intenso y trascendental proceso de cambio. Preparaban el camino hacia la entrada en una nueva época, la era de la protección de datos, que encuentra en el 7 de octubre de 1970 una fecha de referencia fundamental, por ser la de promulgación de la *Datenschutzgesetz* de Hesse, como primera ley que, además de la evidente aportación de su nombre al derecho a la protección de datos, supone una regulación completa y acabada de cuanto preocupaba al legislador europeo de la época: la creación de bases de datos personales de carácter público percibidas socialmente como instrumentos de control que podían poner en riesgo el honor y la intimidad de las personas.

Acto seguido verán la luz las leyes suecas de 1973, la Ley del Land de Renania-Palatinado de 1974, la Ley federal alemana de 1977, la francesa, noruega, austriaca y las dos danesas de 1978, la de Luxemburgo en 1979, la suiza e islandesa de 1981…; hasta que, ya entrada la década de los 90, y cuando solo Italia y Grecia carecían de ella, se promulga en España la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal[9].

Muchos años de diferencia en el itinerario que conduce, empero, a una misma dirección. Netamente distinta respecto de la que, en paralelo, se iba abriendo camino en Estados Unidos (en cuyo trasfondo cabrá descubrir esa dialéctica que llevó en su momento a contraponer los conceptos de *privacy* y los derechos de la personalidad –*Persönlichkeitsrechte*–[10]), de manera harto ilustrativa resumida en una opción entre dos posiciones que, presentadas en sus extremos, puede resultar más gráfica: "una seguida por la legislación americana que se concreta en el principio de que todo está permitido, salvo lo que está prohibido, y otra cuyo representante principal es Alemania, la cual entiende que cualquier actividad relativa al procesamiento de datos está prohibida, salvo cuando está permitida"[11].

La diferencia cronológica significada se dejará sentir, obviamente, en el contenido y planteamiento de las normas, pero también en el diálogo constitucional con el haz de principios y derechos que recogen, no en vano sus preceptos otorgan cobertura a actividades,

[9] Sobre este proceso de desarrollo legal, con sus vicisitudes y las diferentes tendencias que cabía descubrir en las distintas normas nacionales, PASCUAL HUERTA, P.: *La génesis del derecho fundamental a la protección de datos personales*, Tesis Doctoral, Madrid (Universidad Complutense), 2017, pp. 227-248, en http://eprints.ucm.es/43050/1/T38862.pdf.

[10] Ilustrativos los resúmenes que, en diferentes épocas, ofrecen KRAUSE, H.: "The right to privacy in Gemany: Pointers for American legislation?", *Duke Law Journal*, núm. 3, 1965, pp. 481 y ss. o SIMITIS, S.: "Privacy. An endless debate?", *California Law Review*, Vol. 98, 1989, pp. 1189 y 1190. Excelente la contraposición de modelos en ÁLVAREZ CARO, M.: *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, Madrid (San Pablo CEU/Cátedra Google), 2015, pp. 85-107.

[11] La frase de FROSINI, V.: "Bases de datos y tutela de la persona", *Revista de Estudios Políticos*, nueva época, núm. 30, 1982, p. 30. Su adecuada matización en REBOLLO DELGADO, L. y SERRANO PÉREZ, M.M.: *Manual de Protección de datos*, 2ª ed., Madrid (Dykinson/UNED), 2017, p. 37.

públicas o privadas, que afectarán a derechos, bienes e intereses de indudable alcance constitucional.

Así, su acomodo será muy diverso según el momento de la promulgación[12]. Durante la primera época, en algunos Estados, como Bélgica y Holanda, cuanto garantizaban las normas de protección de datos aparecía vinculado al derecho a la intimidad recogido en sus constituciones, mientras cuantos carecían de tal reconocimiento hubieron de buscar otra ubicación, como ocurrió en Francia (que lo situó en la libertad) o Alemania (donde aparece articulado dentro del reconocimiento de la dignidad humana), asumiendo los Tribunales Constitucionales la labor de tal incardinación[13]. En un segundo momento, y persistiendo idéntica labor cuando no habían variado ni la Constitución ni la ley ordinaria, o no se habría estimado conveniente dotar de mayor precisión a la una o a la otra[14], la tónica pasará por incluir en la Norma Fundamental preceptos que abordan la cuestión de la informática y los peligros que pueden derivar para los derechos fundamentales (así ocurre, por ejemplo, en los casos de Portugal y España o, más próximos en el tiempo, Grecia, Polonia, Hungría o República Checa), y sobre tales preceptos se asentará su protección al máximo nivel[15].

Por una vía o por la otra el resultado final de las singulares trayectorias seguidas en cada ordenamiento europeo será muy semejante, para mostrar un estado de madurez que llama a una base común, ya como producto del grado de evolución alcanzado sobre parámetros semejantes, ya como dato precursor o precedente de la ordenación nueva que se acomete[16].

2.2. La influencia de la construcción norteamericana en los instrumentos normativos internacionales de finales del siglo XX

El camino que llevará a la construcción de un derecho con fundamento supranacional de acento europeo no resultó sencillo, pues la influencia de la concepción norteamericana se proyectó de manera evidente sobre los dos textos que, a comienzos de la década de los 80 del siglo pasado, afrontaron la delicada cuestión de proporcionar respuesta a las transferencias internacionales de datos, conscientes de que cualquier intento de establecer un nivel interno de protección en la materia que no fuera seguido de medida semejantes en los Estados del entorno, bien vería mermada de manera notable su eficacia, bien –o también– perjudicaría de forma evidente los normales intercambios comerciales y culturales entre países.

De este modo, tanto las "Directrices en relación con el flujo internacional de datos personales y la protección de la intimidad y las libertades fundamentales", aprobadas por Recomendación del Consejo [de Ministros] de la OCDE de 23 de septiembre 1980, como el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio núm. 108 del Consejo de Europa), hecho en Estrasburgo el 28 de enero de 1981, se vinculan de manera expresa a la preservación de la privacidad.

Los dos textos surgen en el seno de organizaciones internacionales de cooperación y

[12] De Hert, P. y Gutwirth, S.: "European data protection's constitutional Project", en AA.VV. (Gutwirth, S. *et alii*, Eds.): *Reinventing data protection?*, Dordrech (Springer), 2009, p. 10.

[13] Murillo de la Cueva, P.L.: *El derecho a la autodeterminación informativa*, Madrid (Tecnos), 1990, pp. 125 y ss; sobre la vinculación al concepto de libre desarrollo de la personalidad, Ryszard Kosmider, M.: "El contenido jurídico del concepto de libre desarrollo de la personalidad con referencia especial a los sistemas constitucionales alemán y español", *Revista de Derecho UNED*, núm. 23, 2018, pp. 667 y ss.

[14] Arenas Ramiro, M.: *El derecho fundamental a la protección de datos personales en Europa*, Valencia (Tirant lo Blanch/ Agencia Española de Protección de Datos), 2006, p. 79.

[15] Pascual Huerta, P.: *La génesis del derecho fundamental a la protección de datos personales*, *cit.*, p. 12.

[16] González Fuster, G.: *The emergence of personal data protection as a fundamental right of the EU*, Dordrech (Springer), 2014, en particular pp. 75-107.

presentan un contenido similar (algo que no puede extrañar, a la vista del dato de ser varios los miembros que estuvieron presentes en la elaboración de ambos[17]), aun cuando obra el notable elemento de separación dado por el hecho de que, mientras las Directrices no pasan de ser un conjunto de principios o consejos que (a pesar de su notoria influencia por el hecho de haber servido de inspiración a la regulación de muchos países) solo obligan moralmente[18], el Convenio aparece como el primer instrumento internacional jurídicamente vinculante. Más allá de este dato relevante, preciso será reconocer una diferencia en la arquitectura de ambos referentes que, si bien no es notoria en el plano sustantivo en un primer momento, terminará llevando progresivamente a esa disímil evolución.

En efecto, procederá observar cómo –a semejanza de las Directrices, aun cuando de modo menos explícito– el Convenio acaba vinculando privacidad y protección de datos, al punto de clasificar las normas nacionales en la materia como normas de privacidad, cuya noción, además, presenta como enraizada en el art. 8 del Convenio Europeo de Derechos Humanos de 1950 (CEDH), destinado a garantizar el derecho a la vida privada y familiar[19]. A pesar de ello, preciso será reconocer cómo, en tanto la redacción de las Directrices obedece a un patrón propio del derecho anglosajón (ideas más generales, sin aspiraciones a constituir una codificación cerrada, cuyo sentido en el caso concreto queda confiado al quehacer de los órganos judiciales), el Convenio responde al diseño de Derecho europeo y asienta un modo de regular que sigue vigente en la actualidad, con una ordenación de detalle en la cual, tras las definiciones, dibuja nítidamente los principios y derechos que constituyen su objeto[20].

Consideraciones que pueden ser trasladadas a la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos, pues la inspiración del Convenio núm. 108 sigue determinando en gran medida las previsiones destinadas a proporcionar garantías a los ciudadanos, y ello aun cuando se trate de un objetivo que debió coexistir con el de articular un estándar de protección relativamente elevado para así eliminar los obstáculos a la libre circulación de los datos personales (en este sentido constituiría "la máxima expresión de reconocimiento del derecho por la puerta trasera"[21]), para muchos considerado como fin principal, del cual aquel no pasaría de ser un efecto indirecto[22].

Con todo, no cabrá menospreciar –sino resaltar en la medida adecuada– cuanto de importante aportación diferencial a la Directiva proviene de los ordenamientos nacionales y recoge a lo largo de su desarrollo, pudiendo mencionar, como uno de los ejemplos más destacados, la notable influencia que alcanzó la Sentencia del Tribunal Constitucional alemán sobre la Ley del Censo de 1983[23]. En ella

[17] BURKERT, H.: "Privacy-data protection. A German/European perspective", en AA.VV. (ENGER, Ch. y HELLER, K.H., Eds.): *Governance of global networks in the light of differing local values*, Baden-Baden (Nomos), 2000, pp. 46 y 47.

[18] Una exposición cuidada de su contenido, proyección y actualización en 2013 en PÉREZ MIRAS, J.: *El derecho a la protección de datos y a la privacidad. Una perspectiva comparada entre la Unión Europea y los Estados Unidos*, Tesis Doctoral, Sevilla (Universidad de Sevilla), 2018, pp. 20-26, en https://idus.us.es/xmlui/bitstiezen/handle/11411/83475/TesisJorgePerezMiras.pdf?sequence=1&isAllowed=y.

[19] La argumentación, en detalle, en BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, Madrid (Bosch/Wolters Kluwer), 2019, pp. 55 y 56.

[20] Sobre este elemento de diferenciación como detonante principal que facilita y orienta la evolución seguida del ordenamiento europeo, LLOYD, I.J.: *Information Tecnology Law*, Londres (Butterworths), 1997, p. 49.

[21] RALLO LOMBARTE, A.: "El nuevo derecho de protección de datos", *cit.*, p. 51.

[22] ESTADELLA YUSTE, O.: *La protección de la intimidad frente a la trasmisión internacional de datos personales*, Madrid (Tecnos), 1995, pp. 68 y 69.

[23] Sentencia de la Primera Sala del BVerfGn (65,1) de 15 de diciembre de 1983 ("*Volkszählungsurteil*"). Un comentario en su 25 aniversario, atendiendo a su sentido histórico y la evolución que ha continuado sobre sus cimientos, en HORNUNG, G. y SCHNABEL, Ch.: "Data protection in Germany I: The population census decision and the right to informational 'self-de-

se recrea el derecho a la autodeterminación informativa que doce años antes habían propugnado, dentro un informe para el Ministerio del Interior, un grupo de profesores universitarios[24], y más tarde –hasta la actualidad– alcanzará, en particular a través de la Directiva[25], notable éxito bajo el patrón de un derecho en el cual cabrá descubrir dos caras, o, si se prefiere, una regla y una excepción.

Así, en el plano positivo proclama "la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede a revelar situaciones referentes a la propia vida". Teniendo presente, a tal fin, que "el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad; antes bien, adquieren vital importancia las circunstancias bajo las cuales sea utilizado" el dato. Y ello por cuanto, en definitiva, "la eclosión de la personalidad presupone, en las condiciones modernas de la elaboración de datos, la protección del individuo contra la recogida, el almacenamiento, la utilización y la trasmisión ilimitada de los datos concernientes a su persona"[26].

Por su parte, y como envés o límites a la facultad, se sienta que "el individuo no tiene ningún derecho sobre 'sus' datos, en el sentido de una soberanía absoluta y sin restricciones, sino que es más bien una personalidad que se desenvuelve dentro de una comunidad social y que está llamada a comunicarse. La información, incluso en la medida en que se refiera a la persona como tal, ofrece un retrato de la realidad social que no cabe asignar exclusivamente al interesado (…), y el individuo tiene, por tanto, que aceptar en principio determinadas limitaciones a su derecho a la autodeterminación informática en aras del interés predominante de la colectividad".

Cabe asistir, por tanto, a una continuidad en el plano internacional que es solo aparente, pues en la Directiva ya aparecen apuntes bastantes para el cambio[27], ordenado a seguir afirmando la singularidad de ese gemelo no idéntico que, bajo la referencia a protección de datos, está llamado a convertirse en un derecho con entidad propia[28].

---

termination'", *Computer Law & Security*, Vol. 25, núm. 1, 2009, pp. 84-94. Una valoración en detalle, que al tiempo constituye un planteamiento pionero en España, en HEREDERO HIGUERAS, M.: "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la ley del Censo de la Población de 1983", *Documentación Administrativa*, núm. 198, 1983, pp. 139-158.

[24] De ahí el sentido de la afirmación que deshace malentendidos muy difundidos y pone de manifiesto cómo este pronunciamiento no es el acta de "nacimiento de un nuevo derecho fundamental, y especialmente no lo es de un derecho fundamental a la protección de datos", al igual que tampoco resulta novedosa la expresión "'derecho a la autodeterminación informativa'", DENNINGER, E.: "El derecho a la autodeterminación informativa", en AA.VV. (PÉREZ LUÑO, A.E., Ed.): *Problemas actuales de la documentación y la informática jurídica*, Madrid (Tecnos/Fundación Luño Pena), 1987, p. 271 y nota 29.

[25] ÁLVAREZ CARO, M.: *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, *cit.*, pp. 67-85.

[26] En narración ejemplar se destaca el aspecto del derecho que proclama el Tribunal cuando sienta cómo "la autodeterminación individual presupone (…) que a los individuos se les dé libertad para decidir sobre qué actividades emprender y cuáles omitir, incluyendo la posibilidad de comportarse efectivamente de conformidad con esa decisión. Quien no pueda estimar con suficiente seguridad qué informaciones sobre sí mismo son conocidas en determinadas esferas de su medio social, y quien no pueda de algún modo valorar el conocimiento previo que los posibles interlocutores tienen de uno mismo, puede verse restringido esencialmente en su libertad para planear o decidir con base en su propia autodeterminación. Un ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer quiénes, cuándo y en qué circunstancias saben qué sobre ellos, serían incompatibles con el derecho a la autodeterminación de la información. Quien piense que los comportamientos atípicos pueden en todo momento ser registrados y archivados como información, utilizados o retransmitidos, intentará no llamar la atención incurriendo en ese tipo de comportamientos (…) Esto no sólo iría en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar".

[27] FERNÁNDEZ DOMÍNGUEZ, J.J. y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Madrid (Agencia Española de Protección de Datos), 1997, pp. 136 y 137.

[28] KUNER, C.: "An international legal framework for data protection: Issues and prospects", *Computer Law & Security Review*, Vol. 25, núm. 4, 2009, p. 309.

2.3. Los primeros pasos del derecho en el ordenamiento español

Conforme ha quedado significado, y frente a cuanto fue el íter compartido en los países punteros en Europa, la primera aproximación a la protección de datos no tuvo lugar en España a través de una ley, sino de una mención en la Constitución que recogía el eco de cuanto estaba acaeciendo alrededor, donde no solo se asistía a la proliferación de normas estatales, sino a los trabajos preparatorios de lo que luego tomaría forma en las Directrices de la OCDE y en el Convenio núm. 108 del Consejo de Europa.

En este contexto fértil (que sirvió, por ejemplo, para que la Constitución portuguesa de 1976 consagrará, por primera vez en la historia del constitucionalismo, un precepto destinado a "la utilización de la informática") discurre la elaboración del art. 18.4 CE, a cuyo tenor "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal de los ciudadanos y el pleno ejercicio de sus derechos".

Importará destacar que, tras la sucinta referencia final del art. 18.4 CE a la limitación del uso de la informática, el debate parlamentario sirve para aclarar, tanto que los constituyentes conocían las tendencias europeas en este ámbito, como el sentido más extenso que, ya de partida, se quiso conferir al precepto[29].

Así procederá colegirlo del hecho de conformidad con el cual hasta en tres ocasiones se rechaza de forma expresa que el precepto fuera innecesario o reiterativo[30], y en otras tres que cuanto debería regularse fuera cualquier técnica o procedimiento técnico potencialmente peligroso para los derechos fundamentales[31]. Dejando claro, frente a cualquier restricción o ampliación, que los peligros para los derechos fundamentales que trataba de soslayar habían de provenir de la informática, y solo de ella; completándose con la referencia a "el pleno ejercicio de sus derechos", que cobra un sentido concreto por mor de la justificación incorporada en la enmienda a partir de la cual se añade tal tenor al texto del Proyecto debatido. Esta afirmaba literalmente que "la limitación establecida en el presente artículo al uso de la informática, centrada exclusivamente en el honor y la intimidad personal y familiar, parece ignorar que los posibles perjuicios del uso de la informática pueden producirse, además y de manera fundamental, en el ejercicio de los derechos tanto políticos como cívicos por parte de los ciudadanos".

A la previsión constitucional siguieron años de silencio. Palmaria prueba de que la protección de los datos personales distó de constituir una de las preocupaciones prioritarias para el legislador postconstitucional español, según muestra de manera significativa la ausencia de cualquier mención en la Ley Orgánica 1/1982, de 5 de mayo, de protección

[29] El contenido de estos debates en CORTES GENERALES: *Constitución Española. Trabajos parlamentarios*, T. I, Madrid (Cortes Generales), 1980, pp. 121 y ss. y 1068 y ss.

[30] En concreto las enmiendas en el Congreso núms. 2 (Sr. Lamo Martínez, Alianza Popular) y 716 (Sr. Sancho Rof, UCD), así como la núm. 145 (Sr. Cela y Trulock). En el primer caso, por reiterativo respecto de otros artículos; en el segundo, por considerarlo subsumido en el apartado 1 del art. 18; en el último, "por obvio".

[31] Enmiendas en el Congreso núm. 16 (Sr. Jarabo Páya, Alianza Popular, quien propuso la ampliación del mandato a otros ámbitos, con referencia a "cualesquiera otros procedimientos que pudieran dañar el honor y la intimidad personal y familiar de los ciudadanos") y núm. 716 [Sr. Sancho Rof, UCD, quien exponía cómo "la informática es solo un medio técnico (...) no entiendo por qué hay que hacer una mención expresa a la informática y no otra serie de técnicas o medios que pueden ir contra la intimidad personal y familiar y contra el honor de los ciudadanos], o núm. 261 en el Senado (Sr. Zaragoza Burillo, Grupo Mixto). Esta última presentaba un sentido parcialmente diferente, al advertir sobre la posible obsolescencia rápida cuando afirmaba que "tenemos que situarnos en el futuro (...) vendrán otras muchas técnicas –no solo la informática–, y resulta imprescindible prevenir y prepararnos para ellas adecuadamente y no quedarnos desplazados en la carrera, aun antes de haber salido de la meta (...). El mundo y las personas están cambiando a ritmo inimaginables. Hemos de prepararnos para entender este mundo y proteger los derechos de los ciudadanos en los ambientes individuales, familiar y social (...). Hay que evitar la traición de la tecnología; hay que arbitrar nuevos sistemas de valores".

de la intimidad, el honor y la propia imagen. E igual interpretación cabrá seguir sosteniendo a pesar de la ratificación del Convenio núm. 108 del Consejo de Europa –mediante Instrumento de 27 de enero de 1984–, pues, al no venir acompañada de una normativa interna al respecto, careció de cualquier eficacia real[32].

Ni más ni menos que quince años después (y solo con optimismo cabrá tildar como "elogiable su anticipación" con la vista puesta en la Directiva de 1995[33]) se promulgará la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, cuyo fundamento se asentaba sobre una poco clara distinción entre "intimidad" y "privacidad"[34], y con un contenido –incluido su desarrollo a través del RD 428/1993– valorado con total justicia como "un intento no acabado de equilibrio entre intereses (…) [,como la] libertad de circulación de datos y [la] privacidad del individuo, [pues a pesar del mérito de proceder por primera vez a regular una cuestión tan necesitada de atención], en el otro platillo de la balanza se sitúan numerosas limitaciones y excepciones a la regulación general de los derechos establecidos en la misma que, en algunos casos, impiden hacer efectivos los derechos e incumplen (…) la legislación internacional y constitucional en la materia"[35].

El contexto legal, poco propicio tanto en el momento en el cual se inició el recurso como en aquel en el cual se pronunció la sentencia, hizo que el primer pronunciamiento del Tribunal Constitucional sobre el art. 18.4 CE se moviera bajo una calculada ambigüedad, con las dudas propias de cuanto evoluciona con enorme rapidez en el tiempo[36].

Muchos de los comentarios que ha merecido este pronunciamiento de comienzos de los años 90 se quedan en el sentido final de su fallo y la imbricación última que realiza de la protección de datos con la intimidad, cuando sienta sin ambages que, "al negarse a comunicarle la existencia e identificación de los ficheros automatizados que mantiene con datos de carácter personal, así como los datos que le conciernen a él personalmente, la Administración (…) vulneró el contenido esencial del derecho a la intimidad". Calificación que, por otra parte, se ampara en el Convenio 108 del Consejo de Europa, el cual, como referencia interpretativa, le mueve a concluir que "la protección a la intimidad de los ciudadanos requiere que estos puedan conocer la existencia de aquellos ficheros automatizados".

Con todo, otros dos aspectos no pueden pasar desapercibidos en el pronunciamiento,

[32] Aun cuando no resultaba infrecuente sostener que tampoco era necesaria, por cuanto la intimidad ya proporcionaba suficiente cobertura al ámbito de privacidad del individuo digno de protección. Así se afirmaba que "la alusión a la 'protección de datos' no deja de ser una concesión –por cierto, escasamente aceptable desde mi punto de vista– a la terminología foránea, que goza –por mor de la moda neologista imperante– de cierta popularidad, con la que en realidad se suele denominar a las normas jurídicas cuyo objetivo fundamental es, precisamente, el de la tutela de la intimidad personal contra el uso de los medios informáticos", Bermejo Vera, J.: "Premisas jurídicas de la intimidad personal y de la protección de datos en el Derecho español", en AA.VV. (Gómez-Ferrer Morant, R., Coord.): *Libro homenaje al profesor José Luis Villar Palasí*, Madrid (Civitas), 1989, p. 144.

[33] En valoración de Pérez Luño, A.E.: *Manual de Informática y Derecho*, Barcelona (Ariel), 1994, p. 64.

[34] Mostrándolo con ejemplos harto elocuentes referidos al desarrollo de la relación laboral, Del Rey Guanter, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la 'intimidad informática' del trabajador)", *Relaciones Laborales*, núm. 15, 1993, pp. 14 y ss.; con mayor amplitud, Cardona Rubert, M.B.: *Informática y contrato de trabajo (Aplicación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal)*, Valencia (Tirant lo Blanch), 2014, en especial pp. 45 y ss.

[35] Anticipando su cuestionamiento constitucional, que dará lugar a las SSTCo 290 y 292/2000, de 30 de noviembre, así como ofreciendo las principales infracciones que su texto supone a los Convenios celebrados y ratificados por España, en especial el Convenio Europeo para la Protección de los Derechos y Libertades Fundamentales de 1950 y el Convenio 108 del Consejo de Europa, Torne-Dombidau Jiménez, J. y Castillo Blanco, F.A.: "Informática y protección de la privacidad del individuo", *Actualidad Administrativa*, T. I, 1993, pp. 282-288.

[36] Murillo de la Cueva, P.L.: "La primera jurisprudencia sobre el derecho a la autodeterminación informativa", *Datos personales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 1, 2003.

pues llevan a intuir que, lejos de haberse cerrado la cuestión, quedaba abierta a mayor completitud en un futuro, no en vano[37]:

a) Se trata de un derecho que requiere un desarrollo legislativo, "de configuración legal" por tanto, cuyo contenido, respetando el núcleo esencial recogido en la Constitución, ha de ser completado por el legislador; en consecuencia, y para el que aquí concita la atención, se nutrirá de los derechos derivados que recoja la norma sobre protección de datos, encargada de otorgarle su dimensión última[38].

b) Precisamente indagando en ese contenido mínimo, o esencial, se sienta el "carácter bifronte" del derecho reconocido en el art. 18.4 CE[39]: "nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza a la dignidad y a los derechos de la persona (…). En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegitimo del tratamiento mecanizado de datos, lo que la CE llama 'la informática' ".

A resultas de tal afirmación, aparece ya en estado embrionario, pero aún oculto por el peso de la tradición, un derecho que aspira a expandirse más allá de la intimidad y no se agota en facultades puramente negativas, de exclusión, sino que incluye el derecho al control de los datos relativos a la propia persona o *habeas data*[40].

El parecer anterior va tomando cuerpo concreto a través de dos vías, la jurisprudencial y la legal, que, sin salirse del contorno dibujado del derecho fundamental, descubren nuevos matices para perfilarlo con mayor fidelidad, augurando un rápido tránsito hacia otra dimensión.

La doctrina constitucional volverá a destacar la exigencia de ampliar el derecho a la intimidad, en la medida en la cual el tratamiento de la información no puede agotar su contenido en facultades puramente negativas[41]; descubrirá la vinculación de la protección de datos con otro derecho fundamental, como es el de libertad sindical, con una aplicación del art. 18.4 CE que, de nuevo, solo en apariencia está actuando como vía instrumental o de garantía de otros derechos, pues en realidad, si bien *obiter dicta*, los 16 pronunciamientos datados entre 1998 y 1999 por el Tribunal Constitucional, ante hechos sustancialmente iguales, vienen a reconocer y afirmar ese derecho fundamental en estado latente que –en los supuestos analizados– impulsa reconocer la vulneración del contenido característico de la libertad informática[42]; más aún, y para un

[37] Destacando ambos factores, VILLAVERDE MENÉNDEZ, I.: "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *Revista Española de Derecho Constitucional*, núm. 41, 1994, pp. 187 y ss; también, ROIG BATALLA, A.: "Derecho Público y tecnología de la información y la comunicación", *Revista Catalana de Dret Públic*, núm. 35, 2007, pp. 3 y 4.

[38] En referencia concreta al art. 18.4 CE y a la falta de regulación legal que descubre la sentencia comentada, NOREÑA SALTO, J.A.: "Acerca del contenido esencial de los derechos de configuración legal", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 18, 2003, p. 1868, nota 17.

[39] PULIDO QUECEDO, M.: "¿Numerus clausus o numerus apertus en materia de derechos fundamentales?: el derecho a la protección de datos", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 20, 2000, p. 1717.

[40] RALLO LOMBARTE, A.: "De la 'libertad informática' a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político*, núm. 100, 2017, p. 650. Volviendo la vista atrás, extremadamente agudo el pronóstico sobre la evolución que efectuaba ORTÍ VALLEJO, A.: "El nuevo derecho fundamental (y de la personalidad) a la libertad informática (A propósito de la STC 254/1993, de 20 de julio)", *Derecho Privado y Constitución*, núm. 2, 1994, pp. 305-310.

[41] STC 143/1994, de 9 de mayo.

[42] Remitiendo todos los pronunciamientos posteriores, en sustancia, a cuanto vino a sentar la STC 11/1998, de 13 de enero. Entre los numerosísimos comentarios de una doctrina laboralista especialmente preocupada por este tema, puede servir la remisión a los efectuados por CORREA CARRASCO, M.: "Libertad sindical y libertad informática en la empresa (Comentario a la STC 11/1998, de 13 de enero)", *Revista de Derecho Social*,

supuesto de tratamiento de datos relativos a bajas médicas por incapacidad temporal destinado a controlar el absentismo, sin que el interesado hubiera prestado su consentimiento, considera la medida como inadecuada, desproporcionada y, por ende, que conculca tanto el derecho a la intimidad como a la libertad informática, aun cuando otorga el amparo por vulneración de aquel primero, al haber sido el único invocado[43].

El desempeño legal, por su parte, ofrece el interés de ser el llamado a desarrollar y completar la referencia contenida en el art. 18.4 CE; si se prefiere, de conferirle esa identidad propia que, con los matices añadidos al contenido esencial, dote a la previsión constitucional de eficacia[44]. En este sentido, la Ley Orgánica 15/1999, que inicia su andadura como proyecto de reforma de la Ley Orgánica 5/1992, pero acaba –tras una polémica tramitación parlamentaria[45]– con la derogación de la norma de referencia (y, quizá por ello, carece de una Exposición de Motivos que hubiera sido de enorme ayuda para el intérprete), viene marcada por un doble factor a partir del cual define su contenido en cuanto ahora importa[46]: en primer lugar, la necesidad de trasponer la Directiva 95/45/CE, motivo por el cual recibe los elementos de evolución que en aquella han sido destacados; en segundo término –y además de su redacción descuidada en algunos aspectos y ciertos defectos sistemáticos[47]–, y según se percibe de manera palmaria, la influencia de la constitucionalidad cuestionada y pendiente de sentencia, así como los trabajos preparatorios de cuanto habrá de figurar en la Carta de Derechos Fundamentales de la Unión Europea. De la conjunción de ambos factores, y si bien la intimidad sigue estando presente a lo largo de su texto de manera reiterada, la autodeterminación informática gana peso específico[48] –mucho más patente tras su desarrollo por RD 1720/2007, de 21 de diciembre[49]– y anticipa el cambio que se aventuraba tanto a nivel internacional como nacional.

3. EL NACIMIENTO DEL DERECHO A LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL AUTÓNOMO

Prácticamente coincidiendo en el tiempo, y a comienzos de siglo, ha lugar a un doble punto de inflexión en el ordenamiento europeo y en el estatal, llevando a la emancipación del

núm. 2, 1998, pp. 117 y ss.; ORTIZ LALLANA, M.C.: "Vulneración del derecho a la libertad sindical mediante uso desviado de datos informatizados sobre la afiliación del trabajador. Libertad sindical y derecho a la intimidad informática", *Aranzadi Social*, T. V, 1999, pp. 359 y ss. o MENÉNDEZ SEBASTIÁN, P.: "La lesión de la libertad sindical mediante la utilización de datos laborales automatizados", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 14, 1999, pp. 15 y ss.

[43] STC 202/1999, de 8 de noviembre. Un análisis del pronunciamiento que avanza en la doble vía de protección de los derechos del trabajador en GARCÍA MURCIA, J.: "Derecho a la intimidad y contrato de trabajo: la anotación de las bajas médicas (Comentario a la STC 202/1999, de 8 de noviembre)", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 13, 2000, pp. 13 y ss.

[44] DAVARA RODRÍGUEZ, M.A.: "Los principios de la protección de datos y los derechos de las personas en la Ley Orgánica de Protección de Datos de Carácter Personal", *Actualidad Informática Aranzadi*, núm. 34, 2000. En idéntico sentido, pero bajo la perspectiva de los límites y deberes que genera cada derecho, ALEGRE MARTÍNEZ, M. A.: "Los deberes de la Constitución Española: esencialidad y problemática", *Teoría y Realidad Constitucional*, núm. 29, 2009, pp. 274 y ss.

[45] MURILLO DE LA CUEVA, P. L.: "Las vicisitudes del Derecho de la protección de los datos personales", *Revista Vasca de Administración Pública*, núm. 58, 2000, pp. 217 y ss.

[46] FERNÁNDEZ LÓPEZ, J.M.: "La nueva Ley de Protección de Datos de Carácter Personal de 13 de diciembre de 1999. Su porqué y sus principales novedades", *Actualidad Informática Aranzadi*, núm. 34, 2000.

[47] Con detalle sobre ambos, TÉLLEZ AGUILERA, A.: *Nuevas tecnologías. Intimidad y protección de datos*, Madrid (Edisofer), 2001, pp. 107-109.

[48] Por extenso, HERRÁN ORTIZ, A.I.: *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, Madrid (Dykinson), 2002, pp. 195 y ss.

[49] MARTÍNEZ MARTÍNEZ, R.: "El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: aspectos claves", *Revista Jurídica de Castilla y León*, núm. 16, 2008, pp. 257 y ss. y, con más detalle aún, del mismo autor, *Protección de datos. Comentario al Reglamento de desarrollo de la LOPD*, Valencia (Tirant lo Blanch), 2009, pp. 80-87 y 121-125.

derecho a la protección de datos, que pasa así, formalmente, a disponer de identidad propia.

3.1. El valor del art. 8 de la Carta de Derechos Fundamentales de la Unión Europea

En pleno proceso de actualización del elenco de los derechos compartidos por todos los Estados de la Unión Europea, con la incorporación de los denominados "de tercera generación", la promulgación de la Directiva 95/46 supuso, sin duda, el punto a partir del cual se forja el reconocimiento de uno nuevo que, sobre la raíz del derecho a la intimidad, crece hasta trascenderlo[50] para, manteniendo los lazos de vinculación que –obviamente– no desaparecen nunca[51], figurar en la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) tal y como lo concibió el Grupo de Trabajo del art. 29 –a través de su Dictamen 4/1999, de 7 de septiembre–: formalmente separado (aunque correlativo) al que hasta ese momento resultaba ser su soporte y al que servía de manera instrumental[52].

La línea de tendencia que en la evolución mostraban unos Estados –con la pujante influencia cuanto se había avanzado en Alemania[53]– encuentra en la Carta un papel que no es de simple codificación o consolidación, sino innovador o transformador[54] (luego seguido por el Tratado de Funcionamiento –art. 16.2– y por el Tratado de la Unión –art. 39–), en tanto la protección de datos, que el Tribunal Europeo de Derechos Humanos sigue reconduciendo al art. 8 CEDH ("derecho al respeto a la vida privada y familiar"), en su texto se desgaja para adquirir una identidad característica[55]. Lo hace en la medida en la cual, mientras el art. 7 sigue aludiendo a aquella perspectiva de "derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones", el art. 8 supera la estructura tradicional[56] al proclama que:

> "1.– Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 2.– Estos datos se tratarán de modo legal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación".

Abandona, con ello, esa visión restrictiva que había acompañado inicialmente al *habeas data*, para alumbrar "un proceso inédito, hasta ahora desarrollado solo en la Unión Europea, donde es posible anunciar la creación de un nuevo 'modelo' que, reforzando la esfera privada, refuerza al mismo tiempo el peso de cada uno en la esfera pública. De este modo, es posible concluir que el derecho fundamental a la protección de datos personales se transforma en un elemento básico de la ciudadanía electrónica". Y ello en la medida en la cual otorga

[50] PÉREZ LUÑO, A.E.: *La tercera generación de derechos humanos*, Cizur Menor (Aranzadi/Thomson), 2006, pp. 23 y ss.

[51] Según demuestra, para destacar al tiempo los rasgos que diferencian al nuevo derecho, CONDE ORTÍZ, C.: *La protección de datos personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid (Dykinson), 2005.

[52] Sobre tan interesante justificación, y la recomendación final sobre su inclusión por separado, RUIZ MIGUEL, C.: "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", *Revista de Derecho Comunitario Europeo*, núm. 14, 2003, pp. 8 y 29-30.

[53] KRANENBORG, H.: "Commentary to article 8: Protection of personal data", en AA.VV. (PEERS, S. *et alii*, Eds.): *The EU Charter of Fundamental Rights. A Commentary*, Oxford (Hart Publishing), 2014, p. 229.

[54] La idea en BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, p. 57.

[55] COUDHRY, S.: "Commentary to article 7: Right to respect for private and family life (Family life aspects)", en AA.VV. (PEERS, S, *et alii*, Eds.): *The EU Charter of Fundamental Rights. A Commentary*, *cit.*, p. 154.

[56] KOKOTT, J. y SOBOTTA, C.: "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR", *International Data Privacy Law*, Vol. 3, núm. 4, 2013, p. 224.

un sentido sociopolítico concreto a la privacidad a través de su engarce con la democracia: "representa una condición preventiva para poder gozar enteramente de otros derechos fundamentales, que constituyen exactamente el núcleo de las libertades democráticas"[57].

El "bloque de constitucionalidad europeo" aparece notoriamente enriquecido, dotando de un contenido concreto al "nuevo" derecho a través de varias notas que presentan singular relieve[58]:

A.– Con extensión a todas las personas físicas y –en principio– a toda la información que concierna e identifique a cada una en particular o permita hacerlo, recoge las obligaciones de procedimiento que pesan sobre quien efectúa el tratamiento de los datos, que habrá de tener lugar de manera "leal", "para fines concretos" (por tanto, no solo legítimos, sino explícitos y determinados) y asentados sobre el consentimiento del afectado. Este último aparece expresamente destacado como regla para la regularidad procedimental y verdadera clave de bóveda del modelo, destinado a garantizar el control final sobre el flujo de la información, que solo habrá de ceder ante otro interés legítimo expresamente enunciado en la norma.

B.– Correlato lógico del señalado, constitutivo de su núcleo esencial, son las facultades que explícitamente han de acompañar al derecho, cuyo enunciado –frente a la simple proclamación que recoge en la mayor parte del resto de los artículos– tal vez obedezca, precisamente, al intento por deslindar de manera más acabada cuanto incorpora el art. 8 respecto o frente al derecho al respeto a la vida privada y familiar. En verdad el elenco dista de ser acabado, y, sin duda, son tantos los principios y derechos que omite como los que enuncia (pues además de las pautas destinadas a orientar el tratamiento, entre los derechos únicamente menciona los de acceso y rectificación[59]); con todo, también este óbice será fácil de salvar, e incluso podrá encontrársele un sentido positivo.

Tal el que cabe seguir de tener presente cuanto dispone el art. 53 CDFUE, pues ninguna de sus disposiciones puede ser interpretada de forma que amparen la limitación o lesión de los derechos reconocidos por el Derecho de la Unión; en este sentido, las exigencias de tratamiento recogidas en su art. 8.2 llevarían a remitir en bloque a cuanto dispusiere la norma comunitaria en cada momento[60]. Por este motivo, el hecho de que solo enuncie los principios y derechos más salientes y no trate de agotarlos, como tampoco lo hace en los otros preceptos, evita un rígido corsé y habilita que el Derecho derivado acometa las reformas exigidas por la evolución tecnológica, remodelando el conte-

[57] RODOTÀ, S.: "Democracia y protección de datos" (traducción de PIÑAR MAÑAS, J.L.), *Cuadernos de Derecho Público*, núm. 19-20, 2013, pp. 16 y ss., los literales de pp. 18 y 20, respectivamente.

[58] Condensando las reflexiones que con más detalle exponen, entre otros, RUIZ MIGUEL, C.: "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea", *cit.*, pp. 9 y ss.; BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, pp. 60-63; ARENAS RAMIRO, M.: *El derecho fundamental a la protección de datos personales en Europa*, *cit.*, pp. 225 y ss.; KRANENBORG, H.: "Commentary to article 8: Protection of personal data", *cit.*, pp. 228 y ss. o MARTÍN Y PÉREZ DE NANCLARES, J.: "Artículo 8: Protección de datos de carácter personal", en AA.VV. (MANGAS MARTÍN, A., Dir., y GONZÁLEZ ALONSO, N., Coord.): *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo*, Bilbao (Fundación BBVA), 2008, pp. 229-241.

[59] Con detalle sobre cuanto silencia o delimita de manera insuficiente, RUIZ MIGUEL, C.: "El derecho a la protección de los datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", *cit.*, pp. 39 y 40. Una contestación aún más firme en GUERRERO PICÓ, M.C.: "El derecho fundamental a la protección de los datos de carácter privado en la Constitución Europea", *Revista de Derecho Constitucional Europeo*, núm. 4, 2005, pp. 321 y 322.

[60] ABERASTURI GORRIÑO, U.: "El derecho a la protección de datos de carácter personal. La autodeterminación informativa como derecho autónomo en la Carta de Derechos Fundamentales de la Unión Europea", en AA.VV. (CORDEÑANA Gezuraga, I., Dir.): *La Carta de los Derechos Fundamentales de la Unión Europea y su reflejo en el ordenamiento jurídico español*, Cizur Menor (Aranzadi/Thomson), 2014, pp. 172 y 173.

nido final del derecho en función de las necesidades de cada época[61].

C.– La anterior es, por otra parte, la lectura que cabe obtener del Tribunal de Justicia de la Unión Europea –TJUE– (también por el Tribunal Europeo de Derechos Humanos –TEDH–, aun cuando –según se ha anticipado y verá con mayor detalle– resultará ser una cuestión con otras implicaciones, dado que el art. 8 de la Carta no tiene correspondencia directa con el Convenio Europeo de Derechos Humanos), pues en su sentencias venía a poner en conexión las disposiciones de la Directiva 95/46 con los derechos reconocidos en la CDFUE, en una relación que llevaba desde los principios generales del Derecho cuyo respeto garantiza el Tribunal y están recogidos en la Carta, a la Directiva en cuanto portadora del necesario desarrollo exigido por el tratamiento de datos para preservar las libertades y derechos fundamentales[62].

3.2. La confirmación de la protección de datos como derecho fundamental autónomo en la doctrina del Tribunal Constitucional

Fue solo cuestión de tiempo que la vía abierta en 1993, y cuidadosamente precisada en pronunciamientos posteriores[63], llevará a cuanto era un final casi natural. De él consta un anticipo resaltado en el voto particular que, el mismo día del cambio definitivo, recoge el parecer de un Magistrado exponiendo las razones por las cuales en la sentencia en cuestión "debió afirmarse de modo explícito, en la argumentación de ella, que nuestro Tribunal Constitucional reconoce y protege ahora un derecho fundamental, el derecho de libertad informática que no figura en la Tabla del texto de 1978"[64].

Razón no le faltaba, pues en el fallo del pronunciamiento ya aparecía explícita una identificación individualizadora cuando se afirmaba: "el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer de los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos y con qué finalidad, así como el derecho a oponerse a esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de sus datos"[65].

---

[61] BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, p. 63.

[62] El planteamiento de tal parecer en STJUE de 20 de mayo de 2003, asuntos acumulados C-465/00, C-138/01 y C-139/01, Österreichischer Rundfunk y otros; STJUE de 13 de mayo de 2016, asunto C-131/12, *Google Spain*; STJUE de 11 de diciembre de 2014, asunto C-212/13, *Rynes* o STJUE de 6 de octubre de 2015, asunto C-362-14, *Schrems*. Con superior detalle, SÁNCHEZ GONZÁLEZ, M.B.: *Implicaciones institucionales de la Ley de Protección de Datos*, Tesis Doctoral, Universidad de Málaga, 2015, p. 97, en: http://educación.gob.es/teseo/imprimirFichero-Tesis.doidfichero=%2FaiA4TuDrto%3D.

[63] Un resumen muy medido de este camino con un importante recorrido en PARDO FALCÓN, J.: "La protección de datos", en AA.VV. (CASAS BAAMONDE, Mª.E. y RODRÍGUEZ-PIÑERO Y BRAVO-FERRER, M., Dirs.): *Comentarios a la Constitución Española*, Madrid (Wolters Kluwer), 2008, pp. 456 y ss. o CASTRO ARGÜELLES, M.A.: "Protección de datos de carácter personal en el ámbito laboral", en AA.VV. (GARCÍA MURCIA, J., Coord.): *Nuevas tecnologías y protección de datos personales en las relaciones de trabajo*, Lugones (Edición del Coordinador), 2019, p. 17.

[64] Sin perjuicio de disentir sobre la consideración acerca del *numerus apertus* en la lista de derechos fundamentales, la valoración del Magistrado JIMÉNEZ DE PARGA contenida en la STC 290/2000, de 30 de noviembre.

[65] En la interpretación de este texto, especialmente acertado el comentario de ALGUACIL GONZÁLEZ-AURIOLES, J.: "La libertad informática: aspectos sustantivos y competenciales (SSTC 290 y 292/2000)", *Teoría y Realidad Constitucional*, núm. 7, 2001, pp. 379 y 380. Añadiendo la consideración sobre la circunstancia de que "el derecho a la intimidad no aporta por sí solo una protección diferente frente a esta nueva realidad derivada del progreso tecnológico", el discurso de GARCÍA COCA, O.: *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, Murcia (Laborum), 2016, p. 31, nota 32.

Es en el segundo de los pronunciamientos dedicados a la materia de esa fecha, sin embargo, donde ha lugar el tránsito definitivo hacia la configuración de la protección de datos como un derecho autónomo, abriendo una nueva etapa en la cual sus características fundamentales aparecen ya aquilatadas, aun cuando no dejen de incorporar matices de interés en su evolución[66].

Los rasgos llamados a marcar la impronta pueden ser condensados en las siguientes afirmaciones literales[67]:

1.– "Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley". La peculiaridad radica, por consiguiente, "en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran".

2.– Por cuanto al objeto hace, el derecho a la protección de datos "no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

3.– Respecto a su contenido, mientras que "el derecho a la intimidad personal y familiar confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido (…), el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales".

4.– A la luz de todo lo cual está en disposición de ofrecer, con el detalle requerido, noticia del contenido del derecho. Sienta al respecto que "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero reca-

[66] Una taxonomía de la evolución en etapas del derecho, con rigor y argumentos de interés para tal clasificación, en CUADROS GARRIDO, M.E.: *Trabajadores tecnológicos y empresas digitales*, Cizur Menor (Aranzadi/Thomson), 2018, pp. 149-153.

[67] Un desarrollo adecuado de los rasgos destacados en texto en TRONCOSO REIGADA, A.: *La protección de datos personales: en busca del equilibrio*, Valencia (Tirant lo Blanch), 2011, p. 111 o CANALES GIL, A.: "La protección de datos como derecho fundamental", *Revista Jurídica de Castilla y León*, núm. 16, 2007, pp. 21-26.

bar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan 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, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el 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 usos".

Desde un punto de vista pragmático, y para hacer operativas estas últimas posibilidades, se confiere al interesado la facultad de exigir de titular del fichero "que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

Tan detallada aproximación ha tenido línea de continuidad en otros pronunciamientos que abundan a la hora de fijar doctrina; a su lado, sin embargo, aparecen elementos de innovación cuya decantación última, sin duda, habrá de estar y pasar por una consolidación de la que hoy en día carecen.

En cuanto a los aspectos que se asientan en pronunciamientos ulteriores, cabría destacar tres reiterados con énfasis[68]:

a) El carácter autónomo del derecho a controlar el flujo de información que concierne a cada persona, remitiendo a la CDFUE y al Convenio 108 como fuentes "constitucionales" de origen internacional, y –en su momento– a la Directiva 95/46 como norma de desarrollo de un derecho que ya no se puede reducir a la protección de datos íntimos, sino que ha de extenderse a cualquier dato personal.

b) El consentimiento informado en la recogida, tratamiento y uso o usos posibles, como elemento esencial en el poder de disposición y control que forma parte del contenido del derecho fundamental. A tal punto que únicamente cabrá constreñir su operatividad en atención a derechos y bienes de relevancia constitucional, cuando su limitación esté justificada, sea proporcionada y, además, venga establecida por Ley[69].

c) El carácter relativo, por tanto, que también se debe predicar del derecho, aun cuando la Constitución no le haya puesto límites específicos, ni remita a los poderes públicos para su determinación, pues el principio de unidad de la Constitución conlleva, *per se*, la necesaria comunión con los restantes bienes y derechos por aquella amparados.

Con ser de interés tal recordatorio, superior relieve procede otorgar a las variantes que, en sendos asuntos relativos a la video-

[68] SSTC 96/2012, de 7 de mayo; 217/2013, de 31 de enero o 151/2014, de 25 de septiembre. Haciéndose eco de esta línea asentada en la evolución, HERNÁNDEZ LÓPEZ, J.M.: *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Cizur Menor (Aranzadi/Thomson), 2013, en particular pp. 87-97; RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, Cizur Menor (Aranzadi/Thomson), 2019, pp. 165 y ss.; o PRECIADO DOMENECH, C.H.: *El derecho a la protección de datos en el contrato de trabajo*, Cizur Menor (Aranzadi/Thomson), 2017, pp. 139 y 140.

[69] Sobre el contrato de trabajo como base para la legitimación del tratamiento en este ámbito y los problemas que suscita en su aplicación cotidiana, BLÁZQUEZ AGUDO, E.M.: *Aplicación en la práctica de la protección de los datos en las relaciones laborales*, Madrid (Wolters Kluwer), 2018, p. 49. Con interesante propuesta sobre la oportunidad de cambiar la denominación del derecho a la protección de datos por "libertad de datos" o "autodeterminación de datos", dato el matiz pasivo o reactivo del consentimiento al cual cabría oponer el rol proactivo que también puede jugar su titular, ADSUARA VALETA, B.: "El consentimiento", AA.VV. (PINAR MAÑAS, J.L., Dir. y ÁLVAREZ CARO, M. y RECIO GAYO, M. Coords.): *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Madrid (Reus), 2016, pp. 168 y 169.

vigilancia laboral, vienen a dar un sentido propio a cuanto dispone el art. 18.4 CE. En este sentido, y si hasta este momento estas situaciones habían sido abordadas desde el plano de la posible afectación a intimidad y la aplicación del principio de proporcionalidad[70], a partir de 2013 ha lugar a un cambio de rumbo trascendental cuando la cuestión pasa a ser examinada bajo la perspectiva de la protección de datos, por cuanto "la captación de las imágenes de las personas constituye un tratamiento de datos personales incluido en el ámbito de la normativa [de protección de datos]". Sobre tal premisa analiza el conflicto de interés en presencia y sitúa al principio de transparencia o deber de información como pieza de convicción, en tanto el conocimiento de quien dispone de los datos y el uso al que los está sometiendo constituye una garantía instrumental básica a la hora de proteger el derecho al control y disposición por el interesado[71]. "Elemento caracterizador" o "núcleo del derecho", en consonancia con la relevancia que se le reconoce, que demanda una interpretación rigurosa, un canon de control de constitucionalidad del deber o principio de transparencia más rígido[72], para comprender "la información previa y expresa, precisa, clara e inequívoca (…) de la finalidad de control de la actividad (…) a la que la captación podía ser dirigida".

La exigencia de información habrá de operar en cualquier supuesto, incluso cuando exista habilitación legal para recabar datos sin necesidad del consentimiento del titular; ampliando, de este modo –y de manera considerable–, el ámbito objetivo del derecho[73].

Tal línea de interpretación dista de haber tenido continuidad, pues para un supuesto con notable semejanza se recupera la visión clásica y se rompe de manera elocuente con el criterio precedente[74], no solo –aunque también– respecto a si existe o no habilitación legal (art. 20.3 ET), sino, sobre todo, reformulando la naturaleza de la autorización que en aquel entonces recogía la Ley Orgánica 15/1999, al entender que puede ser indirecta, y no personal (pese a que afecta a personas perfectamente identificables a través de una relación contractual), e igualmente puede no especificar la finalidad del control; provocando, al mermar su núcleo esencial, un apreciable descenso en el grado de protección que otorga el art. 18.4[75].

[70] Una visión acabada de tal enfoque, por todos, en GOÑI SEIN, J.L.: *La videovigilancia empresarial y la protección de datos personales*, Cizur Menor (Aranzadi/Thomson-Agencia de Protección de Datos), 2007, pp. 265 y ss. Entre los muchos comentarios a estas sentencias que abren camino, ÁLVAREZ ALONSO, D.: "Derecho a la intimidad y vigilancia audiovisual en el medio de trabajo: sentencia TC 98/2000, de 10 de abril", en AA.VV. (GARCÍA MURCIA, J., Coord.): *Derechos del trabajador y libertad de empresa*, Cizur Menor (Aranzadi/Thomson), 2013, pp. 339 y ss. o THIBAULT ARANDA, J.: *Control multimedia de la actividad laboral*, Valencia (Tirant lo Blanch), 2006, pp. 21 y ss.

[71] En este punto, con gran detalle y finura jurídica, GALLARDO MORA, R.: "El derecho fundamental a la protección de datos y la videovigilancia empresarial", *Revista de Derecho Social*, núm. 62, 2013, pp. 168 y 169 y RODRÍGUEZ COPÉ, M. L.: "Facultades de control empresarial y circuito cerrado de televisión. STC 29/2013, de 11 de febrero", *Temas Laborales*, núm. 121, 2013, pp. 189-200.

[72] DESDENTADO BONETE, A. y MUÑOZ RUIZ, A.: "Trabajo, videovigilancia y controles informáticos. Un recorrido por la jurisprudencia", *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 39, 2014 (RI § 415516).

[73] JIMÉNEZ-CASTELLANOS BALLESTEROS, I.: "Videovigilancia laboral y derecho fundamental a la protección de datos", *Temas Laborales*, núm. 136, 2017, p. 138.

[74] Según dejan patente algunos comentaristas muy críticos con el primer pronunciamiento, bajo el entendimiento de que resultaba "incomprensible" el cambio en el precepto de referencia (el art. 18.4 en vez del art. 18.1), en particular por cuanto la obligación de informar al trabajador con carácter previo constituye una cuestión de legalidad ordinaria en el caso del derecho a la intimidad; al respecto, por ejemplo, GUDE FERNÁNDEZ, A.: "La videovigilancia laboral y la protección de datos de carácter personal", *Revista de Derecho Político*, núm. 91, 2014, pp. 70-72.

[75] CABELLOS ESPIÉRREZ, M.A.: "El derecho a ser informado como elemento esencial del derecho a la protección de datos. Una visión crítica de la jurisprudencia del Tribunal Constitucional y su cambio de doctrina en la STC 39/2016", *Revista Vasca de Administración Pública*, núm. 106, 2016, p. 213 y GONZÁLEZ GONZÁLEZ, C.: "Control empresarial de la actividad laboral, videovigilancia y deber informativo. A propósito de la STC de 3 de marzo de 2016", *Revista Aranzadi Doctrinal*, núm. 5, 2016, BIB 2016/21165.

Como bien se ha afirmado, "una involución evidente", "un cumplimiento devaluado de los presupuestos formales del deber de trasparencia" capaz de conducir a que "el deber de información termine por poseer en este contexto una relevancia meramente formal"[76], según acaba por acoger, como nueva dirección, la jurisprudencia ordinaria[77].

Al amparo todavía del acervo europeo que culminaba en el tiempo con la CDFUE, la doctrina del TEDH ha ofrecido a lo largo de los tres últimos años [es decir, una vez ya publicado el Reglamento (UE) 2016/679 e, incluso, la Ley Orgánica 3/2018] una interesante aproximación al derecho que concita la atención, aun cuando –se repite por tercera vez– lo deba hacer siempre a través del derecho al respeto a la vida privada y familiar recogido en el art. 8 CEDH, que en este sentido ha de ser interpretado de manera abierta en un doble sentido[78]: de un lado, para integrar los distintos derechos fundamentales de la personalidad en que la vida privada se descompone cuando se traslada al ordenamiento interno, comprendiendo el honor, la intimidad personal y la propia imagen –art. 18.1 CE–, el secreto de las comunicaciones –art. 18.2 CE– y a la protección de datos –art. 18.4 CE–; de otro, "sin prestarse a una definición exhaustiva, sino de una forma dinámicamente amplia"[79].

En realidad, su aproximación resulta ser fluctuante, e incluso cabría tildarla de "líquida"[80], en la medida en que acoge pronunciamientos difíciles de cohonestar, cuyo examen presenta el interés de comprobar tanto que, efectivamente, el derecho de protección de datos está en plena construcción (lo cual justifica las contradicciones puntuales que pudieran surgir), como que muy probablemente otro pueda ser el rumbo de la mano de las nuevas directrices del legislador europeo.

La referencia viene dada por las Sentencias del TEDH en los conocidos como asuntos *Barbulescu II* y *López Ribalda II*[81]. El ordinal incorporado tras el apellido del protagonista indica que obra un pronunciamiento de la Gran Sala, con la curiosa circunstancia de que, en ambos casos, corrige a la Sala, y en el segundo de ellos no deja de cuestionar alguna de las conclusiones que parecían firmes en el primero, así como en su continuación por el propio Tribunal[82].

El asunto debatido que interesa a este discurso viene dado, en ambas ocasiones –y como en los supuestos de videovigilancia laboral que examinó el Tribunal Constitucional–, por

[76] Goñi Sein, J.L.: "Sentencia del Tribunal Constitucional 39/2016, de 3 de marzo. Instalación de cámaras de videovigilancia para la obtención de pruebas y deber de información previa", *Ars Iuris Salmanticensis*, Vol. 4, núm. 2, 2016, p. 290 o, en extensísima valoración conclusiva, Jiménez-Castellanos Ballesteros, I.: "Videovigilancia laboral y derecho fundamental a la protección de datos", *cit.*, pp. 149-156.

[77] Encabezada por las SSTS 31 enero y 1 y 2 de febrero 2017 (Rec. 3331, 3325/2015 y 554/2016) y con un resumen harto elocuente, por ejemplo, en STS 18 septiembre 2018 (Rec. 1092/2018): "la prueba consistente en reproducción de imágenes y sonidos (videovigilancia) es lícita, siempre que el trabajador conozca la instalación de las cámaras y su ubicación por motivos de seguridad (...), de suerte que la circunstancia de que el trabajador hubiese sido o no advertido expresamente de la finalidad de control de la actividad laboral y del destino que se le pueda dar a las grabaciones (...) resulta ahora intrascendente". Una valoración medida de esta minoración tanto del núcleo esencial del derecho constitucional, como de su trascendencia legal y judicial, en Preciado Domenech, C.H.: "La vídeo vigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos de carácter personal", *Revista de Derecho Social*, núm. 77, 2017, pp. 194; también, Goñi Sein, J.L.: "Vigilancia empresarial y protección de datos: doctrina jurisprudencial", *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*, núm. 143, 2019, pp. 202 y 203.

[78] Casas Baamonde, M.E.: "Informar antes que 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*, núm. 2, 2018, p. 104.

[79] Abundando en la idea el literal de Sánchez Trigueros, C. y Cuadros Garrigo, M.E.: "Autodeterminación informativa: un derecho en alza", *cit.*, p. 98.

[80] Molina Navarrete, C.: "Ahora que el TC recela de la 'cámara oculta', el TEDH la respalda en las empresas: la insoportable 'liquidez' de la jurisprudencia", *CEF Laboral Social*, 18 de octubre de 2019, en https://www.laboral-social.com.

[81] SSTEDH de 5 de septiembre de 2017 y de 17 de octubre de 2019, respectivamente.

[82] La referencia lo es, en concreto, a la STEDH de 28 de noviembre de 2017, asunto *Antovic y Mirkovic*.

la configuración de la información que debe recibir el titular de los datos. En la primera, tras el conjunto de interrogantes que configuran el conocido como "test Barbulescu", se establece un exigente patrón susceptible de ser calificado como "doctrina general, no sobre mensajería instantánea [cuestión debatida en el caso concreto], sino sobre las TICs en general y las pautas de control"[83], para establecer varios ítems a ponderar[84]: la exigencia de notificación previa sobre la captación de datos como garantía de comunicación inicial básica; el nivel de intromisión (tiempo, datos o personas con acceso) que va a suponer el tratamiento; la exigencia de una razón legítima que ampare la pretensión de control y la inexistencia de otras alternativas menos invasivas; en fin, la adecuación del uso (resultado) al objetivo perseguido.

El criterio parecía consolidarse en la continuación que supuso la sentencia en el caso *López Ribalda I*[85], pues incidía en la obligación de informar a los interesados previamente, de manera precisa e inequívoca, sobre la existencia y características particulares de cualquier sistema que recopile datos. De este modo, se subordinaba la validez del cumplimiento del deber de información a la observancia escrupulosa de las exigencias normativas, entre las cuales se encuentra, en cualquier ley, la obligación de informar a los titulares del derecho sobre el acopio de datos, su tratamiento y los fines pretendidos[86].

Con una destacable coincidencia el TEDH y los votos particulares discrepantes de la que fue tesis mayoritaria en el Tribunal Constitucional parecían concordar en la exigencia de transparencia[87]. Pero justo cuando el criterio de este último varía para acercarse a los postulados del primero[88], es este quien matiza sus posiciones y, sin negar el valor principal que merece la información, recupera esa constante en la doctrina sobre la autodeterminación informativa que viene dada por la invocación a la hábil categoría dada por "expectativa razonable de privacidad"[89]. Considera, en el caso, que la protección de los bienes y el buen fun-

[83] SÁNCHEZ TRIGUEROS, C. y CUADROS GARRIDO, M.E.: "Autodeterminación informativa: un derecho en alza", *cit.*, p. 95. Opinión semejante en ROMERO BURILLO, A.M.: "Las nuevas TICs y el despido disciplinario del trabajador", *Revista de Derecho Social*, núm. 85, 2019, pp. 37 y 38 o BLASCO JOVER, C.: "Trabajadores transparentes: la facultad fiscalizadora del empresario vs. derechos fundamentales de los empleados (I)", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, Vol. 6, núm. 3, 2018, pp. 37-40.

[84] Siguiendo las reflexiones de GOÑI SEIN, J.L.: "La protección en las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional", *Trabajo y Derecho*, núm. 40, 2018, pp. 11 y ss. y DESDENTADO BONETE, A. y DESDENTADO DAROCA, E.: "La segunda sentencia del Tribunal Europeo de Derechos Humanos en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", *Información Laboral*, núm. 1, 2018 (BIB 2018/6059).

[85] STEDH de 9 de enero 2018. La línea de continuidad destacada por CASAS BAAMONDE, M.E.: "Informar antes de vigilar, ¿tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa digital? La necesaria intervención del legislador laboral", *cit.*, en especial pp. 111-116 o MOLINA NAVARRETE, C.: "De '*Barbulescu II*' a '*López Ribalda*': ¿qué hay de nuevo en la protección de datos de los trabajadores?", *Revista de Trabajo y Seguridad Social (CEF)*, núm. 419, 2018, pp. 136-146.

[86] RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, pp. 182 y ss. o PRECIADO DOMENECH, C.H.: "Comentario de urgencia a la STEDH de 9 de enero de 2018. Caso López Ribalda y otros c. España", *Información Laboral*, núm. 1, 2018 (BIB 2018/6060). Sobre la posibilidad de cámaras ocultas, el precedente dado por la STEDH de 5 de octubre de 2010, asunto *Köpke*.

[87] "Podía decirse, valga la simplificación, que los votos particulares discrepantes (...) concuerdan con la doctrina mayoritaria del TEDH", CASAS BAAMONDE, M.E.: "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", *cit.*, p. 118. La coincidencia también es resaltada por ROJO TORRECILLA, E.: "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)", *Derecho de las Relaciones Laborales*, núm. 2, 2018, p. 151.

[88] STC 25/2019, de 25 de febrero. Reclamando este cambio y a partir del contraste en la evolución entre la doctrina del TEDH y el TC, CABEZA PEREIRO, J.: "El necesario cambio en la jurisprudencia constitucional sobre vigilancia y control de mensajería electrónica de los trabajadores a la vista de la doctrina del TEDH", *Temas Laborales*, núm. 141, 2018, pp. 13-36.

[89] Cuya utilización explícita aparece en la STEDH de 25 de julio de 1997, asunto *Halford*; se recuerda, por ejemplo, en

cionamiento de la empresa que está sufriendo robos respalda su decisión de colocar cámaras, tanto para descubrir a los responsables de la conducta ilegal, como, también, para obtener las pruebas a utilizar en los subsiguientes procedimientos disciplinarios. En aras de la tutela a la libertad de empresa y el derecho de propiedad se justifica que, en el conflicto de derechos, no sea exigible ningún deber de información sobre la captación de tales datos ya que: primero, existían "sospechas razonables [la mera sospecha no sería bastante] de que se ha cometido una infracción grave [obediente a] una acción concertada por parte de varios empleados"; y, segundo, "informar a cualquier miembro del personal podría haber impedido alcanzar los objetivos perseguidos"[90].

Sopesando la limitación espacial y temporal de la medida, al igual que salvaguarda de la protección de la privacidad que los afectados podían esperar, se sienta que "el requisito de transparencia y el consiguiente derecho a la información son de naturaleza fundamental, particularmente en el contexto de las relaciones laborales, donde el empleador tiene poderes significativos con respecto a los empleados y se debe evitar cualquier abuso de esos poderes. Sin embargo (…), la provisión de información al individuo que se está vigilando y su alcance constituyen solo uno de los criterios a tener en cuenta para evaluar la proporcionalidad de una medida de este tipo en un caso dado. Si falta dicha información, las salvaguardas derivadas de los otros criterios serán aún más importantes".

Sirvan estas muestras jurisprudenciales en materia laboral, en una época de cambios trascendentes, para entender que, bajo las nuevas referencias normativas, con gran probabilidad la jurisprudencia del TEDH y la del TC habrán de evolucionar a la luz de los requerimientos contenidos en el nuevo Reglamento de Protección de Datos para la Unión Europea, el Reglamento (UE) 2016/679, de 27 de abril (RGPD), cuyos arts. 12 a 15 –y más en concreto los arts. 13 y 14– establecen la exigencia de una información de calidad que, en su texto, no admite excepciones.

Y este resulta ser un punto importante que, afectando al factor que puntualmente concita la atención, lo trasciende, por cuanto el RGPD, en virtud del TFUE, resulta ser "obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro"; es decir, la norma llamada de manera más directa y completa a desarrollar la Carta de Derechos Fundamentales (así asume el RGPD, en su art. 1, la llamada contenida en el art. 8 CDFUE), ya no a ofrecer una regulación de mínimos para una armonización, sino una regulación completa.

Construcción bajo la cual habrá de asegurarse que es el RGPD el que habilita a los Estados Miembros a completar su regulación[91], para así garantizar su eficacia y adaptar su contenido a las tradiciones jurídicas y diversos contextos nacionales; ajustándose, en todo caso, al límite de no cuestionar sus objetivos ni obstaculizar la armonización.

Relación entre el RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, que trae consigo un hecho inédito en este ámbito: al pasar aquel a ser fuente principal (lo cual explica su regulación tan detallada y que, bajo el rango de Reglamento, se ofrezca el cuerpo propio de una Directiva), y adquirir la Ley un papel complementario, la configuración del derecho fundamental, en

la STJEDH de 24 de abril de 1999, asunto *Huvig y Krusting*; y se consolida en STEDH de 3 de abril de 2007, asunto *Copland*.

[90] Sobre el conflicto de derechos en presencia y su justificación en este contexto concreto, comulgando, por tanto, con la tesis del TEDH, y considerando el interés del pronunciamiento "para nuestra desproporcionadamente garantista jurisprudencia laboral (que, a mi juicio, desprotege los derechos de los empleadores)"; al final, ponderando que "esta sentencia es una excelente oportunidad para modificar esta jurisprudencia", ALFARO ÁGUILA-REAL, J.: "La Gran Sala del TEDH en el caso López Ribalda", *Almacén de Derechos*, 17 de octubre de 2019, en https://almacendederecho.org/la-gran-sala-del-tedh-sobre-el-caso-lopez-ribalda/.

[91] STJUE de 11 de enero de 2001, asunto C-403/1998, *Monte Arcosu*.

tanto derecho de desarrollo legal, queda afectada de manera significativa[92].

No se trata solo de la primacía del art. 8 CDFUE sobre el art. 18.4 CE, confirmada ya en la Declaración 1/2004 del Tribunal Constitucional, de 13 de diciembre, cuando sentó que, *ex* art. 93 CE, la CDFUE goza de la primacía propia del Derecho de la Unión Europea y, en virtud del art. 10.2 CE, constituye pauta para la interpretación de las normas relativas a los derechos fundamentales y las libertades que la Constitución reconoce.

Procederá ir más allá, y no quedarse en ese umbral de mínimos europeo susceptible de desarrollo a nivel interno, pues "la convivencia del art. 8 CDFUE y el art. 18.4 CE está pacíficamente garantizada por vía hermenéutica, en la medida en que el derecho fundamental garantizado por el art. 18.4 CE va a ser directa y principalmente regulado por el RGPD, desplazándose el centro de protección del derecho fundamental a la interpretación que del art. 8 CDFUE haga el TJUE"[93]. Ello quiere decir, en breve –y entre otras consecuencias–, que el derecho de protección de datos queda garantizado conforme a lo previsto en el RGDP y, por vía prejudicial, por la jurisdicción europea; a sus resultas, que las instancias legislativa y jurisdiccional españolas habrán de ajustarse a la conformación dada de ese derecho europeo[94].

Así lo ha establecido el Tribunal de Justicia de la Unión Europea ante la alegación de que el art. 53 CDFUE autorice de forma general que un Estado miembro aplique el estándar de protección de los derechos fundamentales garantizado por su Constitución cuando sea más elevado que el de la Carta e ignore la aplicación de las disposiciones del Derecho de la Unión. Niega tal posibilidad con carácter general, aduciendo que "menoscabaría el principio de primacía del Derecho de la Unión, ya que permitiría que un Estado miembro pusiera obstáculos a la aplicación de actos del Derecho de la Unión plenamente conformes con la Carta, si no respetarán los derechos fundamentales garantizados por la Constitución de ese Estado". Añadiendo de manera firme, además, que: "cuando un acto del derecho de la Unión requiere medidas nacionales para su ejecución, las autoridades y tribunales nacionales siguen estando facultados para aplicar estándares nacionales de protección de los derechos fundamentales, siempre que esa aplicación no afecte al nivel de protección previsto en la Carta, según su interpretación por el Tribunal de Justicia, ni a la primacía, la unidad y la efectividad del derecho de la Unión"[95].

A la vista de todo lo expuesto, la imagen que cabe transmitir a día de hoy del derecho a la protección de datos muestra un núcleo esencial cuyo objeto (datos personales que identifiquen o permitan identificar a una persona) y un contenido (poder de control y disposición sobre sus datos personales) exige un haz de facultades definidas en el desarrollo de ese derecho por el RGPD (según demanda la Carta de Derechos Fundamentales de la Unión Europea) interpretadas por el Tribunal de Justicia. Todo ello sin perjuicio de la labor

[92] García Mexía, P.: "La singular naturaleza jurídica del Reglamento General de Protección de Datos de la UE. Sus efectos en el acervo nacional sobre protección de datos", en AA.VV. (Piñar Mañas, J.L., Dir.): *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Madrid (Reus), 2016, pp. 25-27; de similar parecer, Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, pp. 165 y ss.

[93] Rallo Lombarte, A.: "El nuevo derecho de protección de datos", *cit.*, p. 58.

[94] Por extenso, Matía Artilla, F.J.: "Primacía del Derecho de la Unión y derechos constitucionales. En defensa del Tribunal Constitucional", *Revista Española de Derecho Constitucional*, núm. 106, 2016, pp. 479 y ss. o Ugartemendía, J.I. y Ripol, S.: *El Tribunal Constitucional en la encrucijada europea de los derechos fundamentales*, San Sebastián (IVAP), 2017.

[95] STJUE de 26 de febrero de 2013, asunto C-300/11, *Melloni* (apartados 58 y 60, respectivamente). Un tan sucinto como expresivo comentario de las consecuencias prácticas a seguir de tal pronunciamiento y su proyección sobre todos los derechos recogidos en la Carta en Gordillo Pérez, L.I. y Tapia Trueba, A.: "Diálogos, monólogos y tertulias. Reflexiones a propósito del Caso Melloni", *Revista de Derecho Constitucional Europeo*, núm. 22, 2014, pp. 245 y ss.; en particular, pp. 266 y 267.

de complemento que asume la Ley Orgánica 3/2018, como desarrollo, a su vez, del art. 18.4 CE y de la labor hermenéutica atribuida al Tribunal Constitucional en esta reordenación trascendental de fuentes acaecida en los últimos años.

4. LA DELIMITACIÓN FUNCIONAL DEL DERECHO A LA PROTECCIÓN DE DATOS A PARTIR DE SU RELACIÓN CON LOS OTROS DERECHOS FUNDAMENTALES DESTINADOS A PROTEGER LA INDIVIDUALIDAD

En el pórtico del presente análisis se había acudido a dos expresiones harto gráficas para advertir sobre cómo la configuración del derecho a la protección de datos exige, como tarea primera, aquilatar su objeto y contenido; sin embargo, su dimensión última requerirá ponerlo en conexión con el resto de los derechos fundamentales, pues solo a partir de una adecuada ponderación de las relaciones que con aquellos mantenga cabrá aspirar a decantar su funcionalidad última.

Estas dos expresiones, "agujero negro que lo absorbe todo y no deja escapar nada de su entorno", y "posibilidad cierta, como tendencia, de que la protección de la privacidad abarque y 'se coma' a la intimidad", daban cuenta de una impresión de la cual participa un gran número de autores: la conversión de la protección de datos en el "derecho de todo" al calor de la amplitud de los conceptos de protección de datos y tratamiento, que se extiende a "cualquier información" (y en realidad todo es o al menos contiene informaciones) "relacionada con" (bajo la variable panoplia de tipos de vinculación existentes que imaginarse pudiere) una persona que a su través resulta "identificada o identificable"[96].

Lejos de sucumbir a tal inclinación, "en tanto conduce a una extensión no deseable de la protección de datos, al provocar un evidente desequilibrio en el régimen de garantías que en su conjunto deben proporcionar los derechos fundamentales"[97], preciso resultará convenir que, ni cabe seguir de la jurisprudencia europea y española que la protección de datos se diluya en una simple faceta más de la vida privada y familiar[98], ni tampoco que de su autonomía derive esa *vis expansiva* capaz de ensombrecer la operatividad de otros derechos[99].

De hecho, y dado el objeto y contenido tan amplio con el que la norma dibuja sus perfiles, resulta sencillo colegir los elementos de contacto que se pueden producir con la práctica totalidad de los restantes derechos fundamentales –u ordinarios–, como recoge el Tribunal Constitucional tras esa afirmación de su doble funcionalidad, no en vano está llamado a ser un "instituto de garantía para otros derechos, fundamentalmente el honor y la intimidad" y, a la vez, "en sí mismo, un derecho o libertad fundamental"[100].

---

[96] A partir de los ejemplos que proporcionan, sobre tales términos, las SSTJUE de 6 de noviembre de 2003, asunto C-101-01, *Linqvist*; 17 de julio de 2014, asuntos acumulados C-141/12 y C-372/12, *YS y otros*; 19 octubre 2016, asunto C-582/14, *Breyer*; o, en una última muestra, 20 diciembre 2017, asunto C-434/16, *Nowak*. Muy fundado parecer que, a su calor, proporciona PURTOVA, N.: "The law of everything. Broad concept of personal data and feature of EU data protection law", *Law, Innovation and Tecnnology*, Vol. 10, núm. 1, 2018, pp. 40-81; la referencia a las "consecuencias desproporcionadas" especialmente en pp. 61-68.

[97] BRKAN, M.: "The unstoppable expansion of the EU fundamental right to data protection: little shop of horrors?", *Maastrich Journal of European and Comparative Law*, Vol. 23, núm. 5, 2012, mereciendo especial atención al resumen conclusivo contenido en pp. 837 y 838.

[98] DE HERT, P. y GUTWIRTH, S.: "Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action", en AA.VV. (GUTWIRTH, S. *et alii*, Eds.): *Reinventing data protection*?, *cit.*, pp. 19-25.

[99] Sobre tal tentación, así como sus consecuencias, VAN DER SLOOT, B.: "Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation", *International Data Privacy Law*, Vol. 4, núm. 4, 2014, en particular pp. 320 y 321.

[100] Premisa en el sugerente y original análisis de HERNÁNDEZ CORCHETE, J.A.: "Expectativas de privacidad, tutela de la intimidad y protección de datos", en AA.VV. (DE LA QUADRA-SALCEDO, T. y PIÑAR MAÑAS, J.L., Dirs. y BARRIO ANDRÉS, M. y TORREGROSA VÁZQUEZ, J., Coords.): *Sociedad digital y Derecho*, Madrid (Agencia Estatal del BOE), 2018, en especial pp. 283-285.

Desde el primero de los planos, no cabrá olvidar que lo instrumental no puede aspirar nunca a ocupar el espacio del interés, bien o derecho principal al cual ayuda a completar; por tanto, y lejos de un conflicto, cuanto procederá apreciar es una relación de complementariedad[101]. Desde el segundo, "como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona"[102], ha lugar a ese entronque con la raíz común a todos los derechos, fundamentales o no: la dignidad y el libre desarrollo de la personalidad, constituidos "en el punto de referencia de todas las facultades que se dirigen al reconocimiento y afirmación de la dimensión moral de la persona"[103].

Valor superior y principio general que actúa tanto de fundamento, orientación en la interpretación e integración del ordenamiento, como de norma de conducta y límite en el ejercicio de los derechos[104], su proyección axiológica se tiñe bajo la singularidad de cada uno de ellos, y al igual que se ha reconocido de manera expresa en el derecho a la protección de datos, acaece en aquellos con los que esta pudiera entrar en colisión, debiendo atender a la esencia de cada uno para resolver, siempre en cada contexto en cuestión, cuál es el llamado a primar, convertido así en un límite concreto para aquel llamado a ceder en la concreta ocasión[105].

Constan ya a lo largo del discurso algunos ejemplos en los cuales el derecho la protección de datos ha primado sobre la intimidad[106], y algunos más en los cuales ha debido ceder ante otros como el derecho a la propiedad[107]. Cabría añadir varios más en los que se detecta igual conflicto en referencia también a la intimidad[108], a la propiedad (derechos de autor)[109] o la libertad de información o expresión[110], y, por supuesto, cabría imaginar hipótesis de muy variado tipo y con muy heterogénea mezcla de derechos.

Con todo, preciso será dejar noticia de que, junto con la intimidad, probablemente la relación mejor definida del derecho a la protección de datos sea la trabada con la libertad sindical; mostrado, en función de las circuns-

[101] BRKAN, M.: "The unstoppable expansion of the EU fundamental right to data protection: little shop of horrors?", *cit.*, pp. 818-820. Sobre las implicaciones de esa faceta instrumental, ALEGRE MARTÍNEZ, M.A.: "Artículo 18 CE: la protección constitucional de la individualidad", en AA.VV. (VILLANUEVA TURNES, A., Coord.): *Derechos fundamentales (Aspectos básicos y actuales)*, Santiago de Compostela (Andavira), 2017, pp. 203 y 204.

[102] PÉREZ LUÑO, A.E.: *Derechos humanos, Estado de Derecho y Constitución*, 13ª ed., Madrid (Tecnos), 2019, p. 49.

[103] ALEGRE MARTÍNEZ, M. A.: *La dignidad de la persona como fundamento del ordenamiento constitucional español*, León (Universidad de León), 1996, p. 15.

[104] Cada una de estas facetas en GONZÁLEZ PÉREZ, J.: *La dignidad de la persona*, 3ª ed., Madrid (Aranzadi/Thomson), 2017, pp. 112-126.

[105] LYNSKEY, O.: *The foundations of EU Data Protection Law*, Oxford (Oxford University Press), 2015, Parte II, apartado 5, pp. 135-160.

[106] Con el pronunciamiento donde se reconoce el carácter autónomo del derecho recogido en el art. 18.4 CE a la cabeza, STC 292/2000, de 30 de noviembre. En variante donde se aprecia el consentimiento informado previo a una prueba biológica, SSTC 5/2008, de 7 de enero y 135/2014, de 8 de septiembre; la utilización de ADN con fines identificativos en STC 199/2013, de 5 de diciembre.

[107] STEDH 17 de octubre de 2019, asunto *López Ribalda II*. Interesantes las observaciones que casi diez años antes efectuaron, en un sentido muy semejante, YU, X. y ZHAO, Y.: "Dualism in data protection: balancing the right to personal data and the data property right", *Computer Law & Security Review*, Vol. 35, núm. 5, 2010, en https://www.sciencedirect.com/science/article/pii/S0267364918304369.

[108] SSTC 43/2009, de 12 de febrero, y 169/2011, de 3 de noviembre. La primera en torno al dato de la adscripción política de un candidato electoral. Respecto del cual ningún poder de disposición corresponde al interesado; la segunda estableciendo que quien voluntariamente decide apoyar con su firma la presentación de una candidatura, ni está siendo obligado a declarar sobre su ideología, ni los datos personales que ha de facilitar afectan a la intimidad del avalista. Sobre la forma de transmitir los datos con trascendencia tributaria en poder de las Administraciones, STC 233/1999, de 16 de diciembre.

[109] STJUE de 19 de abril de 2012, asunto C-461/10, *Bonnier*, sosteniendo que en los supuestos de derechos de autor cabe requerir al proveedor de acceso a internet para que comunique la identidad del abonado respecto a la cesión de datos bancarios, STC 96/2012, de 7 de mayo.

[110] STEDH de 10 de mayo de 2011, caso *Mosley*, y, como variante de la libertad de prensa, STEDH de 21 de septiembre de 2010, caso *Polanco Torres* y *Movilla Polanco*.

tancias, otra vez esa "doble cara"[111]: "lo que significa que, en supuestos como el presente, el artículo citado [18.4 CE] es, por así decirlo, un derecho instrumental ordenado a la protección de otros derechos fundamentales, entre los que se encuentra, desde luego, la libertad sindical"; sin embargo, y ahora como derecho autónomo, "trata de evitar que la informatización de datos personales propicie comportamientos discriminatorios", como, por ejemplo, la utilización de "un dato sensible que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio de libertad sindical"[112]. En definitiva, y según ha dejado ver la doctrina en numerosas ocasiones, el potente haz de garantías que acompaña al desarrollo del art. 18.4 puesto al servicio del derecho consagrado en el art. 28 CE[113], sin perjuicio del relieve propio que pudiera merecer la autodeterminación informativa en las variadas situaciones en las que la libertad sindical esté en juego[114].

Pero, de seguro, las mayores dificultades para el deslinde afectarán al resto de los derechos ubicados en el art. 18 CE, pues, según ha quedado expuesto, solo una visión simplista sobre la interpretación que del art. 8 CEDH han efectuado los órganos judiciales europeos podría llevar a entender que la vida privada y familiar absorbe por entero el derecho a la protección de datos. Aunque ciertamente hubiera sido deseable que tras la entrada en vigor del Tratado de Lisboa se hubiera profundizado en la distinción que sí se establece en los arts. 7 y 8 CDFUE[115], una lectura atenta de los últimos pronunciamientos permite localizar rasgos suficientes para apreciar cómo, bajo el literal de aquellos razonamientos, los derechos del art. 8 CEDH se descomponen en la serie de derechos fundamentales de la personalidad que en la Constitución Española vienen referidos al honor, la intimidad personal y familiar y a la propia imagen (art. 18.1), al secreto de las comunicaciones (art. 18.3) y al derecho a la protección de datos (art. 18.4)[116].

De este modo, cabrá aspirar a trazar un cuadro en el cual, de la mano de la jurisprudencia europea y constitucional, quepa clarificar la urdimbre de relaciones establecidas entre los que han sido calificados como derechos de la individualidad, o lo que es igual, la delimitación armonizadora de los espacios privativos o característicos[117] que, sin perjuicio de

[111] RODRÍGUEZ ESCANCIANO, S.: *Poder de control empresarial, sistemas tecnológicos y derechos fundamentales*, Valencia (Tirant Lo Blanch), 2015, p. 237 y ss.

[112] Literal luego tantas veces reproducido que anuncia de la STC 11/1998, de 13 de enero.

[113] CRUZ VILLALÓN, J.: *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador*, Albacete (Bomarzo), 2019, p. 23.

[114] Entre muchas, y además de las *supra* mencionadas, cabría remitir a las reflexiones que al respecto efectúan TRONCOSO REIGADA, A.: "Libertad sindical, libertad de empresa y derecho a la intimidad y a la protección de datos de los trabajadores", en AA.VV. (FARRIOLS I SOLÁ, A.): *La protección de datos de carácter personal en los centros de trabajo*, Madrid (Cinca/Fundación Largo Caballero), 2006, pp. 103 y ss.; RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales de los trabajadores como garantía de la libertad sindical", *Revista General de Derecho del Trabajo y de la Seguridad Social*, núm. 27, 2011, pp. 46 y ss.; RUIZ CASTILLO, M.M.: "Intimidad, protección de datos y libertad sindical: sentencia 11/1998, de 13 de enero", en AA. VV. (GARCÍA MURCIA, J., Dir.): *Libertad sindical y otros derechos de acción colectiva de trabajadores y empresarios: 20 casos de jurisprudencia constitucional*, Cizur Menor (Aranzadi/Thomsom), 2014, pp. 261 y ss. o NAVARRO NIETO, F.: "El ejercicio de la acción sindical a través de las tecnologías de la información y las comunicaciones", *Temas Laborales*, núm. 138, 2017, en particular p. 76. Sobre el detalle de las muy variadas situaciones en presencia (derecho de información y consulta, ejercicio de la actividad sindical, remuneraciones, copia básica de los contratos, censo electoral, crédito horario, cuota sindical, cesiones a representantes unitarios o sindicales, etc.), aportando no solo resoluciones judiciales, sino interesantes criterios de la Agencia Española de Protección de Datos que han de servir para resolver los diferentes conflictos en presencia, DOMENECH, C.H.: *El derecho a la protección de datos en el contrato de trabajo*, *cit.*, pp. 356 y ss.

[115] LYNSKEY, O.: "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, Vol. 3, núm. 3, 2014, pp. 573 y 574.

[116] CASAS BAAMONDE, M.E.: "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", *cit.*, pp. 104 y 105.

[117] Sobre esta propuesta como alternativa al "conflictivismo", la sugerente propuesta de APARICIO ALDANA, R.K.: *Los de-*

su modulación en el contexto dado (o por la constitucionalización de nuevos derechos digitales[118]), llevarán a su aplicación preferente[119]:

A.– En relación con la intimidad, el dato apuntado por el Tribunal Constitucional sobre la incardinación durante bastante tiempo de la protección de datos en el derecho contemplado en el art. 18.1 CE da cuenta de la existencia de importante ámbito objetivo donde coincide o se puede solapar la intervención de ambos derechos fundamentales.

Este vínculo, que permanecerá siempre, no impide descubrir los elementos diferenciales patentes, situados por el Tribunal Constitucional en el objeto y contenido más extenso del derecho a la protección de datos, y que también deja entrever el TEDH como una especie de "valor añadido" conferido por la atribución del derecho a un mayor control sobre más tipos de datos[120].

En este sentido, la intimidad encuentra su espacio característico en garantizar un ámbito reservado de la vida (corporal[121], personal[122] y familiar[123]) que resulta imprescindible para que el titular mantenga su dignidad como persona; por su parte, el derecho a la protección de datos va más allá de ese deber de abstención, para extender la tutela a todos los datos, cualesquiera sea su naturaleza (sean o no "íntimos" y de origen público como privado), que resulten relevantes o incidan en el ejercicio de un derecho, no importa si fundamental o no, siempre y cuando hayan sido objeto de un tratamiento. Convirtiendo, a tal fin, la noticia fidedigna del uso y destino de la información personal y el consentimiento de afectado en elementos clave para medir su respeto o conculcación.

De prestar atención a la línea hermenéutica del TEDH, aunque sea menos clara, cabrá descubrir que el círculo de la intimidad, encerrado en el círculo más amplio de la protección de datos, es semejante al doble paso que siempre acompaña a su jurisprudencia respecto al derecho a la vida privada y familiar: en primer lugar, ponderar si existe un interés en proteger la privacidad; más tarde, examinar si obra o no una afectación del interés protegible. Algo que no es necesario cuando, fuera de ese primer círculo más restringido, cuanto ocurre es que se utilizan datos de la persona sin su consentimiento informado, pues el interés protegible resulta afectado sin necesidad de mayor indagación, excepto si se trate de alguna de las excepciones previstas a su común exigencia.

La perspectiva anterior se completa tomando en consideración cómo "la funcionalidad del derecho a la intimidad es defensiva, frente a la activa o de disposición relativa a la apreciación de datos"[124]. Quienes más han

rechos fundamentales en la relación laboral: una alternativa al conflictivismo, Tesis Doctoral, Madrid (Universidad Rey Juan Carlos), 2015, en https://www.educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=PLqTcDsuJ1k%3D

[118] Ilustrativa la sugerencia que al respecto eleva, por ejemplo, RALLO LOMBARTE, A.: "Nuevas tecnologías, nuevos derechos", en AA.VV. (PENDÁS, B., Dir. y GONZÁLEZ, E. y RUBIO, R. Coords.): *España constitucional (1978-2018). Trayectorias y perspectivas*, T. II, Madrid (Centro de Estudios Políticos y Constitucionales), 2018, pp. 2378 y 2379.

[119] Interesante información sobre situaciones de conflicto resueltas por los Tribunales, con aportación de resúmenes de cuantiosas sentencias en GAMELA CARBALLO, S. (Ed. Lit.): *Derecho al honor, intimidad y propia imagen en relación con las nuevas tecnologías*, Las Rozas (Sepín), 2018.

[120] En la sugerente perspectiva que ofrece LYNSKEY, O.: "Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *cit.*, p. 574.

[121] "Frente a toda indagación o pesquisa que sobre el cuerpo quiera imponerse contra la voluntad de la persona, cuyo sentimiento o pudor queda así protegido por el ordenamiento, en tanto responda a criterios arraigados en la cultura de la comunidad", SSTC 37/1989, de 15 de febrero, y 218/2002, de 25 de noviembre.

[122] "Existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario –según las pautas de nuestra cultura– para mantener una calidad mínima de la vida humana", SSTC 231/1988, de 2 de diciembre y 179/1991, de 19 de septiembre, entre otras.

[123] "Aspectos de la vida de otras personas con la que se guarda una especial y estrecha vinculación (...); aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 CE protegen", STC 231/1988, de 2 de diciembre.

[124] Coincidiendo a la hora de destacar este dato, SAN MARTÍN ALCÁZAR, M.T.: "La protección de datos: el nuevo derecho fun-

profundizado en este rasgo no dudan en destacar que en esta finalidad diferente radica la diferencia sustancial en los instrumentos de protección de uno y otro derecho, no en vano la protección de datos ha de servir a un doble propósito tácito[125]: de un lado, reducir sensiblemente el temor a la existencia de consecuencias negativas o repercusiones indeseadas derivadas del ejercicio de un derecho; de otro, reducir las posibilidades de que se adopten decisiones fundadas sobre circunstancias personales cuya revelación no esté justificada y pudieran traer aparejadas consecuencias discriminatorias directas o indirectas.

Provocará, en consecuencia, un doble efecto tutelar que excede cualquier planteamiento desde el derecho a la intimidad: de un lado, si la revelación de datos personales es motivo para inhibir o retraer a la persona de ciertas conductas (una suerte de efecto "panóptico"[126]), la autodeterminación informativa está en disposición de actuar en el sentido inverso, ayudando al libre desarrollo de la personalidad; de otro, se adecuarían las asimetrías en el manejo de la información, susceptibles de ser traducidas en asimetrías de poder[127], por cuanto el derecho a la protección de datos, a través de los principios de consentimiento y finalidad, proporcionaría una tutela a quien socialmente aparece como más débil que no sería posible sin su reconocimiento y garantía a través de una norma propia[128].

La lectura anterior, con todo, nunca podrá prescindir del círculo interior dado por la intimidad –aun cuando sí pueda y deba proceder a reconfigurarlo[129]–, que la Ley 3/2018 refuerza de manera expresa cuando, colmando una laguna legal patente[130], procede a regular el derecho a la educación digital mediante un aprendizaje "que sea seguro y respetuoso ante la dignidad humana, los valores constitucionales, lo derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales" (art. 83.1); de igual modo, el derecho de rectificación en Internet cuando los usuarios atentan contra el derecho al honor, la intimidad personal y familiar y el derecho a comunicar o recibir libremente información veraz por esta vía (art. 85.2). Pero, sobre todo, presenta a la intimidad como un valor en alza dentro del ámbito laboral, pues, además de reconocer el derecho a la desconexión digital fuera del tiempo de trabajo a fin de garantizar –entre otros bienes y derechos– "su intimidad personal y familiar" (art. 88.1), pone límites al ejercicio del poder de supervisión empresarial que se dirigen de manera expresa a salvaguardar el derecho a la intimidad de los trabajadores tanto en el uso de dispositivos digitales puestos a disposición por el empleador (art. 87), como frente a dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89) o respecto al empleo de sistemas de geolocalización en el ámbito laboral (art. 90). Más aun, y a través de la disp. adicional 13ª, añade un art. 20 *bis* para recoger en la norma sustantiva laboral cuanto proclama en la destinada a regular la protección de datos –e igual proceder sigue para los empleadores públicos con el añadido de una letra j) *bis* al

damental del siglo XXI", *Revista Jurídica de la Comunidad de Madrid*, núm. 10, 2001, pp. 120 y 121 o García Coca, O.: *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, *cit.*, p. 37.

[125] Baz Rodríguez, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, p. 70.

[126] El planteamiento aparece ampliamente desarrollado en Mercader Uguina, J.R.: "Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?", *Relaciones Laborales*, núm. 1, 2001, pp. 665-686.

[127] Pérez Luño, A.E.: *Los derechos humanos en la sociedad tecnológica*, Madrid (Universitas), 2012, pp. 138 y ss.

[128] Siguiendo el discurso de Baz Rodríguez, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, p. 72.

[129] Algunas propuestas en Martínez de Pisón Cavero, J.: "Vida privada sin intimidad. Una aproximación a los efectos de las intromisiones tecnológicas en el ámbito íntimo", *Derechos y Libertades*, núm. 37, 2017, pp. 51 y ss.

[130] El apunte de tal laguna en Carrillo, M.: "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación" y Revenga Sánchez, M.: "El derecho a la intimidad: un derecho en demolición (y necesitado de reconstrucción)", ambos en AA.VV.: *El derecho a la privacidad en un nuevo entorno tecnológico*, *cit.*, pp. 11 y ss. y 99 y ss., respectivamente.

art. 14 EBEP mediante la disp. adicional 14ª–: "los trabajadores tienen derecho a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales"[131].

B.– La práctica totalidad de los autores españoles que acometen el análisis relacional aquí emprendido ni siquiera se plantean la eventual colisión de la protección de datos con el honor, en gran medida por constituir este un concepto tan indeterminado como extrajurídico y cambiante que ciertamente resulta difícil determinar su contenido y las facultades que otorga a su titular[132]. Destacan en él tanto el aspecto negativo (conductas que lo lesionan), situado en "ataques o intrusiones que (…) provocan el desmerecimiento en la consideración ajena"[133], como el positivo de "amparar la buena reputación"[134] y el "prestigio profesional"[135]. Doble base sobre la cual el Tribunal Constitucional proporciona una triple clave para su separación del derecho a la protección de datos: en primer lugar, el hecho de que, como "la intimidad (…), son realidades intangibles cuya extensión viene determinada en cada sociedad y en cada contexto histórico"[136], lo cual se contrapone abiertamente a la tangibilidad como cualidad intrínseca al dato a proteger[137]; en segundo término, su limitación a unos datos concretos consistentes en "expresiones" o "mensajes" portadores del descrédito[138], frente al carácter mucho más amplio del dato personal como objeto en sí mismo de protección jurídica; por último, la distinta finalidad a la que cada uno sirve, en los términos en los que han quedado delimitados sus respectivos objetos[139].

C.– El derecho a la propia imagen ha sido entendido como aquel "que atribuye a su titular un derecho a delimitar la información gráfica generada por sus rasgos físicos personales que puede tener difusión pública. La facultad otorgada por este derecho consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad –informativa, comercial, científica, cultural, etc.– perseguida por quien la capta o difunde"[140].

Bajo tal acepción, no cabe duda de que la imagen constituye un dato de carácter personal por sí misma (art. 5 RGPD), lo cual, en línea de principio, llevará a que su tratamiento se ajuste a la normativa al respecto, proporcionándole al titular una serie de garantías que refuerzan su posición como ciudadano[141], de manera tal que, aun cuando en

[131] Un temprano comentario resaltando la revalorización del derecho a la intimidad en su relación con la protección de datos en RODRÍGUEZ ESCANCIANO, S.: "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley*, núm. 9328, 2 de enero de 2019, Editorial, p. 3, también QUÍLEZ MORENO, J. M.: "La garantía de derechos digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores", *Revista Española de Derecho del Trabajo*, núm. 217, 2019, pp. 217 y ss.

[132] Por referencia al propio literal del art. 2.1 Ley Orgánica 1/1982 y las consideraciones al respecto incluidas en la STC 223/1992, de 14 de diciembre, CHINCHILLA MARTÍN, C.: "El derecho al honor en la jurisprudencia del Tribunal Constitucional", en AA.VV.: *Honor, intimidad y propia imagen*, Madrid (Ministerio de Justicia e Interior), 1995, p. 107 o GÓMEZ SÁNCHEZ, Y.: *Derechos fundamentales*, Cizur Menor (Aranzadi/Thomson), 2018, pp. 265-267.

[133] STC 176/1995, de 11 de noviembre.

[134] SSTC 49/2001, de 26 de febrero y 216/2006, de 3 de julio.

[135] STC 1250/1999, de 11 de octubre.

[136] STC 171/1990, de 12 de noviembre.

[137] HERRERA DE LAS HERAS, R.: *Responsabilidad civil por vulneración del derecho del honor en las redes sociales*, Madrid (Reus), 2017, pp. 43-47.

[138] SSTC 176/1995, de 11 de diciembre; 49/2001, de 26 de enero o 216/2006, de 3 de julio.

[139] En aplicación a las listas negras, por ejemplo, CRUZ VILLALÓN, J.: *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador*, *cit.*, p. 60.

[140] Seguida luego de otras muchas, sirva el tenor de la STC 8/2001, 26 marzo 2001; sobre la variabilidad de contenidos del derecho, ALEGRE MARTÍNEZ, M.A.: *El derecho a la propia imagen*, Madrid (Tecnos), 1997, pp. 91 y ss.

[141] CÓRDOVA CASTROVERDE, D. y DÍEZ-PICAZO GIMÉNEZ, L.M.: "Reflexiones sobre la protección de la privacidad en un entorno digital", *cit.*, pp. 102 y 103.

muchos casos "no pueda decidir sobre la captación de su imagen, al menos tendrá el derecho a conocer la existencia de los dispositivos de captación y ejercitar una amplia gama de derechos para su protección"[142].

La evidente relación de género a especie que cabe apreciar en esta ocasión no impide destacar los elementos de separación, provenientes de la distinta regulación, pues mientras que para la operatividad de la normativa que desarrolla el derecho a la protección de datos es preciso que actúe algún tipo de tratamiento, la vulneración del derecho a la propia imagen puede tener lugar por cualquiera de las formas previstas en los arts. 7.5 y 6 de Ley Orgánica 1/1982, de 5 de mayo, siempre que no se obtenga la conformidad del titular de la imagen y la actividad vaya encaminada a una cesión y difusión a terceras personas[143]. En consecuencia, aun cuando sean ocasiones residuales (y lo normal –conforme ocurre con el resto de los derechos contemplados en el art. 18.1– es que así sea), si concurriera alguno de los supuestos previstos en los apartados del precepto mencionado sin haber tenido lugar ninguna forma de tratamiento, cabría aludir a un atentado contra el derecho a la propia imagen sin aplicación del derecho de protección de datos[144].

D.– El derecho al secreto de las comunicaciones protege, de manera implícita, su libertad; de forma explícita, su reserva frente a la interceptación por cualquier sistema o su conocimiento antijurídico por personas ajenas. De este modo, garantiza su carácter impenetrable por terceros, tanto respecto de su contenido, como de la identidad de los comunicantes, así como de otros aspectos externos, con independencia de su carácter íntimo y mientras el proceso de comunicación esté abierto[145].

Así concebido, y aun cuando la Constitución se refiera "especialmente" a las comunicaciones postales, telegráficas y telefónicas, no cabe la menor duda que también incluye las electrónicas[146], motivo por el cual, de nuevo, obra un importantísimo espacio de intersección entre los derechos reconocidos en los apartados 3 y 4 del art. 18 CE[147].

En esta ocasión, y en virtud de haber entendido en el sentido tan amplio que se ha expuesto el secreto de las comunicaciones, y haberlo situado, además, como una barrera de protección sin cuya efectividad se podría vaciar de contenido el sistema entero de derechos fundamentales, obra una coincidencia básica en el planteamiento del TEDH y en el del Tribunal Constitucional, destacando

---

[142] GÓMEZ CORONA, E.: *La propia imagen como categoría constitucional*, Cizur Menor (Aranzadi/Thomson), 2014, pp. 158 y 159. Sobre su criterio, el literal de ARRÚE MENDIZÁBAL, M.: *El derecho a la propia imagen de los trabajadores*, Cizur Menor (Aranzadi/Thomson), 2019, p. 60, con extenso desarrollo en pp. 376 y ss.

[143] GARCÍA COCA, O.: *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, *cit.*, p. 42.

[144] APARICIO SALOM, J.: "El derecho a la imagen y a la protección de datos", *Aranzadi de Derecho y Nuevas Tecnologías*, núm. 7, 2005, pp. 26-28 o REBOLLO DELGADO, L.: "La imagen como dato", *Anuario de la Facultad de Derecho* (Universidad de Alcalá), núm. 2, 2009, pp. 196-202.

[145] SSTC 114/1984, de 29 de noviembre; 241/2012, de 17 de diciembre o 170/2013, de 7 de octubre. Sobre todos y cada uno de estos extremos, MARTÍN MORALES, R.: *El régimen constitucional del secreto de las comunicaciones*, Madrid (Civitas), 1995, pp. 40 y ss. o RODRÍGUEZ RUIZ, B.: *El secreto de las comunicaciones: tecnología e información*, Madrid (McGraw Hill), 1998, pp. 17 y ss. Una dura crítica al contenido del fallo a partir de la relación entre intimidad y secreto de las comunicaciones en CARDONA RUBERT, M.B.: "Reinterpretación de los derechos de intimidad y secreto de las comunicaciones en el modelo constitucional de relaciones laborales: un paso atrás. Comentario a la STC 241/2012, de 17 de septiembre", *Revista de Derecho Social*, núm. 60, 2012, pp. 169 y ss. y CABEZA PEREIRO, J.: "El necesario cambio en la jurisprudencia constitucional sobre videovigilancia y control de mensajería electrónica de los trabajadores a la vista de la doctrina del TEDH", *cit.*, pp. 21-29.

[146] Concluyente el tenor de las SSTC 70 y 123/2002, de 3 de abril y 20 de mayo. De este modo, queda claro que el objeto de protección es tanto el contenido como el soporte, sin alcanzar, por ende, ni a la comunicación directa, ni a la que rige entre los propios comunicantes; al respecto, SÁNCHEZ TRIGUEROS, C. y CUADROS GARRIDO, M.E.: "Autodeterminación informativa: un derecho en alza", *cit.*, p. 89. Sobre su operatividad en algunos supuestos de comunicación directa, APARICIO ALDANA, R.K.: *Los derechos fundamentales en la relación laboral: una alternativa al conflictivismo*, *cit.*, pp. 343 y 344.

[147] SEPÚLVEDA GÓMEZ, M.: "Los derechos fundamentales inespecíficos a la intimidad y al secreto de las comunicaciones y el uso del correo electrónico en la relación laboral. Límites y contra límites", *Temas Laborales*, núm. 122, 2013, p. 210.

este último que el derecho reconocido en el art. 18.3 CE presenta la "versatilidad necesaria para ofrecer una suerte de defensa adelantada que solo dependerá de un dato objetivo: la existencia de comunicación"[148].

Podría haber inclinado su parecer en favor de la realización o no de algún tratamiento de datos (pues, como afirma de manera concluyente la jurisprudencia, si las comunicaciones identifican a una persona o permiten hacerlo por el medio a través del que se realiza o por su contenido, se trataría, evidentemente, de datos personales[149]), para así llevar a la aplicación del art. 18.4 CE[150]. Ha preferido, empero, acudir a esa vía de tutela más temprana o previa que puede ofrecer el derecho al secreto de las comunicaciones, bajo la convicción de que "en una sociedad tecnológicamente avanzada como la actual (…) constituye no solo garantía de libertad individual, sino instrumento de desarrollo cultural, científico y tecnológico colectivo"[151].

Esta primacía –que resulta implícita, también, en los argumentos de la más reciente jurisprudencia del TEDH[152]– es mantenida sin fisuras por el Tribunal Constitucional a la hora de abordar la cuestión[153], lo cual no empece, en absoluto, que se pueda aplicar también la normativa en vigor sobre protección de datos, en particular por cuanto hace a los requisitos de trasparencia y –en su caso– consentimiento informado, pero al servicio del derecho cuya procedencia aplicativa se ha impuesto por vía tácita[154].

***

Finalizado este breve recorrido, cabrá concluir destacando que el análisis del derecho a la protección de datos ofrece un balance teñido de la provisionalidad dada por su rapidísima evolución, en un proceso que dista de haber alcanzado su fin. Preciso será seguir atendiendo a la configuración de los elementos esenciales sobre los que se asienta su autonomía, así como sopesando su carácter de "derecho europeo" en atención a las fuentes que lo regulan de manera directa (sin menospreciar, por supuesto, el valor complementario de la norma y jurisprudencia nacionales); al tiempo, y como nota derivada, el sistema de relaciones que traba con otros derechos constitucionales, en atención, siempre, a los distintos contextos que enriquecen el mosaico de su realidad con las variadísimas con teselas de las circunstancias presentes en cada ocasión.

---

[148] MARTÍNEZ MARTÍNEZ, R.: "Secreto de las comunicaciones v. protección de datos en el ámbito laboral. A propósito de la Sentencia 281/2005 del Tribunal Constitucional Español y del Informe 101/2008 de la Agencia Española de Protección de Datos", *Aranzadi Social*, núm. 13, 2008, p. 101. En tal sentido, igualmente, PÉREZ DE LOS COBOS ORIHUEL, F. y GARCÍA RUBIO, M.A.: "El contrato empresarial sobre las comunicaciones electrónicas del trabajador: criterios convergentes de la jurisprudencia del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos", *Revista Española de Derecho del Trabajo*, núm. 196, 2017, pp. 41 y 54.

[149] STEDH de 2 de agosto de 1984, asunto *Malone*, o SSTC 114/1984, de 29 de noviembre y 123/2002, de 20 de mayo.

[150] En defensa de tal criterio, GARCÍA COCA, O.: *La protección de datos de carácter personal en los procesos de búsqueda de empleo*, *cit.*, p. 39 y DEL PINO PADRÓN, M.C.: "El impacto de las tecnologías de la información en el Derecho Laboral, especial referencia a la intimidad del trabajador y el secreto de sus comunicaciones", *Cadernos de Dereito Actual*, núm. 8, 2017, p. 160.

[151] STC 133/2002, de 20 de mayo.

[152] STEDH de 22 de enero de 2018, asunto *Libert*; igual apreciación en MOLINA NAVARRETE, C.: "El derecho a la vida privada de los trabajadores en el Tribunal Europeo de Derechos Humanos: ¿diálogo o conflicto con la jurisprudencia nacional?", *Temas Laborales*, núm. 145, 2018, p. 142 o NAVARRO NIETO, F.: "El alcance del derecho al respeto de la correspondencia del trabajador en la jurisprudencia del Tribunal Europeo de Derechos Humanos", *Temas Laborales*, núm. 145, 2018, pp. 163 y 172. Sobre la proyección que luego habrá de seguirse en el Tribunal de Justicia de la Unión Europea, PIÑAR MAÑAS, J.L. y RECIO GALLO, M.: *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, Madrid (Wolters Kluwer), 2018, pp. 25 y 26.

[153] Así lo destaca SANTIAGO REDONDO, K.M.: "Intimidad, secreto de las comunicaciones y protección de datos de carácter personal. El art. 18 CE", *Relaciones Laborales*, núm. 1, 2014, pp. 122-124.

[154] RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, pp. 175 y ss. o LLAMOSAS TRÁPAGA, A: *Relaciones laborales y nuevas tecnologías de la información y la comunicación: una relación fructífera no exenta de dificultades*, Madrid (Dykinson), 2015, pp. 98-150

RESUMEN La evolución del derecho a la protección de datos ha llevado, en menos de cincuenta años, a una transformación tan evidente que incluso sorprende en su comparación con otros derechos de tercera generación. Frente a la tendencia norteamericana que vinculaba a la intimidad (en su sentido más amplio de privacidad) los peligros para los bienes e intereses de la persona en la recogida, tratamiento y uso de los datos, la interpretación de los Tribunales en los distintos Estados europeo-continentales se ha venido inclinando por vincular el contenido de las leyes nacionales en la materia con los derechos de la personalidad, asentados sobre la dignidad y el libre desarrollo de la personalidad. Inspiración para que las Constituciones más modernas le dediquen una mención específica y, en la mayor parte de las ocasiones, configuren un derecho con entidad propia.

Tras ese desarrollo subyace un movimiento internacional que arranca de las Directrices de la OCDE de 1980 y el Convenio núm. 108 del Consejo de Europa, textos en los cuales la influencia norteamericana explica la conexión instrumental o subsunción de la protección de datos en otros derechos, como de manera significativa ocurrió en España, donde la referencia contenida en el art. 18.4 CE durante sus primeros años de vigencia encontró desarrollo a través del derecho a la intimidad del art. 18.1 CE.

Construcciones como el derecho a la autodeterminación informativa, difundido en su formulación por el Tribunal Constitucional alemán, incidieron de manera notable en el resultado que ofreció la Directiva 95/46/CE, dando pie a nuevas claves para la lectura de un derecho que expresamente se reconocen como de configuración legal.

Se avanza así, de manera decidida, hacia la consideración como un derecho autónomo, que en el ámbito internacional tiene lugar con la separación entre el derecho a la vida privada y familiar y el derecho a la protección de datos recogida en la Carta Derechos Fundamentales de la Unión Europea. En el ámbito nacional a través de reconocimiento de tal naturaleza por el Tribunal Constitucional, en tanto derecho autosuficiente al que se dota de un objeto específico, situado en los datos personales, como noción que supera los estrictamente íntimos para extenderse a cuantos identifican o pueden identificar a personas; también del contenido necesario para garantizar el poder de disposición sobre ellos: consentimiento para la recogida y tratamiento, así como información suficiente sobre su destino y uso, con los subsiguientes derechos a acceder, rectificar y cancelar los datos.

Con las dudas que abre la última jurisprudencia del TEDH sobre las excepciones al deber de información, la lectura que se haga de los arts. 11 a 15 RGPD (los cuales no admiten excepción alguna) obligará a estar muy atentos a la nueva dimensión del derecho constitucional, "abducido" para convertirlo en un derecho europeo. A sus resultas, obligando a atender, para aquilatarlo en su dimensión última, a cuanto detalla la norma europea y su interpretación por el TJUE, reservando un papel complementario tanto a la Ley Orgánica 3/2018, como la interpretación del art. 18.4 CE por el Tribunal Constitucional.

El perfil del derecho exige, por otra parte, descubrir sus relaciones con el resto de los derechos. Sin perjuicio de la potencialidad que tiene para poder coincidir en su aplicación con la práctica totalidad de los que recoge la Constitución, la jurisprudencia del Tribunal Constitucional muestra su particular relación con los derechos a la intimidad, propiedad o la libertad sindical. Dada la imposibilidad de hacerlo con todos, el estudio se centra en su delimitación con el resto de los derechos recogidos en el art. 18 CE, también conocidos como derechos de la personalidad o de la individualidad, para resaltar los elementos en común y los contextos bajo los cuales la protección de

datos tendrá prioridad aplicativa o funcionalidad instrumental respecto del honor, la intimidad, la propia imagen o el secreto de las comunicaciones.

Palabras clave: Derecho de protección de datos; intimidad; honor; propia imagen; secreto de las comunicaciones.

ABSTRACT In just fifty years, the evolution of the right to data protection has led to a transformation that surprises in comparison with other third generation rights.

US legal system has tended to link the dangers of personal data with privacy; on the other hand, European Courts have preferred to connect national laws on the subject with personality rights, based on dignity and free personality development. Inspiration for the most recent Constitutions, under the idea of providing it a specific mention and, in most cases, set up a right with its own entity.

Under that development, lies an international movement that starts from the 1980 OECD Guidelines and Council of Europe Convention No. 108, whose America influence explains the instrumental connection, or subsumption, of data protection in others rights. This was the case of Spain, where art. 18.4 CE acted through the right enshrined in art. 18.1 CE.

Constructions such as the right to informational self-determination, disseminated by the German Constitutional Court, had a significant impact on the result offered by the Directive 95/46/CE, giving rise to new keys to conceive this "legal configuration right". Thus, it advances decisively toward the consideration as an autonomous right, that take place in the international sphere with the separation between the right to private and family life and the right to data protection. In the national sphere it happens through the recognition by the Constitutional Court of an autonomous right: firstly, due to its goal, placed in the personal data, as a concept which exceed the strictly intimate ones, to also understand those that identify or can identify a person; secondly, due to its content, which must be composed of set of powers that guarantees the power of disposal, that is, informed consent for its reception, treatment and use; finally, the operational right that allow access, rectification and cancellation of data.

The latest jurisprudence of the CEHR raises doubts about the exceptions to the duty of information, which can find a firmer line of interpretation from the reading of articles 11 to 15 of General Data Protection Regulation. The reason lies in the "abduction" of the constitutional right to convert it into a European right, with the consequent need to attend, for its final configuration, the development in the European norm and its interpretation by the Court of Justice of the European Union. In parallel, the Spanish norm, and the interpretation of the article 18.4 CE by the Constitutional Court, will play a complementary role.

On the other hand, understanding the right in all its dimensions makes it necessary to inquire about its relations with the rest of the rights. Despite its potential to converge with all constitutional rights, the jurisprudence shows its particular relationship with the rights to privacy and property or with the freedom of association. The impossibility of putting it in relation to all, leads to focus the study on the delimitation with the rest of the rights regulated in art. 18 CE, also known as rights of individuality, to highlight the elements in common and the contexts where it will have priority in the application or will act with an instrumental function regarding honour, privacy, the right to protection of one's image or the secrecy of communications.

Keywords: Right to personal data; privacy; honor; one's own image; secrecy of communications.

Contenido y elementos principales al derecho de protección de datos

Content and core elements of the right to data protection

MARÍA BELÉN CARDONA RUBERT*

1. EL NUEVO CONTEXTO DEL DERECHO A LA PROTECCIÓN DE DATOS

Durante décadas las tecnologías informáticas y las tecnologías de la información y de la comunicación han ido transformando paulatinamente y en profundidad la sociedad. Primero fue el correo electrónico, la navegación por internet, los programas de mensajería instantánea instalados en el ordenador; la implantación y uso del software social, blogs, wikis, foros, chats o la aceptación de la firma electrónica como modo de contraer obligaciones contractuales; el tratamiento automatizado de datos, la videovigilancia, la huella digital, la reputación online, el teletrabajo y, particularmente, las redes sociales; después llegaron la digitalización de las relaciones de todo tipo, particularmente las laborales, la robotización, la inteligencia artificial, el big data, el internet de las cosas, el blockchain o la impresión 3D.

Desde hace varios años asistimos a un extenso debate sobre los efectos de la digitalización en nuestras sociedades. Es indudable que gracias al enorme incremento experimentado en la potencialidad de las tecnologías nuestra vida está cambiando y, también, la forma de organizar la sociedad y la economía, a un ritmo trepidante.

La digitalización es un fenómeno global que está afectando a todas las sociedades, cambiando nuestra forma de comunicarnos y relacionarnos, nuestra forma de trabajar y de crear valor. Y probablemente lo que más ha transformado estas relaciones es el intercambio de información, grandes cantidades de datos relativos a las personas que permiten la construcción de perfiles susceptibles de ser tratados con las finalidades más diversas. Un imparable caudal de información de gran precisión y calidad y que con la incorporación de la técnica de los algoritmos permite, incluso, la previsión de comportamientos futuros y la adopción de decisiones por sistemas expertos basadas en dichas informaciones, es decir, la adopción de decisiones automatizadas.

En expresión de Pérez Luño "la información es poder (…) y ese poder se hace decisivo cuando convierte informaciones parciales y dispersas en informaciones en masa y organizadas"[1].

El conocimiento ordenado de datos personales puede dibujar un determinado perfil de la persona o configurar una determinada reputación o fama que es, en definitiva, expresión del honor. Y este perfil puede resultar luego valorado, favorable o desfavorablemen-

* Catedrática de Derecho del Trabajo y de la Seguridad Social. Universitat de València

[1] PÉREZ LUÑO, A., Derechos Humanos. Estado de Derecho y Constitución. Ed. Tecnos, Madrid, 1991, p. 347.

te, para las más diversas actividades públicas o privadas, como pueden ser la obtención de un empleo, la concesión de un préstamo o la admisión en determinados colectivos.

La forma de acceder y recopilar la información se abarata y facilita, la capacidad de procesamiento de la misma y la adopción de decisiones, a través de la inteligencia artificial, reducen la intervención del ser humano hasta un escenario de mínimos (machine learing).

Cuando hablamos de economía digital es importante no desconocer que el principal producto que se intercambia es la información y que la digitalización supone una transformación profunda en las formas de hacer negocios, dando lugar a tecnologías disruptivas, a nuevas formas de producir en un entorno plenamente digitalizado.

Si hay un entorno en que estas tecnologías ha impactado, definitivamente, es en el de las relaciones de trabajo y el mundo empresarial, hasta el punto de hablarse de Cuarta Revolución Industrial, de la industria 4.0, de una nueva era, para referirse a los cambios que la digitalización de la economía y la robotización están ocasionando.

Esta transformación se ha operado paulatinamente pero de forma contundente y no has situado en un escenario de no retorno. Transformación que, por supuesto, no puede darse por concluida, puesto que la experiencia de las últimas décadas pone en evidencia que el análisis sobre el impacto de la tecnología en las relaciones sociales debe ser por necesidad un análisis abierto, construido a la par que se introduce y normaliza el empleo de las tecnologías en los distintos ámbitos de la vida social y económica. Parece claro que los cambios van a continuar sucediéndose en el futuro. Algunas de las cuestiones que se enuncian parecen dignas más que de un debate jurídico o social, de relatos de ciencia ficción.

Indudablemente, la vida ordinaria y profesional de las personas, la actividad productiva, los negocios, la educación, etc. se han visto enormemente facilitadas y agilizadas por la utilización de estas nuevas técnicas, pero estas indudables ventajas no han evitado que su implantación genere numerosas dudas e incertidumbres, puesto que se trata de tecnologías con una nada despreciable potencialidad lesiva para la esfera de los derechos fundamentales. Desde la dignidad, el derecho a la intimidad y privacidad, a la protección de datos, a la libertad de expresión e información, a la integridad física y moral, a la libertad ideológica, a la igualdad y no discriminación, hasta los derechos a la libertad sindical y a la huelga, en el caso específico de la empresa, pueden verse comprometidos como consecuencia de ese acceso masivo y cualificado a la información.

La aplicación de la informática y de tecnologías afines somete a duro examen la capacidad del ordenamiento jurídico para responder a los nuevos interrogantes que se plantean ya que, en esta situación, es el Derecho el llamado a encontrar el equilibrio entre la utilización de las tecnologías y el respecto a los derechos y libertades del individuo. Las tecnologías disruptivas abren nuevos horizontes al papel regulador del Derecho. Estamos ante desafíos globales, un cambio de paradigma y de época.

2. EL NUEVO MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS

La regulación del derecho de protección de datos o derecho de autodeterminación informativa cuenta con una dilatada trayectoria.

A nivel internacional el Convenio nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981, se remite a los propios Estados firmantes para que desarrollen leyes y adopten medidas en cumplimiento de los principio enunciados en su texto.

A nivel de la Unión Europea, es la Directiva 95/46/CE, del Parlamento y del Consejo de la Unión Europea, de 24 de octubre de 1995,

sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, la que introduce el concepto e impone a los Estados miembros su transposición a sus respectivos ordenamientos nacionales.

Con posterioridad otras normas comunitarias han ido incidiendo sobre la regulación del derecho de protección de datos a la par que los nuevos retos tecnológicos y sociales exigían su adaptación a las nuevas realidades. Las Directivas 97/66/CE, de 15 de diciembre de 1997 y 2002/58/CE, de 12 de julio son buena muestra de esto.

El respaldo definitivo a la consideración internacional del derecho a la protección de datos como un derecho independiente respecto al derecho al respeto a la vida privada se obtiene en la Carta de Derechos Fundamentales de la Unión Europea en la que se consagra el derecho fundamental de toda persona a la protección de datos de carácter personal que la conciernen (art. 8).

Por su parte, la mayoría de los Estados han llevado a cabo la constitucionalización del derecho a la autodeterminación informativa y, entre ellos, el nuestro, en el art. 18. 4 de nuestra Carta Magna. Aunque existe acuerdo en considerar a este precepto como el fundamento constitucional del derecho, en puridad el artículo se limita a introducir un mandato para el legislador para que garantice los derechos fundamentales frente al uso de la informática. En el año 1992 se produce la primera respuesta legislativa al mandato constitucional a través de la Ley Orgánica 5/1992, de 29 de octubre, de regulación de tratamiento automatizado de los datos de carácter personal (LORTAD), que será sustituida por exigencias de adaptación a la Directiva 95/46/CE, por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (LOPD).

El punto de inflexión a nivel europeo llega de la mano del Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), que deroga la Directiva 95/46/CE. El RGPD es directamente aplicable en todos los Estados miembro y obligatorio en todos sus elementos, sin necesidad de norma de transposición. Eso sí, a los Estados nacionales se les exige proceder a la depuración de sus ordenamientos, derogaciones de normas incompatibles, cuando proceda; al tiempo que se les incita a completar su regulación y adaptarla a las tradiciones jurídicas propias y al contexto nacional. En el caso español, estas exigencias conducen a la promulgación de una nueva norma de protección de datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), que junto al RGPD, constituyen el nuevo marco normativo de la protección de datos.

El RGDP permite que la LOPDGDD proceda a su adaptación "siempre que no ponga en cuestión sus objetivos ni obstaculice la normalización jurídica que persigue" en el conjunto de la Unión Europea. La adopción de una norma dirigida a concretar a nivel nacional los requisitos impuestos por el RGPD deber procurar la seguridad jurídica y no excederse hasta el punto de restringir "las potencialidades aplicativas del RGPD"[2].

La LOPD queda así derogada por la nueva LOPDGD que es aplicable a cualquier tratamiento de datos personales con independencia de si este se lleva a cabo de manera total o parcialmente automatizada o no y cuyo objeto es, por una parte, adaptar el ordenamiento jurídico español al RGPD y, por otra, garantizar los derechos digitales de la ciudadanía.

3. LA NECESARIA REVISIÓN DEL CONCEPTO DE DERECHO A LA PROTECCIÓN DE DATOS

Transcurridos dieciocho años desde la promulgación de la LORTAD, la primera norma

[2] RALLO LOMBARTE, A., El nuevo derecho de protección de datos. Revista Española de Derecho Constitucional, n. 116, 2019, p. 65.

que ofreció una regulación legal al derecho a la protección de datos, es oportuno plantearse la vigencia y actualidad del concepto en el nuevo contexto tecnológico, económico y social, con el trasfondo de un marco normativo nuevo y original como es la combinación de la norma comunitaria de aplicación prioritaria, el RGPD, y la norma nacional, la LOPDGDD, complementaria al RGPD.

El derecho a la protección de datos o derecho a la autodeterminación informativa se concibe como la capacidad y derecho de los individuos de ejercer el control sobre las informaciones que les atañen. Dicho derecho se constituye a partir de la noción de intimidad pero la supera por incluir una función dinámica de control sobre las informaciones que se refieren al individuo. Y es precisamente esta función la que lo configura como un derecho autónomo con respecto al derecho a la intimidad.

El concepto tradicional de intimidad se revela como insuficiente para ofrecer cobertura frente a potenciales lesiones derivadas del uso de las tecnologías que puedan incidir sobre la esfera más privada y reservada de la persona. La posibilidad casi ilimitada de recoger, almacenar, conectar y procesar datos y la gran reducción de costes y tiempo necesarios para realizar tales funciones permiten a quien posea los datos, obtener un perfil de la persona, un perfil completo que puede incluir o del que se pueden deducir informaciones sensibles y que posibilite valoraciones de la misma y decisiones sobre ella.

El derecho a la protección de datos se apoya en un conjunto de derechos subjetivos, deberes, procedimientos y reglas objetivas, mediante las que se permite al individuo definir según Murillo de la Cueva "la intensidad con la que desea que se conozcan y circulen su identidad y circunstancias, combatir las inexactitudes o falsedades que las alteren y defenderse de cualquier utilización abusiva"[3] que se pretenda hacer de las mismas.

En el derecho a la protección de datos se reconoce una doble vertiente. Por una parte, una dimensión positiva, entendida como derecho de control activo sobre los datos personales; por otra, se reconoce el carácter institucional de garantía-presupuesto del ejercicio de otros derechos constitucionales como el derecho de asociación, libertad ideológica y religiosa, derecho a la no discriminación, derecho al trabajo, derecho a la igualdad, etc., constituyéndose en un derecho instrumental ordenado a la protección de otros derechos fundamentales.

Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento de datos (STC 254/1993).

El derecho a la autodeterminación informativa se convierte en la defensa eficaz para la esfera privada del individuo frente al peligro de procesamiento de los datos personales. En este contexto, la protección de datos personales proporciona los instrumentos destinados a limitar y racionalizar la utilización de las tecnologías de la información y comunicación, para impedir los perjuicios que el uso incontrolado de aquellas pueda ocasionar a las personas.

La Jurisprudencia del Tribunal Constitucional ha reforzado el reconocimiento del derecho a la protección de datos como un derecho autónomo y, particularmente, en sus sentencias 290/2000 y 292/2000, en las que establece la diferenciación entre el derecho a la intimidad y a la protección de datos personales. Según estas "la función del derecho fundamental a la intimidad del art. 18.1.CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (…) En cambio, el

[3] Murillo de la Cueva, P.L., El derecho a la autoderminación informativa. Ed. Tecnos, Madrid, 1990, p. 174.

derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de **impedir su tráfico ilícito y lesivo** para la dignidad y derecho del afectado".

En esta jurisprudencia se acotan los perfiles y el contenido del derecho fundamental a la protección de datos, considerándolo como un derecho autónomo e independiente en nuestro sistema constitucional, de manera coincidente con la LOPDGDD.

El derecho a la protección de datos puede definirse como el poder de disposición y de control sobre los datos personales, que habilita a la persona a determinar que datos y a decidir en que medida cuales de estos datos proporciona "a un tercero, sea el Estado o un particular, o cuales puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso" (STC292/2000). Se trata, en definitiva, de un derecho horizontal que puede ser ejercido frente a todos, de un derecho de toda persona al tratamiento leal y lícito de sus datos, para finalidades concretas y con su consentimiento previo.

En definitiva, el derecho a la autodeterminación informativa o a la protección de datos confiere al titular de los datos la facultad de conocer y controlar cuantas transacciones y operaciones se realicen con sus datos, así como la de decidir sobre dichas operaciones, a través del otorgamiento informado de su consentimiento, poniendo en sus manos cuantos instrumentos válidos de defensa prevea el ordenamiento, convirtiéndolo en el principal garante de su privacidad. Y este concepto sigue siendo valido en el actual contexto tecnológico y económico social.

El concepto de autodeterminación informativa, por tanto, es un concepto vigente cuyos perfiles, eso sí, han variado matizadamente para hacer frente a las nuevas exigencias de tutela de la información personal del titular de los datos procesados, en un mundo digitalizado.

4. LA NUEVA DIMENSIÓN DEL CONTENIDO Y ELEMENTOS DEL DERECHO A LA PROTECCIÓN DE DATOS: LA NECESARIA ADAPTACIÓN A LOS CAMBIOS CONTEXTUALES

El derecho a la protección de datos sin un contenido que le dote de efectividad no sería más que una mera entelequia, por ello incluye una serie de garantías y derechos que otorgan a la persona titular de los datos la posibilidad de determinar el nivel de protección frente a posibles invasiones en la esfera de sus derechos. En este contenido efectivo es en el que se han producido las principales adaptaciones de los perfiles del derecho a las nuevas realidades.

Es aquella la sede en la que es posible identificar las verdaderas transformaciones del derecho que ha ido adaptándose y haciendo frente a los retos contextuales de la digitalización, mediante la atribución de más y más incisivos instrumentos a través de los cuales hacer efectivo y real el derecho a la protección de datos. Puesto que la protección efectiva de los datos personales exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal.

Como señala el RGPD en su Considerando 6, la evolución tecnológica y la globalización han planteado nuevos retos para la protección de datos personales. "La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa", ya que tanto las empresas privadas como las propias administraciones utilizan datos personales en "una escala sin precedentes" y las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. Este escenario exige compaginar la facilitación de la libre circulación de datos personales en la Unión Europea y la transferencia a terceros países, con un elevado nivel de protección de datos personales.

Desde los conocidos como derechos ARCO (derechos de acceso, rectificación, cancelación y oposición) configurados como derechos personalísimos a favor del titular de los datos, previstos en la LOPD, hemos alcanzado el horizonte de su actual configuración en el RGPD y la LOPDGDD, en el que aparecen reforzados de manera significativa.

El nuevo orden legal proporciona nuevas respuestas en el fondo y la forma a los retos de la era de la disrupción digital. En términos generales, se redimensionan los derechos del interesado, a través de su fortalecimiento y diversificación, respetando el esquema inicial de los principios de protección de datos.

4.1. El consentimiento

El consentimiento es sin duda, tal como ha sido configurado en la legislación de protección de datos, el cimiento básico y elemento fundamental del derecho de autodeterminación informativa. Aparece en aquella como causa habilitante para el tratamiento lícito de datos (art. 6.1.a) RGPD y art. 6 LOPDGDD).

El consentimiento debe darse mediante un acto afirmativo, claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen (art. 4. 11. RGPD). Las manifestaciones de la voluntad del afectado por el tratamiento se pueden articular a través de una declaración por escrito, incluidos los medios electrónicos o mediante una declaración verbal. Lo fundamental es que la declaración o conducta indique claramente que el interesado acepta el tratamiento de sus datos personales.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe otorgarse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

En el nuevo marco legal, se refuerza la idea de que el consentimiento válido ha de ser consciente y para ello es imprescindible que se de cumplimiento a las exigencias de la transparencia, cuyo pilar fundamental es la información. En consecuencia, el legislador no está pensando en un consentimiento cualquiera sino en un consentimiento informado sobre el que recaen todas las obligaciones vinculadas a la transparencia (Capítulo III RGPD y art. 11 LOPDGDD). No supone, en definitiva, un cambio sustancial con la regulación previa pero si una adaptación a las nuevas tendencias y exigencias de transparencia que invaden la vida social y económica.

En cuanto a los supuestos, en los que resulta viable eludir la obtención del consentimiento para proceder al tratamiento de los datos, el art. 6 RGPD prevé una serie de excepciones que permiten igualmente un tratamiento lícito de la información personal del interesado.

De entre ellas merece la pena destacar una que puede fácilmente relacionarse con la exclusión de tratamientos en el ámbito laboral, en concreto, cuando el tratamiento sea necesario para la ejecución de un contrato en el que interesado es parte o para la aplicación de este de medidas contractuales la prevista en el 6.1. b).

A pesar de que la LOPD hacía mención expresa a las relaciones de naturaleza laboral como relaciones exceptuadas de la necesidad de recabar el consentimiento del afectado (art. 6), nada ha cambiado sustancialmente porque entonces como ahora, en el caso de los contratos de trabajo, el peso de la tutela del derecho a la protección de datos se traslada al derecho de información, en la legislación anterior previsto en el art. 5.

4.2. Transparencia e información

El derecho de información en el sentido en el que es regulado en los artículos 12, 13 y 14 RGPD, aparece en primer término como concreción del principio de transparencia que obliga al responsable del tratamiento a facilitar la información prevista en los arts 13 y 14 y cualquier comunicación relativa al tratamiento (arts. 15 a 22 y 34) y a hacerlo en forma concisa, transparente e inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cuando la información se dirija a menores.

Otras de las vertientes del derecho de información y, no menos importante, es la de considerarlo como fase o requisito previo al otorgamiento del consentimiento (art. 4.11RGPD).

El derecho a la información, obviamente, mantiene una estrecha relación con el principio de transparencia y permite al sujeto ejercer un verdadero control sobre sus datos personales, confiriendo validez a la prestación del consentimiento tras haber ejercido el derecho de información. Un consentimiento otorgado sin que se hayan cumplido, de forma adecuada, por parte del responsable del tratamiento las obligaciones de información, es un consentimiento que carece de validez.

La información se facilitará por escrito o por otros medios, incluidos, los electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios (art. 12 RGPD y art. 11 LOPDGDD).

La información que debe facilitarse por el responsable del tratamiento sobre la recogida, tratamiento, uso, plazo de conservación y destino varia ligeramente en función del origen de los datos personales, según se hayan recabado del interesado o no (arts. 13 y 14 RGPD y 11LOPD).

El contenido previsto en ambos casos es extenso y prácticamente coincidente. Así sería preciso informar sobre: la identidad y contacto del responsable y de su representante; del del delegado de protección de datos; de los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; los destinatarios o las categorías de destinatarios de los datos personales; la intención, en su caso, de transferir datos personales a un tercer país u organización internacional; el plazo de conservación de los datos; los derechos que puede ejercer el interesado; cuando la comunicación de datos sea un requisito legal o contractual, la obligación de prestar el consentimiento y consecuencias de no hacerlo; la existencia de decisiones automatizadas y elaboración de perfiles; en el caso de preverse tratamiento ulterior de los datos con un fin distinto del inicial, deberá proporcionar información sobre dicho fin.

En el supuesto en el que los datos personales no hubieran sido recabados del afectado, además de la información anterior, se tendrá que incluir la referida a las categorías de datos objeto de tratamiento y a las fuentes de las que procedieran los datos.

Como conclusión, se observa en la actual configuración del derecho de información que, con la finalidad de asegurar que el consentimiento del interesado se otorgue con mayores garantías de validez, aquel se ha extendido hasta abarcar un numero mayor de informaciones que las exigidas de acuerdo al anterior marco legal. La cuestión es si esta redimensión del derecho de información es adecuada y compatible con la obligación de proporcionar la información de forma clara, sencilla y accesible, es decir, con las exigencias de la transparencia (art. 12 RDGPD) ya que en la práctica se puede ocasionar una sobrecarga informativa que confunda al interesado a la hora de prestar su consentimiento y, en definitiva, reste intensidad efectiva al cumplimiento de los deberes de información que recaen sobre el responsable del tratamiento.

El GT29 en relación a estas eventuales contradicciones que pueden producirse entre el deber de proporcionar información completa y la de hacerlo de forma concisa y clara, introduce

la posibilidad de proporcionar la información por capas o niveles. Así en el Considerando 36 del Documento WP260 rev 01 se establece un orden y una priorización de la información que se debe facilitar a los interesados[4]. No se trata de prescindir de proporcionar la plenitud de la información legalmente prevista pero sí de proporcionarla en niveles o capas en función de su relevancia para el interesado, garantizando así que la misma se proporciona de forma transparente, es decir, de forma clara, sencilla y accesible. Así, por ejemplo el primer nivel, al que hace referencia el Considerando 36, incluiría información relativa a los fines, la identidad del responsable y una descripción de los derechos del interesado.

Por lo que, en definitiva, parece conveniente que la información se proporcione modularmente, mediante niveles o capas, para garantizar que el interesado aprehende dicha información de manera correcta y adecuada para acabar otorgando un consentimiento debidamente informado y, por lo tanto, válido. Y sin que en ningún caso eso comporte renunciar a acceder al conjunto de las informaciones que prevén las normas[5].

4.3. La redimensión de los derechos ARCO. Los derechos de acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento y derecho de oposición, decisiones individuales automatizadas, incluida la elaboración de perfiles

Estos derechos se encuentran regulados en los arts. 15 a 22 RGPD y en los arts. 12 a 18 LOPGDD. Constituyen un haz relevante de derechos a través de los que el interesado puede ejercer eficazmente su derecho a la protección de datos. Son medios de auto tutela del titular de la información tratada por el responsable.

El Tribunal Constitucional indicaba ya en su Sentencia 292/2000 que el núcleo esencial del derecho a la autodeterminación informativa se haya no sólo en el consentimiento informado sino que también lo integran esas otras facultades que confieren al titular de los datos personales un poder de disposición sobre la información a él relativa y, en consecuencia, de configurar su propia privacidad.

El Tribunal Constitucional en esta sentencia hacía referencia a los derechos reconocidos al afectado según la legislación vigente, es decir, los derechos de acceso, rectificación, cancelación y oposición al tratamiento, los derechos ARCO. A ellos hay que sumar el derecho al olvido y los derechos de portabilidad y de limitación del tratamiento.

Estos derechos podrán ser ejercidos, en su actual configuración, directamente por el afectado o por medio de representante legal o voluntario. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer dichos derechos, medios que deberán ser accesibles y gratuitas las acciones que permitan dar satisfacción a las solicitudes para su ejercicio.

4.3.1. El derecho de acceso

El derecho de acceso es, sin duda, uno de los derechos más interesantes en cuanto permite la tutela de los propios datos personales de un modo directo, al facilitar el control del sujeto afectado sobre la información tratada. Consiste en la facultad que se le reconoce al afectado de solicitar y obtener del responsable del tratamiento información sobre los datos que le conciernan, con el fin de conocer y verificar la licitud del tratamiento.

[4] Documento WP 260 rev.01 del Grupo de Trabajo del art. 29 (GT29) "Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679", de 29 de noviembre de 2017, revisado y adoptado el 11 de abril de 2018. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[5] Esta información por niveles es la recomendada en la Guía para el cumplimiento del deber de informar, elaborada por la AEPD, la Agencia Vasca de Protección de Datos y la Agencia Catalana de Protección de Datos, https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

El interesado tiene derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en su caso, derecho de acceso a los datos personales y a la siguiente información: fines del tratamiento; categorías de datos personales tratados; destinatarios o categorías de destinatarios a los que se comunicaron o serán comunicados los datos; plazo previsto de conservación o criterios para su determinación; la existencia de ejercicio de los derechos de rectificación, supresión, limitación del tratamiento u oposición; derecho a presentar una reclamación ante una autoridad de control; si no se obtuvieron los datos del titular, información sobre su origen; la existencia de decisiones automatizadas, incluida la elaboración de perfiles (art. 15 RGPD).

4.3.2. Los derechos de rectificación, supresión (derecho al olvido) y limitación del tratamiento

Los derechos de rectificación y supresión, completan al derecho de acceso, puesto que una vez ejercido este, el titular de los datos tratados puede identificar si son inexactos, incorrectos o incompletos.

El derecho de rectificación tiene por objeto obtener la corrección de aquellos datos que resulten incorrectos o incompletos, abriendo a favor del afectado la facultad de exigir la modificación y actualización de la información que está desfasada (art. 16 RGPD y art. 14 LOPDGDD).

Estas previsiones se entrelazan con las obligaciones impuestas al responsable del tratamiento de velar por la exactitud y actualización de los datos personales tratados y de adoptar todas las medidas razonables para que se supriman o rectifiquen, sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan (art.4 LOPDGDD, art. 5.1.d) RGPD)

El derecho de supresión, por su parte, tiene por objeto eliminar del fichero aquellos datos personales que sean inadecuados o excesivos. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, cuando los datos ya no sean necesarios en relación con los fines para los que fueron recogidos; el interesado retire el consentimiento en que se base el tratamiento; el interesado se oponga al tratamiento; los datos hayan sido tratados ilícitamente; los datos deban suprimirse para el cumplimiento de una obligación legal; los datos se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

El derecho de supresión, lógicamente no es un derecho absoluto y de hecho no se podrá materializar cuando el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información; para el cumplimento de una obligación legal impuesta; por razones de interés público en el ámbito de la salud pública o por alguna otra de las razones previstas en el art. 17. 3 RGPD.

En relación al derecho al olvido el RGPD se refiere a él pero lo hace a penas de soslayo e induciendo a que ambos se interpreten como derechos equivalentes, puesto que el art. 17 los utiliza como términos sinónimos, "derecho de supresión (derecho al olvido)". Si bien en su apartado 2 aunque no menciona expresamente el derecho al olvido, sin embargo, incluye una evidente manifestación del mismo. En concreto, cuando prevé que si se hubieran hecho públicos los datos y el responsable estuviera obligado a suprimirlos, se deberán adoptar medidas razonables, incluidas técnicas, para informar a los responsables que estén tratando los datos personales, de la solicitud del interesado, para en alguna medida limitar el impacto de esta difusión[6].

Más explícito es el legislador nacional que dedica sendos artículos al derecho al olvido,

[6] Rallo Lombarte, A., Del derecho de protección de datos a la garantía de nuevos derechos digitales, en AA.VV. El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Ed. Tirant lo Blanch, Valencia, 2019, p. 147.

en concreto, en búsquedas en internet (art. 93 LOPDGDD) y en servicios de redes sociales y servicios equivalentes (art. 94 LOPDGDD), abrazando la doctrina del Tribunal de Justicia de la Unión Europea, en su sentencia de 13 de mayo de 2014, en el asunto C-131/12 (Google contra España).

En virtud de dicha regulación se proclama el derecho de toda persona a que los motores de búsqueda e internet eliminen de las listas de resultados obtenidas a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona, cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo.

También podrá ejercerse este derecho al olvido cuando las circunstancias personales invocadas por el afectado, evidencien la prevalencia de sus derechos sobre el mantenimiento de los enlaces generados por el servicio de búsqueda (art. 93).

Ahora bien, si existe algún ámbito en el que resultaba especialmente pertinente reconocer el derecho al olvido era, sin duda, en el ámbito de las redes sociales.

El usuario de la red social está obligado a proporcionar datos personales desde el momento que pretende generar su descripción o perfil. Dicho perfil puede ser más o menos amplio o, dicho de otro modo, incluir más o menos datos y referirse o no a informaciones sensibles. A ello hay que añadir los datos que describen las acciones e interacciones con otras personas, la adscripción a grupos determinados, aceptar las invitaciones de otros, etc. Pero además de ello, los usuarios pueden colgar on line fotografías o información relativa a otras personas, a las que se puede perjudicar, en su derecho a la intimidad y a la protección de datos.

Todo ello permite crear un perfil preciso de los intereses, personalidad y actividades del usuario. Se trata de datos personales que pueden ser utilizados por terceros, por el empresario, con fines absolutamente distintos e, incluso, contrarios a aquellos para los que se proporcionó, inicialmente, la información.

La peculiaridad más importante es que el usuario, en principio, tiene la facultad de determinar y acotar la información personal que sobre su persona, contactos, vida quiere mostrar y a qué personas va a permitir el acceso a la misma, y de qué manera. El problema estriba en que estos soportes virtuales son modelos de negocio que fundamentan su potencial en la riqueza de la información de las personas que las utilizan y disponen de potentes herramientas de intercambio de información, capacidad de procesamiento y análisis de dicha información. Además, las redes sociales permiten a los motores de búsqueda de internet indexar en sus búsquedas los perfiles de los usuarios, información de contacto, perfiles de amigos, lo que implica otro riesgo para la privacidad.

En la práctica, el usuario medio acaba publicando en la red social mucha más información y de carácter más sensible de lo que es consciente, informaciones que revelan el origen racial o étnico, opiniones políticas, convicciones religiosas, afiliación sindical, datos relativos a la salud, vida sexual, etc. Incluida la información relativa a terceros, que puede perjudicar la intimidad y a la protección de datos de sus titulares, generando su indefensión puesto que en muchas ocasiones son desconocedores de que la información que a ellos se refiere se encuentra disponible en la red.

Además, con frecuencia, no se protege convenientemente dicha información, al permitir el acceso de terceros a los datos sin restricciones, a todo tipo de detalles íntimos.

La información proveniente de las redes sociales suele ser la suma de la acción y de la información proporcionada por distintos agentes y en distintos actos. Por una parte, es, sin duda, resultado de la propia acción del usuario, quien de manera voluntaria, ya en el momento de la adquisición de su condición de usuario de una red social, proporciona para

la configuración y posterior publicación de su perfil, datos identificativos, características personales, circunstancias sociales, detalles de su vida privada, datos académicos, profesionales, aficiones, preferencias de todo tipo, etc. Información que se amplía y completa como resultado de la interacción con otros agentes, usuarios, ya sea aceptando participar en grupos, aceptando invitaciones a convertirse en fan de determinados eventos o personaje, etc.

El legislador recoge en el art. 94 LOPDGDD el derecho al olvido en redes sociales y establece que toda persona dispone del derecho a que los datos que hubiese facilitado para su publicación por redes sociales o servicios de la sociedad de la información equivalentes, sean suprimidos "a su simple solicitud" (art. 94). Se suprimirán los datos cuando sean inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido así por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron y el tiempo transcurrido.

La supresión procederá igualmente, cuando sin concurrir las circunstancias anteriores, las circunstancias personales invocadas evidencien la prevalencia de los derechos del titular de los datos sobre el mantenimiento de los datos por el servicio.

Se trata, en resumen, de proporcionar un derecho al interesado que contribuya eficazmente a la defensa del derecho a la autodeterminación informativa.

En relación al derecho a la limitación del tratamiento, la legislación nacional remite directamente a la regulación establecida en el RGPD sin matiz ninguno (art. 16 LOPDGDD).

Según el art. 18 RGPD el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumplan algunas de las condiciones previstas y que son que el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable su verificación; que el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en cambio la limitación de su uso; que el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, ejercicio o defensa de reclamaciones; y, por último, que el interesado se haya opuesto al tratamiento en tanto se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

4.3.3. Derecho de oposición, decisiones individuales automatizadas, incluida la elaboración de perfiles

De nuevo, para conocer el contenido de este derecho la ley nacional remite a la regulación establecida en el RGPD sin matiz ninguno (arts. 21 y 22 LOPDGDD).

Reconocer al titular de los datos el derecho de oposición significa poner en sus manos la facultad de oponerse a que los datos que le conciernen sean objeto de tratamiento o se cese en el mismo.

Por otra parte cuando, una decisión referida al interesado esté basada únicamente en un tratamiento automatizado de sus datos de carácter personal, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, aquel podrá oponerse a ella (art. 22 RGPD).

Con esta previsión se establece a favor de los interesados el derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, únicamente, basada en un tratamiento automatizado de datos, destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

Se trata de reconocer expresamente el derecho del afectado a oponerse o impugnar actos administrativos o decisiones privadas que impliquen una valoración, cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal, que ofrezca una definición de sus características o personali-

dad. Se trata de una garantía sustancial que se coloca en las manos del interesado, una garantía que le permita evitar los efectos perniciosos que sobre su persona o vida personal o profesional pueda tener una decisión fundada exclusivamente en una valoración de su persona, producto de una elaboración informática.

5. CONCLUSIONES

En el nuevo entorno digitalizado resulta ineludible cuestionarse sobre la vigencia y capacidad del derecho a la protección de datos para hacer frente a los nuevos retos y a las amenazas siempre más sofisticadas para la esfera de los derechos fundamentales del titular de los datos personales sometidos a tratamiento. Y ello en el marco normativo actual, determinado por el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), que deroga la Directiva 95/46/CE, directamente aplicable en todos los Estados miembro y obligatorio en todos sus elementos, sin necesidad de norma de transposición; combinado con la nueva norma de protección de datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), que junto al RGPD, constituyen el nuevo marco normativo de la protección de datos.

Es en el contenido efectivo del derecho a la autodeterminación informativa, es decir, garantías y derechos que otorgan a la persona titular de los datos la posibilidad de determinar el nivel de protección frente a posibles invasiones en la esfera de sus derechos, en el que se han producido las principales adaptaciones de los perfiles del derecho a las nuevas realidades.

Es aquella la sede en la que es posible identificar las verdaderas transformaciones del derecho que paulatinamente se ha ido adaptando y haciendo frente a los retos contextuales de la digitalización, mediante la atribución de más y más incisivos instrumentos a través de los cuales hacer efectivo y real el derecho a la protección de datos. Puesto que la protección efectiva de los datos personales exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal: el consentimiento, el derecho de transparencia e información y los derechos de acceso, rectificación, supresión, limitación del tratamiento y derecho de oposición y decisiones individuales automatizadas, incluida la elaboración de perfiles.

Las conclusiones pueden resumirse en la vigencia y actualidad del derecho a la protección de datos, de su capacidad para proporcionar protección a la esfera de derechos fundamentales de las personas, cuyos datos personales son objeto de tratamiento. Y que el nuevo orden legal proporciona nuevas respuestas en el fondo y la forma a los retos de la era de la disrupción digital.

En términos generales, se redimensionan los derechos del interesado, a través de su fortalecimiento y diversificación, respetando el esquema inicial de los principios de protección de datos. Nuevas formas para viejas cuestiones con una revisión y actualización necesaria al nuevo contexto socioeconómico, del concepto de autodeterminación informativa que se mantiene fiel a su esencia con algunas matizaciones en sus perfiles que le permiten seguir siendo un concepto jurídico válido y suficiente para la era de la disrupción digital.

BIBLIOGRAFÍA

Murillo de la Cueva, P.L., El derecho a la autoderminación informativa. Ed. Tecnos, Madrid, 1990.

Pérez Luño, A., Derechos Humanos. Estado de Derecho y Constitución. Ed. Tecnos, Madrid, 1991.

Rallo Lombarte, A., El nuevo derecho de protección de datos. Revista Española de Derecho Constitucional, n. 116, 2019.

Rallo Lombarte, A., Del derecho de protección de datos a la garantía de nuevos derechos digitales, en AA.VV. El Reglamento General de Protección de Datos. Un enfoque nacional y comparado. Ed. Tirant lo Blanch, Valencia, 2019.

RESUMEN Transcurridos dieciocho años desde la promulgación de la LORTAD, la primera norma que ofreció una regulación legal al derecho a la protección de datos, es oportuno plantearse la vigencia del concepto en el nuevo contexto tecnológico y económico social y con un marco normativo nuevo y original como es la combinación de la norma comunitaria de aplicación prioritaria, el RGPD, y la norma nacional, la LOPDGDD, complementaria al RGPD.

Desde hace varios años asistimos a un extenso debate sobre los efectos de la digitalización en nuestras sociedades. Es indudable que gracias al enorme incremento experimentado en la potencialidad de las tecnologías está cambiando nuestra vida y la forma de organizar la sociedad y la economía, a un ritmo trepidante.

Indudablemente, la vida ordinaria y profesional de las personas, la actividad productiva, los negocios, la educación, etc se han visto enormemente facilitadas y agilizadas por la utilización de estas nuevas técnicas, pero estas indudables ventajas no han evitado que su implantación genere numerosas dudas e incertidumbres puesto que se trata de tecnologías con una nada despreciable potencialidad lesiva para la esfera de los derechos de los fundamentales, que pueden verse comprometidos. Desde la dignidad, el derecho a la intimidad y privacidad, a la protección de datos, a la libertad de expresión e información, a la integridad física y moral, a la libertad ideológica, a la igualdad y no discriminación, hasta los derechos a la libertad sindical y a la huelga, en el caso específico de la empresa, pueden verse afectados como consecuencia de ese acceso masivo y cualificado a la información.

La aplicación de la informática y de tecnologías afines somete a duro examen la capacidad del ordenamiento jurídico para responder a los nuevos interrogantes que se plantean ya que, en esta situación, es el Derecho el llamado a encontrar el equilibrio entre la utilización de las tecnologías y el respecto a los derechos y libertades del individuo. Las tecnologías disruptivas abren nuevos horizontes al papel regulador del Derecho. Estamos ante desafíos globales, un cambio de paradigma y de época.

Por ello este artículo se propone revisar el concepto del derecho de protección de datos o a la autodeterminación informativa, su contenido y elementos principales. Analizar su vigencia y su capacidad para hacer frente a los nuevos retos de un entorno y economía digitalizado, en el que las amenazas a los derechos fundamentales del titular de la información personal son siempre más sofisticados.

Para ello se procede a revisar el actual marco normativo, determinado por el Reglamento (UE) 2016/679, de 27 de abril de 2016, General de Protección de Datos (RGPD), que deroga la Directiva 95/46/CE, directamente aplicable en todos los Estados miembro y obligatorio en todos sus elementos, sin necesidad de norma de transposición; combinado con la nueva norma de protección de datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD), que junto al RGPD, constituyen el nuevo marco normativo de la protección de datos.

El análisis se centra en el contenido efectivo del derecho a la autodeterminación informativa, es decir, en las garantías y derechos que otorgan a la persona titular de los datos la posibilidad de determinar el nivel de protección frente a posibles invasiones en la esfera de sus derechos. En este contenido efectivo es en el que se han producido las principales adaptaciones de los perfiles del derecho a las nuevas realidades.

Es aquella la sede en la que es posible identificar las verdaderas transformaciones del derecho que paulatinamente se ha ido adaptando y haciendo frente a los retos contextuales de la digitalización, mediante la atribución de más y más incisivos instrumentos a través de los cuales hacer efectivo y real el derecho a la protección de datos. Puesto que la protección

efectiva de los datos personales exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal: el consentimiento, el derecho de transparencia e información y los derechos de acceso, rectificación, supresión, limitación del tratamiento y derecho de oposición.

Las conclusiones pueden resumirse en la vigencia y actualidad del derecho a la protección de datos, de su capacidad para proporcionar protección a la esfera de derechos fundamentales de las personas, cuyos datos personales son objeto de tratamiento. Y que el nuevo orden legal proporciona nuevas respuestas en el fondo y la forma a los retos de la era de la disrupción digital. En términos generales, se redimensionan los derechos del interesado, a través de su fortalecimiento y diversificación, respetando el esquema inicial de los principios de protección de datos. Nuevas formas para viejas cuestiones con una revisión y actualización necesaria al nuevo contexto socioeconómico, del concepto de autodeterminación informativa que se mantiene fiel a su esencia con algunas matizaciones en sus perfiles que le permiten seguir siendo un concepto jurídico válido y suficiente para la era de la disrupción digital.

Palabras clave: Proteccion de datos; derecho a la autodeterminación informativa; derechos fundamentales; privacidad; derechos digitales.

ABSTRACT Eighteen years after the promulgation of the LORTAD (Organic Law on the Automated Treatment of Data), the first rule that offered a legal regulation to the right to data protection, it is appropriate to consider the currency of the concept in the new technological and economic social context and with a new and original regulatory framework, which combines the Community legislation of prior application, the GDPR, and the national rule, the LOPDGDD, complementary to the GDPR.

For several years now, we have been witnessing an extensive debate on the effects of digitalization on our societies. There is no doubt that due to the enormous increase in the potential of technologies, our life and the way we organise society and the economy is changing at a rapid pace.

Undoubtedly, people's ordinary and professional lives, productive activity, business, education, etc. have been enormously facilitated and expedited by the use of these new techniques, but these undoubted advantages have not prevented their implementation from generating numerous doubts and uncertainties, since these are technologies with a not inconsiderable potential that is harmful to the sphere of fundamental rights, which may be compromised. From dignity, the right to privacy and intimacy, to data protection, to freedom of expression and information, to physical and moral integrity, to ideological freedom, to equality and non-discrimination, including the rights to freedom of association and to strike, in the specific case of the company, all may be affected as a consequence of this massive and qualified access to information.

The application of information technology and related technologies subjects the capacity of the legal system to respond to the new arising questions to a hard examination, since, in this situation, it is the Law that is called for finding a balance between the use of technologies and respect for the rights and freedoms of the individual. Disruptive technologies open new horizons for the regulatory role of the Law. We are facing global challenges, a change of paradigm and of era.

For this reason, this article aims to revise the concept of the right to data protection or to informational self-determination, its content and main elements. It analyses its validity and its capacity to face the new challenges of a digitalised environment and economy, in which the threats to the fundamental rights of the holder of personal information are always more sophisticated.

To this end, the current legal framework, determined by the General Data Protection Regulation (EU) 2016/679, of 27 April 2016 (GDPR), which repeals Directive 95/46/EC, directly applicable in all Member States and obligatory in all its elements, without the need for a transposition rule, shall be revised; which, combined with the new data protection legislation, the Organic Law 3/2018, of December 5th, on Personal Data Protection and Guarantee of Digital Rights (LOPDGDD), constitute the new regulatory framework for data protection.

The analysis addresses the effective content of the right to informational self-determination, that is to say, on the guarantees and rights that grant the data owner the possibility of determining the level of protection against possible invasions in the sphere of his rights. It is in this effective content that the main adaptations of the profiles of the right to the new realities have taken place.

In fact, this is the sphere where it is possible to identify the true transformations of the law that has been gradually adapted and faced with the contextual challenges of digitalisation, by means of the attribution of more and more incisive instruments through which to make the right to data protection effective and real. Since the effective protection of personal data requires the rights of data subjects and the obligations of those who process and determine the processing of personal data to be strengthened and specified: consent, the right to transparency and information and the rights of access, rectification, erasure, limitation of processing and the right to object.

The conclusions can be summarized in the currency and actuality of the right to data protection, in its capacity to provide protection to the sphere of fundamental rights of the persons, whose personal data is processed. And that the new legal order provides new responses in terms of both substance and form to the challenges of the era of digital disruption. In general terms, the rights of the data subject are redimensioned, through their strengthening and diversification, respecting the initial scheme of the data protection principles. New forms for old issues with a necessary revision and updating to the new socioeconomic context, of the concept of informational self-determination which remains faithful to its essence with some nuances in its profiles that allow it to continue being a valid and sufficient legal concept for the era of digital disruption.

Keywords: Data protection; right to informational self-determination; fundamental rights; privacy; digital rights.

Recogida y tratamiento de datos personales en el contexto del contrato de trabajo

Collection and processing of personal data in the context of the employment contract

ALBERTO CÁMARA BOTÍA*

1. INTRODUCCIÓN: EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, UNA DIMENSIÓN INSEPARABLE DE LA RELACIÓN LABORAL

El derecho fundamental a la protección de datos[1] (arts. 18.4 CE, 8 CDFUE y 16.1 TFUE), que atribuye a las personas un poder de disposición y de control sobre sus datos personales (STC 292/2000, de 30 de noviembre [FJ 7][2]), encuentra una de su más importantes aplicaciones en el ámbito de la relación laboral[3].

* Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de Murcia.

[1] Sobre su formación y configuración, OLLERO TASSARA, A.: *De la protección de la intimidad al poder de control sobre los datos personales*, Madrid, Real Academia de Ciencias Morales y Políticas, 2008, pp. 137 a 168.

[2] El amplio contenido de este derecho fundamental queda descrito en la STC 292/2000, de 30 de noviembre: "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan 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, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el 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 usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele" (FJ 7). Véase SAN MARTÍN MAZZUCCONI, C.: "El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos", en SAN MARTÍN MAZZUCCONI, C. (Dir.): *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, León, Eolas, 2014, pp. 211 a 213.

[3] GARCÍA MURCIA, J.; RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216 (2019), p. 9 (versión electrónica). TRONCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010, p. 1 (citado según la versión electrónica del capítulo 13 del libro ["La protección de datos personales en el ámbito laboral"], TOL2.029.308).

Su ciclo vital (selección, contratación, cumplimiento y extinción) permite disponer de una información masiva sobre el trabajador, de un elevadísimo número de datos personales sobre sus más variadas circunstancias[4]: identificación, localización, aptitud, formación, salud, afiliación sindical, situación familiar, horario, rendimiento, salario, relaciones humanas, etc. No resultará extraño, por tanto, afirmar que la normativa sobre protección de datos personales se ha convertido en una dimensión inseparable de la puramente laboral[5]. En este sentido se ha señalado que la "legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo" y éste, a su vez, "no puede aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos"[6]. O dicho de otro modo, que buena parte del Derecho del Trabajo puede ser mirado desde el singular punto de vista proporcionado por el derecho fundamental a la protección de datos personales, conforme al cual el empresario aparece como responsable del tratamiento[7] y el trabajador como interesado[8], alineándose de modo inescindible con la relación laboral otra derivada de la vigencia del derecho a la protección de datos. Esta afirmación puede sustentarse en las siguientes bases:

1.º Sería imposible la celebración, cumplimiento y extinción del contrato de trabajo sin la disposición de datos personales de los trabajadores[9]. Más aún, "muchas actividades realizadas de forma rutinaria en el ámbito del empleo implican el tratamiento de datos personales de los trabajadores"[10]. Esto es así porque siendo el de trabajo un contrato personalísimo en el que su objeto, el trabajo, es inseparable de la persona que lo presta, su celebración, cumplimiento y extinción exigen mantener un flujo de datos personales en diferentes direcciones: del trabajador al empresario y de éste a aquél[11]; del empresario a la administración laboral y a los representantes de los trabajadores; de los representantes de los trabajadores a los trabajadores representados. Recogida y tratamiento de datos que unas veces vendrá exigida por la propia "naturaleza de las cosas" (¿cómo se podría celebrar un contrato sin disponer de los datos de los contratantes?), otras por las leyes que obligan a comunicar datos personales, y otras, por no alargar más la enumeración, por el interés y conveniencia del empresario que, por ejemplo, usa instrumentos de control del personal que conllevan necesariamente el tratamiento de sus datos personales.

2.º Todos los actos anteriores suponen la disposición del derecho fundamental a la protección de datos, un capítulo más del tema de la vigencia de los derechos fundamentales inespecíficos del trabajador en el contrato de trabajo, pues como se viene afirmando, "la celebración de un contrato de trabajo no implica en modo alguno

[4] Rodríguez Escanciano, S.: "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Revista de Trabajo y Seguridad Social CEF*, núm. 423 (2018), p. 22.

[5] Como señala Martínez Moya "la transversalidad del derecho fundamental a la protección de datos tiene su claro reflejo en las relaciones laborales". Martínez Moya, J.: "El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores", *Revista de Jurisprudencia Laboral*, núm. 1 (2019), p. 8.

[6] Dictamen 8/2001, sobre el tratamiento de datos personales en el contexto laboral (13.9.2001), adoptado por el Grupo de Trabajo del Artículo 29. Citado en el Informe 0529/2009 de la AEPD de donde se toma.

[7] Art. 4.7 RGPD.

[8] Art. 4.1 RGPD.

[9] García Murcia, J.: "La protección de datos personales en el ámbito laboral: una sucinta reseña jurisprudencial a partir de cinco sentencias del Tribunal Supremo", *Revista Galega de Dereito Social*, núm. 5 (2018), p. 10.

[10] Dictamen del Grupo de Trabajo del artículo 29 (8/2001), sobre el tratamiento de datos personales en el contexto laboral.

[11] Un ejemplo bien significativo: Art. 8.3 ET.

la privación para una de las partes, el trabajador, de los derechos que la Constitución le reconoce como ciudadano. Ni las organizaciones empresariales forman mundos separados y estancos del resto de la sociedad ni la libertad de empresa que establece el art. 38 del texto constitucional legitima el que quienes prestan servicios en aquélla por cuenta y bajo la dependencia de sus titulares deban soportar despojos transitorios o limitaciones injustificadas de sus derechos fundamentales y libertades públicas, que tienen un valor central y nuclear en el sistema jurídico constitucional" (STC 88/1985, de 19 julio [FJ 2]).

3.º De los dos elementos anteriores, necesidad del tratamiento de datos personales para el desenvolvimiento de la relación laboral y atribución al trabajador de un poder de disposición y de control sobre los mismo configurado como derecho fundamental, resultará la modulación del derecho fundamental a la protección de datos. Así sucede con carácter general cuando se confrontan los derechos fundamentales del trabajador con los del empresario (arts. 33 y 38 CE)[12] o de otros sujetos (art. 28.1 CE) que también pueden tener interés legítimo en el acceso a datos personales de los trabajadores. Lo peculiar del derecho a la protección de datos es que el equilibrio con otros derechos fundamentales no queda remitido sólo a la ponderación judicial, sino que cuenta con una importante regulación legislativa que ya la ha efectuado: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD)[13].

El derecho fundamental a la protección de datos personales se convierte así en un punto desde el que el Derecho del Trabajo, y particularmente el contrato de trabajo, puede ser mirado en su integridad[14]. A la luz de este derecho fundamental, entre el trabajador, como "interesado", y el empresario, como "responsable del tratamiento" de los datos personales, se anudan un complejo conjunto de derechos y obligaciones. De ese amplio conjunto de obligaciones y derechos corresponde a este trabajo el estudio de la recogida y tratamiento de datos personales en el contexto del contrato de trabajo. Ese contexto, amplísimo, de algún modo resulta definido en el art. 88 RGPD: contratación de personal; ejecución del contrato; 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; efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo; extinción de la relación laboral. Obviamente no se va a estudiar en este artículo toda la problemática que plantea la recogida y tratamiento de datos personales en el contrato de trabajo, por cuanto en otros estudios de este mismo número de la *Revista del Ministerio* se analizan los aspectos específicos del derecho analizado: la protección de datos en los procesos de selección de personal; el tratamiento de de

[12] STC 90/1997, de 6 mayo (FJ 4).

[13] Deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (en adelante, LOPD-1999).

[14] A la "reinterpretación del conjunto del Ordenamiento jurídico en clave de protección de datos" alude R. MARTÍNEZ MARTÍNEZ: "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política*, núm. 5 (2007), p. 52.

las categorías especiales de datos personales a las que se refiere el art. 9 RGPD (datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física); la protección de datos y el registro de la jornada de trabajo; denuncias internas (art. 24 LOPDGDG); o, en fin, el estudio de los derechos digitales expresamente nominados en la LOPDGDG: intimidad y uso de dispositivos digitales (art. 87), desconexión digital (art. 89); intimidad frente al uso de sistemas de videovigilancia y grabación de sonidos (art. 89); sistemas de geolocalización (art. 90); o al papel de la negociación colectiva en la protección de datos (art. 91). También, por supuesto, se estudian en otros artículos de este volumen los aspectos generales del derecho: marco normativo, configuración y contenido del derecho. Por tanto, para evitar innecesarias y tediosas reiteraciones, se ha optado por presentar en estas páginas, siguiendo la ordenación sistemática habitual[15], una sucinta reseña de la casuística más destacada que ha planteado la recogida y tratamiento de datos en el contexto del contrato de trabajo[16].

2. RECOGIDA Y TRATAMIENTO DE DATOS EN LA CELEBRACIÓN DEL CONTRATO DE TRABAJO: CONSENTIMIENTO DEL TRABAJADOR, EJECUCIÓN DEL CONTRATO Y CUMPLIMIENTO DE OBLIGACIONES LEGALES

2.1. Tratamiento de datos personales necesario para la ejecución del contrato y consentimiento del trabajador

La celebración del contrato de trabajo es un momento en el que se concentra de modo importante la recogida y tratamiento de datos personales de los trabajadores. El mismo contrato de trabajo puede ser instrumento útil para el cumplimiento de dos importantes funciones: recabar el consentimiento del trabajador para el tratamiento de datos [art. 6.1.a) RGPD] e informarle sobre el tratamiento realizado [arts. 12 y 13 RGPD]. Respecto de los datos que el empresario puede recabara hay que estar al principio de "minimización de datos": los datos personales han de ser "recogidos con fines determinados, explícitos y legítimos" [art. 5.1.b) RGPD] y "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" [art. 5.1.c) RGPD].

Basta leer un formulario de contrato de trabajo para apreciar el importante número de datos personales que requiere su formalización: nombre y apellidos, número de documento nacional de identidad, fecha de nacimiento, número de afiliación a la Seguridad Social, nacionalidad, domicilio y nivel formativo. Además en función de la clase de contrato de que se trate podrán exigirse otros datos relativos a situaciones personales del trabajador: discapacidad, desempleo, exclusión social, víctima de violencia de género, de terrorismo o de trata de seres humanos y grado de parentesco con el empresario. Son datos que se encuentran bajo el poder de disposición y control del trabajador cuyo tratamiento resulta absolutamente necesario para la celebración

[15] DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, Valladolid, Lex Nova, 2012, pp. 90 a 92. RODRÍGUEZ ESCANCIANO, S.: *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Albacete, Bomarzo, 2009, pp. 9 a 15. PRECIADO DOMENECH, C. H.: *El derecho a la protección de datos en el contrato de trabajo*, Cizur Menor (navarra), 2017. MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3ª ed., Madrid, Lefebvre, Madrid, 2019. GARCÍA MURCIA; RODRÍGUEZ CARDO: *cit.*, p. 9.

[16] Sobre la recogida y tratamiento de datos en el contexto de las relaciones colectivas de trabajo véase MERCADER UGUINA, J. R.; DE LA PUEBLA PINILLA, A.: "Protección de datos y relaciones colectivas", *Revista de Trabajo y Seguridad Social. CEF*, núm. 423 (2018).

del contrato de trabajo. Por tanto la licitud de su recogida y tratamiento se encuentra en la regla del art. 6.1.b) RGPD: el tratamiento será lícito si "es necesario para la ejecución de un contrato en el que el interesado es parte". Como ha señalado la STC 39/2016 "en el ámbito laboral el consentimiento del trabajador pasa […] como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes". No es necesario, por tanto, recurrir al principio del consentimiento del interesado [art. 6.1.a) RGPD] para hacer lícito el tratamiento de estos datos indispensables para la celebración y posterior ejecución del contrato de trabajo. Igual régimen que los datos citados anteriormente tendrían otros, también necesarios para el cumplimiento de obligaciones empresariales durante el desarrollo del contrato de trabajo, que se suelen recoger en el momento de la celebración del contrato como sucede con la cuenta bancaria para el abono del salario (art. 29.4 ET)[17].

Más allá de los datos personales necesarios para la ejecución del contrato de trabajo puede que el empresario tenga interés en acceder a otros que no son necesarios pero cuya recogida y tratamiento puede resultarle conveniente. Así sucedería con datos personales de muy frecuente uso en el trato social como son la dirección particular de correo electrónico y el número del teléfono privado que, salvo excepciones, no son necesarios para el cumplimiento del contrato de trabajo. En estos casos la única fuente de licitud del tratamiento de estos datos sería el consentimiento del trabajador, por lo que resulta pertinente plantear cuáles serían los requisitos de una válida prestación de consentimiento del trabajador para ser considerada una "manifestación de voluntad libre, específica, informada e inequívoca" del interesado (art. 4.11 RGPD). La normativa sobre protección de datos personales contempla con muchas limitaciones y cautelas la prestación del consentimiento del interesado en el mismo contrato para el tratamiento de datos que no están necesariamente relacionados con su celebración y cumplimiento. La razón de estas precauciones es clara: se trataría de una cláusula inseparable del mismo contrato, de modo que el trabajador lo acepta o lo rechaza íntegramente. La aceptación del empleo va unida a la del tratamiento de esos datos personales que no están relacionados con el mantenimiento del contrato: o lo toma todo o lo deja todo. En una relación como la laboral, de posiciones asimétricas y de debilidad contractual del trabajador, se podría afirmar que el consentimiento para el tratamiento de esos datos personales dista de haber sido prestado en condiciones de plena libertad[18]. En este sentido las *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679* del Grupo de Trabajo del artículo 29 sobre Protección de Datos afirman que "dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas"[19].

[17] SEMPERE NAVARRO, A. V.: "El deber de facilitar una cuenta corriente bancaria", *Revista de Jurisprudencia Laboral*, núm. 7 (2019).

[18] De "fuerza o compulsión económica" habla VILLALBA SÁNCHEZ, A.: "El derecho fundamental a la protección de datos del trabajador frente a los riesgos de la contratación estandarizada", *Nueva Revista Española de Derecho del Trabajo*, núm. 207 (2018), p. 105. SÁNCHEZ QUIÑONES, L.: "El marco legislativo de la protección de datos en el ámbito laboral. Especial referencia al consentimiento del trabajador", *Diario La ley*, núm. 9377 (2019), (versión electrónica La Ley 2789/2019).

[19] Dice así el citado documento: "También en el contexto del empleo se produce un desequilibrio de poder. Dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. Parece poco probable que un empleado pudiera responder libremente a una solicitud de consentimiento de su empleador para, por ejemplo, activar sistemas de vigilancia por cámara en el lugar de trabajo o para rellenar

El propio RGPD recoge esta problemática en su art. 7.4 RGPD cuando dice que para evaluar si el consentimiento se ha prestado libremente "se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato"[20]. De igual modo conforme al art. 6.3 LOPDGDD "no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual".

Se trata de una cuestión que ha dado lugar a una cierta litigiosidad en la que se puede apreciar dos grandes grupos de casos. Uno en el que los datos personales para cuyo tratamiento se presta el consentimiento no guardan relación con el objeto del contrato de trabajo y otro en el que los datos personales sí están implicados en la prestación laboral del trabajador. En el primer caso no se considera válida la prestación del consentimiento, en el segundo sí. Dentro del primer grupo la STS de 21 de septiembre de 2015 (rec. 259/2014)[21] tuvo que resolver sobre la validez de la siguiente cláusula-tipo incorporada por el empresario en los contratos de trabajo:

> "Ambas partes convienen expresamente que cualquier tipo de comunicación relativa a este contrato, a la relación laboral o al puesto de trabajo, podrá ser enviada al trabajador vía SMS o vía correo electrónico, mediante mensaje de texto o documento adjunto al mismo, sin menoscabo del cumplimiento por parte de la empresa de los requisitos formales exigidos por la normativa laboral vigente, y según los datos facilitados por el trabajador a efectos de contacto. Cualquier cambio o incidencia con respecto a los mismos, deberá ser comunicada a la empresa de forma fehaciente y a la mayor brevedad posible"[22].

El razonamiento del Tribunal Supremo para resolver el problema se construye sobre dos fundamentos bien claros:

1.º El número de teléfono móvil y la dirección de correo electrónico son datos personales que no resultan necesarios para el cumplimiento del contrato, por lo que la licitud de su tratamiento no puede hallarse en la regla del art. 6.1.b) RGPD. Que no resultan ni necesarios ni imprescindibles lo muestra claramente la circunstancia de que "la relación laboral pueda desenvolverse –lo ha veni-

impresos de evaluación, sin sentirse presionado a dar su consentimiento.

Por tanto, el GT29 considera problemático que los empleadores realicen el tratamiento de datos personales de empleados actuales o futuros sobre la base del consentimiento, ya que no es probable que este se otorgue libremente. En el caso de la mayoría de estos tratamientos de datos en el trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores [artículo 6, apartado 1, letra a)] debido a la naturaleza de la relación entre empleador y empleado.

No obstante, esto no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas". COSTA, R.: "Protección de datos en el ámbito laboral", en RALLO LOMBARTE, A.: *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019, p. 7 [versión electrónica TOL7.218.410].

[20] El considerando 43 del preámbulo del RGPD señala que "para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento".

[21] RJ 2015, 4353.

[22] AH 4.º

do haciendo hasta las recientes fechas en que tales avances tecnológicos eran inexistentes– sin tales instrumentos, evidencia que no puedan considerarse incluidos en aquella salvedad general" del art. 6.1.b) RGPD (FJ 3).

2.º Al no resultar necesarios para el cumplimiento del contrato la licitud de su tratamiento requerirá el consentimiento del trabajador: el "Tribunal en absoluto niega que voluntariamente puedan ponerse aquellos datos a disposición de la empresa, pues ello es algo incuestionable; es más, incluso pudiera resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos" (FJ 3).

La cuestión queda así desplazada a la determinación de las características que debe tener la prestación del consentimiento del trabajador para ser considerada válida, para que se estime que se está ante una "manifestación de voluntad libre, específica, informada e inequívoca" del interesado (art. 4.11 RGPD). El Tribunal Supremo, siguiendo los criterios restrictivos de la normativa de protección de datos, no "niega que voluntariamente puedan ponerse aquellos datos a disposición de la empresa, pues ello es algo incuestionable; es más, incluso pudiera resultar deseable, dado los actuales tiempos de progresiva pujanza telemática en todos los ámbitos", pero se opone a que "en el contrato de trabajo se haga constar –como específica cláusula/tipo– que el trabajador presta su «voluntario» consentimiento a aportar los referidos datos personales y a que la empresa los utilice en los términos que el contrato relata, siendo así que el trabajador es la parte más débil del contrato y ha de excluirse la posibilidad de que esa debilidad contractual pueda viciar su consentimiento a una previsión negocial referida a un derecho fundamental, y que dadas las circunstancias –se trata del momento de acceso a un bien escaso como es el empleo– bien puede entenderse que el consentimiento sobre tal extremo no es por completo libre y voluntario". La conclusión es clara: la falta de garantías para la prestación del consentimiento lleva a considerar "que tal cláusula es nula por atentar contra un derecho fundamental, y que debe excluirse de los contratos de trabajo" (FJ 3).

También sobre una cláusula tipo inserta en los contratos de trabajo que, indirectamente, implica la obligación del trabajador de comunicar su número de teléfono móvil y dirección de correo electrónico trata la SAN de 6 de febrero de 2019 (rec. 318/2018)[23]. Indirectamente, porque a lo que se obligaba el trabajador, repartidor de comida a domicilio, era a aportar su propio teléfono móvil en el que debía descargarse la aplicación informática de la empresa facilitada a través de su dirección de correo electrónico. De este modo se pretendía tenerlo geolocalizado durante su jornada laboral[24]. La sentencia de la Audien-

[23] AS 2019, 905.

[24] El texto de la cláusula era el siguiente: "Para el desarrollo de las funciones propias del puesto de trabajo, concretamente en la realización de las funciones de reparto de productos, objeto del presente contrato, el trabajador deberá aportar un teléfono móvil de su propiedad con conexión a internet (Smartphone) que permita la instalación y correcto funcionamiento de la aplicación (app) creada por Telepizza a dichos efectos.

El teléfono móvil y aplicación mencionados deberán utilizarse durante la totalidad de la jornada laboral del trabajador a efectos de que tanto la empresa como sus clientes puedan realizar un seguimiento en tiempo real y mediante geolocalización, de la ubicación de los pedidos que se realizan.

Será responsabilidad del trabajador acudir al centro de trabajo con el citado dispositivo en plenas condiciones de utilización (batería cargada, tarifa de datos disponible, etc.) y obligación suya desconectarse de la aplicación (app) una vez finalizada su jornada laboral.

La aportación de teléfono móvil por parte del trabajador deberá realizarse en los términos y resto de condiciones de utilización que en cada momento consten en la normativa interna de la empresa y, en caso de incumplimiento de la misma, será de aplicación el régimen disciplinario previsto en el convenio colectivo aplicable.

La negativa reiterada o imposibilidad sobrevenida de aportación de esta herramienta por parte del trabajador, o de la aplicación informática antes mencionada, será causa suficiente para la extinción del contrato de trabajo al amparo de lo previsto en el artículo 49.1.b) del Texto Refundido de la Ley del Estatuto de los Trabajadores.

Concretamente el trabajador, tendrá un plazo de diez días para repararlo y ponerlo de nuevo en funcionamiento al undécimo día. A partir del momento de la carencia del teléfono

cia Nacional no entra en la valoración del consentimiento del trabajador para el tratamiento de estos datos, por entender que el sistema de geolocalización instalado vulnera de pleno el derecho a la privacidad de los trabajadores[25] al establecer un sistema desproporcionado de control[26]: "la medida implantada, si bien obedece a fines constitucionalmente legítimos en el desarrollo del derecho a la libre empresa como son el control el empleado en el desempeño de su puesto de trabajo y la oferta de un mejor servicio al cliente– de forma que éste pueda conocer en todo momento la ubicación de su pedido, dotando a la empresa de capacidad para proporcionar servicios que se afirma ya ofrecen otras empresas del sector–, no supera a juicio de la Sala el necesario juicio de proporcionalidad". Esa finalidad legítima "se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados como pudieran ser la implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos que no implican para el empleado la necesidad de aportar medios propios y lo que es más importante, ni datos de carácter personal como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema" (FJ 6). Pese a que no sea objeto de pronunciamiento en la sentencia, de ella puede deducirse que el consentimiento del trabajador en el momento de la celebración del contrato resulta irrelevante si el tratamiento es desproporcionado. Se trataría de una específica aplicación del art. 3.1.c) ET: cláusula contractual menos favorable o contraria a disposición legal.

Dentro del segundo grupo, prestación de consentimiento para el tratamiento de datos personales del trabajador que sí están implicados en el objeto del contrato, la STS de 10 de abril de 2019 (rec. 227/2017)[27] analiza la validez de una cláusula tipo contenida en los contratos que una empresa del sector de *contact center*, antiguo telemarketing, celebra con sus trabajadores[28]: "El trabajador consiente expresamente, conforme a la LO 1/1982, de 5 de mayo, RD 1720/2007 de Protección de Datos de carácter personal y Ley Orgánica 3/1985 de 29 de mayo, a la cesión de su imagen, tomada mediante cámara web o cualquier otro medio, siempre con el fin de desarrollar una actividad propia de telemarketing y cumplir, por tanto, con el objeto del presente contrato y los requerimientos del contrato mercantil del cliente". La empresa, con unos seis mil trabajadores en plantilla, presta servicios que incluyen la realización de videollamadas. En el momento de la reclamación tenía contratos con dos clientes cuyo cumplimiento exigía la realización de videollamadas en las que intervenían quince trabajadores. Por otra parte, cuando la empresa utiliza la imagen de sus empleados para realizar actividades promocionales les solicita una autorización específica.

En la instancia la SAN de 15 de junio de 2017 (rec. 137/2017)[29] declaró la invalidez de

o bien finalizado el período de diez días sin que el trabajador hubiese aportado nuevamente su propio teléfono, se procederá a suspender el contrato de trabajo del citado empleado por un período máximo de dos meses. Finalizado dicho periodo el contrato se dará por definitivamente finalizado. Durante el período de suspensión" (HP 4º).

[25] Como dice Martínez Moya la sentencia "se refiere a la privacidad, sin mayores precisiones, cuando el derecho fundamental a la protección de datos es de más amplio espectro" (*cit.*, p. 7).

[26] Además "para la implantación del sistema de geolocalización por parte del empleador se ha prescindido de proporcionar a los trabajadores de la información a que se refieren los arts. 12 y 13 del Reglamento 679/2016, 5 de la anterior Ley de protección de datos y 11 y 90 de la vigente LO 3/2018 " (FJ 6).

[27] RJ 2019, 1880.

[28] Cano Galán, Y.: "Cláusulas contractuales tipo sobre cesión de derechos de imagen de los trabajadores y cumplimiento de la normativa sobre protección de datos de carácter personal", *Diario La Ley*, 24 de Mayo de 2018 (LA LEY 7684/2019). García-Perrote Escartín, I.; Mecader Uguina, J. R.: "Datos personales y cláusulas contractuales: los límites del consentimiento en la doctrina reciente del Tribunal Supremo", *Revista Española de Derecho del Trabajo*, núm. 223 (2019). Arias Domínguez, Á.: "Video-llamadas en trabajos de contact-center y cesión de derechos de imagen", *Revista de Jurisprudencia Laboral*, núm. 3 (2019).

[29] AS 2017, 1528.

esta cláusula contractual. Su razonamiento se alza sobre la idea de que no forma parte de la prestación comprometida por el trabajador el uso de su imagen, por lo que su captación requiere el consentimiento del trabajador que no se puede entender prestado libremente en una cláusula tipo del contrato de trabajo:

a) La captación y uso de la imagen del trabajador resulta imprescindible para la realización de las videollamadas. Sin embargo esta actividad resulta muy infrecuente en la empresa: sólo participan en ella quince de sus seis mil trabajadores.

b) Por tanto se puede trabajar en esta empresa sin necesidad de que se produzca la captación y uso de la imagen el trabajador, de modo que "no es absolutamente imprescindible para el cumplimiento del objeto del contrato, puesto que se utiliza [la videollamada], al menos hasta ahora, de manera absolutamente excepcional".

c) La captación, uso y cesión de la imagen del trabajador por el empresario, al no formar parte del objeto del contrato, requiere el consentimiento expreso del trabajador. Un consentimiento que debe ser específico y distinto del genérico constitutivo del contrato.

d) Ese consentimiento no puede expresarse en la cláusula tipo incluida en el contrato de trabajo puesto que la situación de inferioridad en que se encuentra el trabajador en el momento de celebrar el contrato impide que se pueda hablar de un consentimiento libre de acuerdo con la STS de 21 de septiembre de 2015.

e) El momento idóneo para manifestar el consentimiento del trabajador surgirá "cuando la empresa destine a sus trabajadores a la realización de servicios de video llamada, porque lo requiera así el contrato mercantil con el cliente, deberá solicitar, en ese momento, el consentimiento del trabajador, que deberá ajustarse de manera precisa y clara a los requerimientos de cada contrato, sin que sea admisible la utilización de cláusulas tipo de contenido genérico, que no vayan asociadas a servicios concretos, requeridos por contratos específicos, por cuanto dicha generalización deja sin contenido real el derecho a la propia imagen de los trabajadores, que queda anulado en la práctica, aunque se diera consentimiento genérico al formalizar el contrato".

El Tribunal Supremo, sin embargo, ha declarado la validez de la cláusula contractual. Con carácter general parte de que la imagen[30] constituye un dato personal cuya captación y tratamiento requiere el consentimiento del interesado, salvo que sea necesario para la ejecución de un contrato del que se es parte (6.1.b RGPD). Descendiendo al caso concreto planteado en esta empresa, considera que la participación en videollamadas forma parte del oficio del trabajador, de su prestación laboral, por lo que se trata de realizar "funciones propias del objeto del contrato celebrado, aunque no sean las habituales" (FJ 2)[31]. A ello no obsta la reducida incidencia y frecuencia con se requieren los servicios de videollamada en la empresa, sólo con dos clientes y por quince trabajadores entre los seis mil de la empresa, "porque lo importante no es el mayor o menor uso que se haga de esa función, sino que el consentimiento está implícito en el contrato por su objeto y además

[30] Véase CRISTÓBAL RONCERO, R.: "Protección del derecho a la propia imagen en el trabajo", *Nueva Revista Española de Derecho del Trabajo*, núm. 199 (2017), pp. 75 a 95.

[31] El "objeto del contrato y su ejecución es la realización de labores de telemarketing incluso con video-llamadas, lo que es hasta cierto punto lógico porque, dados los avances tecnológicos existentes, la capacidad de inspirar confianza y de convencer es mayor cuando vemos la cara de nuestro interlocutor y desechamos la idea de que se habla con una máquina o con un desconocido. En este sentido se puede señalar que la información sobre una mercancía y su venta resultan más fáciles cuando el comprador ve el producto y al vendedor, como en las tiendas tradicionales" (FJ 2).

que se ha explicitado en él por el trabajador, quien en todo momento puede revocarlo (art. 7 del Reglamento), o negarse a realizar tareas en condiciones que escapen al contenido propio de su contrato, sin perjuicio de las consecuencias que ello pueda tener" (FJ 2).

Una vez afirmado que la participación en videollamadas forma parte de la prestación del trabajador las consecuencias se derivan necesariamente: a) no será necesario el consentimiento del trabajador para su tratamiento, sino que estaremos ante la excepción del art. 6.1.b) RGPD; y b) la cláusula contractual en cuestión es válida y en cuanto expresa un consentimiento del trabajador innecesario, pues va dirigido a autorizar un tratamiento de datos requerido para el cumplimiento del contrato, cumple una finalidad meramente informativa. Así puede leerse en su fundamento jurídico segundo: "si se trata de la realización de funciones propias del objeto del contrato celebrado, aunque no sean las habituales, es lo cierto que la cláusula controvertida se limita a advertir al nuevo contratado de la posibilidad de tener que realizar una de las funciones propias del contrato que suscribe y, a la par que el mismo queda advertido de ello, presta, expresamente, su consentimiento a la cesión de su imagen, pero con una salvaguarda: "siempre con el fin de desarrollar una actividad propia de telemarketing y cumplir, por tanto, con el objeto del presente contrato", esto es que la cesión de la imagen, el dato, venga condicionada a que su fin sea cumplir con el objeto del contrato". Por tanto la cláusula controvertida "no es abusiva, sino, más bien, informativa y a la par receptora de un consentimiento expreso que no era preciso requerir", de acuerdo con la normativa de protección de datos conforme a la cual "el consentimiento no es necesario prestarlo hoy día, ni lo era entonces, cuando los datos, la imagen, se ceden en el marco del cumplimiento de un contrato de trabajo cuyo objeto lo requiere. Por ello, la cláusula controvertida no se puede considerar abusiva, ni calificar de nula, porque es lícita, dado que es manifestación de un consentimiento expreso que el trabajador da a la cesión de su imagen, cuando la actividad propia del telemarketing, la del convenio colectivo, la desarrolle por video-llamada y que está implícito en el objeto del contrato" (FJ 2).

El Tribunal Supremo cierra su argumentación distinguiendo el supuesto examinado de los que fueron objeto de decisión en la STC 99/1994, de 11 de abril y en la ya citada STS de 21 de septiembre de 2015. En el archiconocido caso de la STC 99/1994 sobre el deshuesador de jamones, la cesión de la imagen del trabajador no formaba parte de las tareas contratadas lo que sí sucede en el supuesto ahora resuelto: por tanto en el caso de la empresa de *contact center* la restricción de los derechos a la propia imagen y a la protección de datos personales "viene impuesta por la naturaleza de las tareas contratadas" (FJ 2). Por otra parte, la distinción con el supuesto de la STS de 21 de septiembre de 2015 es obvia: en ella se enjuició una cláusula contractual en virtud de la cual el trabajador aceptaba el tratamiento de datos innecesarios para el cumplimiento del contrato, mientras que en ésta la cláusula enjuiciada "se limita a expresar cual puede ser una de las labores a realizar y la aceptación de ese deber" (FJ 2).

* * * * * *

No son infrecuentes los pactos, individuales o colectivos[32], en virtud de los cuales el empresario asume la obligación de concertar algún tipo de seguro en favor del trabajador, por

[32] Un par de ejemplos. *Convenio colectivo estatal del sector de desinfección, desinsectación y desratización* (BO de 10 de abril de 2018). Artículo 32. Seguro colectivo de accidentes. Las empresas establecerán un seguro colectivo de accidentes para todos/as los/as trabajadores/as que garanticen a los mismos la percepción de 16.500– euros, en caso de que como consecuencia del accidente el/la trabajador/a quede en situación de incapacidad permanente absoluta, o de 23.100– euros si como consecuencia del accidente se produjera el fallecimiento, cantidad que percibirán sus beneficiados. *Convenio colectivo de centros de asistencia y educación infantil* (BOE de 26 de julio de 2019). Artículo 75. Responsabilidad civil y accidentes. Todos los Centros deberán contratar pólizas de seguros que garanticen la cobertura de accidentes y responsabilidad civil de todo el personal afectado por este Convenio. Deberán estar en vigor durante el período correspondiente, pudiendo prorrogarse o modificarse a petición de las organizaciones firmantes.

lo que también en el momento de la contratación habrá que proceder a la recogida y tratamiento de sus datos personales a tal efecto. Tratándose de una condición más beneficiosa individual o de una obligación impuesta por el convenio colectivo la licitud del tratamiento derivaría del art. 6.1.b) RGPD (tratamiento necesario para la ejecución de u contrato del que se es parte), pues tanto el contrato como el convenio colectivo son fuente de la relación laboral [art. 3.1.b) y c) ET][33].

Como señala la Guía de la Agencia Española de Protección de Datos (en adelante, AEPD) *La protección de datos en las relaciones laborales* en estos casos[34] el empresario puede realizar uno de estos dos tratamientos de datos: la comunicación a la aseguradora de los datos de contacto del trabajador para que ésta recabe los datos necesarios a efectos de formalizar el seguro correspondiente o la recogida y comunicación a la seguradora de todos los datos necesarios. El tratamiento de datos en ambos casos, también según la *Guía* citada, estaría legitimado por el consentimiento del trabajador o por el propio contrato de trabajo. La *Guía* señala que "desde el punto de vista de un tratamiento absolutamente respetuoso con el derecho fundamental lo más adecuado puede consistir en, previa información a los trabajadores, ceder a la aseguradora, o a la gestora del plan de pensiones, únicamente los datos de los asegurados o partícipes del plan de pensiones, dejando en sus manos el desarrollo de ulteriores gestiones"[35].

La AEPD ha tenido ocasión de examinar en su Resolución E/02259/2015 la cesión de datos del trabajador por parte del empresario a la empresa depositaria de un plan de pensiones. Este plan se configura como premio de fidelización para los trabajadores de cierta antigüedad, es adicional a otros planes de pensiones y ahorro con los que ya contaba la empresa y forma parte de su club de fidelización. La adhesión de los trabajadores al plan se produce de modo automático al alcanzar la antigüedad requerida, de acuerdo con lo previsto en el art. 28.2 del Reglamento de Planes y Fondos de Pensiones (incorporación directa del trabajador al plan en virtud de acuerdo adoptado por la empresa con los representantes de los trabajadores, con información al trabajador y derecho de éste a oponerse a la incorporación)[36].

[33] Los datos necesarios para el mantenimiento y cumplimiento del contrato de trabajo incluyen "no sólo las obligaciones derivadas del contrato de trabajo, sino también las impuestas por la ley y, de manera más problemática, las que puedan derivar de otras normas laborales, como el convenio colectivo" (DESDENTADO BONETE; MUÑOZ RUIZ: *cit.*, p. 105).

[34] Página 16.

[35] Página 17.

[36] RD 304/2004, de 20 de febrero. Artículo 28. Adhesión de partícipes en planes de empleo.

1. Efectuada la comunicación de la admisión del plan en el fondo prevista en el artículo anterior, podrá hacerse efectiva la incorporación al plan de partícipes, y la comisión promotora del plan de empleo deberá instar la constitución de la pertinente comisión de control del plan en un plazo no superior a 12 meses desde la formalización del plan. En tanto no se constituya la comisión de control, las funciones atribuidas a ésta por este Reglamento corresponderán a la comisión promotora.

2. Cuando en el convenio colectivo se haya establecido la incorporación de los trabajadores directamente al plan de pensiones, se entenderán adheridos a éste, salvo que, en el plazo acordado a tal efecto, declaren expresamente por escrito a la comisión promotora o de control del plan que desean no ser incorporados al plan. Lo anterior se entenderá sin perjuicio de que, en su caso, el convenio condicione las obligaciones de la empresa con los trabajadores a su incorporación al plan de pensiones.

Asimismo, en virtud de acuerdo adoptado por la empresa con los representantes de los trabajadores en ésta, la comisión promotora, una vez formalizado el plan de pensiones del sistema de empleo, podrá efectuar directamente la incorporación al plan de los partícipes y, en su caso, de los beneficiarios, debiendo señalarse un plazo para que los que no deseen incorporarse al plan se lo comuniquen por escrito. También será admisible la suscripción de documentos individuales o colectivos de adhesión al plan del sistema de empleo en virtud de delegación expresa otorgada por los partícipes.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio de que, en su caso, el convenio colectivo o disposición equivalente que establezca los compromisos por pensiones condicione la obligación de la empresa a su instrumentación a través de un plan del sistema de empleo, o de las acciones y derechos que corresponda ejercitar en caso de discrepancia o información inadecuada sobre los procesos de incorporación al plan.

3. El trabajador que reúna las condiciones para acceder al plan podrá ejercitar su derecho de incorporación en cualquier momento y en tanto no se haya extinguido la relación laboral con el promotor, sin perjuicio del régimen de aportaciones y prestaciones aplicable en cada caso.

En el caso contemplado, la empresa informó a los trabajadores a través de diversas acciones internas (eventos en tienda, reparto de información y comunicación en distintos soportes, noticias en la intranet corporativa, carteles informativos, etc.) y disponía de una plataforma *online* para que los empleados pudieran comprobar los requisitos de acceso al programa, recabar información y cursar baja en caso de no estar interesados. La AEPD estimó que existía un consentimiento tácito del trabajador para el tratamiento de sus datos por dos razones: el trabajador solo formuló la denuncia un año después de la constitución del plan y este plan resultaba complementario de otros de los que ya era beneficiario. También estimó que el empresario había cumplido con su deber de informar a través de las diferentes acciones antes descritas. Por todo ello la AEPD afirmó que la cesión de datos a la entidad depositaria del plan había sido legítima según el art. 11.2.c) LOPD-1999[37]. Téngase en cuenta que con la normativa vigente no resulta admisible el consentimiento tácito[38], por lo que en cuanto en estos casos se trate de una obligación derivada de las reglas del contrato (legales, convencionales o contractuales) será el cumplimiento de éste la fuente de legitimación del tratamiento.

2.2. Tratamiento de datos necesario para el cumplimiento de obligaciones legales del empresario

Con la celebración del contrato de trabajo surgen varias obligaciones del empresario que van a requerir el tratamiento de datos personales del trabajador: la comunicación del contrato a la oficina pública de empleo (art. 8.3 ET), la entrega de la copia básica del contrato a los representantes de los trabajadores (art. 8.4 ET) y el alta del trabajador en la Seguridad Social (arts. 16, 139 y 140 LGSS). En todos estos casos se va a producir lo que la LOPD-1999 definía como "cesión o comunicación de datos" [art. 3.j)], es decir, una "revelación de datos realizada a una persona distinta del interesado", un tercero (administración pública, representantes de los trabajadores). La cesión o comunicación de datos exigía, como regla general, el previo consentimiento del interesado junto con la legitimidad del fin para el que se producía la cesión (art. 11.1). Esta regla general contemplaba varias excepciones entre las cuales se encontraban dos que resultaban particularmente aplicables en la relación laboral: la autorización de la ley [art. 11.2.a)] y la "libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros" [art. 11.2.c)]. Sin embargo ni el RGPD ni la LOPDGDD establecen un régimen específico para la cesión o comunicación de datos, por lo que resulta aplicable el régimen general del tratamiento[39]. En efecto, el art. 4.2) RGPD incluye la comunicación entre las operaciones integradas en la noción de tratamiento y el art. 4.9) RGPD define al "destinatario" como la persona, autoridad pública, servicio u otro organismo al que se comuniquen datos personales. Será por tanto el criterio del art.6.1.c) RGPD, tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento[40], el fundamento de este tipo de tratamiento de datos.

De acuerdo con los arts. 8.4 y 64.4 ET el empresario debe entregar a la representa-

Teniendo en cuenta lo previsto en el artículo 25.2, párrafo segundo, en los casos en que se prevea la incorporación al plan de trabajadores que hubieran extinguido su relación laboral con el promotor, las especificaciones precisarán las condiciones para su incorporación y el régimen de aportaciones y prestaciones aplicable.

[37] No será necesario el consentimiento del interesado "cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros".

[38] Preámbulo de la LOPDGDD, apartado V.

[39] Messía de la Cerda Ballesteros, J. A.: "La evolución del concepto de cesión o comunicación de datos personales", *Actualidad Civil*, núm. 10 (2017), p. 8 (citado según versión digital La Ley 14126/2017).

[40] Art. 8.1 LOPDGDD.

ción de los trabajadores una copia básica de todos los contratos que deban celebrarse por escrito. El contrato contiene datos personales del trabajador de los que debe excluirse en la copia básica el número del documento nacional de identidad, el número de identidad del extranjero, el domicilio, el estado civil y cualquier otro que pudiera afectar a la intimidad personal. El art. 8.4 ET impone al empresario la obligación de entregar a los representantes de los trabajadores una copia básica del contrato, por lo que la entrega de cualquier copia que no fuera "básica" no podría estar fundada en el art. 6.1.c) RGPD. Conforme al art. 5.1.b) RGPD estos datos no podrán ser tratdos ulteriormente de manera incompatible con el fin para el que son recogidos: comprobar la adecuación del contenido del contrato a la legalidad vigente (art. 8.4 ET).

El salario ha sido el dato personal contenido en el contrato de trabajo que ha generado una mayor conflictividad en relación con el cumplimiento de la obligación impuesta por el art. 8.4 ET. Una litigiosidad, por otra parte, tangencial al derecho a la protección de datos personales como se explica a continuación.

a) A raíz de la promulgación de la Ley de 2/1991, de 7 de enero, precedente del vigente art. 8.4 ET, se discutió si el salario es un dato personal que afecta a la intimidad del trabajador. La consecuencia de la respuesta a esa cuestión era importantísima: si es dato que afecta a la intimidad del trabajador debe excluirse de la copia básica que se entrega a la representación de los trabajadores. La cuestión fue resuelta por la STC 142/1993, de 22 de abril en el sentido de que el salario no es dato relativo a la intimidad del trabajador. Por tanto será el derecho a la protección de datos el único que se vea afectado con su tratamiento por el empresario en estos casos pues, como es bien sabido, se trata de derechos autónomos: mientras el derecho a la intimidad se refiere a datos íntimos el de protección de datos afecta a cualesquiera datos personales[41].

b) El otro factor de litigiosidad no afecta tanto al derecho a la protección de datos como al ámbito del derecho de información de los representantes de los trabajadores. Se trata de la práctica de configurar el contenido de determinadas cláusulas contractuales por remisión al convenio colectivo aplicable ("según convenio"). Surge entonces el conflicto entre el empresario que entiende cumplida su obligación con la entrega de la "copia" básica en la que tal cual se trasladan las cláusulas "según convenio", pues una copia es "una reproducción literal" de un escrito de modo que no puede aparecer en la copia lo que no consta en el original, y los representantes de los trabajadores que no se conforman con la entrega de la "copia", sino que exigen la determinación precisa de la correspondiente condición contractual. Como puede apreciarse es cuestión que no afecta al derecho a la protección de datos personales, pues éstos han de comunicarse a los representantes de los trabajadores tanto si hay determinación específica o como si se efectúa por remisión al convenio colectivo aplicable, sino al ámbito del derecho de información de estos representantes. La STS de 24 de marzo de 1998 (rec. 2714/1997)[42] declaró que el empresario no sólo no está obligado a comunicar datos distintos de los que figuran en el texto original, sino que si así lo hiciera estaría incumpliendo la obligación que el art. 8.4 ET le impone (FJ 3). En el mismo sentido resuelve la reciente SAN 118/2019, de 18 de octubre de 2019[43]: "si se solicita que se declare el derecho a que la copia básica de los contratos que entregue la empresa figuren determinados datos y, en la medida que

[41] TRONCOSO REIGADA: *cit.*, p. 5.
[42] RJ 1998, 3009.
[43] JUR 2019, 302523.

tales datos no figuran en los contratos originales, no es posible incluir tales datos formando parte de la copia, sin que el mandato legal amplíe la obligación de suministrar a los representantes legales de los trabajadores datos que no figuran en el contrato original" (FJ 2).

3. RECOGIDA Y TRATAMIENTO DE DATOS DURANTE EL CUMPLIMIENTO DEL CONTRATO DE TRABAJO

El derecho a la protección de datos, más allá de los supuestos de recogida y tratamiento de datos de los trabajadores, puede condicionar aspectos importantes del desarrollo de la relación laboral. Un buen ejemplo es la llamada política de "escritorios limpios" adoptada por empresas que tienen acceso y tratan datos personales de sus clientes. Esta política de "escritorios limpios" va dirigida garantizar la seguridad de los datos de sus clientes evitando, particularmente, que los trabajadores de la empresa con acceso a los datos hagan un uso ilícito de los mismos[44] y para ello se prohíbe la introducción en los lugares de trabajo de efectos que podrían utilizarse para apropiarse de esos datos (bolsos, mochilas, abrigos, memorias usb, teléfonos móviles, memorias externas, software de intercambio de ficheros, software de mensajería instantánea, PDAs, cámaras digitales, papel y bolígrafos)[45], de modo que el escritorio esté "limpio" de todos esos objetos, sobre todo limpios de papel, de instrumentos de escritura y de aparatos electrónicos que permitan la captación y almacenamiento de datos personales.

Son decisiones empresariales que entran dentro del ámbito de ejercicio del poder empresarial para dirigir y organizar el trabajo pero que, en algún supuesto, pueden entrar en conflicto con otros derechos y bienes jurídicamente protegidos como muestra la existencia de algunos litigios. En la SAN de 15 de noviembre de 2018 (rec. 187/2018)[46] se plantea la compatibilidad de estas políticas empresariales con los derechos de los representantes de los trabajadores a difundir información [arts. 8.1.b) y c) LOLS y 68.d) ET], concretamente si la política de "escritorios limpios" podría excluir la distribución de comunicados sindicales en papel y la utilización de teléfonos móviles. El tribunal resuelve la cuestión aplicando el principio de proporcionalidad, llegando a soluciones distintas para cada uno de estos dos problemas.

En relación con la distribución de información sindical en papel el tribunal entiende que el derecho a difundir información de los representantes de los trabajadores sólo podría verse limitado por las medidas de seguridad que la empresa puede legítimamente imponer si fueran idóneas, razonables y proporcionadas al fin pretendido. Para ello la empresa debería haber acreditado que "la introducción de papel escrito en las plataformas constituye un riesgo patente y actual, aunque no se permita a los trabajadores introducir medios para escribir en él, para la seguridad de los datos personales de sus clientes y usuarios" (FJ 4). Al no haberlo hecho "la prohibición de introducir papel escrito en las plataformas, teniendo en cuenta, además, que no se permite ningún medio para escribir en dichos papeles, si es que pudiera escribirse algo en ellos, es absolutamente inidónea, irrazonable y desproporcionada" (FJ 4). Tampoco cabe, a juicio de la sala, imponer unilateralmente la distribución de la información sindical por medios digitales salvo "que se hubiera acreditado, que no es el caso, que la introducción de comunicados en papel constituyera una amenaza exorbitante para la seguridad de los datos" (FJ 4). La conclusión es clara: los representantes de los trabajadores tienen derecho a distribuir en

[44] El objetivo básico de esta política, dice la SAN de 15 de noviembre de 2018 (rec. 187/2018), es "asegurar que no se filtre información sobre datos reservados" de los "clientes y usuarios" (FJ 4). Véase también, sobre supuesto idéntico, la SAN de 3 de mayo de 2019 (rec. 60/2019; AS 2019, 1630).

[45] SAN de 15 de noviembre de 2018 (rec. 187/2018).

[46] AS 2019, 164.

los puestos de trabajo "información sindical en papel, siempre que se notifique a la empresa y no se disturbe la actividad normal del trabajo" (FJ 4).

Distinta es la respuesta del tribunal a la pretensión del sindicato reclamante de permitir el uso de teléfonos móviles "porque su prohibición les impedía comunicarse eficientemente con sus sindicatos y sus representados" (HP 7), petición a la que la empresa había respondido habilitando teléfonos móviles en el puesto de trabajo que sólo se podrían utilizar para "cuestiones sindicales" (HP 7). La solución del tribunal se construye sobre dos argumentos: a) el empresario puede impedir el uso de teléfonos móviles en la empresa por razones de seguridad; y b) la incomunicación telefónica de los representantes podría impedir el desarrollo de sus funciones sindicales. En el caso concurre la primera circunstancia, es razonable prohibir el uso de teléfonos móviles dada su idoneidad para fotografiar datos relevantes y la imposibilidad de su control absoluto, pero no la segunda, puesto que la empresa facilita teléfonos móviles en caso de necesidad. Por tanto, como la empresa había puesto a disposición de los representantes de los trabajadores teléfonos suficientes para que puedan recibir llamadas del exterior y comunicarse con sus sindicatos y asesores se desestima la pretensión "puesto que pueden ejercitar, sin impedimentos reales, su función sindical dentro de al empresa, quien está legitimada para no autorizar móviles en el centro de trabajo por unos motivos de seguridad, […] razonables" (FJ 5).

3.1. Empresa, clientes y datos de los trabajadores

Las relaciones de una empresa con sus clientes generan situaciones, de modo destacado en el sector servicios, en las que puede haber interés en que los clientes tengan acceso a datos personales de sus trabajadores por muy variadas razones: desde la protección de la seguridad de personas y cosas hasta la mejora de la calidad empresarial pasando por la asunción de responsabilidades derivadas del negocio. Por otra parte el tipo de datos sobre los que puede recaer este interés son también variados: desde la simpe identificación de los trabajadores hasta los que forman parte del contenido de la relación laboral.

Los trabajadores son la imagen de la empresa, quienes prestan los servicios correspondientes al cliente que tiene en ellos su punto de referencia y conexión con la empresa. No es de extrañar, por tanto, que el art. 19 LOPDGDD declare que, salvo prueba en contrario, se presumirá amparado en el art. 6.1.f) RGPD (satisfacción de intereses legítimos) el tratamiento de los datos de contacto y los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica, siempre que el tratamiento se refiera a los datos necesarios para su localización profesional y su finalidad sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios[47].

Un ejemplo de la problemática a que puede dar lugar el tratamiento de datos personales de los trabajadores con la finalidad de identificarlos ante los clientes puede verse en la STS de 18 de diciembre de 2006 (rec. 112/2005)[48]. El conflicto se plantea en unos grades almacenes en los que los trabajadores exhiben tarjetas identificativas y se hace constar en los recibos de compra de los clientes el nombre y apellidos del vendedor, precedido de las abreviaturas "Sr". o "Srta". Antes de implantar este nuevo sistema, que se ha hecho sin recabar el consentimiento expreso de los tra-

[47] Precedente de esta norma es el art. 2.2 del Reglamento de desarrollo de la LOPD-1999 (Real Decreto 1720/2007, de 21 de diciembre): "este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales".

[48] RJ 2007, 750.

bajadores afectados, en los *tickets* de compra sólo aparecía un número de identificación del vendedor. Se impugnó la decisión empresarial por entender que constituía una lesión del derecho a la intimidad de los trabajadores afectados, al no estar expresamente autorizada por la ley ni existir un interés empresarial o de tercero que la justificara ni ser necesaria o imprescindible.

El Tribunal Supremo no consideró que hubiera lesión del derecho a la intimidad de los trabajadores, pues lo datos tratados carecían de naturaleza íntima y eran los usados "en todo tipo de relaciones humanas en contacto con el público" (las abreviaturas Sr. o Srta. se consideran mera fórmula de cortesía aplicable con independencia del estado civil de la mujer). Además se trata de una medida que atiende a fines legítimos en interés tanto del empresario como del trabajador. Si por una parte busca mejorar la atención al cliente, por otra "sirve a la fundamental tarea de dignificar la persona, evitando su cosificación, individualizándolo del resto de sus compañeros, dotándole de la dignidad que le corresponde al evitar designarlo con una clave numérica como un mero factor de producción" (FJ 2). Apareciendo así como una "medida idónea, necesaria y proporcionada" (FJ 2).

El derecho a la protección de datos personales no aparece mencionado específicamente en la argumentación de la sentencia pero se utilizan razonamientos que muy bien se hubieran podido aplicar para excluir su infracción. Frente a la hipótesis de que se tratara de datos personales tratados sin consentimiento del trabajador se alza la necesidad el tratamiento para el cumplimiento de contratos de los que es parte: "las tareas encomendadas al trabajador implicaban la restricción de su derecho a permanecer en el anonimato de tal suerte que pudiera entenderse que era la propia voluntad del trabajador –expresada al celebrar el contrato– la que legitimaba la misma, pues es claro que existen actividades que traen consigo, con una relación de conexión necesaria, una restricción en tal derecho por su propia naturaleza, como son las actividades en contacto con el público o accesibles a él". También se desestima la alegación de que el posible uso del nombre y apellidos del trabajador coordinado "con los que son objeto de divulgación general, como el domicilio y el número de teléfono (por ejemplo a través de la guía telefónica)" pudiera ofrecer "una imagen casi completa de los aspectos vinculados a su intimidad", porque "si el cliente estuviese interesado en conocer estos otros aspectos, también podría realizar tal coordinación partiendo de los datos consignados en la placa de identificación".

Sí hay referencia expresa a la normativa de protección de datos en otro caso, resuelto por la STSJ Madrid de 30 de junio de 2008 (rec. 2351/2008)[49], en el que se discutía la licitud de la comunicación del nombre, apellidos y número de documento nacional de identidad del trabajador por parte de su empresario a un cliente. La empresa había concertado un contrato de prestación de servicios con una compañía de seguros (empresa cliente) en virtud del cual se encargaría de la atención a sus asegurados, para lo cual los trabajadores de la empresa de servicios debían acceder a las bases de datos de la compañía de seguros. A tal efecto la empresa de servicios comunicó a la compañía de seguros el nombre, apellidos y documento nacional de identidad del trabajador, discutiéndose en el caso si se trataba de una cesión ilícita de datos personales al efectuarse sin consentimiento del trabajador. La sentencia del TSJ de Madrid entendió que el consentimiento del trabajador era innecesario en este caso pues el tratamiento de datos tenía su fundamento en el cumplimiento del contrato de trabajo (art. 6.2 LOPD-1999), "pues en definitiva se trata del desarrollo de una campaña de soporte de telemarketing, consistente en prestar asistencia telefónica a los clientes de la empresa principal […] y para ello es necesario la aportación por la contratista de unos mínimos datos personales del trabajador

[49] AS 2008, 2186.

adscrito a tales cometidos, a fin de poder entrar en contacto con las bases de datos de sus clientes, lo que se revela así en indispensable, tanto para el mantenimiento de dicha vinculación, como para el cumplimiento del contrato de trabajo, por lo que ha de concluirse que en tal supuesto no es necesario el previo consentimiento del trabajador afectado" (FJ 2).

Sobre la comunicación del número del documento nacional de identidad de los trabajadores tiene interés la STS (CA) de 25 abril de 2016 (rec. 49/2014)[50] que declaró la nulidad de la previsión contenida en la Orden INT/318/2011, de 1 de febrero sobre Personal de Seguridad Privada. Según esta disposición debía constar en la tarjeta de identidad profesional del personal "el número del Documento Nacional de Identidad o del Número de Identificación de Extranjero, con todos sus caracteres alfanuméricos". Para el Tribunal Supremo "la necesidad de identificación del personal de seguridad privada ante los cuerpos de seguridad y ante los ciudadanos afectados que por razones del servicio así lo soliciten […] no exige la constancia en la tarjeta de identidad profesional del número de DNI o del Número de Identificación de Extranjero, pues como razona la sentencia […] recurrida […], la identificación de los vigilantes de seguridad resulta del conjunto de datos expresados en la tarjeta de identidad profesional (entre ellos la fotografía, el nombre y apellidos, las habilitaciones para las que el documento autoriza a su titular y el número y fecha de cada habilitación), y puede reforzarse con facilidad con otro número o registro que no sea coincidente con el número del DNI, por lo que es acertada la conclusión de la Sala de instancia de que no resulta indispensable para la identificación que el número de la tarjeta coincida con el número del DNI" (FJ 4)[51].

La comunicación de la fotografía de los trabajadores al cliente es un supuesto sobre el que se pronuncia el Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo sobre Protección de Datos del Artículo 29. La licitud del tratamiento de este dato dependerá del carácter no excesivo de su recogida y tratamiento en función del servicio prestado al cliente. Por lo que si el tratamiento no es proporcionado carecerá de fundamento, sin que se pueda basar en el consentimiento del trabajador pues éstos "no están en condiciones, habida cuenta del desequilibrio de poder, de dar su libre consentimiento al tratamiento de sus datos personales". El mismo dictamen pone el ejemplo de la empresa de mensajería que, amparándose en su interés legítimo, comunica a sus clientes un enlace al nombre y ubicación de los repartidores así como una foto de su pasaporte que permitiría al cliente comprobar si el repartidor es la persona correcta. El dictamen afirma que "no es necesario facilitar el nombre y foto del repartidor a los clientes" y que "dado que no existe ningún otro motivo legítimo para este tratamiento, la empresa de mensajería no está autorizada a facilitar estos datos personales a los clientes".

Como puede apreciarse en estos dos últimos supuestos sobre tratamiento del número de documento nacional de identidad y de la fotografía de los trabajadores, la legitimidad del fin con que se recogen estos datos personales y su carácter adecuado, pertinente y limitado en relación con dicho fin [art. 5.1.b) y c) RGPD] serán los elementos que permitan plantear el criterio de licitud del tratamiento (art. 6 RGPD).

* * * * * *

Un cliente muy singular es el empresario (empresario principal) que contrata con otro (empresario auxiliar) la realización de obras o servicios correspondientes a su propia actividad empresarial (art. 42 ET). El empresario principal es responsable solidario de las obligaciones de naturaleza salarial y de seguridad social contraídas por los empresarios auxilia-

[50] RJ 2016, 2026.

[51] Véanse, no obstante, en SAN MARTÍN MAZZUCCONI (*cit.*, pp. 235 y 236) los Informes de la AEPD que consideran adecuada a la normativa de protección de datos la inclusión del número del DNI en tarjetas identificativas de trabajadores.

res durante la realización de las correspondientes obras o servicios (art. 42.2 ET). Se entiende que exista en estos casos un interés legítimo del empresario principal en tener acceso a los datos salariales y de seguridad social de los trabajadores de los empresarios auxiliares frente a los cuales puede ser declarado responsable solidario.

Esta cuestión se planteó en el Informe 0412/2009 de la AEPD[52], concretamente si la comunicación de los recibos de salario (la "nóminas") y los documentos de cotización de los trabajadores de una empresa auxiliar al empresario principal resultaría ajustada a la normativa de protección de datos personales. Este Informe concluyó que la comunicación de dichos datos se encontraba amparada por la LOPD-1999: puesto que el empresario principal es responsable solidario de las obligaciones salariales y de seguridad social generadas durante la contrata debería conocer el contenido íntegro de dicha obligación para poder cumplirla. El tratamiento de datos que implica esta comunicación no requeriría el consentimiento del trabajador afectado, al tener por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario. Sin embargo la cuestión puede complicarse pues en algunos casos los documentos de cotización pueden contener datos relativos a la salud del trabajador y la nómina el dato de afiliación sindical que son datos especialmente protegidos (art. 9 RGPD). En relación con los documentos de cotización que contuvieran datos relativos a la salud del trabajador el Informe citado concluyó que su cesión estaría amparada por el art. 7.3 LOPD-1999 (tratamiento de los datos de salud cuando "lo disponga una ley o el afectado consienta expresamente") en relación con el art. 42.2 ET. Puesto que el Estatuto de los Trabajadores "impone un deber al empresario principal" la comunicación del TC resultaría adecuada a la normativa de protección de datos "pues se haya expresamente prevista en una norma con rango de Ley. Además el propio Código Civil exige atender íntegramente las obligaciones solidarias por lo que es preciso conocer el contenido de la misma". En la normativa vigente la comunicación de los documentos de cotización vendría amparada por el art. 9.2.b) RGPD "en relación con el ET art. 42.2 y por el alcance que Código Civil impone a las obligaciones solidarias"[53]. En relación con las nóminas que contuvieran el dato de la afiliación sindical el Informe citado llegó a la conclusión de que su cesión al empresario principal resultaba lícita. Para ello realizó una interpretación conjunta de los arts. 7.2 (la afiliación sindical es dato que sólo puede ser objeto de tratamiento con el consentimiento del afectado) y 4.2 LOPD-1999 (prohibición de uso de los datos objeto de tratamiento para finalidad incompatible para la que hubieran sido recogidos). A la vista de ambos el Informe señaló que "el tratamiento del dato relativo a la afiliación sindical se efectúa por el empresario, para que de la nómina se detraiga la cuota sindical correspondiente. Dado que la finalidad de dicho tratamiento va ligada al pago de la nómina y que en virtud de la obligación solidaria que impone el artículo 42.2 del Estatuto de los Trabajadores, al contratista principal, para el pago de las deudas salariales correspondientes, podemos concluir que el tratamiento de dicha información es para un fin idéntico del que justifica el tratamiento efectuado por el subcontratista. Por ello, siendo los fines idénticos, podemos entender que la comunicación de dichos datos es conforme con el artículo 7.2 en conexión con el art. 4.2 de la Ley Orgánica 15/1999 y la obligación impuesta por el artículo 42.2 del Estatuto de los Trabajadores".

* * * * * *

Junto a casos, como los anteriores, en que se efectúa una comunicación de datos desde la empresa a los clientes, también hay otros en los que los datos recorren el camino inverso: del cliente a la empresa. No es infrecuente que un empresario (cliente) externalice la gestión de

[52] Reproducido por el Informe 0223/2009.

[53] MERCADER UGUINA: p. 209.

recursos humanos en una empresa especializada que, entre otras cosas, se ocupará de confeccionar las nóminas de sus trabajadores y de las gestiones de seguridad social[54], produciéndose así un *data outsourcing*[55]. En estos casos el contratista deberá tratar los datos personales de los trabajadores necesarios para la confección de las nóminas, asumiendo la posición de "encargado del tratamiento", es decir, de persona que trata datos personales por cuenta del responsable del tratamiento (art. 4.8 RGPD) que es el empresario de los trabajadores. La figura del encargado del tratamiento está minuciosamente regulada en el art. 28 RGPD que determina las principales obligaciones derivadas del contrato que vincula al responsable con el encargado del tratamiento (art. 28.3 RGPD). El encargado, que no podrá subcontratar el encargo salvo autorización previa del responsable (art. 28.2 RGPD), debe ofrecer garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado (art. 28.1 RGPD). A la figura del encargado del tratamiento se refiere el art. 33 LOPDGDD. Conforme a este precepto el acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla con la normativa de protección de datos.

3.2. Poderes empresariales y protección de datos personales

El ejercicio de los poderes empresariales de dirección, control y sanción de los trabajadores va unido muy frecuentemente al tratamiento de datos personales. Puesto que varios estudios de este volumen se dedican al análisis específico de las implicaciones que el derecho a la protección de datos sobre las facultades de control del empresario, aquí sólo se hará mención a la casuística que ha planteado la aplicación en algunas empresas de programas de evaluación del desempeño de sus trabajadores. Estas evaluaciones se plasman en datos personales[56] cuya recogida y tratamiento por el empresario estaría fundada en el art. 6.1 RGPD. Los problemas surgen cuando esos datos personales salen fuera de la relación anudada entre empresario y trabajador, comunicándose a otros trabajadores o clientes de la empresa o al público en general. Con muy variadas finalidades puede que el empresario quiera hacer públicos esos datos: ejemplaridad frente a los demás trabajadores, garantía de calidad para los clientes, promoción empresarial ante el público interesado, etc. No parece que este tratamiento de datos pueda tener el mismo fundamento que el que se agota en el exclusivo conocimiento del empresario. La AEPD ha tenido ocasión de pronunciarse sobre varios de estos supuestos.

La comunicación de estos datos al resto de trabajadores de la empresa es estudiada en el Informe 0529/2009 de la AEPD. Específicamente analiza la práctica empresarial consistente en comunicar verbalmente la productividad de un trabajador a sus compañeros, incluir en archivadores los resultados obtenidos por los trabajadores y publicarlos en la intranet de la empresa. Para la AEPD se trata de operaciones que implican tratamiento de datos personales pues los datos de los trabajadores "van a ser tratados no sólo por el empresario sino que van a ser cedidos a todos sus compañeros de trabajo". La licitud del tratamiento de estos datos requerirá el consentimiento del trabajador, con todas las dificultades ya señaladas para perfi-

[54] Blázquez Agudo, E. M.: "La protección de datos en el desarrollo de la relación laboral", en *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid, CISS, 2018, p. 2, citado según versión electrónica La Ley 2592/2018.

[55] Preciado Domènech, C.H.: *Los Derechos Digitales de las Personas Trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales*, Clzur Menor (Navarra), Aranzadi, 2019, p. 66.

[56] Recomenadación 1/2001, sobre datos d evaluación de los trabajadores (22.3.2001), adoptada por el Grupo del Artículo 29. Citada en el Informe 0529/2009 de la AEPD, de donde se toma.

lar su libre prestación. Para la AEPD "la comunicación de datos relativos a la productividad de los trabajadores a otros trabajadores, ya sea mediante publicación de dichos datos en tablones, o en la intranet, deberá efectuarlo voluntariamente el trabajador, salvo que el Comité de Empresa se pronuncie considerando estas medidas como controles que efectúa el propio empresario a su trabajador al amparo del artículo 20.3 del Estatuto de los Trabajadores, en cuyo caso la cesión vendría amparada en el mencionado artículo".

El Informe 0039/2010 de la AEPD trata de la publicación en la página web de la empresa de datos personales de sus trabajadores (identificación, fotografía, perfil profesional y aficiones), la evaluación de que han sido objeto por los clientes y la difusión por estos en las redes sociales. Para la AEPD "cabe concluir que el consentimiento para la comunicación masiva por Internet de los datos de sus empleados, incluidas las evaluaciones sobre los mismos, no podría entenderse válidamente prestado en el contexto de la relación laboral si sus negativa a darlo, llevase aparejada algún tipo de consecuencia adversa o discriminatoria, no pudiendo hablarse de consentimiento libre". Por ello concluye que "la comunicación de los datos de los empleados en Internet, no puede ampararse en el consentimiento del trabajador, en el ámbito de la relación laboral". Sobre la difusión de esos datos por los clientes en internet debe tenerse en cuenta que "la publicación de contenidos con información y datos respecto de terceros no puede ser realizada si éstos no han autorizado expresamente su publicación".

La Resolución R/02223/2009 de la AEPD[57] resuelve la denuncia presentada frente a la empresa que publica en su tablón de anuncios, ubicado en un lugar al que tienen acceso trabajadores de otras empresas colaboradoras y clientes, un cuadro que contiene una relación de los trabajadores de la empresa junto con la valoración de sus conocimientos y eficacia en el puesto de trabajo. La empresa afirma que la publicación de estos se justifica en el desarrollo de la relación laboral: se trata de facilitar y agilizar las suplencias de los trabajadores en los cambios de producción y de disponer de un baremo interno que mida la capacidad de los trabajadores. Se trataría, por tanto, de hacer frente a exigencias organizativas del trabajo en la empresa y de cumplimiento de la normativa de seguridad y prevención de riesgos laborales. Sin embargo la AEPD entiende que la publicación de estos datos es desproporcionada al permitir el acceso de terceros a dichos datos e implica una vulneración del deber de secreto: "por medio de un tablón de anuncios se ha difundido información de los trabajadores que revelan sus actitudes profesionales de cara a la realización de unas tareas determinadas, fuera de su ámbito adecuado y siendo accesibles a terceras personas, lo que implica una vulneración de dicho deber de secreto".

4. RECOGIDA Y TRATAMIENTO DE DATOS EN LA EXTINCIÓN DEL CONTRATO DE TRABAJO

4.1. Los datos personales del trabajador despedido

La extinción del contrato de trabajo, sobre todo en los casos de despido, es un momento en el que normalmente se producirá el uso de datos personales del trabajador. El carácter causal del despido obliga a describir los hechos (art. 55.1 ET) o causas [art. 53.1.a) ET] que lo motivan, hechos o causas que, muy frecuentemente, consistirán en información sobre el trabajador despedido, otros trabajadores o terceros, es decir, datos personales. Algunos de esos datos personales de los trabajadores procederán de tratamientos anteriores efectuados en la empresa (filmaciones, grabaciones o registros de jornada para acreditar un incumplimiento contractual) con arreglo a las normas específicas previstas en al LOPDGDD[58].

[57] PS/00118/2009.

[58] Arts. 87, 89 y 90 LOPDGDD. Véanse los estudios correspondientes ene este mismo número de la *Revista*.

Los problemas que se plantean en el momento del despido se refieren fundamentalmente a si el uso de los datos personales en la carta de despido y su necesaria comunicación a terceros en caso de impugnación judicial (jueces, peritos, otras partes, etc.) requieren el consentimiento del trabajador o se encuentran amparados por el mismo contrato de trabajo, pues el tratamiento es necesario para su extinción [art. 6.1.b) RGPD], o por el cumplimiento de una obligación legal [art. 6.1.c) RGPD], ya que es la ley la que obliga a incorporar a la carta de despido los hechos (art. 55.1 ET) o causas [art. 53.1.a) ET] que lo motivan.

Que no es necesario el consentimiento del trabajador despedido para proceder al tratamiento de los datos personales justificativos del despido queda claro en la SAN (CA) de 19 de octubre de 2005 (rec. 1139/2003)[59]. El supuesto base fue el despido de un empleado de banca por disponer irregularmente en beneficio propio de fondos del banco. La entidad de crédito acreditó el incumplimiento contractual grave y culpable del trabajador mediante informes periciales y de su área de auditoría para cuya elaboración se usaron datos de carácter personal del despedido, ente otros los relativos a la utilización de su tarjeta de crédito y del contrato de préstamo que mantenía con la misma entidad. El trabajador denunció al banco por tratar sus datos personales sin su consentimiento, así como por revelarlos al juzgado, al personal del banco que elaboró el informe de auditoría y al perito. El tribunal estimó que no era necesario el consentimiento del trabajador pues las investigaciones realizadas por el banco a través de su servicio de auditoría interna y del informe pericial sobre las actuaciones del trabajador como empleado de la entidad "están vinculadas o afectan al mantenimiento y cumplimiento de la relación laboral existente entre ambos, exigiendo dicha relación un deber de lealtad y fidelidad que, al parecer o, al menos a juicio de la empleadora, fue incumplido por el referido trabajador" (FJ 3). También entendió el tribunal que no había cesión de datos en el acceso a los mismos por el servicio de auditoría (que es personal del responsable del fichero), juzgado, perito y abogados, justificado en el art. 11. LOPD-1999.

En los despidos por ineptitud [art. 52.a) ET] justificados de algún modo por la alteración de la salud del trabajador se ha planteado la cuestión de la suficiencia de la carta de despido cuando el empresario sólo incluye en ella la referencia a la calificación de ineptitud proporcionada por el servicio médico o de prevención correspondiente y no la descripción del proceso patológico. Aparecen aquí en tensión de un aparte, la necesaria suficiencia de la carta de despido que no deje en situación de indefensión al trabajador y de otra, no sólo el derecho a la protección de datos personales sino el mismo derecho a la intimidad del trabajador. Los datos de salud están sometidos a u régimen especial (art. 9 RGPD) y el art. 22 LPRL somete a los datos derivados de la vigilancia de la salud a una especial reserva: debe llevarse a cabo respetando el derecho a la intimidad del trabajador y la confidencialidad de toda la información relacionada con el estado de salud (art. 22.2 LPRL). Los "resultados" de los reconocimientos médicos serán comunicados al trabajador (art. 2.3 LPRL) y el acceso a la información médica se limitará al personal médico y a las autoridades sanitarias sin que pueda facilitarse al empresario o a terceros sin consentimiento expreso del trabajador (art. 22.4 LPRL). El empresario será informado de las "conclusiones" que se derive de los reconocimientos médicos en relación con la aptitud del trabajador para el desempeño del puesto de trabajo (art. 22.4 LPRL). El empresario sólo dispone de estas conclusiones, que es lo que puede aportar a la carta de despido. La STS de 22 de julio de 2005 (rec. 1333/2004)[60] proporciona un buen ejemplo de esta problemática. El supuesto se refiere al despido de un vigilante de seguridad al que el servicio de prevención declara no apto para el cumpli-

[59] JUR 2005, 268851.

[60] RJ 2006, 84.

miento de sus funciones de acuerdo con la normativa de seguridad privada. El empresario despide al trabajador al amparo del art. 52.a) ET, sin que en la carta de despido conste la concreta alteración de salud inhabilitadora, sino sólo la conclusión de "no apto" del servicio de prevención de riesgos laborales. La cuestión que se plantea es si con sólo esa mención se cumple con el requisito de suficiencia de la carta de despido [art. 53.1.a) ET] sin generar indefensión del trabajador, la tensión entre intimidad y prohibición de indefensión del trabajador. La sentencia entiende que, ante la literalidad de la LPRL, el empresario no tiene otra opción sin que se cause indefensión al trabajador porque puede recabar del servicio de prevención los resultados de su reconocimiento médico. Cuestión distinta es que haya vinculación necesaria entre la declaración de "no apto" del servicio de prevención y la procedencia del despido: "la declaración de no apto por el servicio de prevención, propio o ajeno, no excusa al empleador de justificar la concurrencia de los requisitos legales del despido por ineptitud sobrevenida, para lo cual puede valerse de cualquiera de los medios de prueba admisibles a derecho, por ejemplo, citando ajuicio al facultativo que suscribió el informe declarando no apto al trabajador para que explique cuáles son las concretas dolencias que le aquejan y por qué no puede desempeñar sus funciones" [STSJ Aragón de 21 de febrero de 2018 (rec. 45/2018)[61]].

4.2. Datos personales de otros trabajadores

El tratamiento de datos personales de trabajadores distintos del despedido se ha planteado en algunos casos de despido colectivo (art. 51 ET) a propósito de la aplicación de los criterios seguidos para determinar los trabajadores que son despedidos. El interés del trabajador despedido en conocer la situación de otros trabajadores que no son despedidos reta tanto al derecho a la protección de datos personales, pues sería un caso de comunicación de datos (art. 4.2 RGPD), como a la suficiencia de la carta de despido. En este contexto la STSJ País Vasco de 8 de abril de 2014 (rec. 527/2014)[62] enjuicia el despido de un trabajador en un procedimiento de despido colectivo en el que el criterio para seleccionar a los despedidos era la menor capacidad o rendimiento en el puesto de trabajo, de acuerdo con la correspondiente evaluación interna, excluyéndose en todo caso quienes acreditaran una capacidad o rendimiento superiores al normal. El trabajador impugnó el despido alegando que en la carta de despido no se identificaba a los trabajadores que, pese a su menor antigüedad, acreditaban una capacidad o rendimiento superiores. Para la sentencia era innecesario que la carta de despido "detallara la concreta calificación obtenida por el demandante en el proceso de evaluación e identificara a los trabajadores con menor antigüedad a la suya que habían logrado la máxima, y menos aún que recogiera todos los datos reflejados en las correspondientes fichas, lo que además podría colisionar con lo dispuesto en los artículos 10 y 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal". En cualquier caso si el trabajador "tenía conocimiento de que la valoración negativa de su capacidad y rendimiento, y la positiva de los de otros trabajadores adscritos al mismo centro y grupo profesional, estaba basada en las hojas de evaluación realizadas por la empresa, como se reflejaba en el propio acuerdo suscrito con los representantes del personal, y en la carta de despido se le informaba de que era su menor capacidad y rendimiento respecto de otros compañeros que acreditaban la máxima, la determinante de su elección, ningún impedimento existía para que solicitase, por conducto judicial, la aportación por parte de la demandada, de la ficha de evaluación propia y de los demás trabajadores de la fábrica, incluso como prueba anticipada, al objeto de verificar la valoración con detalle

[61] JUR 2018, 95275.

[62] AS 2014, 830.

y rebatirla eficazmente a través de los medios de prueba adecuados a tal fin" (FJ 4).

4.3. Datos personales de terceros

No es infrecuente que en algunos despidos se plantee si datos personales de terceros, como los clientes de la empresa, deben acceder a la carta de despido. Piénsese, por ejemplo, en despidos por ofensas, daños o fraude a clientes o a otras personas. Un supuesto de este tipo fue resuelto por la STSJ Extremadura de 17 de noviembre de 2015 (rec. 464/2015)[63] al enjuiciar el despido disciplinario de un vendedor por las numerosas irregularidades cometidas en su trabajo. El trabajador despedido alegó indefensión porque la empresa no había incorporado en la carta de despido los nombres de los clientes afectados por las irregularidades sino solo el número asignado por la empresa. El tribunal declaró que la actuación empresarial había sido correcta y había cumplido con la LOPD-1999 pues se trataba de datos personales de terceros sobre los que la empresa estaba obligada a guardar secreto y además la empresa había comunicado al trabajador despedido que facilitaría los datos si el juzgado lo requería: "actuó correctamente remitiéndole a quien puede determinar si procedía comunicar los datos sin necesidad de consentimiento de los clientes, al órgano judicial, como previene, según se dijo, el art. 11. Por ello, si el trabajador no hizo uso de esa posibilidad, en las diversas formas que, como se alega en la impugnación, le permitía la LRJS, no puede ahora achacar a la empresa las posibles consecuencias de su inacción" (FJ 2).

4.4. La comunicación del despido a terceros: "listas negras"

La STS (Civil) de 12 de noviembre de 2015 (rec. 899/2014)[64] aborda la cuestión de la comunicación a terceros de los hechos, datos personales, motivadores del despido disciplinario, comunicación de datos hecha no con una simple y aséptica finalidad informativa sino con la de excluir al trabajador despedido de futuros empleos en otras empresas del sector, es decir, para formar una "lista negra"[65]. Los hechos del caso fueron los siguientes. La subcontratista de una de las principales empresas del sector despidió a un trabajador, acusado de cobrar a un cliente por una actuación que debía ser gratuita. El despido fue declarado improcedente al no quedar acreditados los hechos imputados, optando el empresario por la extinción indemnizada del contrato. La empresa auxiliar comunicó a la principal los datos relativos a las causas del despido que quedaron incorporados a un fichero de "personal conflictivo" lo que imposibilitó la posterior contratación del trabajador por otras empresas auxiliares de la principal. La sentencia del Tribunal Supremo encuadra esta conducta empresarial dentro de la formación de las llamadas "listas negras"[66] cuya ilicitud declara por, entre otros, lesionar el derecho a la protección de datos personales: "Al tratarse de ficheros de datos personales formados sin el consentimiento de los afectados, en tanto no les fuera aplicable ninguna de las excepciones del art. 11.2 LOPD (RCL 1999, 3058), la cesión de datos que se hicie-

[63] JUR 2015, 297085.

[64] RJ 2015, 5063.

[65] Monereo Pérez, J. L.; Fernández Bernat, J. A.: "Listas negras de trabajadores conflictivos (a propósito de la STS de 12 de noviembre de 2015)", *Trabajo y Derecho*, núm. 16 (2016).

[66] La sentencia del Tribunal Supremo asume la definición del Grupo de Trabajo del Artículo 29: "ficheros de datos personales formados mediante la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación », entre las que destacan las que incluyen datos sobre la causa de suspensión o extinción de la relación laboral, existencia de reclamaciones judiciales contra la empresa efectuadas por el trabajador, así como si es susceptible de nueva contratación en función de respuestas a preguntas que no se concretan, extremos estos últimos que pueden afectar negativamente a la reputación del trabajador y a su futura empleabilidad " (FJ 3).

ra para la formación de tales ficheros sería ilícita, vulneraría el derecho fundamental a la protección de los datos personales y, si los datos objeto del tratamiento ilícito pudieran dañar el honor o la intimidad de los afectados, también constituiría una vulneración de estos derechos fundamentales de la personalidad" (FJ 3). Afirmada esta regla general la aplica al caso consistente en la comunicación por parte de la empresa auxiliar a la principal de datos personales del trabajador sobre las causas de su despido: "tal cesión de datos fue ilícita, porque no contó con el consentimiento del afectado, no resultaba amparada en ninguno de los supuestos en los que el art. 11.2 LOPD exime de la exigencia de consentimiento del afectado para que la cesión sea lícita, y, además, no respetaba el principio de calidad de datos pues los datos cedidos no eran veraces (la sentencia del Juzgado de lo Social los había considerado como no acreditados) y no se concedía al demandante la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, regulados en los arts. 15 a 17 LOPD" (FJ 4). De todo ello resulta la vulneración del derecho a la protección de datos, a la que se añade la del derecho al honor del trabajador "pues los datos comunicados no cumplían el requisito de la eracidad y afectaban negativamente a su reputación" (FJ 4).

4.5. Situación de los datos personales una vez extinguido el contrato de trabajo

Con la extinción del contrato de trabajo desaparecerá el fundamento principal del tratamiento de los datos del trabajador. A partir de ese momento ya no hay contrato cuya ejecución haga necesaria la recogida y tratamiento de datos [art. 6.1.b) RGPD]. El deber de confidencialidad del empresario se mantendrá aunque se hubiera extinguido el contrato (art. 5.3 LOPDGDD). Esos datos fueron recogidos con el fin determinado, el cumplimiento del contrato, que cesa con la extinción del contrato sin que sea posible su tratamiento ulterior de modo incompatible con dicho fin [art. 5.1.b) RGPD]. Conforme al art. 17.1 RGPD el trabajador tendrá derecho a obtener la supresión de sus datos personales cuando éstos "ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otros modos" [art. 17.1.a) RGPD][67]. El empresario, en estos casos, estará obligado a bloquear los datos (art. 32.1 LOPDGDD), operación consistente en la identificación y reserva de los datos "adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el pazo de prescripción de las mismas". Pasado ese plazo "deberá procederse a la destrucción de los datos" (art. 32.2 y 3 LOPDGDD)[68].

Es claro que una vez extinguido el contrato de trabajo pueden plantearse reclamaciones judiciales o extrajudiciales del trabajador o actuaciones de las administraciones públicas por infracciones administrativas (de orden social, tributarias, protección de datos, etc.) que se refieran o deriven de datos personales del trabajador, por lo que se plantea la cuestión del plazo de conservación de los datos. Cada una de estas responsabilidades tiene plazo de prescripción distinto[69], por lo que parece que los datos deberían conservarse durante un plazo coincidente con el de más amplio contemplado por las normas en concurrencia[70].

---

[67] Art. 15.1 LOPDGDD.

[68] Para la normativa anterior, art. 16 LOPD-1999.

[69] Acciones derivadas del contrato de trabajo: (art. 59.1 ET). Infracciones en el orden social: art. 4 LISOS. Infracciones en materia de protección de datos: arts. 72.1, 73 y 74 LOPDGDD.

[70] En el caso de extinción de la relación laboral el empresario debe proceder al bloqueo de los datos "hasta que finalice el plazo de prescripción de acciones judiciales [TRONCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010, p. 2 (citado según la versión electrónica del capítulo 13, "La protección de datos personales en el ámbito laboral", en *tirantonline*)]. Según

El uso empresarial de datos personales de antiguos trabajadores de la empresa ha dado lugar a algunos litigios en los que se ha discutido la licitud de dicho tratamiento. La determinación del orden jurisdiccional competente para conocer las reclamaciones por vulneración del derecho a la protección de datos planteadas por antiguos trabajadores de la empresa se trató en la STSJ Andalucía (Sevilla) de 28 de septiembre de 2017 (rec. 2762/2017)[71]. La AEPD consideró infracción grave la conducta de la empresa que envió ofertas comerciales a antiguos trabajadores utilizando los datos que había obtenido por la previa y extinta relación laboral, sin que los trabajadores hubieran autorizado su uso para finalidad distinta [art. 44.3.b) LOPD-1999]. Planteada reclamación judicial ante los tribunales del orden social por vulneración del derecho fundamental a la protección de datos la sentencia indicada declaró que una vez concluida la relación laboral el empresario seguía obligado a "respetar los derechos fundamentales de los actores pero no en la condición de trabajadores de la empresa, que ya no ostentan ni conforme a lo dispuesto en las normas laborales y a la doctrina constitucional sobre el contenido y límites de los derechos fundamentales en el marco de una relación de esa naturaleza, sino como personas que podrán recabar la tutela judicial frente a la actuación que consideran lesiva de su derecho fundamental a la protección de datos por la vía privilegiada del artículo 53.1 CE, no ante los tribunales laborales, que carecen de competencia para conocer de las demandas de tutela de los derechos fundamentales que se suscitan fuera del ámbito de la relación de trabajo, aunque tengan una conexión más o menos próxima con una previa relación laboral, sino ante los del orden civil, en ejercicio del derecho a la tutela judicial efectivo reconocido por el artículo 24.1 CE" (FJ 2).

En algún caso el tratamiento de datos una vez extinguido el contrato se hace con la finalidad de evitar conductas desleales de los antiguos trabajadores. Así fue en el supuesto que dio lugar a la SAN (CA) de 15 de junio de 2005 (rec. 669/2003)[72]. Tras la creación de una sociedad por antiguos trabajadores de un distribuidor el fabricante, utilizando los datos de los antiguos trabajadores facilitados por el distribuidor y a petición suya, comunicó a sus clientes no guardaba relación alguna con la nueva sociedad formada por los antiguos trabajadores. Esta conducta fue sancionada como infracción administrativa grave por utilizar los datos personales de los trabajadores con finalidad distinta para la que se recogieron [art. 44.3.d) LOPD-1999]. Sin embargo la AN estimó que los datos no se habían utilizado "con una finalidad distinta de aquella para la que habían sido recabados", pues se utilizaron para una "finalidad derivada, o al menos directamente relacionada de dicha relación laboral" porque al extinguirse los contratos de trabajo la empresa "trató de evitar los perjuicios que le podía suponer una posible competencia desleal de aquellos antiguos trabajadores, al servirse de la cartera de clientes de dicha empleadora, y por en consecuencia puede considerarse "compatible" con dicha relación laborar el enviar una carta a los clientes de la empresa advirtiéndoles del cese en ella de tales trabajadores" (FJ 4).

PRECIADO DOMÈNECH "parece que los datos de los trabajadores deberían bloquearse a la extinción del contrato, conservarse bloqueados durante 4 años y suprimirse después" (*El derecho, cit.*, p. 294); conclusión a la que llega tras ponderar los plazos de prescripción de las infracciones de la LOPD-1999 (tres años), tributarias (cuatro años, art. 66 LGT), de seguridad social (cuatro años, art. 4.2 LISOS) y la regla general de las infracciones de orden social (tres años, art. 4.1 LIOSOS). Pero téngase en cuenta que las infracciones my graves en materia de prevención riesgos laborales prescriben a los cinco años (art. 4.3 LPRL). Para MERCADER UGUINA "de forma orientativa, se ha venido señalando que dicho período coincidirá típicamente con el tiempo necesario para la prescripción de las acciones que pudieran derivarse de la relación jurídica que vincula al responsable con el interesado" (MERCADER UGUINA, J. R.: "Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679", [La Ley 3360/2018, p. 15, versión digital]).

[71] JUR 2017, 263201.

[72] JUR 2005, 240213.

BIBLIOGRAFÍA

ARIAS DOMÍNGUEZ, Á.: "Video-llamadas en trabajos de contact-center y cesión de derechos de imagen", *Revista de Jurisprudencia Laboral*, núm. 3 (2019).

BLÁZQUEZ AGUDO, E. M.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid, CISS, 2018.

CANO GALÁN, Y.: "Cláusulas contractuales tipo sobre cesión de derechos de imagen de los trabajadores y cumplimiento de la normativa sobre protección de datos de carácter personal", *Diario La Ley*, 24 de Mayo de 2018 (LA LEY 7684/2019).

COSTA, R.: "Protección de datos en el ámbito laboral", en RALLO LOMBARTE, A.: *Tratado de Protección de Datos*, Valencia, Tirant lo Blanch, 2019.

CRISTÓBAL RONCERO, R.: "Protección del derecho a la propia imagen en el trabajo", *Nueva Revista Española de Derecho del Trabajo*, núm. 199 (2017).

DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B.: *Control informático, videovigilancia y protección de datos en el trabajo*, Valladolid, Lex Nova, 2012.

GARCÍA MURCIA, J.: "La protección de datos personales en el ámbito laboral: una sucinta reseña jurisprudencial a partir de cinco sentencias del Tribunal Supremo", *Revista Galega de Dereito Social*, núm. 5 (2018).

GARCÍA MURCIA, J.; RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216 (2019).

GARCÍA-PERROTE ESCARTÍN, I.; MECADER UGUINA, J. R.: "Datos personales y cláusulas contractuales: los límites del consentimiento en la doctrina reciente del Tribunal Supremo", *Revista Española de Derecho del Trabajo*, núm. 223 (2019).

MARTÍNEZ MARTÍNEZ, R.: "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política*, núm. 5 (2007).

MARTÍNEZ MOYA, J.: "El derecho a la protección de datos personales y sistema de geolocalización impuesto por la empresa a los trabajadores-repartidores", Revista de Jurisprudencia Laboral, núm. 1 (2019).

MERCADER UGUINA, J. R.: Protección de datos y garantía de los derechos digitales en las relaciones laborales, 3ª ed., Madrid, Lefebvre, 2019.

— : "Protección de datos y relaciones laborales: apuntes prácticos sobre la entrada en vigor del Reglamento (UE) 2016/679", (La Ley 3360/2018).

MERCADER UGUINA, J. R.; DE LA PUEBLA PINILLA, A.: "Protección de datos y relaciones colectivas", *Revista de Trabajo y Seguridad Social. CEF*, núm. 423 (2018).

MESSÍA DE LA CERDA BALLESTEROS, J. A.: "La evolución del concepto de cesión o comunicación de datos personales", *Actualidad Civil*, núm. 10 (2017).

MONEREO PÉREZ, J. L.; FERNÁNDEZ BERNAT, J. A.: "Listas negras de trabajadores conflictivos (a propósito de la STS de 12 de noviembre de 2015)", *Trabajo y Derecho*, núm. 16 (2016).

OLLERO TASSARA, A.*: De la protección de la intimidad al poder de control sobre los datos personales*, Madrid, Real Academia de Ciencias Morales y Políticas, 2008.

PRECIADO DOMENECH, C. H.: *El derecho a la protección de datos en el contrato de trabajo*, Cizur Menor (Navarra), Aranzadi, 2017.

— : *Los Derechos Digitales de las Personas Trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales*, Cizur Menor (Navarra), Aranzadi, 2019.

RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Revista de Trabajo y Seguridad Social CEF*, núm. 423 (2018).

RODRÍGUEZ ESCANCIANO, S.: *El derecho a la protección de datos personales de los trabajadores: nuevas perspectivas*, Albacete, Bomarzo, 2009.

SAN MARTÍN MAZZUCCONI, C.: "El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos", en SAN MARTÍN MAZZUCCONI, C. (Dir.): *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, León, Eolas, 2014.

SÁNCHEZ QUIÑONES, L.: "El marco legislativo de la protección de datos en el ámbito laboral. Especial referencia al consentimiento del trabajador", *Diario La ley*, núm. 9377 (2019).

SEMPERE NAVARRO, A. V.: "El deber de facilitar una cuenta corriente bancaria", *Revista de Jurisprudencia Laboral*, núm. 7 (2019).

TRONCOSO REIGADA, A.: *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010.

VILLALBA SÁNCHEZ, A.: "El derecho fundamental a la protección de datos del trabajador frente a los riesgos de la contratación estandarizada", *Nueva Revista Española de Derecho del Trabajo*, núm. 207 (2018).

RESUMEN

El derecho fundamental a la protección de datos encuentra una de sus más importantes aplicaciones en el ámbito de la relación laboral. Su ciclo vital (selección, contratación, cumplimiento y extinción) permite y exige disponer de una información masiva sobre el trabajador, de un elevadísimo número de datos personales sobre sus más variadas circunstancias. De este modo resulta que: a) Sería imposible la celebración, cumplimiento y extinción del contrato de trabajo sin la disposición de datos personales de los trabajadores. b) Estos actos suponen la disposición del derecho fundamental a la protección de datos, un capítulo más del tema de la vigencia de los derechos fundamentales inespecíficos del trabajador en el contrato de trabajo. c) De los dos elementos anteriores, necesidad del tratamiento de datos personales para el desenvolvimiento de la relación laboral y atribución al trabajador de un poder de disposición y de control sobre los mismo configurado como derecho fundamental, resultará la modulación del derecho fundamental a la protección de datos.

La protección de datos personales se convierte así en un punto de vista desde el que el Derecho del Trabajo, y particularmente el contrato de trabajo, puede ser mirado en su integridad. A la luz de este derecho fundamental, entre el trabajador, como "interesado", y el empresario, como "responsable del tratamiento" de los datos personales, se anudan un complejo conjunto de derechos y obligaciones. De ese amplio conjunto de obligaciones y derechos corresponde a este trabajo el estudio de la recogida y tratamiento de datos personales en el contexto del contrato de trabajo. Como en otros artículos de este volumen se estudian destacados aspectos generales y específicos del derecho a la protección de datos en las relaciones laborales, para evitar innecesarias y tediosas reiteraciones, se ha optado por presentar en estas páginas un sucinto análisis de la casuística más destacada generada por la recogida y tratamiento de datos en el contexto del contrato de trabajo. Siguiendo la estructura habitual de los principales estudios publicados sobre el tema estas páginas se estructura en tres grandes apartados, según la recogida y tratamiento de datos personales de los trabajadores se produzca: 1) en el momento de la celebración del contrato de trabajo; 2) durante su cumplimiento, y 3) en su extinción.

La celebración del contrato de trabajo es un momento en el que se concentra de modo importante la recogida y tratamiento de datos personales de los trabajadores. El mismo contrato de trabajo puede ser instrumento útil para el cumplimiento de dos importantes funciones: recabar el consentimiento del trabajador para el tratamiento de los datos e informarle sobre el tratamiento realizado. El principal criterio de licitud para el tratamiento de los datos personales en este momento es el de su necesidad para la ejecución del contrato de trabajo del que el trabajador es parte. De este modo el consentimiento del trabajador pasa, como regla general, a un segundo plano. No es necesario, por tanto, recurrir al principio del consentimiento del interesado para hacer lícito el tratamiento de estos datos indispensables para la celebración y posterior ejecución del contrato de trabajo. Por otra parte la normativa de protección de datos personales contempla con muchas restricciones la prestación del consentimiento del trabajador para el tratamiento de sus datos personales, habida cuenta de su situación de debilidad contractual. Se trata de una cuestión que ha dado lugar a una cierta litigiosidad en la que se puede apreciar dos grandes grupos de casos. Uno en el que los datos personales para cuyo tratamiento se presta el consentimiento no guardan relación con el objeto del contrato de trabajo y otro en el que los datos personales sí están implicados en la prestación laboral del trabajador. En el primer caso no se considera válida la prestación del consentimiento, en el segundo sí. También se estudia en esta primera parte el tratamiento de datos necesario para el cumplimiento de obligaciones legales del empresario, fundamentalmente la entrega de la copia básica del contrato a los representantes de los trabajadores.

La segunda pare del estudio se dedica al análisis de la recogida y tratamiento de datos durante el cumplimiento del contrato de trabajo. Fundamentalmente es objeto de estudio el flujo de datos personales de los trabajadores que se produce entre empresarios y clientes intervinientes en relaciones negociales: identificación de los trabajadores ante los clientes, comunicación de salarios y cotizaciones a la seguridad social por el empresario auxiliar al principal, externalización de la gestión de personal y *data outsourcing*. Finalmente se plantea en este apartado las consecuencias que desde el punto de vista de la protección de datos tienen las prácticas empresariales de evaluación del desempeño de los trabajadores y su comunicación a clientes y compañeros de trabajo.

La última parte se dedica al estudio del tratamiento de datos personales que se puede producir con ocasión de la extinción de la relación laboral. La extinción del contrato de trabajo, sobre todo en los casos de despido, es un momento en el que normalmente se producirá el uso de datos personales del trabajador. El carácter causal del despido obliga a describir los hechos que lo motivan, hechos o causas que, muy frecuentemente, consistirán en información sobre el trabajador despedido, otros trabajadores o terceros, es decir, datos personales. Los problemas que se plantean en el momento del despido se refieren fundamentalmente a si el uso de los datos personales en la carta de despido y su necesaria comunicación a terceros en caso de impugnación judicial requieren el consentimiento del trabajador o se encuentran amparados por el mismo contrato de trabajo, pues el tratamiento es necesario para su extinción, o por el cumplimiento de una obligación legal, ya que es la ley la que obliga a incorporar a la carta de despido los hechos o causas que lo motivan. Finalmente se estudia la situación producida una vez extinguido el contrato de trabajo al desaparecer el fundamento principal del tratamiento de los datos del trabajador. A partir de ese momento ya no hay contrato cuya ejecución haga necesaria la recogida y tratamiento de datos. El deber de confidencialidad del empresario se mantendrá aunque se hubiera extinguido el contrato. Esos datos fueron recogidos con el fin determinado, el cumplimiento del contrato, que cesa con la extinción del contrato sin que sea posible su tratamiento ulterior de modo incompatible con dicho fin, abriéndose los procesos de bloqueo y destrucción de datos.

Palabras clave: datos personales; derechos fundamentales; derecho a la protección de datos; relación laboral.

ABSTRACT The fundamental right to data protection finds one of its most important applications in the field of labor relations. Its life cycle (selection, hiring, compliance and extinction) allows and demands to have a massive information about the worker, a very high number of personal data about his most varied circumstances. Thus it turns out that: a) It would be impossible to conclude, fulfill and terminate the employment contract without the provision of personal data of the workers. b) These acts involve the provision of the fundamental right to data protection, another chapter on the issue of the validity of the nonspecific fundamental rights of the worker in the employment contract. c) Of the two previous elements, the need for the processing of personal data for the development of the labor relationship and attribution to the worker of a power of disposition and control over the same configured as a fundamental right, will result the modulation of the fundamental right to protection of data.

The protection of personal data thus becomes a point of view from which Labor Law, and particularly the employment contract, can be viewed in its entirety. In light of this fundamental right, between the worker, as "interested", and the employer, as "responsible for the processing" of personal data, a complex set of rights and obligations are tied. Of this broad set of obligations and rights corresponds to this paper the study of the collection and processing of personal data in the context of the employment contract. As in other articles of this volume are studied outstanding general and specific aspects of the right to data protection in labor relations, to avoid unnecessary and tedious repetitions, we have chosen to present in these pages a succinct analysis of the most outstanding casuistry generated for the collection and processing of data in the context of the employment contract. Following the usual structure of the main studies published on the subject, these pages are structured in three main sections, depending on the collection and processing of personal data of the workers: 1) at the time of the conclusion of the employment contract; 2) during its fulfillment, and 3) in its extinction.

The conclusion of the employment contract is a time in which the collection and processing of personal data of workers is concentrated. The same employment contract can be a useful instrument for the fulfillment of two important functions: to obtain the consent of the worker for the treatment of the data and to inform him about the treatment carried out. The main criterion of legality for the processing of personal data at this time is that of their need for the execution of the employment contract to which the worker is a party. In this way the worker's consent, as a general rule, goes to the background. It is not necessary, therefore, to resort to the principle of the consent of the interested party to make lawful the processing of these essential data for the conclusion and subsequent execution of the employment contract. On the other hand, the personal data protection regulations contemplate with many restrictions the provision of the worker's consent for the processing of their personal data, given their situation of contractual weakness. This is an issue that has given rise to a certain litigation in which you can see two large groups of cases. One in which the personal data for which the consent is given is not related to the object of the employment contract and the other in which the personal data is involved in the worker's labor benefit. In the first case the provision of consent is not considered valid, in the second case. In this first part, the treatment of data necessary for the fulfillment of legal obligations of the employer is also studied, mainly the delivery of the basic copy of the contract to the workers' representatives.

The second part of the paper is dedicated to the analysis of the collection and processing of data during the fulfillment of the employment contract. Fundamentally, the flow of personal data of workers that occurs between employers and clients involved in business relationships is studied: identification of workers before clients, communication of salaries and social security contributions by the auxiliary employer to the principal, outsourcing of personnel management and data outsourcing. Finally, this section considers the consequences that, from the point of view of data protection, business practices have to assess the performance of workers and their communication to customers and co-workers.

The last part is dedicated to the study of the processing of personal data that may occur during the termination of the employment relationship. The termination of the employment contract, especially in cases of dismissal, is a time when the use of personal data of the worker will normally occur. The causal nature of the dismissal makes it necessary to describe the facts that motivate it, facts or causes that, very frequently, will consist of information about the dismissed worker, other workers or third parties, that is, personal data. The problems that arise at the time of dismissal refer fundamentally to whether the use of personal data in the letter of dismissal and its necessary communication to third parties in case of judicial challenge require the consent of the worker or are covered by the same contract of work, because the treatment is necessary for its extinction, or for the fulfillment of a legal obligation, since it is the law that forces to incorporate to the letter of dismissal the facts or causes that motivate it. Finally, the situation produced after the employment contract is terminated when the main basis of the worker's data processing disappears. From that moment there is no contract whose execution makes the collection and processing of data necessary. The employer's duty of confidentiality will be maintained even if the contract has been terminated. These data were collected for the purpose determined, the fulfillment of the contract, which ceases with the termination of the contract without further processing in a manner incompatible with that purpose, opening the processes of blocking and destruction of data.

Keywords: personal data; fundamental rights; right to data protection; employment relationship.

Categorías especiales de datos personales en el ámbito de la relación de trabajo

Special categories of personal data in the labour relationship

ÁNGEL LUIS DE VAL TENA*

1. SOBRE EL TRATAMIENTO DE DATOS PERSONALES DEL TRABAJADOR EN EL MARCO DE UNA RELACIÓN LABORAL

El conocimiento de determinados datos personales del trabajador otorga a su empleador un poder más extenso cuando ha de tomar decisiones organizativas y de gestión de personal, además de orientar o ejecutar la actividad de control sobre la prestación de servicios, de manera más precisa e intensa[1].

Ciertamente, el "dato personal" –toda información sobre la persona trabajadora, como, por ejemplo, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social– y su "tratamiento" –cualquier operación o conjunto de operaciones, realizadas por el empresario o por un encargado suyo, sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción– cuando sea necesario para la génesis y posterior ejecución del contrato de trabajo, conjuntamente, aportan información relevante y de considerable valor para adoptar determinaciones, ordinarias o extraordinarias, sobre los recursos humanos, en aras a su optimización desde la perspectiva de los resultados empresariales.

Bajo esta premisa, las nuevas tecnologías[2], incorporadas también a la administración de la empresa, multiplican las posibilidades de obtener datos personales, además de profesionales, del trabajador y perfeccionan su tratamiento, amplificando las interrelaciones de unos datos con otros, de manera que provocan la "hiperdatificación"[3], si bien incrementan, al mismo tiempo, el riesgo de lesión de los derechos y libertades del interesado, de ahí la imperativa necesidad de adoptar nor-

* Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de Zaragoza. ORCID: http://orcid.org/0000-0003-3276-5983

[1] *Vid.* VALDÉS DAL-RE, F.: "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", *Revista de Derecho Social*, núm. 79, 2017, p. 19.

[2] Así lo advierte MOLINA NAVARRETE, C.: "La «gran transformación» digital y bienestar en el trabajo: riesgos emergentes, nuevos principios de acción, nuevas medidas preventivas", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. extraordinario 1, 2019, p. 11.

[3] Ha destacado la "hiperdatificación" del lugar de trabajo, MERCADER UGUINA, J. R.: "El mercado de trabajo y el empleo en un mundo digital", *Información Laboral*, núm. 11, 2018, p. 4 (BIB 2018/13994).

mas que garanticen la protección de esos derechos y libertades a propósito del tratamiento de datos personales de los trabajadores en el ámbito laboral.

No se olvide que algunas notas identificativas de la relación jurídico-laboral inciden de manera particular en el tratamiento de los datos personales del trabajador, actualizando continuadamente aquellos riesgos, y así se ha subrayado[4], entre otras: su carácter personalísimo, que hace más complejo el tipo de datos a considerar; su perdurabilidad, que supone la necesaria conservación de los datos; y –habría que añadir– sus diversas proyecciones, individual y colectiva, que implican un aprovechamiento de los datos para evaluar diferentes realidades.

Como no han dejado de crecer las posibilidades de acumular datos de los trabajadores en "ficheros" –conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica– y de combinar esos datos para elaborar "perfiles" –forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física–, se ha de aplicar la normativa sobre protección de datos personales también a la empresa en relación con los datos conocidos de sus trabajadores para que su tratamiento alcance las mismas garantías que en otros escenarios jurídicos, de igual forma que se reconocen a otros interesados.

El trabajador, como ciudadano, también es titular del derecho fundamental a la protección frente al tratamiento de los datos personales –"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" [art. 18.4 Constitución Española (en adelante, CE)]–, que le garantiza "el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados" y se configura como "una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención"[5]. Aunque imbricado con otros derechos constitucionales, como el derecho a la intimidad (art. 18.1 CE), se considera un derecho autónomo e independiente, que consiste en "un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[6].

También la normativa comunitaria reconoce expresamente este derecho. Así, la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, CDFUE) recoge que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan" (art. 8.1 CDFUE) y el Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) dispone que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" (art. 16.1 TFUE), trasladando al Parlamento Europeo y al Consejo la obligación de establecer, con arreglo al procedimiento legislativo ordinario, "las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades

[4] *Vid.* DEL REY GUANTER, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la «intimidad informática» de trabajador)", *Relaciones Laborales*, T. II, 1993, pp. 135-160.

[5] STC 94/1998, de 4 de mayo.

[6] STC 292/2000, de 30 de noviembre.

comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos" (art. 16.2 TFUE).

Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión Europea, el Reglamento 2016/679/UE, de 27 de abril, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), aplicable a partir del 25 de mayo de 2018, refuerza la seguridad jurídica y la transparencia en la provisión y gestión de los datos personales, con carácter general. Singularmente en el ámbito de las relaciones de trabajo[7], habilita a las disposiciones legislativas y a los convenios colectivos para establecer normas más específicas[8] que garanticen la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores, en particular "a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral" (art. 88.1 RGPD).

A nivel nacional, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDyGDD) adapta el ordenamiento español a la referida norma europea y completa sus disposiciones, aunque, desde la perspectiva exclusivamente laboral, no introduce novedades en cuanto al tratamiento de los datos de las personas trabajadoras y sí, en cambio, regula un conjunto de "derechos digitales"[9] de los trabajadores con la finalidad de garantizar su intimidad, fundamentalmente; y ello sin perjuicio del reconocimiento expreso del rol a desempeñar por la negociación colectiva para establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral (art. 91 LOPDyGDD). En esa línea, incorpora un nuevo artículo 20 bis al vigente texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, TRLET), intitulado "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión", confirmando que "los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

No se pone en duda la aplicación de las normas sobre protección de datos personales en las relaciones de trabajo, que repercute en sus dimensiones individual y colectiva, en materia de prevención de riesgos laborales e, igualmente, en su vinculación con el sistema público de Seguridad Social. Como "interesado" o sujeto titular de los datos, el trabajador se beneficiará del conjunto de garantías articulado por la normativa sobre protección de

[7] Sobre las implicaciones que para las relaciones laborales, individuales y colectivas, tiene la aprobación del RGPD, *vid.* Miñarro Yanini, M.: "Implicaciones laborales del Reglamento comunitario de protección de datos: principales puntos críticos", en García Mahamut, R. y Tomás Mallén, B. (Edits.): *El Reglamento General de Protección de Datos*, Tirant lo blanch, Valencia, 2019, pp. 461 y ss.

[8] No necesariamente más protectora, como subrayan García Murcia, J. y Rodríguez Cardo, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo*, núm. 216, 2019, p. 11 (BIB 2019\1432).

[9] Son los siguientes: "Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral" (art. 87 LOPDyGDD), "Derecho a la desconexión digital en el ámbito laboral" (art. 88 LOPDyGDD), "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo" (art. 89 LOPDyGDD) y "Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral" (art. 90 LOPDyGDD).

datos. Ahora bien, según las recomendaciones de los órganos consultivos nacionales e internacionales en materia de protección de datos, la legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo y las prácticas laborales y tampoco estos, a su vez, pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos[10]. Ensamblar y armonizar ambos sectores del ordenamiento jurídico puede contribuir a aplicar soluciones que protejan convenientemente los derechos e intereses de los trabajadores, máxime cuando el terreno laboral se revela propicio para que surjan vulneraciones de los derechos, fundamentales o no, y actuaciones discriminatorias originadas por el conocimiento y tratamiento de datos personales[11].

Enlazar, asimismo, el interés legítimo del empresario en sacar provecho de las posibilidades que le ofrecen las nuevas tecnologías para conocer las señas de identidad, personales y profesionales, de sus trabajadores a la hora de desarrollar la actividad empresarial, en general, y la gestión del personal, en particular, con los derechos fundamentales –por supuesto, los inespecíficos también– de los asalariados en el seno de una relación laboral, no deviene en una tarea fácil, puesto que, más que buscar el equilibro[12] entre los derechos de uno y otro en juego, se deberá ponderar aquellos derechos según su valor constitucional.

El Reglamento comunitario y la legislación nacional sobre protección de datos personales aportan seguridad y salvaguardan la privacidad de los datos de trabajadores interesados. El nuevo ordenamiento sobre protección de datos personales distingue, sobre todo el conjunto, aquellas "categorías especiales de datos" a las que dedica un haz de cautelas sobre su tratamiento, por cuanto el riesgo no está implícito en el dato concreto, sino en su tratamiento[13] por el empleador responsable, resultando así datos especialmente sensibles y protegidos.

2. DATOS PERSONALES Y «CATEGORÍAS ESPECIALES» DE DATOS PERSONALES

La privacidad, más que la intimidad[14], como "escudo de protección" frente al tratamiento de los datos personales, deriva del derecho fundamental reconocido *ex* artículo 18.4 CE, formulado como garantía constitucional[15], que compele al legislador a limitar el uso de la informática –y de las nuevas tecnologías– para garantizar el honor y la intimidad personal de los ciudadanos y el pleno ejercicio de sus derechos. Dicho con otras palabras, se obliga a que la ley garantice la privacidad informática de la persona, que se traduce en el reconocimiento del "derecho a la autodeterminación informativa"[16], tendente a proteger jurídicamente la identidad personal; autodeterminación informativa que consiste en el control que ejerce el interesado sobre su información personal para preservar, en última instancia, la propia identidad, dignidad y libertad. Y es que solo cuando el sujeto titular puede determinar el alcance de la utilización de sus datos quedarán garantizados sus derechos.

---

[10] Lo ha destacado, acertadamente, MERCADER UGUINA, J. R.: "El mercado de trabajo y el empleo en un mundo digital", *cit.* p. 4.

[11] Al respecto, GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y de archivo de datos", en ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA R. (Coords.): *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004, p. 55.

[12] VALDÉS DAL-RE, F.: "Nuevas tecnologías y derechos fundamentales de los trabajadores", *Derecho de las Relaciones Laborales*, núm. 2, 2019, p. 130.

[13] *Vid.* TRONCOSO REIGADA, A.: "La protección de datos personales en el ámbito laboral", en VV.AA.: *La protección de datos personales en busca del equilibrio*, tirant lo blanch, Valencia, 2010, pp. 1563-1612.

[14] Con precisión, en relación con los datos genéticos, *vid.* ÁLVAREZ GONZÁLEZ, S.: "Derecho a la «privacidad» e información genética", en ÁLVAREZ GONZÁLEZ, S. y GARRIGA DOMÍNGUEZ, A. (Dirs.): *Un nuevo reto para los derechos fundamentales: los datos genéticos*, Dykinson, Madrid, 2017, pp. 22-26.

[15] STC 254/1993, de 20 de julio.

[16] LUCAS MURILLO DE LA CUEVA, P.: *Informática y protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1993, p. 33.

Sin llegar a establecer una clasificación directa de los datos personales, el Reglamento comunitario diferencia el "tratamiento de categorías especiales de datos personales" (art. 9. RGPD), lo que también tiene reflejo en nuestra legislación nacional[17] (art. 9 LOPDyGDD). De esa distinción se colige un doble nivel de protección aplicable a los datos personales según el bien jurídico tutelado[18]: por un lado, aquellos datos que se incluyen en las categorías especiales, estrechamente vinculados a la dignidad y personalidad humana, que reciben una protección reforzada, al quedar prohibido su tratamiento, salvo en los supuestos legalmente tasados; por otro, el resto de datos personales no incluidos en las categorías especiales. Quedan al margen los datos de naturaleza penal, es decir, los datos personales relativos a condenas e infracciones penales, que también son objeto de un particular tratamiento (art. 10 RGPD).

Entre los datos especiales por su tratamiento, también llamados "datos sensibles"[19], se identifican aquellos "datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical", así como también "datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física" (art. 9.1 RGPD).

No es nueva esta identificación separada de diversas categorías de datos, igualmente calificadas como "particulares"[20] o "especiales". La derogada Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos, enumeraba las siguientes categorías especiales de datos en cuanto a su tratamiento: "datos personales que revelen origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como (…) los datos relativos a la salud o a la sexualidad" (art. 8.1 Directiva 95/46/CE); obsérvese que no se recogían, de manera expresa e individualizada, los datos genéticos y los datos biométricos. En la misma línea, se calificaron como "datos especialmente protegidos", en la terminología de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, "los datos de carácter personal que revelen ideología, afiliación sindical, religión y creencias" y también "los datos de carácter personal que hagan referencia al origen racial (o étnico), a la salud y a la vida sexual" (art. 7.2 y 3 LO 15/1999).

2.1. Definición de datos personales

Con la técnica habitual del legislador de la Unión Europea, el RGPD incluye un precepto con definiciones, "a efectos del presente Reglamento", para facilitar la aplicación e interpretación de la norma.

En primer lugar, qué se entiende por dato personal: "toda información sobre una persona física identificada o identificable («el interesado»)" [art. 4.1) RGPD; tenor literal idéntico al derogado art. 2.a) Directiva 95/46/CE]. Se adopta un concepto amplio, quizá porque de-

[17] Desde la perspectiva del tratamiento, cabría diferenciar los datos sujetos a "tratamientos concretos", datos que tienen características singulares o que se manejan en contextos particulares. Al respecto, García Murcia, J. y Rodríguez Cardo, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 19.

[18] Rodríguez Escanciano, S.: "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. 423, 2018, p. 53.

[19] Cfr. Considerando 10 RGPD.

[20] El Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, incluye como "categorías particulares de datos" los de carácter personal que revelen "el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones", así como los datos de carácter personal relativos a "la salud o a la vida sexual" (art. 6).

finir el concepto de datos personales equivale a determinar lo que entra o queda fuera del ámbito de aplicación de las normas sobre protección de datos.

El –así llamado– "Grupo del artículo 29"[21] (en adelante, GT29), en su Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, analiza esa definición de "datos personales" y concluye que el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona física: desde el punto de vista de su naturaleza, abarca información "objetiva" como, por ejemplo, la presencia de una determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones "subjetivas", como, por ejemplo, una valoración del trabajador; desde la perspectiva de su contenido, se incluyen todos aquellos datos que proporcionan información cualquiera, ya sea relativa a la vida privada y familiar del individuo *stricto sensu*, ya sea información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social; y en cuanto al formato o el soporte en que se dispone la información, se admite cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo.

Se puede considerar que la información versa "sobre" una persona física cuando se refiere a ella; así, los datos incluidos en el fichero de una persona guardado en el departamento de personal de su empresa están claramente relacionados con su situación como empleado de dicha empresa. Bien sea por su contenido, finalidad o resultado, el dato personal podrá estar referido a una persona o a varias.

Una persona física estará identificada cuando, dentro de un colectivo de personas, se la distingue de todos los demás miembros del grupo. En cambio, se considerará persona identificable "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" [art. 4.1) RGPD][22]. Ciertamente, para que exista un dato de carácter personal –en contraposición con un dato disociado– no es imprescindible la plena coincidencia entre el dato y una persona concreta, sino que "es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados"; y así para determinar si una persona es identificable "hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona"[23], en contraposición a aquellos datos anónimos, sin un nexo con una persona identificada o identificable.

Las normas de protección de datos personales se aplican a las personas físicas, según se deduce de la definición de datos personales que hace referencia solamente a ellas. La información relativa a las personas jurídicas no está, en principio, cubierta por aquellas normas, si bien nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la norma comunitaria a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello[24]. Distinto es el supuesto de aquella información referente a personas jurídicas que también pueda ser considerada, en función de sus características, como información "sobre" perso-

[21] Este Grupo se creó en virtud de lo dispuesto en el artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la Unión Europea, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad; sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

[22] La STJUE de 6 de noviembre de 2003, Asunto C-101/01, *Bodil Lindqvist*, señaló que el concepto de dato personal incluye, sin duda, la identificación de una persona por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones.

[23] SAN de 8 de marzo de 2002 (Rec. núm. 948/2000).

[24] STJUE de 6 de noviembre de 2003, Asunto C-101/01, *Bodil Lindqvist*.

nas físicas. Lo que sucede, por ejemplo, cuando la denominación de la persona jurídica tiene su origen en el nombre de una persona física.

Como se ha apuntado *ut supra*, no son personales, a estos efectos, los "datos anónimos", es decir, cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. En relación con ese tipo de datos, se acuñan los "datos anonimizados", que son aquellos datos anónimos que con anterioridad se referían a una persona identificable, pero cuya identificación ya no es posible. La anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible la identificación de una persona física, de manera que cualquier técnica de anonimización eficaz ha de impedir a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos –o dos registros pertenecientes a conjuntos diferentes– e inferir cualquier tipo de información a partir de dicho conjunto[25].

A diferencia de esas técnicas, la "seudonimización" conlleva el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable [art. 4.5 RGPD]. Si con la utilización de un seudónimo existe la posibilidad de seguir un rastro hasta llegar a la identidad de la persona, aunque solo en condiciones previamente definidas, consecuentemente los datos personales seudonimizados se deben considerar información sobre una persona física identificable, sin que se excluya para ellos ninguna medida relativa a la protección de datos por más que puedan reducirse los riesgos para los interesados afectados (considerando 26 RGPD); de modo que la aplicación de la seudonimización a los datos personales puede ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos (considerando 28 RGPD). Los datos cifrados son un paradigma[26] de técnica de seudonimización: la información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir, para establecer la correspondencia entre el código y los identificadores habituales de la persona –nombre, fecha de nacimiento, dirección, etc.– se guardan por separado.

2.2. Datos particularmente sensibles: las «categorías especiales de datos personales»

Especial protección –según el certero criterio del legislador comunitario– merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento puede entrañar importantes riesgos para los derechos y las libertades fundamentales (considerando 51 RGPD). Por esta razón se identifica un conjunto de informaciones para su tratamiento diferenciado como "categorías especiales de datos personales". Lógicamente, pertenecen al género común de datos personales, esto es, constituyen información sobre una persona física identificada o identificable, si bien una parte

[25] Cfr. Dictamen 5/2014, de 10 de abril de 2014, sobre técnicas de anonimización, adoptado por el GT29. Igualmente, el documento "Orientaciones y garantías en los procesos de anonimización de datos personales", redactado por la Agencia Española de Protección de Datos (en adelante, AEPD) (https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf)

[26] Otros: función hash, función con clave almacenada, cifrado determinista o función hash con clave con borrado de clave, descomposición en tokens (Dictamen 5/2014, de 10 de abril de 2014, sobre técnicas de anonimización, adoptado por el GT29).

de esos datos se separan para aplicarles reglas específicas, de protección reforzada, cuando se proceda a su tratamiento. Valorando, principalmente, a su contenido, al tratar categorías especiales de datos personales se atenderá a la regulación particular, a modo de régimen excepcional, de su tratamiento, sin perjuicio de que deban aplicarse los principios generales y otras normas comunes, sobre todo en lo relativo a las condiciones de licitud del tratamiento, como más adelante expondremos.

Únicamente cuando establecen los requisitos específicos de ese tratamiento, se enumeran las categorías especiales de datos, a saber: datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud y datos relativos a la vida sexual o la orientación sexual de una persona física (art. 9.1 RGPD). Cabe anotar una mayor precisión respecto del listado recogido en la –ya derogada– Directiva 95/46/CE y también su ampliación con los datos biométricos y los genéticos, diferenciando estos últimos de los propios de la salud o de carácter médico.

En la legislación española vigente, al incorporar normas más definidas –*ex* artículo 6.2 RGPD– para garantizar la protección de los derechos y libertades en relación con el tratamiento lícito de categorías especiales de datos personales, asume la misma enumeración, sin mencionar qué datos se incluyen, ante la expresa remisión al precepto del Reglamento comunitario (art. 9 LOPDyGDD).

Por supuesto, algunas categorías especiales de datos, más que otras, tienen una notable incidencia sobre la persona trabajadora y su tratamiento en las relaciones laborales, significativamente –pero no solo– los datos que revelen la afiliación sindical, los datos biométricos dirigidos a identificar de manera unívoca a una persona y también datos relativos a la salud[27]. Ello no es óbice para que precisemos todos y cada uno de esos datos, máxime cuando la normativa en vigor no se ha ocupado de aportar una mínima descripción, en algún caso.

2.2.1. Datos sobre el origen racial o étnico

La información sobre el origen racial o étnico de un individuo revela un rasgo de la persona física. La prohibición general de tratamiento de datos personales de esta naturaleza trata de evitar situaciones discriminatorias, incluso lesivas de la dignidad de la persona, en particular en el acceso al empleo o durante la ejecución de la prestación de trabajo, señaladamente. El origen de una persona hay que ligarlo al lugar de nacimiento o a la pertenencia, en función del nacimiento, a un grupo social, donde tuvo principio su familia, que puede quedar reconocido por la raza o etnia de referencia.

La acepción más próxima del término raza es la que determina "cada uno de los grupos en que se subdividen algunas especies biológicas y cuyos caracteres diferenciales se perpetúan por herencia"[28]. Referido a las personas, en su concepción antropológica, designaría a cada uno de los cuatro grandes grupos étnicos en los que se suele dividir la especie humana, tomando ciertas características físicas distintivas, como el color de la piel, que se transmiten por herencia de generación en generación. La palabra etnia, por su parte, califica a una comunidad humana definida por afinidades raciales, lingüísticas, culturales, sociales o de otro tipo.

Aunque, en puridad, raza y etnia tienen significados propios, un reciente informe de la

[27] Por todos, García Murcia, J. y Rodríguez Cardo, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 10, y Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, p. 128 y ss.

[28] Según el Diccionario de la Lengua Española, editado por la Real Academia Española de la Lengua (en adelante DRAE), otro significado es "casta o calidad del origen o linaje".

Comisión Europea[29], que analiza en profundidad el concepto del origen étnico o racial y su interpretación por parte de tribunales internacionales y nacionales, considera el origen racial o étnico como una categoría conceptual única, transversal y compuesta para aplicar el derecho antidiscriminatorio y como base jurídica útil para practicar la interpretación legal en el vacío actual de definiciones universalmente aceptadas.

En todo caso, el uso del término "origen racial" en el Reglamento europeo no supone aceptar por parte de la Unión Europea cualesquiera teorías que tratan de determinar la existencia de razas humanas separadas (considerando 51 RGPD). Simplemente, esos datos personales de carácter personal que revelen el origen racial o étnico, que existen y no pueden obviarse, se consideran merecedores de un tratamiento más garantista; y ello porque son datos que pueden usarse con fines discriminatorios.

No es preciso hacer referencia a normas internacionales o comunitarias, que también son muchas en el mismo sentido; basta recordar lo que dispone nuestra Constitución, que neutraliza toda discriminación "por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social" (art. 14 CE).

La legislación laboral, de idéntico modo, reconoce el derecho de todo trabajador "a no ser discriminados directa o indirectamente para el empleo, o una vez empleados, por razones de sexo, estado civil, edad dentro de los límites marcados por esta ley, origen racial o étnico, condición social, religión o convicciones, ideas políticas, orientación sexual, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español" [art. 4.2.c) TRLET), e igualmente el derecho "al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo" [art. 4.2.e) TRLET]. Como sanción legal, se entenderán nulos y sin efecto los preceptos reglamentarios, las cláusulas de los convenios colectivos, los pactos individuales y las decisiones unilaterales del empresario que den lugar en el empleo, así como en materia de retribuciones, jornada y demás condiciones de trabajo, (…) a situaciones de discriminación directa o indirecta por razón de sexo, origen, incluido el racial o étnico, estado civil, condición social, religión o convicciones, ideas políticas, orientación o condición sexual, adhesión o no a sindicatos y a sus acuerdos, vínculos de parentesco con personas pertenecientes a o relacionadas con la empresa y lengua dentro del Estado español" (art. 17.1 TRLET).

2.2.2. Datos sobre opiniones políticas o convicciones religiosas o filosóficas

En la misma dirección, sobre la base de la tutela antidiscriminatoria, la prohibición general de tratamiento se aplica a los datos que revelen opiniones, ideas o posicionamientos políticos, así como las convicciones religiosas, filosóficas y –añadimos nosotros– morales o éticas. La ideología la conforma el conjunto de ideas fundamentales que caracteriza el pensamiento de una persona[30] y la opinión política es el juicio o valoración que se forma una persona respecto de las distintas opciones políticas, no solo respecto de los partidos políticos.

Aquella prohibición alcanza a los datos que denotan posicionamientos individuales basados en convicciones religiosas o morales o fundados en preferencias personales conformadoras de un proyecto vital autónomo[31]. El

[29] Cfr. Informe de la Comisión Europea "The meaning of racial or ethnic origin in EU law: between stereotypes and identities" (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54924)

[30] Definición tomada del DRAE.

[31] *Vid.* ALBERT, M.: "Convicciones religiosas y elecciones personales: derecho a la objeción de conciencia y autodeter-

derecho distingue "las convicciones en sentido estricto (articuladas en los términos del Convenio de Roma por la vía del artículo 9, que se ocupa de la libertad de pensamiento, conciencia y religión) de las preferencias, elecciones, opciones y proyectos vitales (articuladas, en cambio, por la vía del artículo 8, que garantiza el derecho a la vida privada personal y familiar)"[32]. Las convicciones implican un convencimiento íntimo, asentado sobre la fe o las creencias; no son simples expresiones de la autonomía personal o del libre desarrollo de la personalidad y tampoco son opiniones o ideas.

También la Constitución garantiza la libertad ideológica, religiosa y de culto de los individuos (art. 16.1 CE) y nadie puede ser obligado a declarar sobre su ideología, religión o creencias (art. 16.2 CE), preservando así la libertad de convicción de los individuos, sus creencias íntimas y el desarrollo y final del ser humano. Asimismo, reconoce y protege el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción [art 20.1. a) CE]. Y los ciudadanos tienen reconocido el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal (art. 23.1 CE).

Si a los trabajadores se les reconocen estos derechos, parece lógico que los datos personales que faciliten información sobre opiniones políticas o convicciones religiosas o filosóficas no puedan se tomados como referencia para adoptar decisiones empresariales. Su libertad de conciencia se manifiesta en opiniones políticas, creencias religiosas o planteamientos vitales que, aun conocidos por el empleador, no pueden ser tratados, como pauta general.

2.2.3. Datos sobre la afiliación sindical

De todas las categorías especiales de datos, la referida a la afiliación sindical es una información de contenido estrictamente laboral, a diferencia del otras que, siendo de carácter más general, pueden tener un incidencia transversal, también –claro está– en las relaciones de trabajo.

Es cierto que el Tribunal Constitucional concluyó que, "siendo los sindicatos formaciones con relevancia social, integrantes de la estructura pluralista de la sociedad democrática, no puede abrigarse duda alguna de que la afiliación a un sindicato es una opción ideológica protegida por el artículo 16 CE", que garantiza al ciudadano el derecho a negarse a declarar sobre ella[33]. Por consiguiente, la manifestación de la afiliación sindical es un derecho personal y exclusivo del trabajador, que deben respetar tanto el empresario como los propios sindicatos.

Por más que la afiliación a un sindicato lleve consigo cierta inclinación por determinados valores socio-políticos, esa afección solo en parte puede considerarse coincidente con lo que hemos definido como ideología en el caso de las organizaciones sindicales, por su vinculación directa a los intereses profesionales. En este contexto, el conocimiento de la afiliación sindical de la persona, cuando se produce en el ámbito laboral, solo se aproximaría a las convicciones socio-políticas de la persona.

Realmente, la protección deriva del derecho fundamental a la libertad sindical, derecho que se proyecta con relevancia incuestionable para los trabajadores en tanto les permite organizarse con fines de promoción y defensa de sus intereses profesionales[34]. Como derecho

minación individual en la jurisprudencia del Tribunal Europeo de Derechos Humanos", *Revista Persona y Derecho*, núm. 77, 2017, p. 251.

[32] ALBERT, M.: "Convicciones religiosas y elecciones personales: derecho a la objeción de conciencia y autodeterminación individual en la jurisprudencia del Tribunal Europeo de Derechos Humanos", *cit.*, p. 253.

[33] SSTC 292/1993, de 18 de octubre, 94/1998, de 4 de mayo, y 145/1999, de 22 de julio.

[34] *In extenso*, GARCÍA MURCIA, J.: "El hecho sindical. La mayor representatividad. Asociacionismo profesional y empresarial. Balance y propuestas de reforma", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. 429, 2018, p. 63.

fundamental de amplio contenido –esencial y derechos y facultades adicionales[35]– reconocido en nuestra Constitución, que sigue la senda de las declaraciones internacionales –Convenios de la Organización Internacional del Trabajo núms. 87 y 98, señaladamente– sobre esta materia, la libertad sindical comprende "el derecho a fundar sindicatos y a afiliarse al de su elección", sin que la afiliación sea forzosa o imperativa, pues "nadie podrá ser obligado a afiliarse a un sindicato" (art. 28.1 CE). Tanto en su vertiente positiva –derecho a afiliarse– como en su vertiente negativa –derecho a no afiliarse–, el derecho a sindicarse libremente, su respeto, lleva aparejado el derecho del trabajador a no declarar su afiliación sindical al empresario, idéntica garantía propia de la libertad ideológica, religiosa y creencias (art. 16.2 CE), por cuanto quedan preservadas esas informaciones por el derecho a la intimidad o privacidad de la persona. Tampoco, en consecuencia, se podrá indagar sobre su pertenencia o vinculación a un sindicato.

Conocerá, obviamente, la afiliación el sindicato elegido por el trabajador, en el que libremente ingresa. La información del trabajador afiliado y el mismo dato de la afiliación constarán en los archivos y ficheros del sindicato, sin que esos datos personales puedan comunicarse a terceros sin el consentimiento del interesado. Para el desenvolvimiento de la relación de adhesión, serán tratados los datos por la organización sindical, pero únicamente con ese fin.

De manera voluntaria, el trabajador podrá hacer pública su afiliación y con su expreso consentimiento se podrá tratar ese dato por quien o quienes lo conozcan, siempre con una finalidad lícita[36]. Recuérdese que será nula cualquier decisión del empresario que de lugar en el empleo, así como en materia de retribuciones, jornada y demás condiciones de trabajo, a situaciones de discriminación directa o indirecta por razón –entre otras– de "adhesión o no a sindicatos y a sus acuerdos" (art. 17 TRLET).

El empleador puede conocer la afiliación del trabajador a un sindicato con motivo del descuento de la cuota sindical. El supuesto está regulado en la Ley Orgánica 11/1985, de 2 de agosto, de libertad sindical (en adelante, LOLS): "el empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de este" (art. 11.2 LOLS). No se impone *ex lege* la obligación del trabajador de declarar su afiliación a un sindicato. Solamente si el trabajador afiliado quiere abonar su cuota al sindicato a través de la fórmula del descuento o retención en su recibo de salarios, podrá facultar al sindicato para que, su vez, pida formalmente al empresario que proceda, primero, al descuento de la cantidad correspondiente y, después, a su transferencia a la cuenta de la organización sindical. No cabe detraer la cuantía anticipadamente ni puede exigirse una manifestación negativa de voluntad al trabajador, pues ello presupone el conocimiento de su afiliación a un sindicato.

Por ser la afiliación sindical un dato sensible y, por tanto, protegido, no incumbe al sindicato solicitar el descuento directamente al empresario. Previo a ese trámite, ha de obtener

---

[35] Entre otras muchas, SSTC 132/2000, de 16 de mayo, 76/2001, de 26 de marzo, y 281/2005, de 7 de noviembre.

[36] Como se afirma en el Preámbulo de la LOPDyGDD, "la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores". Las –así llamadas– listas negras de sindicalistas o de trabajadores conflictivos [STS (Civil) de 12 de noviembre de 2015 (Rec. 899/2014)] se conforman con "la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación" (Informe núm. 0201/2010 de la AEPD). *Vid.* CRUZ VILLALÓN, J.: *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador*, Bomarzo, Albacete, 2019, p. 60.

la conformidad o el consentimiento, expreso, libre e indubitado, del trabajador afiliado, tanto para que el sindicato solicite a la empresa el descuento de la cuota como para que la empresa realice el descuento en la nómina. Solo así el empleador podrá demostrar que el trabajador consintió el tratamiento de ese dato personal (art. 7.1 RGPD)[37]. Será, en definitiva, el sindicato el que facilite a la empresa el dato de la afiliación, junto con el consentimiento explícito[38] del trabajador afiliado para realizar el descuento de la cuota sindical, y sobre esa base el empresario, sin necesidad de recabar una nueva manifestación de consentimiento[39], comunicará al sindicato el traspaso de la cantidad deducida al trabajador, con ningún otro dato adicional, más allá del que sea indispensable para su identificación, ya conocido evidentemente por el sindicato.

También por idéntico motivo, de producirse –conforme a las previsiones legales– el descuento de la cuota sindical, su reflejo en el recibo de salarios ha de ser una información neutra, es decir, no debe identificar que corresponde a su afiliación y, menos aún, el sindicato beneficiario. No debe aparecer el dato de la afiliación sindical, aun cuando haya dado su consentimiento el trabajador para proceder a la retención de esa cantidad a favor del sindicato, ni expresar en la nomina cualquier signo del que se pueda deducir la condición de trabajador afiliado a un sindicato.

La doctrina judicial ha considerado que el dato de afiliación sindical del trabajador reflejado en la nómina –se incluía en el recibo de nómina (entregado en sobre cerrado y personalmente al trabajador) la denominación de la organización sindical a la que se estaba transfiriendo la cuota sindical– no lesiona el derecho a la protección de datos, y ello porque "se trata de un documento estrictamente privado, dirigido exclusivamente a la persona a la que se abona el salario mensual, al que no se da ninguna publicidad y que puede ser mantenido o no en dicho ámbito reservado a voluntad del referido trabajador"[40]. Hay que subrayar que se llega a esa conclusión teniendo en cuenta, sobre todo, el ámbito privado y confidencial –una nómina– en la que se hace constar el dato de afiliación a un concreto sindicato.

Probablemente, la respuesta judicial hubiera sido otra si se hubiera considerado que la hoja de salarios es "un documento de uso común en el tráfico jurídico por su habitual presentación ante entidades públicas y privadas a múltiples efectos", ya que en tal supuesto "la inclusión en la nómina del trabajador de la mención del sindicato, al que pertenece y a cuyo favor se hace el descuento de la cuota sindical, revela la afiliación sindical del trabajador, de modo que un dato que, como hemos dicho, pertenece a la privacidad del trabajador, podría ser fácilmente conocido por terceros"[41]. Por tanto, tratándose de una situación de hecho que incide sobre derechos personales y exclusivos del trabajador, será necesario su consentimiento expreso para que se incorpore su afiliación sindical a la nómina.

---

[37] Anteriormente, se exigía, por el carácter especialmente protegido de la afiliación sindical, que el trabajador consintiera la cesión de ese dato de forma expresa y por escrito (art. 7.2 LO 15/1999).

[38] Documento de trabajo sobre las "listas negras", de 3 de octubre de 2002, elaborado por el GT29: "será necesario contar con el consentimiento expreso y por escrito del afiliado no solo para la comunicación al sindicato de los datos referidos al pago de la cuota sindical por parte del empresario, sino también para la comunicación previa efectuada por el sindicato al empresario de su condición de afiliado que solicita el descuento en la nómina de la citada cuota". *Vid.*, también, el Informe núm. 0434/2010 de la AEPD.

[39] Puede considerarse que "el trabajador lo ha prestado expresamente respecto de las cesiones de datos que hubieran de realizarse entre el empresario y el sindicato para garantizar la efectividad de la forma de pago que el propio trabajador ha elegido" (Informe núm. 0033/2010 de la AEPD). En la doctrina, *vid.* MERCADER UGUINA, J. R. y DE LA PUEBLA PINILLA, A.: "Protección de datos y relaciones colectivas", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. 423, 2018, p. 72.

[40] SAN (C-A) de 14 de septiembre de 2005 (Rec. 458/2003).

[41] STSJ de Cataluña de 9 de noviembre de 2004 (Rec. 5369/2004).

Por otra parte, a cada sindicato se le faculta para el tratamiento del dato de la afiliación de los trabajadores que voluntaria y libremente han decidido pertenecer al mismo, siempre en el ámbito de sus actividades legítimas y con las debidas garantías y sin que puedan comunicar los datos personales de sus miembros a terceros sin el consentimiento de los interesados [art. 9.2.d) RGPD]. Así, los sindicatos asumen el papel de responsables del tratamiento de esos datos.

Podríamos pensar que ese consentimiento, como excepción, debe darse para que el empresario conozca sobre la constitución de una sección sindical *ex* artículo 10 LOLS y la designación de uno o más delegados sindicales. La mera constitución de la sección sindical solo denota la existencia de trabajadores afiliados a un sindicato, si bien indirectamente puede dar a conocer los concretos trabajadores afiliados y, de manera directa, saber la concreta afiliación del delegado o delegados sindicales, al ser elegidos "por y entre" los afiliados al sindicato en la empresa o en el centro de trabajo.

Igualmente, se requiere el consentimiento del trabajador afiliado para que se haga constar en la candidatura a delegado de personal o miembro del comité de empresa, si bien para ser elegible[42] no se exige estar afiliado al sindicato por el que un trabajador decida presentarse, bajos sus siglas[43]. En verdad, la afiliación es un dato no requerido puesto que en el modelo oficial de candidatura[44], tanto a delegados de personal como a miembros de comité de empresa, la columna que se refiere a "sindicato/grupo de trabajadores/coalición" solo que tiene efectos en cuanto a la atribución de resultados y posteriormente para medir la representatividad de los sindicatos. Tampoco debe incluirse la afiliación sindical de los trabajadores, si le consta al empresario, en el censo laboral[45] que este último debe facilitar a la mesa electoral, al no exigirse esa información (art. 6.3 RD 1844/1994).

Finalmente, se debe destacar que si el dato de la afiliación sindical[46] constara en alguna administración o entidad[47] a las que se le aplica las normas que regulan el derecho de acceso a la información pública, en los términos que establece la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, "únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso" (art. 15.1 Ley 19/2013).

2.2.4. Datos genéticos

Resulta una novedad, respecto de la normativa precedente, la inclusión de los datos genéticos como una categoría especial de

[42] Cfr. Art. 69.2 TRLET.

[43] Se podrán presentar candidatos para las elecciones de delegados de personal y miembros del comité de empresa por los sindicatos de trabajadores legalmente constituidos o por las coaliciones formadas por dos o más de ellos, que deberán tener una denominación concreta atribuyéndose sus resultados a la coalición; igualmente podrán presentarse los trabajadores que avalen su candidatura con un número de firmas de electores de su mismo centro y colegio, en su caso, equivalente, al menos, a tres veces el número de puestos a cubrir (art. 69.3 TRLET). En el primer supuesto, la candidatura es sindical, pero no es requisito de validez de la misma que los candidatos sean trabajadores afiliados; es más, si lo fueran y cambiaran su afiliación a otro sindicato, el resultado inicial no se modifica a efectos de atribuir los resultados obtenidos en la elección, es decir, "el cambio de afiliación del representante de los trabajadores, producido durante la vigencia del mandato, no implicará la modificación de la atribución de resultados" (art. 12.3 RD 1844/1994, de 9 de septiembre, por el que se aprueba el Reglamento de elecciones a órganos de representación de los trabajadores en la empresa).

[44] Cfr. Modelo 8 del anexo RD 1844/1994.

[45] Cfr. Modelo 2 del anexo RD 1844/1994.

[46] El mismo criterio se aplica para los datos que revelen la ideología, religión o creencias.

[47] No se incluye, sin embargo, a las organizaciones sindicales, puesto que a estas, como a los partidos políticos y a las organizaciones empresariales, solamente se les aplica el Capítulo II, que desarrolla la "publicidad activa", del Título I de la Ley; por lo tanto, no el Capítulo III, que regula el "derecho de acceso a la información pública", del mismo Título I. Cfr. Art. 3.a) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE de 10 de diciembre de 2013).

datos personales. Se ha podido defender su coincidencia, en su régimen jurídico, o proximidad con los datos relativos a la salud o con los datos médicos. Sin embargo, nada hay que objetar sobre la pertenencia de los datos genéticos al grupo de los datos sensibles, de forma separada o individualizada, sobre todo porque no todos los datos genéticos deben ser considerados datos de salud o deben asimilarse a estos últimos, sino porque "todo dato genético es, por la naturaleza de la información que revela o pudiera revelar, un dato merecedor de protección reforzada"[48].

Por su especificidad respecto de otras categorías especiales de datos y por la limitación que ha conllevado su asimilación a los datos de salud, es acertada la referencia a los datos genéticos, por cuanto merecen una protección autónoma[49]. Y quizá por presentarse como nueva categoría especial, el vigente Reglamento comunitario aporta una definición: "datos personales relativos a las características genéticas, heredadas o adquiridas, de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona" [art. 4.13) RGPD], en particular "a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente" (considerando 34 RGPD).

Previamente, la Recomendación núm. R 5 (97), de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros, sobre protección de datos médicos, ya había aportado un concepto autónomo de dato genético, entendiendo que se refiere a "todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no". Asimismo, la Declaración Internacional sobre los Datos Genéticos Humanos, de 16 de octubre de 2003, aprobada por la 32ª sesión de la Conferencia General de la UNESCO, define los datos genéticos como "información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos".

En nuestro ordenamiento jurídico, la noción de "dato genético de carácter personal" fue introducida por la Ley 14/2007, de 3 de julio, de investigación biomédica (en adelante, LIB), como la "información sobre las características hereditarias de una persona, identificada o identificable, obtenida por análisis de ácidos nucleicos u otros análisis científicos" [art. 3.j) LIB].

Como se observa, la definición de dato genético que aporta el Reglamento comunitario es más amplia y precisa que las anteriores, siendo coincidente en su núcleo esencial. Abarca todas las informaciones sobre la fisiología y la salud de la persona física, obtenida a través de la analítica de una muestra biológica, cualquier análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN) u otro elemento que permita obtener información equivalente[50].

En concreto, las técnicas de análisis de ADN revelan el carácter único[51] de la persona

[48] GÓMEZ SÁNCHEZ, Y.: "La protección de los datos genéticos: el derecho a la autodeterminación informativa", *Derecho y Salud*, vol. 16, núm. extraordinario 1, 2008, p. 62.

[49] ROMEO CASABONA, C. M.: "El tratamiento y la protección de los datos genéticos", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): *Gen-Ética*, Ariel, Barcelona, 2003, p. 240.

[50] *Vid.* LEWIS R.: *Human Genetics: Concepts and Applications*, 12ª ed., McGraw-Hill Science, NewYork (EE.UU.), 2017, *passim*.

[51] *Vid.* CLAYTON, E. W., EVANS, BARBARA J., HAZEL, JAMES W. y ROTHSTEIN, MARK A.: "The law of genetic privacy: applications, implications, and limitations", *Journal of Law and the Bioscien-*

–a excepción de los gemelos monocigóticos[52]– y su configuración genética, por ende tiene un carácter dual: "proporcionan información sobre el cuerpo humano y permiten la identificación inequívoca de una, y solo una, persona"[53]. Esa información genética obtenida permite al propio sujeto obtener información sobre su configuración genética, las consecuencias presentes o futuras de tal configuración y le posibilita la adopción de decisiones y el ejercicio de sus derechos y libertades; permite identificar a la persona, viva o muerta, y relacionarla con otros sujetos; permite conocer a la persona su estado de salud actual y prever la propensión a padecer enfermedades futuras; permite detectar predisposiciones genéticas de los individuos y capacidad de diversa naturaleza; aporta datos relevantes que superan el ámbito individual; aporta información que puede ser utilizada en muy diversos campos de la organización de la sociedad, entre ellos el ámbito laboral, y, por último, aporta información que podrá valorarse en el futuro[54].

No solo por el contenido de la información que aporta, también su singularidad está determinada por las características[55] de la información genética, fundamentalmente dos: permanencia e inalterabilidad, con independencia de la voluntad del individuo, y vinculación biológica con los demás miembros de un grupo familiar o étnico.

Sobre la base de lo expuesto, se deriva la especial naturaleza que poseen los datos genéticos. La más perfecta, en el sentido de exclusiva, relación entre la persona física y la información obtenida, que permite la identificación de aquella a través de esos datos, además de dar a conocer datos relativos a cuestiones estrechamente unidas al núcleo de la personalidad y de la dignidad humanas, hace que tengan especial incidencia en la vida privada, en el ejercicio de las libertades o ante el riesgo de prácticas discriminatorias[56]. De ahí, en suma, la calidad del dato personal, su calificación como dato sensible y su fundamento como categoría especial de dato personal.

El peligro de difundir datos personalísimos y el riesgo de adoptar decisiones discriminatorias en la esfera de las relaciones laborales y en otros –sanitario o de los seguros, por ejemplo– campos, si duda, es cierto, de ahí la interdicción general de tratamiento de los datos genéticos y su reserva, excepto en los supuestos amparados por el legislador. Por la complejidad y la sensibilidad de la información genética, existe un peligro cierto de que el responsable del tratamiento haga un uso indebido de la misma o la reutilice con fines no autorizados. Además, toda discriminación por razón de características genéticas debe quedar prohibida con carácter general[57].

Se ha de recordar, por último, que si el dato genético[58] constara en alguna administración o entidad a las que se le aplica las normas que regulan el derecho de acceso a la información pública, en los términos que establece la –ya citada– Ley 19/2013, "el acceso solo se podrá

ces, vol. 6, núm. 1, 2019, p. 1 (https://academic.oup.com/jlb/article/6/1/1/5489401).

[52] LACADENA, J. R.: "Individualización y mismidad genética en el desarrollo humano", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): *Gen-Ética*, Ariel, Barcelona, 2003, p. 116.

[53] Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, adoptado por el GT29.

[54] Son las conclusiones que presenta GÓMEZ SÁNCHEZ, Y.: "La protección de los datos genéticos: el derecho a la autodeterminación informativa", *cit.*, p. 61.

[55] Las apunta ROMEO CASABONA, C. M.: *Los genes y sus leyes. El derecho ante el genoma humano*, Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, Comares, Granada, 2002, p. 63.

[56] *Vid.* ÁLVAREZ GONZÁLEZ, S.: "Derecho a la «privacidad» e información genética", *cit.*, p. 20, y la bibliografía que cita.

[57] Cfr. Considerando 23 Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[58] El mismo criterio se aplica para datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, los datos biométricos y a los relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública al infractor.

autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley" (art. 15.1 Ley 19/2013).

2.2.5. Datos biométricos

Ex lege, "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" [art. 4.14) RGPD], son datos biométricos e, igualmente, se encuadran entre las categorías especiales de datos personales cuando identifican –se insiste– de manera unívoca a una persona (art. 9.1 RGPD).

Estos datos se han definido como "propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad"[59]. Ejemplos típicos de datos biométricos "identificadores", al corresponder a una única persona, son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces y también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento, como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc. En particular, el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física (considerando 51 RGPD).

Una peculiaridad de los datos biométricos –como sucede, por cierto, con los genéticos– es que se les puede considerar tanto como contenido de la información sobre una determinada persona –el trabajador X tiene estas huellas dactilares– como un elemento para vincular una información a una determinada persona física –este dispositivo lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden al trabajador X; por lo tanto el trabajador X ha tocado este dispositivo–.

A través de sistemas que utilizan información o datos biométricos, se puede identificar a un trabajador, ya sea mediante el análisis de aspectos físicos y morfológicos de la persona –huellas dactilares, patrones de la mano, reconocimiento facial, características de la retina, geometría del iris, rasgos de la voz, estructuras venosas, pulsaciones, ondas cerebrales o estado de atención–, ya sea por la valoración de sus comportamientos o habilidades –comprobación de su escritura, firma o presión sobre las teclas del ordenador–. Con ellos se permite al empleador controlar toda la actividad del trabajador, desde su inicio, pasando por el desempeño de sus funciones durante el tiempo de trabajo, hasta su conclusión. Dicho con otras palabras, el empresario, con los sistemas biométricos, puede controlar la presencia y ubicación precisa de los empleados en sus instalaciones, conociendo con exactitud la hora de entrada y de salida o el tiempo efectivo dedicado a la actividad profesional, lo que permite diferenciar y valorar el tiempo productivo e improductivo, particularmente útil en organizaciones con horario flexible o con jornadas irregulares[60].

Al respecto, el Tribunal de Justicia de la Unión Europea ha confirmado que "un registro del tiempo de trabajo, que incluye la indicación de las horas en que cada trabajador

[59] Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, adoptado por el GT29.

[60] Así lo expone, con razón, RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, p. 158.

inicia y finaliza la jornada, así como de las pausas o periodos de descanso correspondientes, queda comprendido en el concepto de «datos personales»"[61].

También, de modo destacado, son particularmente útiles[62] para garantizar el acceso de los empleados a determinadas dependencias o a la utilización de equipamientos, bien sea por el tipo de actividad desarrollada o por el valor y las posibles consecuencias que los medios materiales –instrumentos, máquinas, etc.– pueden acarrear para el propio trabajador o para terceros. La principal ventaja de estos medios de control es que no permiten la suplantación de la persona física sujeta a control o vigilancia.

Un uso adicional, por último, que permite la evolución tecnológica posibilita la puesta en marcha de procesos de encuadramiento de los individuos en grupos o divisiones, de cara a la elaboración de perfiles y "con fines claramente decisionales"[63].

Para el reconocimiento biométrico del trabajador, el paso previo es proceder a captar, por medio de un sensor específico para cada tipo de técnica biométrica, uno o más rasgos específicos de la persona, y su transformación en una secuencia numérica, conformando una plantilla que queda registrada en una base de datos. Después, la utilización del sistema biométrico requerirá, en cada uso, la comparación entre la plantilla almacenada y la muestra biométrica que se vuelve a tomar para verificar su equivalencia[64].

Esa recogida primera y el tratamiento posterior de datos biométricos puede poner en riesgo los derechos fundamentales de los trabajadores, pues de esos datos se pueden deducir otras informaciones que pertenecen a su esfera de privacidad[65]. Por ello, la licitud del uso de estos modelos de identificación personal se somete al juicio de proporcionalidad[66] por parte de los tribunales cuando han de valorar aquella en supuestos controvertidos. Así, sobre el control horario basado en un método que consiste en la lectura biométrica, basado en el reconocimiento tridimensional de la mano –largo, ancho y espesor– para verificar la identidad biométrica de la persona, se analiza el objetivo propuesto, "objetivo que no es otro que el de lograr un mayor nivel de eficacia en la Administración pública, eficacia que pasa por un control efectivo del cumplimiento de sus obligaciones por parte de los empleados públicos, obligaciones que se inician en el momento del puntual acceso a sus puestos de trabajo y en una estricta observancia de la jornada laboral". Respecto del juicio de rigurosa necesidad, aún existiendo otros sistemas, "hay dos realidades que no pueden negarse, de un lado la lógica posibilidad de incorporación a la Administración pública de las nuevas tecnologías como método de control y, de otro, el notorio carácter imperfecto de los sistemas de control más comúnmente usados, tanto el sistema

[61] STJUE de 30 de mayo de 2013, Asunto C-342/12, *Worten – Equipamentos para o Lar, S. A.*

[62] *Vid.* Goñi Sein, J. L.: "Intimidad del trabajador y poderes de vigilancia y control empresarial", en García Murcia, J. (Coord.): *Jornada sobre derechos fundamentales y contrato de trabajo*, Principado de Asturias, Oviedo, 2017, p. 61.

[63] Baz Rodríguez, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, Bosch Wolters Kluwer, Barcelona, 2019, p. 244.

[64] *Vid.* Poquet Catalá, R.: *El actual poder de dirección y control del empresario*, Cuadernos de Aranzadi Social, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2013, p. 285.

[65] En este sentido, Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, p. 159, pone de relieve esos riesgos para la persona del trabajador, "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".

[66] Como sintetizan las SSTC 66/1995, de 8 de mayo, 55/1996, de 28 de marzo, 207/1996, de 16 de diciembre, y 37/1998, de 17 de febrero, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

de firma, por su posible manipulación, como el sistema de reloj y ficha, por no impedir la sustituibilidad en su cumplimiento". Por último, "la implantación del sistema puede reportar más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, máxime cuando nos encontramos ante la imposición de una obligación a un colectivo vinculado a la Administración mediante una relación de sujeción especial"[67].

Sin embargo, aplicando ese mismo principio de proporcionalidad, más cuestionable –incluso "deplorable"[68]– resulta la implantación de chips subcutáneos, las pulseras de movimientos o las etiquetas de identificación por radiofrecuencia. La Recomendación 2009/387/CE, de 12 de mayo de 2009, de la Comisión Europea, sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia, insiste en que el trabajador conozca el modelo empleado como sistema de control, imponiendo a las empresas la obligación de elaborar y publicar información[69] precisa y fácil de comprender sobre el uso de cada aplicación, que como mínimo debe incluir: a) la identidad y el domicilio de los operadores; b) la finalidad de la aplicación; c) los datos que procesa la aplicación, en particular si se trata de datos personales, y si se controla la localización de las etiquetas; d) un resumen de la evaluación del impacto sobre la protección de datos y la intimidad; y, e) los posibles riesgos para la intimidad, si existen, relacionados con el uso de etiquetas en la aplicación y las medidas que pueden adoptar las personas para reducirlos.

Sobre el tratamiento de las expresiones faciales del trabajador por medios automatizados, de la misma manera se advierte el riesgo de un uso desproporcionado –incluso en el trabajo a distancia, pues ello lo permite las nuevas tecnologías– por su incidencia sobre los derechos y libertades de los trabajadores. Se ha considerado ilegal, en general, y los empresarios, por consiguiente, deben abstenerse de utilizar tecnologías de reconocimiento facial, aunque puede haber algunas excepciones marginales a esta regla, sin que tales escenarios puedan utilizarse para invocar una legitimación general del uso de estas tecnologías[70]. Asimismo, debido a los riesgos particulares asociados a los datos biométricos, antes de comenzar el tratamiento de las imágenes digitales a los fines del reconocimiento facial, se requerirá el consentimiento informado de la persona[71].

2.2.6. Datos relativos a la salud

El Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, entre las "categorías particulares de datos" refiere los de carácter personal –entre otros– relativos a "la salud" (art. 6). Asimismo, la Recomendación núm. R 5 (97), de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros, sobre protección de datos médicos, señala que la expresión "da-

[67] SSTSJ de Cantabria (C-A) de 21 de febrero (Rec. 763/2002) y de 14 marzo de 2003 (Rec. 893/2002). De igual manera, sobre la implantación de un sistema de huella dactilar con lector biométrico en el centro de trabajo para el acceso a las instalaciones, cfr. STSJ de Murcia de 25 de enero de 2010 (Rec. 1071/2009) y STSJ de la Comunidad Valenciana de 8 de febrero de 2017 (Rec. 3489/2016); en la doctrina, Goñi Sein, J. L.: *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018)*, Bomarzo, Albacete, 2018, p. 47.

[68] Así de contundente se expresa Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, p. 161.

[69] La Guía sobre seguridad y privacidad de la tecnología RFID (*Radio Frequency IDentification*), elaborada por la AEPD y el Instituto Nacional de Tecnologías de la Comunicación, recomienda 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.

[70] Dictamen 02/2017, de 8 de junio, sobre el tratamiento de datos en el trabajo, adoptado por el GT29.

[71] Dictamen 02/2012, de 22 de marzo, sobre reconocimiento facial en los servicios en línea y móviles, adoptado por el GT29.

tos médicos" se refiere "a todos los datos personales relativos a la salud de un individuo", esto es, "a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos" (art. 1).

Repite esa idea la –tantas veces citada y derogada– Directiva 95/46/CE, que enumeraba los datos relativos a la salud –característicos de su "identidad física, fisiológica o psíquica" [art. 2.a) Directiva 95/46/CE]– dentro de las categorías especiales de datos personales en cuanto a su tratamiento (art. 8.1 Directiva 95/46/CE), siendo preciso dar una interpretación amplia a la expresión "datos relativos a la salud", de modo que comprenda "la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona"[72]. Al respecto, el GT29, en el Anexo a la Carta "*Health data in apps and devices*", identifica los criterios relevantes para determinar cuándo los datos procesados por las aplicaciones y dispositivos de estilo de vida y bienestar deben considerarse "datos de salud"; así cuando: los datos son inherente o claramente de carácter médico; los datos son datos sin procesar del sensor que se pueden usar en sí mismos o en combinación con otros datos para sacar una conclusión sobre el estado de salud actual o el riesgo para la salud de una persona; se sacan conclusiones sobre el estado de salud o el riesgo para la salud de una persona, independientemente de si estas conclusiones son precisas o inexactas, legítimas o ilegítimas, adecuadas o inadecuadas.

Son "datos especialmente protegidos", según la anterior Ley Orgánica 15/1999, "los datos de carácter personal que hagan referencia a la salud", junto a otros (art. 7.2 y 3 LO 15/1999). Respecto de su tratamiento, además, decía que "las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad" (art. 8 LO 15/1999). Es su norma reglamentaria[73] de desarrollo la que define los "datos de carácter personal relacionados con la salud" como "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética" [art. 5.1.g) RD 1720/2007].

En el presente, el Reglamento 2016/679/UE define los datos sobre la salud como "los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" [art. 4.15) RGPD]. Antes, en su parte expositiva afirma que entre los datos personales referentes a la salud "se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro"; específicamente "se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un mé-

[72] STJUE de 6 de noviembre de 2003, Asunto C-101/01, *Bodil Lindqvist*.

[73] RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

dico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica *in vitro*" (considerando 35 RGPD).

La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, asegura, *ab initio*, que "la dignidad de la persona humana, el respeto a la autonomía de su voluntad y su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica" (art. 2.1 Ley 41/2002) y, reafirma que "toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley" (art. 7.1 Ley 41/2002).

En el ámbito laboral, sin duda, la alteración de la salud puede afectar al trabajador, disminuyendo su rendimiento o, en muchas ocasiones, impidiéndole prestar servicios de manera temporal. Incluso ante las situaciones de riesgo para la salud o cuando ya se haya modificado la salud del trabajador, la intervención de la empresa podrá estar justificada bien para prevenir el desarrollo de enfermedades o patologías o bien para verificar el estado de salud del trabajador[74].

En efecto, por un lado, el empresario "podrá verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico" y la negativa del trabajador a dichos reconocimientos –como sanción– "podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones" (art. 20.4 TRLET), como podrían ser las mejoras voluntarias sobre las prestaciones económicas del sistema público de Seguridad Social, concretamente la prestación de incapacidad temporal.

Se trata, en definitiva, de someter al trabajador a controles médicos adicionales a los efectuados por los servicios públicos de salud y las entidades gestoras y colaboradoras de la Seguridad Social, mediante el servicio médico de empresa o a través del recurso a servicios sanitarios externos, pero sin que sea posible realizar pruebas diagnósticas que no tengan "como finalidad la mejora o estudio de su estado de salud"[75] o utilizar las informaciones obtenidas para fines distintos a los habilitados *ex lege*[76].

De esta extensión del poder de control del empresario, según el Tribunal Constitucional, no se deriva la posibilidad de crear un fichero automatizado denominado "absentismo con baja médica", por cuanto requeriría que mediase el consentimiento expreso de los afectados o que, por razones de interés general, así lo dispusiera una ley; como ninguno de dichos requisitos concurren en el supuesto enjuiciado, ello determina que la creación de esa base de datos vulnera el artículo 18 CE, el derecho a la intimidad personal de los titulares de la información en ella conservada, en relación con el artículo 18.4 CE[77].

Por otro lado, la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales (en adelante, LPRL), obliga al empresario a garantizar a los trabajadores a su servicio "la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo" (art. 22.1, párrafo primero, LPRL). La vigilancia y control de la salud de los trabajadores,

[74] *Vid.*, con detalle y finura jurídica, RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, pp. 138-157.

[75] STS de 25 de enero de 2018 (Rec. 249/2016).

[76] STSJ del País Vasco de 6 de julio de 2004 (Rec. 1232/2004), donde se calificó el reconocimiento médico como desproporcionado y realizado con intención de constituir una prueba a esgrimir en un procedimiento judicial posterior.

[77] STC 202/1999, de 8 de noviembre. *Vid.* GARCÍA MURCIA, J.: "Derecho a la intimidad y contrato de trabajo: la anotación de las bajas médicas (Comentario a la STC 202/1999, de 8 de noviembre)", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 2, 2000, pp. 1937-1956.

siendo una obligación empresarial, se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada (art. 22.6 LPRL).

Esta vigilancia, en principio, solo se puede realizar cuando el trabajador preste su consentimiento. De este carácter voluntario únicamente se exceptúan, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para él mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad (art. 22.1, párrafo segundo, LPRL).

En todo caso, las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud (art. 22.2 LPRL). En efecto, respecto de los datos relativos a la salud obtenidos en los reconocimientos médicos de los trabajadores, rige el principio básico de confidencialidad, como proyección del derecho a la intimidad, lo que supone su "reservabilidad", el mantenimiento en secreto hacia personas que no tienen un interés legítimo para justificar su conocimiento[78]. Ahora bien, esa confidencialidad parece graduarse según la información se presente en forma de resultados o en forma de conclusiones: para los resultados de la vigilancia de la salud la confidencialidad es máxima –modulable solo por el consentimiento del trabajador o un interés legítimo, como el perjuicio a terceros–, mientras que la confidencialidad es mínima para las conclusiones obtenidas, por el tipo de información que incorpora y el mayor número de destinatarios, "bien entendido que en ningún caso debe trascender de la empresa o de los sujetos con responsabilidades en materia de prevención"[79].

Los resultados de la vigilancia de la salud se comunican a los trabajadores afectados (art. 22.3 LPRL) y el acceso a toda la información médica de carácter personal se limita al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador (art. 22.4 párrafo segundo, LPRL). No obstante la anterior prohibición, el empresario y las personas u órganos con responsabilidades en materia de prevención deben ser informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva (art. 22.4 párrafo tercero, LPRL).

Como garantía conexa, más allá del derecho a la protección de los datos relativos a la salud, la información médica de los trabajadores obtenida en los procesos de vigilancia de su salud con fines preventivos, que excede del estricto ámbito de los riesgos profesionales[80], no podrá ser usada "con fines discriminatorios ni en perjuicio del trabajador" (art. 22.4 LPRL). Esos son, perfectamente identificados por el legislador, los riesgos para el trabajador que el conocimiento de datos sobre su salud deriva en el ámbito del empleo y las relaciones laborales.

[78] PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*, núm. 138, 2018, pp. 168-169.

[79] Así, PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *cit.*, p. 169.

[80] BLASCO PELLICER, A.: "El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador", en BORRAJO DACRUZ, E. (Dir.): *Trabajo y libertades públicas*, La Ley, Madrid, 1999, p. 257.

En definitiva, el cumplimiento del deber de vigilancia de la salud conlleva para el personal sanitario encargado la obtención de resultados y elaboración de diagnósticos, mientras que para el empresario comporta el depósito de una muy amplia información sobre los trabajadores que será necesario conservar y organizar a través de ficheros, con su actualización periódica, aunque no tenga acceso a la totalidad de los datos contenidos; responsable del tratamiento de los datos que conformen resultados sobre la salud de los trabajadores será el servicio de prevención ajeno, encargado de la vigilancia de la salud, o la empresa si se encarga de ella un servicio de prevención propio o mancomunado, si bien, como esta no puede tener acceso a esos datos, se tendrán que establecer distintos perfiles y facultades de acceso para evitar su conocimiento por el propio empleador; en cambio, sobre las conclusiones entregadas por el personal sanitario será la empresa[81]. Bien entendido que todos los datos sobre la salud deberán tener un tratamiento informático separado[82] de los otros datos disponibles de los trabajadores, y en todo caso se deberán adoptar medidas adecuadas de seguridad técnica y organizativa para evitar que personas extrañas al servicio médico del empleador tengan acceso a tales resultados.

2.2.7. Datos sobre la vida sexual o la orientación sexual

La norma comunitaria incluye en su listado de categorías especiales de datos personales, por último, los "datos relativos a la vida sexual o a la orientación sexual de la persona física" (art. 9.1 RGPD), modificando así la referencia pretérita a los datos relativos "a la sexualidad" (art. 8.1 Directiva 95/46/CE). En el contexto nacional, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se refería a los datos que hagan referencia "a la vida sexual" (art. 7.3 y 4 LO 15/1999), mientras la legislación en vigor se refiere genéricamente a la "orientación sexual" (art. 9.1 LOPDyGDD).

En cuanto al concepto, la orientación sexual es una atracción emocional, romántica, sexual o afectiva duradera hacia otra persona y se distingue fácilmente de otros componentes de la sexualidad, como el sexo biológico, la identidad sexual –el sentido psicológico de ser hombre o mujer– y el rol social del sexo –respeto de las normas culturales de conducta femenina y masculina–. La atracción puede ser hacia personas del sexo opuesto –heterosexualidad–, hacia personas del mismo sexo –homosexualidad– o hacia personas de su mismo sexo y del sexo opuesto –bisexualidad–.

La orientación sexual es diferente de la vida sexual o de la conducta sexual, mientras la primera se refiere a los sentimientos y al concepto de uno mismo, la segunda, por el contrario, puede o no expresar su orientación sexual. También se diferencia de la identidad de género, que no se relaciona con la atracción hacia otra persona, sino con quién eres: hombre, mujer, transgénero, intergénero, etc.

No se pretende describir todas las variantes acerca de la orientación sexual de las personas físicas, incluso las hay que no sienten ningún tipo de atracción sexual por nadie. La exposición precedente trata de exponer una realidad sobre la que se proyectan múltiples comportamientos discriminatorios conocida la orientación sexual de una persona, señaladamente en el ámbito de las relaciones de trabajo, ya sea en el acceso al empleo, en las condiciones de trabajo o en la extinción del contrato. Las diferencias de trato basadas en la orientación sexual se deben, sin duda, a los prejuicios sociales contra el comportamiento

[81] Sobre los sujetos intervinientes en el tratamiento, *in extenso*, *vid.* PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *cit.*, pp. 175-178.

[82] MERCADER UGUINA, J. R.: "La protección de datos personales del trabajador. La obligación del empresario de informar al trabajador sobre sus condiciones de trabajo", en CASAS BAAMONDE, M. E. y GIL ALBURQUERQUE, R. (Dirs.): *Derecho Social de la Unión Europea. Aplicación por el Tribunal de Justicia*, Francis Lefebvre, Madrid, 2018, p. 776, que cita la Recomendación núm. 2015 (2) del Consejo de Europa.

sexual de los colectivos que no son heterosexuales, jugando las restantes opciones personales como causas de discriminación. Dicho con otras palabras, el ámbito de la discriminación incluirá "cualquier conducta que comporte una tratamiento diferencial peyorativo como consecuencia de la orientación sexual que el individuo ha escogido libremente", si bien los colectivos no heterosexuales son los que requerirán "una mayor protección y una tutela efectiva frente a actitudes discriminatorias"[83].

Aunque la orientación sexual no se encuentra prevista dentro de las causas discriminatorias enumeradas –"por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social"– en el artículo 14 CE, de ser considerada como tal al ser una enumeración abierta y que alude a cualquier otra condición o circunstancia personal o social.

Encuentra plena justificación, por tanto, la mención expresa a la orientación sexual entre las categorías especiales de datos personales, pues cualquier decisión basada en el conocimiento de esa información especialmente sensible puede resultar discriminatoria, quedando prohibido su tratamiento, como regla general, y sin que sea suficiente el consentimiento del concernido para levantar esa interdicción, resultando de aplicación otras circunstancias excepcionales.

3. EL TRATAMIENTO DE LAS CATEGORÍAS ESPECIALES DE DATOS PERSONALES

La especial protección que se debe otorgar a los datos personales que son particularmente sensibles en relación con los derechos y las libertades fundamentales se materializa en un régimen propio para su tratamiento, por cuanto este, de aceptarse, podría entrañar riesgos ciertos para aquellos derechos y las libertades. Esta es la razón ultima que justifica un tratamiento diferenciado de las categorías especiales de datos, que –a tenor del Reglamento comunitario, como se expondrá en breve– no deben ser tratados, a menos que se permita en situaciones delimitadas y contempladas por el legislador, habida cuenta también de que los Estados miembros pueden ordenar disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del Reglamento. Así, se han establecido de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras circunstancias cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas.

No obstante, además de los requisitos particulares de ese tratamiento, deben aplicarse los principios generales y otras normas, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento (considerando 51 RGPD). Se recuerda que el tratamiento solo será lícito si se cumple, al menos, una de las siguientes condiciones: a) que el interesado haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación, a petición de este, de medidas precontractuales; c) que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física; e) que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) que el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales (art. 6.1 RGPD).

[83] CHACARTEGUI JÁVEGA, C.: *Discriminación y orientación sexual del trabajador*, Lex Nova, Valladolid, 2001, p. 24.

El artículo 9 del RGPD y de la LOPDyGDD concretan ese régimen particular y excepcional que se aplica al tratamiento de las categorías especiales de datos personales.

3.1. Prohibición general de tratamiento

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, se puede deber al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular –pero no solo– cuando los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual (considerando 75 RGPD). De ahí que el legislador europeo consagre un principio general en relación con las categorías especiales de datos: la prohibición de tratamiento.

En términos taxativos, "quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física" (art. 9.1 RGPD).

Como a continuación se listan, como excepciones, hasta diez circunstancias causales o situaciones jurídicas que permiten el tratamiento total o parcial de las categorías especiales de datos personales (art. 9.2 RGPD), se podría pensar que la garantía para los interesados es absoluta, cuando realmente no es así, siendo muchas y amplias las salvedades.

Precisamente sobre tales excepciones, el legislador nacional interviene conforme a las posibilidades que abre la norma comunitaria, bien sea por el llamamiento, en general, a enervar o concretar los supuestos de tratamiento excepcional [art. 9.2.a) y b) RGPD] o por el reenvío, solo respecto del tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, a los ordenamientos de los Estados miembros para mantener o introducir condiciones adicionales, inclusive limitaciones (art. 9.4 RGPD).

La prohibición, "a fin de evitar situaciones discriminatorias" (art. 9.1 LOPDyGDD), abarca a un conjunto de datos que revelan rasgos de la persona o de su determinación social, cuyo conocimiento puede provocar, en mayor o menor medida, prejuicios sociales, una posición de desventaja en muchos ámbitos, entre los que incluimos la relaciones de trabajo, e incluso resulta contraria a la dignidad de la persona (art. 10.1 CE). Lo que caracteriza a la prohibición de discriminación, frente al principio genérico de igualdad, "es la naturaleza particularmente odiosa del criterio de diferenciación utilizado, que convierte en elemento de segregación, cuando no de persecución, un rasgo o una condición personal innata o una opción elemental que expresa el ejercicio de las libertades más básicas, resultando así un comportamiento radicalmente contrario a la dignidad de la persona y a los derechos inviolables que le son inherentes"[84].

Eliminado, de raíz, el tratamiento de las categorías especiales de datos personales se imposibilitaría cualquier modo de actuar o decidir que resulte contrario a los principios y derechos fundamentales. El marco jurídico regulador del tratamiento de datos, empero, no es tan estricto por la extensión de las limitaciones que incorpora.

3.2. Excepciones: el tratamiento permitido

Se autorizan excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre

[84] STC 62/2008, de 26 de mayo.

que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, así como cuando sea en interés público (considerando 52 RGPD).

Desde el punto de vista del tratamiento de los datos personales, en el global de datos, los especialmente sensibles forman una categoría con identidad propia, diferenciando dentro de estos últimos dos subcategorías[85]:

– Una, el tratamiento de datos cuya finalidad principal es identificar su origen racial o étnico, ideología, afiliación sindical, religión, creencias u orientación sexual, respecto de los que "el solo consentimiento del afectado no bastará para levantar la prohibición" (art. 9.1 LOPDyGDD), pero que no impedirá su tratamiento al amparo de los restantes supuestos contemplados en el artículo 9.2 RGPD, cuando así proceda.

– Otra, el tratamiento de datos genéticos, datos biométricos y datos relativos a la salud, al que se aplican todos los supuestos excepcionales –incluido el consentimiento del interesado– del artículo 9.2 RGPD que levantan la prohibición general. Además, sobre estos datos y su tratamiento, los Estados miembros pueden mantener o introducir condiciones adicionales, incluso limitaciones (art. 9.4 RGPD).

La regla general que prohíbe el tratamiento de las categorías especiales de datos personales conoce, en total, diez excepciones, supuestos enumerados en el artículo 9.2 RGPD, aunque no todos tienen la misma relevancia laboral[86].

[85] De género y dos especies diferentes habla, respecto de las categorías especiales de datos, MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3ª ed., Francis Lefebvre, Madrid, 2019, p. 27.

[86] La doctrina coincide en destacar tres o cuatro de las circunstancias excepcionales que permiten el tratamiento de categorías especiales de datos. *Vid.* GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 10, y BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, pp. 117-119.

[87] Cfr. Preámbulo de la LOPDyGDD.

3.2.1. El consentimiento explícito del trabajador como interesado

En primer lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado" [art. 9.2.a) RGPD]. Y así, en efecto, la ley española establece un matiz importante puesto que, a fin de evitar situaciones discriminatorias, "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico", si bien respecto de esos concretos datos no se impide su tratamiento conforme a los restantes supuestos excepcionales (art. 9.1 LOPDyGDD).

Por ejemplo[87], siendo uno de los datos especialmente protegidos el de la afiliación sindical, la prestación del consentimiento por parte del trabajador afiliado no da cobertura a la creación de "listas negras" de sindicalistas, si bien eso no significa que pueda tratarse este dato –como se comprueba de seguido– por el empresario para hacer posible el ejercicio de los derechos de los trabajadores [art. 9.2.b) RGPD] o por los propios sindicatos [art. 9.2.d) RGPD].

Como pauta común, el consentimiento del interesado aporta la garantía de licitud sobre el tratamiento de sus datos personales [art. 6.1.a) RGPD]; en otros términos, para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho. El consentimiento debe darse mediante

un acto afirmativo y claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito[88], admitiéndose por medios electrónicos, o una declaración verbal[89] (considerando 32 RGPD), aunque esta alternativa puede acarrear problemas para probar la voluntad de la persona. En verdad, el consentimiento debe proceder de una declaración o de una clara acción afirmativa del afectado, lo que excluye –así se conocía– el "consentimiento tácito".

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines; caso de que el tratamiento tenga una pluralidad de finalidades, debe darse el consentimiento, de manera específica e inequívoca, para todos ellas. En el supuesto de que el consentimiento del interesado se haya solicitado por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Cobra aquí especial relevancia la obligación del responsable del tratamiento de proporcionar información sobre el fin y fines perseguidos con esa acción, al igual que sobre los derechos subjetivos de los que dispone, desde la posibilidad de negarse a prestar el consentimiento hasta su rectificación o retirada en cualquier momento (art. 7.3 RGPD).

En suma, el consentimiento explícito es una característica cualificada[90] del "consentimiento informado"[91]. Sucede, sin embargo, que en el terreno de las relaciones laborales no siempre el consentimiento se puede entender dado válida y libremente, por lo que "en la mayoría de los casos de tratamiento de datos de los trabajadores, la base jurídica de dicho tratamiento no puede y no debe ser el consentimiento de los trabajadores, por lo que se requiere una base jurídica diferente"[92]. Ello como consecuencia de la relación de subordinación entre el trabajador y el empleador, puesto que para garantizar que el consentimiento se ha dado libremente, "este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento" (considerado 43 RGPD).

El legislador nacional es coherente con la conclusión anterior y, en consecuencia, prohíbe que el consentimiento del trabajador sea bastante para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar –entre otras informaciones– la afiliación sindical del trabajador. El solo consentimiento del trabajador afiliado no podrá ser la base jurídica de dicho tratamiento.

3.2.2. 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 segundo lugar, la prohibición de tratamiento de cualquier categoría especial de dato

[88] Una manera evidente de garantizar que el consentimiento es explícito es confirmar de manera expresa dicho consentimiento en una declaración escrita; cuando proceda, el responsable podría asegurarse de que el interesado firma la declaración escrita, con el fin de eliminar cualquier posible duda o falta de prueba en el futuro (Directrices sobre el consentimiento en el sentido del Reglamento 2016/679/UE, adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, por el GT29).

[89] Contrasta esta posibilidad con el criterio más restricto de la –derogada– Ley 15/1999: "solo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias" (art. 7.2 Ley 15/1999).

[90] Así lo subraya MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, *cit.*, p. 48.

[91] TASCÓN LÓPEZ, R.: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, Civitas, Madrid, 2005, p. 103.

[92] Dictamen 02/2017, de 8 de junio, sobre el tratamiento de datos en el trabajo, adoptado por el GT29.

personal no se aplica 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" [art. 9.2.b) RGPD].

La deficiente traducción al castellano –falta la conjunción disyuntiva "o" entre "el Derecho de la Unión" y "de los Estados miembros o un convenio colectivo"– siembra la duda interpretativa, que se resuelve por el contexto y que, asimismo, despeja la norma en su introducción explicativa: "deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones (considerando 52 RGPD).

Interesa destacar el rol que asumen las disposiciones legales y el convenio colectivo en la regulación de los derechos y obligaciones concernientes a la relación laboral (art. 3 TRLET). A estas fuentes de regulación de la relación laboral se refiere el Reglamento comunitario como "títulos de legitimación"[93] del tratamiento de las categorías especiales de datos personales, emplazando al convenio colectivo a asumir esa función ordenadora. El Derecho nacional, a través de disposiciones legislativas o de convenios colectivos, puede 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 la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo (art. 88 RGPD). El reenvío al convenio colectivo, como regulación específica[94], se debe entender hecho al convenio colectivo estatutario[95], como norma jurídica[96] con eficacia *erga omnes*, de cualquier ámbito, "incluidos los «convenios de empresa»" (considerando 155 RGPD).

No se consiente, si más, el tratamiento de estas categorías especiales cuando deban cumplirse obligaciones o ejercer derechos reconocidos en el ordenamiento laboral y de seguridad y protección social, puesto que se requiere una "autorización" para ese tratamiento por parte de una norma jurídica, ya se encuentre esta en el seno del Derecho de la Unión Europea, en el Derecho interno o, como fuente propia del sector normativo referenciado, en un convenio colectivo, siendo dicha norma jurídica la que debe establecer las garantías suficientes

[93] Así lo subraya MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, *cit.*, p. 49.

[94] Advierten, con sumo acierto, GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 11, que esta llamada a la negociación colectiva parece oportuna y razonable, "por su proximidad al terreno y su origen en la autonomía de las partes interesadas", pero desde la perspectiva española de negociación colectiva "tal vez sea más un reto que una probabilidad inmediata, a la vista del contenido que habitualmente revisten los convenios en nuestra experiencia". *Vid.*, al respecto, SERRANO GARCÍA, J. M.: *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*, Bomarzo, Albacete, 2019, pp. 17-26, 34-36 y 85-88.

[95] Entre otros, MERCADER UGUINA, J. R.: "Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre: una aproximación desde la protección de datos", *Trabajo y Derecho*, núm. 52, 2019, pp. 112-113, y BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, p. 43.

[96] El convenio colectivo estatutario, una vez negociado "adquiere eficacia normativa, se incardina en el sistema de fuentes del Derecho y se impone a las relaciones de trabajo incluidas en su ámbito sin precisar el auxilio de técnicas de contractualización ni necesitar el complemento de voluntades individuales" (STC 177/1988, de 10 de octubre).

para preservar los derechos fundamentales e intereses del trabajador.

El Reglamento comunitario admite la licitud del tratamiento de datos cuando "es necesario para la ejecución de un contrato en el que el interesado es parte" [art. 6.1.b) RGPD] y cuando "es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento" [art. 6.1.c) RGPD]. Así, cuando sea necesario en el contexto de un contrato de trabajo, será lícito el tratamiento de los datos personales, de manera que en el ámbito laboral "el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes"[97]. Regla general que cede ante algunas categorías especiales de datos –cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico (art. 9.1 LOPDyGDD)– por no bastar el consentimiento del trabajador para anular la prohibición del tratamiento.

Por ende, más que "requerir situaciones específicas de prestación del consentimiento"[98], respecto del dato relativo a la afiliación sindical se impone una habilitación legal que marcará las garantías y condiciones adiciones para su tratamiento[99]. Así ocurre, como se ha descrito, con el descuento de la cuota sindical, pues el empresario únicamente puede proceder al descuento sobre los salarios y a la correspondiente transferencia, a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de este (art. 11.2 LOLS). Es, entonces, el cumplimiento de una obligación legal, el descuento de la cuota sindical, la base jurídica que ampara el tratamiento del dato referente a la afiliación sindical.

3.2.3. La necesidad de proteger intereses vitales del interesado o de otra persona física

En tercer lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento" [art. 9.2.c) RGPD]. Coincide con una de las condiciones para considerar lícito el tratamiento [art. 6.1.d) RGPD].

En efecto, el tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida o la integridad física del concernido o la de otra persona física, cuando no está en condiciones de dar su consentimiento. Ahora bien, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente (considerando 46 RGPD).

La incapacitación jurídica de la persona, mediante una declaración judicial fundada en enfermedades o deficiencias persistentes de carácter físico o psíquico que impidan a la persona gobernarse por sí misma (arts. 199 y 200

[97] STC 39/2016, de 3 de marzo.

[98] LÓPEZ ÁLVAREZ, L. F.: *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016, p. 114.

[99] El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento 2016/679/UE, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento 2016/679/UE (art. 8.1 LOPDyGDD). Se impone, por consiguiente, una reserva de ley; *vid.* MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, *cit.*, p. 44.

Código Civil), o el deterioro físico o psíquico de la persona, sin la previa incapacitación judicial, justifican el tratamiento de datos relativos a la salud para proteger intereses vitales del interesado. Pensemos en un paciente que, según el criterio del médico que le asiste, carece de capacidad para entender la información a causa de su estado físico o psíquico; en ese supuesto, "la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho" (art. 5.3 Ley 41/2002). Por ejemplo, la comunicación de la historia clínica[100] de una persona que padece una enfermedad degenerativa o se encuentra en estado de coma, que le impida dar el consentimiento para la realización de una prueba o intervención en situación de urgencia vital.

De igual modo, el tratamiento de datos relativos a la salud puede responder a los intereses vitales del interesado o a motivos de interés público como, por ejemplo, cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o provocadas por el hombre.

3.2.4. Fundaciones, asociaciones u organizaciones políticas, filosóficas, religiosas o sindicales, sin ánimo de lucro

En cuarto lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados" [art. 9.2.d) RGPD].

Se excepciona el tratamiento de categorías especiales de datos cuando se vincule a necesidades específicas de fundaciones, asociaciones u organizaciones políticas, filosóficas, religiosas o sindicales, sin ánimo de lucro, en concreto cuando el tratamiento se realiza en el marco de sus actividades, tomando en consideración que su objetivo es permitir el ejercicio de las libertades fundamentales (considerando 51 RGPD). Afecta, fundamentalmente, a datos sobre el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o, específicamente en el ámbito laboral, a la afiliación sindical.

La referencia, desde un punto de vista subjetivo, se reduce a las organizaciones ideológicas o de tendencia, en sentido estricto, que incluye a aquellas organizaciones que tienen como rasgo más específico el ser creadoras o sustentadoras de una determinada ideología o concepción del mundo –llamada "tendencia"– y en función de la misma existen[101], definición en la que se encuadran los partidos políticos, los sindicatos y las confesiones religiosas. Asimismo, se vincula, desde una perspectiva objetiva, al tratamiento –*ad intra*, exclusivamente– de datos personales de los miembros actuales o antiguos de tales organismos o de personas que mantengan contactos regulares con ellos en relación con sus fines; por ello, se exige el consentimiento de los interesados para comunicar o transferir esos datos fuera de la organización de tendencia.

[100] Dictamen 36/2018, de 28 de junio de 2018, de la Autoridad Catalana de Protección de Datos, en relación con una consulta sobre la autorización para el acceso de terceros a la historia clínica.

[101] Sobre este tema, *vid.* APARICIO TOVAR, J.: "Relación de trabajo y libertad de pensamiento en las empresas ideológicas", en VV.AA.: *Derecho del Trabajo en homenaje a los profesores BAYÓN CHACÓN y DEL PESO CALVO*, Universidad Complutense, Madrid, 1980, p. 293. También, DE VAL TENA, A. L.: "Las empresas de tendencia ante el Derecho del Trabajo: libertad ideológica y contrato de trabajo", *Revista Proyecto Social*, núm. 2, 1994, p. 178-180.

No se refiere tanto a los datos personales de los cargos representativos, profesionales y trabajadores de partidos políticos, sindicatos o confesiones religiosas, aunque también, como a los datos personales de su militantes, afiliados o miembros de organizaciones de tendencia, así como de terceras personas ajenas con las que se relacionan. Efectivamente, el dato de la afiliación sindical no se podrá facilitar –insistimos– ni siquiera al empleador para solicitar el descuento de la cuota sindical, salvo previo consentimiento para ello del trabajador afiliado (art. 11.2 LOLS)

3.2.5. Los datos personales públicamente manifestados por interesado

En quinto lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos" [art. 9.2.e) RGPD]. Que el dato sea "manifiestamente" público significa que expresa, indudable y visiblemente se quiere revelar, mostrar o dar a conocer ese dato, que con esa acción de su titular sale del ámbito privado o de los confines de su privacidad.

No se encuentra esta circunstancia entre las condiciones de licitud del tratamiento de datos personales (art. 6 RGPD), por lo que no cabe concluir que es una condición intrínseca aplicable a todos los datos personales, sean categorías especiales de datos o no. Reparando en ello, la conclusión debe ser que también, respecto de los datos hechos públicos de manera voluntaria por el interesado, se requiere cumplir una de las condiciones legales, al menos, para que el tratamiento sea lícito[102], por ejemplo, cumplir una obligación legal o que el afectado de su consentimiento expreso, si bien –no hay que olvidarlo– ese consentimiento no es válido para eliminar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico (art. 9.1 LOPDyGDD).

Se puede disponer de la información, es decir, conocer el dato, pero no se permite su tratamiento por el simple hecho de que el interesado lo haya hecho manifiestamente público o expuesto de manera pública. Si, además concurre una causa o condición de licitud *ex* artículo 6.1 RGPD, se admitirá su tratamiento. Sería el caso de exigir al empresario, que pretende despedir disciplinariamente a un trabajador afiliado a un sindicato, el cumplimiento de la obligación legal de dar audiencia previa a los delegados sindicales de la sección sindical correspondiente a dicho sindicato, si bien habrá que probar que le consta esa información (art. 55.1, párrafo cuarto, TRLET). No hay la menor duda, al empresario le consta ese dato si el trabajador afiliado ha consentido el descuento de la cuota sindical, como se ha explicado *ut supra*.

3.2.6. La formulación, el ejercicio o la defensa de reclamaciones o la actuación de los tribunales en el ejercicio de su función jurisdiccional

En sexto lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial" [art. 9.2.f) RGPD]. A título excepcional, igualmente, se autoriza el tratamiento de las categorías especiales de datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial (considerando 52 RGPD).

Al respecto, son de aplicación los preceptos sobre "protección de datos de carácter personal en el ámbito de la Administración de Jus-

[102] Cfr. Dictamen 757/2017, de 26 de octubre de 2017, del Consejo de Estado, sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

ticia", que se incorporaron a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ), por la Ley Orgánica 7/2015, de 21 de julio, con el objetivo de intensificar la protección de datos en el ámbito de los Tribunales, que carecía hasta entonces de una regulación completa y actualizada. En principio, no será necesario el consentimiento del interesado para que los Tribunales procedan al tratamiento de los datos en el ejercicio de la potestad jurisdiccional, ya sean estos facilitados por las partes o recabados a solicitud del propio Tribunal, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba[103] (art. 236 quáter LOPJ).

Es de interés esta excepción en las relaciones laborales, por su traslación a los procedimientos de solución judicial o extrajudicial de conflictos, tanto individuales o como colectivos; en particular, también, a los procedimientos de conciliación, mediación o arbitraje[104].

3.2.7. Por motivo de un interés público esencial

En séptimo lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2.g) RGPD]. La excepción viene a delimitar, cuando se tratan categorías especiales de datos, la condición de licitud justificada en "el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" [art. 6.1.e) RGPD].

En todo caso, el tratamiento de las categorías especiales de datos personales por este motivo excepcional –al igual que para los dos siguientes– deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad (art. 9.2 LOPDyGDD). Se consagra, por tanto, el principio de reserva de ley, previsión que no alcanza solo a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto del tratamiento de datos relacionados con la salud y de datos genéticos[105].

Así pues, se pueden igualmente imponer "condiciones especiales"[106] al tratamiento de las categorías especiales de datos –considerados sensibles– sobre esta base jurídica, tales como la adopción de medidas suplementarias de seguridad u otras, cuando ello derive del ejercicio de potestades públicas, que solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable si deriva de una competencia atribuida por la ley. Se pretende, en fin, reforzar la licitud del tratamiento, fijando de manera más precisa requisitos específicos[107] de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo.

---

[103] *Vid.* Castro Argüelles, M. A.: "Los derechos fundamentales inespecíficos en el proceso laboral", en VV.AA.: *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Ed. Cinca, Madrid, 2014, pp. 15-17.

[104] Así –*v. gr.*– el procedimiento arbitral obligatorio *ex lege* en materia de elecciones sindicales (art. 76 TRLET).

[105] Cfr. Disposición adicional decimoséptima RGPD.

[106] Cfr. Preámbulo de la LOPDyGDD.

[107] Se habilita formalmente al Derecho de los Estados miembros para introducir disposiciones específicas, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo (art. 6.3 RGPD).

El responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado (considerando 45 RGPD).

Sobre el uso de la videovigilancia con fines de interés público, por ejemplo, "las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones" (art. 22.1 LOPDyGDD).

En el ámbito laboral[108], se permite a los empleadores el tratamiento de las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 TRLET, "siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo" (art. 89.1 LOPDyGDD). Al respecto, se impone a los empleadores la obligación legal de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida. De haberse captado la comisión flagrante de un acto ilícito por los trabajadores, se considera cumplido el deber de informar cuando se haya colocado "un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 RGPD" o se incluya en ese dispositivo informativo "un código de conexión o dirección de internet a esta información" (art. 89.2, párrafo segundo, LOPDyGDD, en relación con el art. 22.4 LOPDyGDD).

En ningún caso se admite la instalación de sistemas de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos (art. 89.12 LOPDyGDD).

3.2.8. Fines médicos y sanitarios

En octavo lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario" [art. 9.2.h) RGPD].

Esta excepción únicamente es oponible si el tratamiento de cualquier categoría de dato personal, fundamentalmente –por su contenido– los datos relativos a la salud, es realizado "por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes" (art. 9.3 RGPD). Todos los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase

[108] *Vid.* GOÑI SEIN, J. L.: *La videovigilancia empresarial y la protección de datos personales*, Civitas, Cizur Menor (Navarra), 2007, *passim*. Recientemente, RODRÍGUEZ ESCANCIANO, S.: "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley*, núm. 9328, 2019, pp. 1-9; BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit*., pp. 191-214; y GARCÍA SALAS, A. I.: "Videovigilancia y control empresarial del trabajador: su regulación en la nueva Ley Orgánica de Protección de Datos", en DE LA PUEBLA PINILLA, A. y MERCADER UGUINA, J. R. (Dirs.): *Tiempo de reformas: en busca de la competitividad empresarial y de la cohesión social*, tirant lo blanch, Valencia, 2019, pp. 537-560.

de este, están sujetas al deber de confidencialidad; obligación que resulta complementaria del deber de secreto profesional exigible en determinadas actividades profesionales.

Ese deber de secreto sobre la información médica del trabajador incumbe al personal y a las autoridades sanitarias que conocen los resultados –datos personales relativos a la salud– de la vigilancia de la salud (art. 22.4, párrafo segundo, LPRL); secreto que se proyecta frente al resto de personas relacionadas, directa o indirectamente, con dicha obligación preventiva y también respecto de terceros[109]. Deber de secreto, en fin, que se extiende sobre los resultados y sobre todo aquello que el trabajador haya confiado[110] al personal responsable o que este haya conocido con ocasión del desarrollo de sus funciones[111].

3.2.9. Razones de interés público en el ámbito de la salud pública

En noveno lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional" [art. 9.2.i) RGPD].

El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública, pero siempre sujeto a medidas adecuadas y específicas con el fin de proteger los derechos y libertades de las personas físicas (considerando 54 RGPD). En ese contexto, "salud pública" debe interpretarse según la definición del Reglamento núm. 1338/2008/CE, de 16 de diciembre, del Parlamento Europeo y del Consejo, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo: "todos los elementos relacionados con la salud, a saber, el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad" [art. 3.c) Reglamento núm. 1338/2008/CE].

Recalcamos que este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como los empresarios, traten los datos personales con otros fines.

A nivel estatal, la Ley 33/2011, de 4 de octubre, general de salud pública, establece que "las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población", quedando obligadas las personas públicas o privadas a ceder a la autoridad sanitaria, cuando así se las requiera, "los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la LO 15/1999, de 13 de diciembre, de protección de

[109] *Vid.* PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *cit.*, p. 171.

[110] Como señala SÁNCHEZ TORRES, E.: "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales", *Relaciones Laborales*, T. II, 1997, p. 113, la comunicación de ciertos hábitos –consumo de drogas– o comportamientos –actividad sexual– personales.

[111] Sobre el secreto médico, extensamente, FERNÁNDEZ-COSTALES MUÑIZ, J.: "El secreto médico profesional y el deber de sigilo de los delegados de prevención en el ámbito del tratamiento y protección de datos de la salud", *Revista Técnico Laboral*, núm. 133, 2012, pp. 360-373.

datos de carácter personal –entiéndase la referencia hecha a la LO 3/2018–" (art. 41.2 y 3 Ley 33/2011).

En consecuencia, el legislador no ha previsto que todo tipo de dato personal relacionado con la salud pueda ser –libremente y sin restricciones– cedido o transmitido entre administraciones públicas, sino exclusivamente por razones imprescindibles, de modo que no será necesario el consentimiento de las personas afectadas para la cesión de datos personales relacionados con la salud por razones de salud pública o por razones epidemiológicas[112].

3.2.10. Otros fines: archivo en interés público, investigación científica o histórica y estadísticos

Finalmente y en décimo lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2.j) RGPD].

Dos precisiones iniciales. Una, primera, el tratamiento de datos personales con fines de investigación científica debe interpretarse de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado; entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública (considerando 159 RGPD) o, en general, en la investigación en salud (disp. adic. decimoséptima LOPDyGDD).

Otra, segunda, por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos; por cierto, los resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica (considerando 162 RGPD). El resultado del tratamiento con fines estadísticos no puede alumbrar datos personales, sino datos agregados, sin que el resultado o los datos personales se puedan utilizar para respaldar medidas o decisiones relativas a personas físicas concretas.

El tratamiento de datos personales con tales fines está supeditado a unas garantías adecuadas para los derechos y libertades del interesado, aplicando medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos, atendiendo a los principios de proporcionalidad y necesidad (considerando 156 RGPD).

Se permite el tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siempre que el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas, como, por ejemplo, la "seudonimización" de datos.

Corresponde a los Estados miembros establecer esas garantías adecuadas, bajo condiciones y procedimientos específicos, para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, sin que, en caso de que el tratamiento sirva también, al mismo tiempo, a otro fin, sea aplicable la excepción (art. 89.3 y 4 RGPD).

[112] Cfr. Informe 0121/2018 del Gabinete Jurídico de la AEPD, sobre la legitimación para el tratamiento de datos en materia de salud pública.

Pueden ser relevantes, respecto de la actividad laboral, el tratamiento de algunas categorías especiales de datos personales, de manera singular los datos relativos a la salud, cuando se realicen estudios de investigación científica o puramente estadísticos sobre enfermedades profesionales o sobre las consecuencias para la salud o la integridad física de los accidentes de trabajo. Asimismo, otros estudios de investigación histórica o estadísticos sobre la afiliación sindical, dado el importante rol constitucional que desempeñan los sindicatos en un sistema democrático (arts. 7 y 28.1 CE).

3.3. Obligaciones en el tratamiento de categorías especiales de datos

En el articulado del Reglamento europeo se recogen algunas obligaciones que afectan exclusivamente a los responsables y encargados del tratamiento de cualquier dato personal que pertenezca a las categorías especiales de datos. Se exponen, a continuación, algunas.

Como pauta general, todo interesado tiene 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 de modo similar, excepto si la decisión (i) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, (ii) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o (iii) se basa en el consentimiento explícito del interesado. Pues bien, esas excepciones a aquella primera regla general "no se basarán en las categorías especiales de datos personales" contempladas en artículo 9.1 RGPD, salvo que se aplique el artículo 9.2, letras a) –consentimiento explícito del interesado– o g) –el tratamiento es necesario por razones de interés púbico esencial–, y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado (art. 22.4 RGPD).

Sobre el registro de actividades de tratamiento y las obligaciones que se establecen *ex lege*, no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, excepto si el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o "incluya categorías especiales de datos personales", o datos personales relativos a condenas e infracciones penales (art. 30.5 RGPD).

En cuanto a la obligación de realizar una evaluación[113] del impacto de las operaciones de tratamiento en la protección de datos personales por parte del responsable, dicha evaluación se exige cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas y –en particular– siempre que se lleve a cabo un "tratamiento a gran escala de las categorías especiales de datos" (art. 35.3 RGPD).

Por último, el responsable y el encargado del tratamiento han de designar un delegado de protección de datos siempre que las actividades principales de aquellos "consistan en el tratamiento a gran escala de categorías especiales de datos personales", o datos personales relativos a condenas e infracciones penales [art. 37.1.c) RGPD].

[113] En la evaluación se debe hacer referencia a las operaciones de tratamiento previstas, a la necesidad y proporcionalidad de dichas operaciones, a los riesgos para los derechos y libertades de los interesados y a las medidas previstas para hacer frente a dichos riesgos. *Vid.* PRECIADO DOMÈNECH, C. H.: *El derecho a la protección de datos en el contrato de trabajo*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017, pp. 150 y ss.

4. A MODO DE VALORACIÓN ÚLTIMA: SOBRE LAS GARANTÍAS MÁS INTENSAS EN EL TRATAMIENTO DE DATOS SENSIBLES DEL TRABAJADOR QUE SE RECONOCEN *EX LEGE* COMO CATEGORÍAS ESPECIALES DE DATOS

Hay una nítida línea de continuidad en el régimen jurídico que se viene aplicando a determinados datos personales del interesado, el trabajador que se convierte en titular del amplio conjunto de garantías delineado por la normativa –internacional, comunitaria y nacional– sobre protección de datos. Llámense –como antes– "categorías especiales de datos" (art. 8 Directiva 95/46/CE) por ser "datos especialmente protegidos" (art. 7 LO 15/1999), o –como ahora– "categorías especiales de datos", sin más precisiones (art. 9 RGPD y, también, LOPDyGDD), lo cierto es que han merecido especial protección aquellos datos personales que, por su naturaleza o su contenido, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que su tratamiento por el empleador u otro responsable puede suponer notables riesgos para esos derechos y las libertades fundamentales.

Ante todo, con su identificación se quiere impedir cualquier efecto discriminatorio sobre las personas físicas, desde la perspectiva de nuestro análisis en los trabajadores, por motivos de raza u origen étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, condición genética, estado de salud u orientación sexual. De ahí que el tratamiento de esos datos, las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deban permitirse en condiciones específicas o tratándose de categorías especiales de datos personales sencillamente no puedan ser autorizadas, salvo excepciones acotadas por el legislador.

Con ocasión de la revisión de la normativa sobre protección de datos personales, primero a nivel europeo y seguidamente a nivel estatal, las categorías especiales de datos personales han merecido un mayor grado de atención, con la finalidad de otorgarles una más y mejor protección cuando se permita su tratamiento, pues la base de su tutela es que tales datos personales no deben ser tratados, a menos que se permita su tratamiento en supuestos o ante circunstancias tasadas, sobre el consentimiento del titular o la concurrencia de otros derechos o intereses merecedores de ser atendidos o preservados. De máxima trascendencia en el tratamiento de las categorías especiales de datos es que, además de los requisitos específicos, deben aplicarse los principios generales relativos al tratamiento de los datos personales y otras reglas comunes, pero sobre todo las condiciones generales de licitud.

A la prohibición general de tratamiento de esas categorías especiales de datos, se enlazan, de forma explícita y muy delimitada, supuestos en los que excepcionalmente decae aquella limitación. Se puede calificar como prohibición relativa, al ser numerosas las hipótesis que habilitan el tratamiento, ciertamente encadenadas algunas a lo dispuesto en el Derecho de la Unión Europea o, principalmente, en el Derecho de los Estados miembros, y ello porque, según los datos a tratar o los supuestos, se reenvía a los ordenamientos nacionales para introducir condiciones adicionales, incluso limitaciones, pero siempre con la finalidad de establecer medidas adecuadas y específicas para proteger los intereses, derechos y libertades de la persona.

Precisamente el tratamiento en el ámbito laboral, permite a los legisladores estatales, bien en las disposiciones legislativas, bien en los 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 la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguri-

dad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral (art. 88.1 RGPD). Normas que incluirán medidas adecuadas y singulares para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos y libertades fundamentales, prestando especial atención a la transparencia del tratamiento.

En el ejercicio de esa competencia reguladora, se impone que el solo consentimiento del trabajador no sirve para remover la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico (art. 9.1 LOPDyGDD), si bien se permite el tratamiento de los referidos datos personales al amparo de los restantes supuestos, por ejemplo, cuando el interesado ha hecho manifiestamente públicos alguno de esos datos o, inclusive, cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea en un procedimiento judicial o en un procedimiento administrativo o extrajudicial.

Uno de los datos que se reconoce como categoría especial, la afiliación sindical, y, al menos, dos circunstancias, de un resultado de diez, se presentan con una clara vinculación: el tratamiento de la afiliación sindical se permite 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 y de la seguridad y protección social, en tanto así lo autorice el Derecho de la Unión, el Derecho de los Estados miembros o un convenio colectivo, siempre que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del trabajador; también cuando sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por la organización sindical, siempre que el tratamiento se refiera exclusivamente a sus miembros actuales o antiguos, quedando prohibía su comunicación externa sin el consentimiento del interesado.

Otros datos, los relativos a la salud y, al menos, cuatro circunstancias, del total de listadas, presentan una evidente conexión: el tratamiento de los datos sobre la salud –en sentido amplio– del trabajador cuando sea necesario para proteger sus intereses vitales, cuando sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, cuando se necesario por razones de interés público en el ámbito de la salud pública y cuando resulte necesario con fines de investigación científica.

Pero no solo esas categorías especiales de datos y esas circunstancias que permiten su tratamiento, de igual manera otros datos personales merecen la tutela intensificada del legislador respecto de su tratamiento a fin de evitar situaciones discriminatorias y las mismas u otras circunstancias excepcionales posibilitarán su tratamiento, también con una incidencia, no meramente tangencial, en las relaciones de trabajo, más en el contexto de la creciente utilización de las nuevas tecnologías en la empresa al servicio de los poderes de dirección y control atribuidos al empleador.

BIBLIOGRAFÍA

ALBERT, M.: "Convicciones religiosas y elecciones personales: derecho a la objeción de conciencia y autodeterminación individual en la jurisprudencia del Tribunal Europeo de Derechos Humanos", Revista Persona y Derecho, núm. 77, 2017.

ÁLVAREZ GONZÁLEZ, S.: "Derecho a la «privacidad» e información genética", en ÁLVAREZ GONZÁLEZ, S. y GARRIGA DOMÍNGUEZ, A. (Dirs.): Un nuevo reto para los derechos fundamentales: los datos genéticos, Dykinson, Madrid, 2017.

APARICIO TOVAR, J.: "Relación de trabajo y libertad de pensamiento en las empresas ideológicas", en VV.AA.: Derecho del Trabajo en homenaje a los profesores BAYÓN CHACÓN y DEL PESO CALVO, Universidad Complutense, Madrid, 1980.

BAZ RODRÍGUEZ, J.: Privacidad y protección de datos de los trabajadores en el entorno digital, Bosch Wolters Kluwer, Barcelona, 2019.

BLASCO PELLICER, A.: "El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador", en BORRAJO DACRUZ, E. (Dir.): Trabajo y libertades públicas, La Ley, Madrid, 1999.

CASTRO ARGÜELLES, M. A.: "Los derechos fundamentales inespecíficos en el proceso laboral", en VV.AA.: Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Ed. Cinca, Madrid, 2014.

CHACARTEGUI JÁVEGA, C.: Discriminación y orientación sexual del trabajador, Lex Nova, Valladolid, 2001.

CLAYTON, E. W., EVANS, BARBARA J., HAZEL, JAMES W. y ROTHSTEIN, MARK A.: "The law of genetic privacy: applications, implications, and limitations", Journal of Law and the Biosciences, vol. 6, núm. 1, 2019 (https://academic.oup.com/jlb/article/6/1/1/5489401).

CRUZ VILLALÓN, J.: Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador, Bomarzo, Albacete, 2019.

DE VAL TENA, A. L.: "Las empresas de tendencia ante el Derecho del Trabajo: libertad ideológica y contrato de trabajo", Revista Proyecto Social, núm. 2, 1994.

DEL REY GUANTER, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la «intimidad informática» de trabajador)", Relaciones Laborales, T. II, 1993.

FERNÁNDEZ-COSTALES MUÑIZ, J.: "El secreto médico profesional y el deber de sigilo de los delegados de prevención en el ámbito del tratamiento y protección de datos de la salud", Revista Técnico Laboral, núm. 133, 2012.

GARCÍA MURCIA, J.: "Derecho a la intimidad y contrato de trabajo: la anotación de las bajas médicas (Comentario a la STC 202/1999, de 8 de noviembre)", Repertorio Aranzadi del Tribunal Constitucional, núm. 2, 2000.

GARCÍA MURCIA, J.: "El hecho sindical. La mayor representatividad. Asociacionismo profesional y empresarial. Balance y propuestas de reforma", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. 429, 2018.

GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", Nueva Revista Española de Derecho del Trabajo, núm. 216, 2019 (BIB 2019\1432).

GARCÍA SALAS, A. I.: "Videovigilancia y control empresarial del trabajador: su regulación en la nueva Ley Orgánica de Protección de Datos", en DE LA PUEBLA PINILLA, A. y MERCADER UGUINA, J. R. (Dirs.): Tiempo de reformas: en busca de la competitividad empresarial y de la cohesión social, tirant lo blanch, Valencia, 2019.

GÓMEZ SÁNCHEZ, Y.: "La protección de los datos genéticos: el derecho a la autodeterminación informativa", Derecho y Salud, vol. 16, núm. extraordinario 1, 2008.

GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y de archivo de datos", en ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA R. (Coords.): Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo, Bomarzo, Albacete, 2004.

GOÑI SEIN, J. L.: La videovigilancia empresarial y la protección de datos personales, Civitas, Cizur Menor (Navarra), 2007.

GOÑI SEIN, J. L.: "Intimidad del trabajador y poderes de vigilancia y control empresarial", en GARCÍA MURCIA, J. (Coord.): Jornada sobre derechos fundamentales y contrato de trabajo, Principado de Asturias, Oviedo, 2017.

GOÑI SEIN, J. L.: La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018), Bomarzo, Albacete, 2018.

LACADENA, J. R.: "Individualización y mismidad genética en el desarrollo humano", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): Gen-Ética, Ariel, Barcelona, 2003.

LEWIS R.: Human Genetics: Concepts and Applications, 12ª ed., McGraw-Hill Science, NewYork (EE.UU.), 2017.

LÓPEZ ÁLVAREZ, L. F.: Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo, Francis Lefebvre, Madrid, 2016.

LUCAS MURILLO DE LA CUEVA, P.: Informática y protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1993.

MERCADER UGUINA, J. R. y DE LA PUEBLA PINILLA, A.: "Protección de datos y relaciones colectivas", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. 423, 2018.

MERCADER UGUINA, J. R.: "El mercado de trabajo y el empleo en un mundo digital", Información Laboral, núm. 11, 2018 (BIB 2018/ 13994).

MERCADER UGUINA, J. R.: "La protección de datos personales del trabajador. La obligación del empresario de informar al trabajador sobre sus condiciones de trabajo", en CASAS BAAMONDE, M. E. y GIL ALBURQUERQUE, R. (Dirs.): Derecho Social de la Unión Europea. Aplicación por el Tribunal de Justicia, Francis Lefebvre, Madrid, 2018.

MERCADER UGUINA, J. R.: Protección de datos y garantía de los derechos digitales en las relaciones laborales, 3ª ed., Francis Lefebvre, Madrid, 2019.

MERCADER UGUINA, J. R.: "Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre: una aproximación desde la protección de datos", Trabajo y Derecho, núm. 52, 2019.

MIÑARRO YANINI, M.: "Implicaciones laborales del Reglamento comunitario de protección de datos: principales puntos críticos", en GARCÍA MAHAMUT, R. y TOMÁS MALLÉN, B. (Edits.): El Reglamento General de Protección de Datos, tirant lo blanch, Valencia, 2019.

MOLINA NAVARRETE, C.: "La «gran transformación» digital y bienestar en el trabajo: riesgos emergentes, nuevos principios de acción, nuevas medidas preventivas", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. extraordinario 1, 2019.

PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", Revista del Ministerio de Trabajo, Migraciones y Seguridad Social, núm. 138, 2018.

POQUET CATALÁ, R.: El actual poder de dirección y control del empresario, Cuadernos de Aranzadi Social, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2013.

PRECIADO DOMÈNECH, C. H.: El derecho a la protección de datos en el contrato de trabajo, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017.

RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. 423, 2018.

RODRÍGUEZ ESCANCIANO, S.: "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales", Diario La Ley, núm. 9328, 2019.

RODRÍGUEZ ESCANCIANO, S.: Derechos laborales digitales: garantías e interrogantes, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019.

ROMEO CASABONA, C. M.: Los genes y sus leyes. El derecho ante el genoma humano, Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, Comares, Granada, 2002.

ROMEO CASABONA, C. M.: "El tratamiento y la protección de los datos genéticos", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): Gen-Ética, Ariel, Barcelona, 2003.

SÁNCHEZ TORRES, E.: "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales", Relaciones Laborales, T. II, 1997.

SERRANO GARCÍA, J. M.: La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia, Bomarzo, Albacete, 2019.

TASCÓN LÓPEZ, R.: El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión, Civitas, Madrid, 2005.

TRONCOSO REIGADA, A.: "La protección de datos personales en el ámbito laboral", en VV.AA.: La protección de datos personales en busca del equilibrio, tirant lo blanch, Valencia, 2010.

VALDÉS DAL-RE, F.: "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", Revista de Derecho Social, núm. 79, 2017.

VALDÉS DAL-RE, F.: "Nuevas tecnologías y derechos fundamentales de los trabajadores", Derecho de las Relaciones Laborales, núm. 2, 2019.

RESUMEN

La rápida evolución tecnológica ha planteado nuevos retos para la protección de los datos personales. Sin duda, la tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades, y ha de facilitar aún más la libre circulación de datos personales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

A nivel europeo, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. La Carta de los Derechos Fundamentales de la Unión Europea (art. 8.1) y el Tratado de Funcionamiento de la Unión Europea (art. 16.1) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

No obstante, el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión Europea y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, ha sido necesario un Reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento. Por ello, se ha aprobado el Reglamento 2016/679/UE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Dicho Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. Se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Al respecto, se considera "datos personales" toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; y "tratamiento", cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Entre los datos personales, especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. En verdad, la norma europea regula el tratamiento de las categorías especiales de datos ("datos sensibles"). Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca

a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas. Pero, además de los requisitos singulares de ese tratamiento, deben aplicarse los principios generales y otras normas del Reglamento europeo, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento.

Las excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales son:

a) El interesado ha dado su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada no puede ser levantada por el interesado. Precisamente, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, establece que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas, la afiliación sindical o la orientación sexual.

b) 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.

c) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

d) El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

e) El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

f) El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g) El tratamiento es necesario por razones de un interés público esencial.

h) El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.

i) El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.

j) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Se estudia, por un lado, el concepto de cada una de las categorías especiales de datos personales y, por otro, las excepciones a la prohibición general de tratar.

Palabras clave: Datos personales; categorías especiales de datos; origen étnico o racial; opiniones políticas; convicciones religiosas o filosóficas; afiliación sindical; datos genéticos; datos biométricos; datos relativos a la salud; orientación sexual; tratamiento de categorías especiales de datos.

ABSTRACT Rapid technological developments have brought new challenges for the protection of personal data. No doubt, technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities, and should further facilitate the free flow of personal data, while ensuring a high level of the protection of personal data.

At the European Union level, the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provides that everyone has the right to the protection of personal data concerning him or her.

Nevertheless, the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality

In order to ensure a consistent level of protection for natural persons throughout the European Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors. For this reason, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, has been adopted, which repeals Directive 95/46/EC.

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing of other not by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

In this regard, “personal data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Indeed, the European standard regulates the processing of special categories of personal data (“sensitive data”). Those personal data should include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

Such personal data should not be processed, unless processing is allowed in specific cases. But, in addition to the specific requirements for such processing, the general principles

and other rules of this Regulation should apply, in particular as regards to the conditions for lawful processing. The derogations from the general prohibition for processing such special categories of personal data are:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the European Union or Member State law provides that the prohibition referred may not be lifted by the data subject. Precisely, Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights, establishes that the only consent of the affected party will not be enough to lift the prohibition on the processing of data whose disclosure racial or ethnic origin, political opinions, religious beliefs, trade union membership, or sexual orientation.

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by the European Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

(e) Processing relates to personal data which are manifestly made public by the data subject.

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) Processing is necessary for reasons of substantial public interest.

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

(i) Processing is necessary for reasons of public interest in the area of public health.

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

On one hand, this paper analyses the concept of each of the special categories of personal data and, on the other hand, the derogations from the general prohibition on processing special categories of personal data.

Keywords: Personal data; special categories of personal data; racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; sexual orientation; processing of special categories of personal data.

Protección de datos personales y procesos de selección de trabajadores

Protection of personal data and worker selection processes

OLGA GARCÍA COCA*

1. MEDIOS DE DIFUSIÓN DE OFERTAS DE EMPLEO

Podría decirse que la difusión de una oferta de empleo es el primer paso para reclutar a un trabajador e insertarlo en el mercado de trabajo. Por ello, es importante seguir unas instrucciones para captar, de esta forma, el mejor talento atrayendo a los mejores candidatos que se ajusten al perfil requerido. Es fundamental que la propuesta de la oferta de empleo sea, por un lado, interesante y, por otro, que reúna determinadas claves para que los demandantes de empleo puedan encontrar la vacante cuando realizan sus búsquedas.

Por tanto, ¿cómo se pueden conseguir estos efectos? En primer lugar, es necesario que el título de la oferta sea claro y breve, además de resumir en pocas palabras, pero que sean claves para identificarlo, el puesto de trabajo, debe constar la responsabilidad del cargo definiendo las funciones y el área en dónde desempeñará la tarea. Si, por ejemplo, se busca un perfil concreto se puede incluir en la oferta una leyenda que establezca la no inclusión en el proceso de aquellos candidatos que no cumplan ese requisito que se considera fundamental para cubrir la oferta de empleo[1].En segundo lugar, es primordial hacer referencia a los requisitos realmente precisos para realizar con éxito las funciones, interesante diferenciar entre los imprescindibles y los valorables. Una de las partes más importantes a la hora de confeccionar una oferta de empleo es la definición de las condiciones laborales por constituir el mayor incentivo de la oferta para el candidato, lo que hace que se anime a participar en el proceso de selección. Resulta útil por ello describir el tipo de jornada laboral, el tipo de contrato, la ubicación, y en la medida de lo posible, las condiciones económicas.

En tercer lugar, la identificación de la empresa que ofrece el empleo genera mayor seguridad para los que se inscriben en la misma, pues pueden decidir participar indagando previamente la infraestructura y demás datos de la empresa. Cuando se incluyen términos como "importante empresa" o "prestigiosa compañía" genera más desconfianza y desinterés que si se indica el nombre de la empresa y a que se dedican. Por eso si se cuenta con una página web donde encontrar información sobre la trayectoria, valores y actividad

* Profesora Ayudante Doctor. Universidad Pablo de Olavide.

[1] Cuando se están recogiendo datos a través de plataformas digitales es muy útil incluir las denominadas preguntas de filtrado o las *killer question*. Se trata de preguntas que se hace al candidato durante su proceso de inscripción en la oferta. Por ejemplo, si se está interesado en contratar a personas con determinado certificado de discapacidad puede preguntarse de forma que todos aquellos candidatos que respondan "No" a la pregunta: *¿Tienes certificado de discapacidad?* queden automáticamente descartados. Garantizan una selección de candidatos más efectiva.

empresarial, mejor. Por último, existen otros factores que propician que una empresa sea más atractiva que otra tales como los valores, la seguridad laboral, el ambiente de trabajo, las perspectivas de futuro y la posibilidad de conciliar la vida laboral con la personal se han convertido en los factores clave a la hora de elegir una empresa u otra para trabajar. En este sentido, contar con una estrategia de *employer branding*[2] adecuada se convierte en una necesidad.

A la hora de incorporar ofertas de empleo en los distintos medios de difusión, ocupa un lugar esencial aplicar las ya conocidas técnicas de *employer branding*, siendo la descripción de la propuesta transparente y real, con una base sólida dando prioridad al talento y creando una oferta atractiva, en otras palabras, remarcando las características del candidato ideal para cubrir las necesidades de empleo que demandan. De hecho, los propios trabajadores de la empresa, en estos casos, son los que pueden llegar a explicar los beneficios que se ofrecen, cómo es la cultura de tu empresa y el ambiente que se respira día tras día. Estas explicaciones, incluso, las pueden dar a través de las redes sociales que se pueden constituir como el canal perfecto para comunicar los valores de la empresa que demanda trabajadores, presentando los mismas a los potenciales candidatos a esas ofertas de empleo.

Una vez redactada la oferta de empleo llega el momento de darle la mayor difusión posible para que llegue al mayor número de candidatos. En este sentido, los mecanismos tradicionales (prensa, anuncios en la empresa, empresas de trabajo temporal, consultoras etc.) se han visto relegados por otros medios tecnológicos, que, obviamente, provocan un mayor alcance y proliferación. Tal es el caso, de los anuncios de empleo publicados en los buscadores webs y en los portales de empleo que proporcionan inmediatez a los candidatos al poder buscar realizando un filtrado objetivo de las ofertas que mejor se adaptan a su perfil formativo y profesional. Por otra parte, las redes sociales son una fuente esencial para la difusión de las ofertas de empleo, pues se presentan como una plataforma con una gran visualización como consecuencia del elevado uso que hacen de ello los ciudadanos y, también, los demandantes de empleo.

En este sentido existen unas pautas a la hora de publicar ofertas de empleo en redes sociales para que estas sean atractivas y lleguen al máximo número de demandantes de empleo. Como es sabido, hay redes sociales que están enfocadas a tratar perfiles profesionales y a fomentar el empleo entre sus usuarios (Linkedin, Xing, etc) pero no son las únicas que pueden llevar a cabo este cometido, aunque sí las mas usuales, pues la publicación de ofertas de empleo es una práctica que se realiza, también, desde el propio Facebook[3]. Es por ello de suma importancia configurar la difusión de la oferta, como se ha comentado, de forma llamativa y cercana.

En las redes sociales, las ofertas de empleo están compitiendo por la atención del usuario con miles de contenidos diferentes, por ello captar la atención de este usuario es esencial. Pero no solo esto: hay que dejar a la vista toda la información para que la oferta resulte atractiva y el candidato decida inscribirse, esté en la red social que esté.

[2] El *Employer Branding* no es otra cosa que la marca de una empresa como empleador. En otras palabras, la imagen que tiene una compañía no sólo hacia sus clientes sino también hacia sus propios empleados y sobre todo, la imagen que perciben sus posibles candidatos.

[3] Esta opción se activa cuando tienes una página de empresa en el propio Facebook pues, de esta manera, si puedes explorar la novedad de publicar una oferta de empleo. Para ello, se habilita un formulario en el que podrás incluir información sobre la oferta rellenando campos como el de "Introducción", en el que puedes escribir una frase que resuma la vacante en 90 caracteres. A medida que avances podrás incluir una foto (mejor sin texto y siempre relacionada con la profesión de la que hablamos), la ubicación de la posición, el salario (opcional) o el tipo de trabajo (a tiempo completo, a tiempo parcial, prácticas, voluntariado o contrato).

Si se pretende publicar una oferta a través de twitter la idea es "decir mucho en pocas palabras" pues la configuración de los denominados tweets no admite textos con muchos caracteres. En este caso, es preciso tener una cuenta de twitter en el que aparezca el logo y la denominación de la empresa que ofrece el empleo para que sea claramente reconocible, en este perfil hay que insertar un mensaje breve y claro en el que se identifiquen los requisitos de la oferta (palabras claves y hashtag[4]) y se inste a los demandantes a inscribirse en la misma a través de una llamada de acción. Los hashtags deben ser claros y no ser abusivos, es decir, no es necesario incluir más de uno, de hecho, hay algunos que están catalogados como los más populares para captar candidatos a raíz de una oferta de empleo, por lo que es una etiqueta identificativa en los anuncios de empleo de las redes sociales que cumple con esa función de difusión. Si por el contrario la publicidad de la oferta se hace por medio de una de las llamadas redes sociales profesionales, como pudiera ser el caso de Linkedin, hay observar más aspectos formales por ser la red profesional por excelencia plataforma. Además de identificar la oferta con palabras clave e incluir una llamada de acción se ofrece la posibilidad de acceder directamente en la oferta al insertar en el texto el enlace a la misma y de recomendar o incluso compartir en otros grupos creados en la propia red Linkedin.

Así pues, estos mecanismos de publicidad son utilizados por las propias empresas y por todas aquellas que realizan labores de intermediación públicas y privadas. Muchos de estos procedimientos, además de ofrecer servicios de registro de datos, se configuran como verdaderas oficinas virtuales de empleo que ofrecen una amplia cartera de servicios para colaborar en la colocación de aquellas personas que estén a la búsqueda de un empleo.

2. EL CURRICULUM VITAE

Una vez que la oferta es publicada de una u otra forma las empresas necesitan filtrar a los candidatos según los CV presentados en los distintos medios de captación de candidatos (portales de empleo, redes sociales, email directo a la empresa que anuncia el empleo, etc.) A simple vista el curriculum no necesita de una profunda presentación concluyendo que simplemente es una relación ordenada de los datos académicos, de formación y profesionales de una persona que busca empleo. El currículum se redacta con el objeto de responder a una oferta de trabajo, pero también puede ser espontáneo, es decir se redacta sin la existencia de oferta y se reparte en distintas empresas para solicitar trabajo.

Es parecido a un buen anuncio o invitación que envía o entrega una persona aspirante a un empleo, el cual incluye toda la información sobre su vida laboral, los datos de contacto e indica el lugar donde reside. El objetivo de un currículum vitae es generar una buena impresión e interés para darse a conocer y así conseguir una entrevista personal, para conseguir ese puesto de trabajo tan deseado. A la hora de redactar un CV se deben tener en cuenta varios factores, pues ya en este momento es cuando se transmite información personal a la empresa que demanda empleo o a aquella otra empresa intermediadora que realiza la selección de personal. Es por ello que se hace necesario conocer la importancia de dar los datos precisos, siendo esa información de fácil lectura y comprensión dejando, de forma clara en el propio CV, los datos de contacto para que puedan notificar su inclusión en el proceso de selección[5].

[4] Etiqueta formada por una o más palabras clave (puedes añadir números pero no símbolos), escritas todas juntas sin espacios, y que van precedidas del símbolo # (llamado almohadilla). Una vez compartas tu contenido, con los hashtags que hayas decidido, éstos se convertirán en un enlace que, si alguien lo pulsa, dirigirá a todos los contenidos que se han compartido con esas mismas palabras clave. De esta forma, los contenidos sobre un mismo tema se agruparán para facilitar la búsqueda de información y facilitará la conversación en torno a éste.

[5] RUBIO, A. *Ganarse el puesto y superar con éxito el período de prueba*, DÍAZ DE SANTOS, 2008, pp. 24-28.

Los datos que deben aparecer, por tanto, en el CV son: nombres y apellidos; N.I.F.; fecha y lugar de nacimiento; estado civil; ubicación de tu domicilio; números de contacto, mínimo dos; dirección del correo electrónico personal a la que accedes frecuentemente; estudios realizados indicando la fecha de comienzo y fin, centro académico, y lugar donde han sido realizados; postgrados, cursos o talleres realizados igualmente indicando la fecha de comienzo y fin, centro, y lugar donde han sido realizados; experiencias profesionales indicando la fecha de comienzo y fin, nombre de la empresa y funciones desempeñadas; idiomas que dominas y en el nivel correspondiente.

Es importante conocer que en la actualidad no sólo llega a los seleccionadores de personal la información mostrada en el CV, sino que como consecuencia de la digitalización y de la proliferación de internet se puede conocer mucha información e incluso tratar, es lo que se conoce como CV social[6]. Es en ese momento cuando entra el juego el debate de ser visible o no en internet, ya que lo que es evidente es que las empresas pueden entrar en ese círculo social pues están en su derecho de conocer como los candidatos se muestran en la sociedad digital.

Se hace por ello importante establecer las pautas e instrucciones dadas en la normativa actual sobre protección de datos de carácter, como se tratará más adelante, para que los candidatos no tengan la sensación de tener su vida privada abierta en internet. Hay que restringir el uso de toda información que no sea necesaria ni adecuada para calificar la aptitud del candidato en el proceso de selección, sobre todo para no contaminar y realizar una clasificación de los demandantes lo más objetiva posible.

Hoy día alcanza gran importancia la configuración de los CV infográficos que ayudan a que la información contenida en el CV sea más atractiva y más fácil de leer para el seleccionador. Pero estos CV, a pesar de suponer una innovación en los recursos humanos pueden generar cierta desconfianza porque a lo mejor pueden enmascarar cierta información para realizar el proceso de selección e incluso perjudicar a un candidato que cumpla los requisitos para el puesto pero que no sepa transmitirlo desde un punto de vista creativo. Para ello, es preciso tener en cuenta que la creación y la difusión de un CV infográfico no impida realzar y enfocar tu perfil profesional, además de asegurarse que el puesto de empleo que se oferta no sea creativo ni innovador, por lo que toda la configuración del CV debe ir en consonancia con la oferta de empleo en la que se quiere participar como candidato[7].

Otra de las formas para lograr una primera toma de contacto con la empresa que ofrece empleo y que está vinculada a las necesidades del nuevo contexto laboral, es el videocurrículum, y, sobre todo, el videocurrículum de marca personal, pues aporta un valor añadido incuestionable y logra la diferenciación del resto de los competidores. El proceso es sencillo y está relacionado con la realización de vídeos en los que el demandante de empleo expone su currículum académico y profesional para optar a un puesto de trabajo, por lo que constituye una herramienta que puede facilitar la inserción laboral, ya que permite personalizar y singularizar al demandante de empleo frente al empleador. Esta nueva herramienta, además, posibilita que el demandante de empleo pueda mostrar otros factores cualitativos de su persona que, junto a sus datos curriculares,

[6] Es el CV formado por toda la huella digital en Internet, donde se puede conocer más a fondo al candidato. Cuando alguien escribe un Tweet está provocando que puedan tener más información de él como por ejemplo pueden ser sus valores, opiniones, intereses, motivaciones, red de contactos, empresas de interés... y *"es aquí donde estamos teniendo información actualizada del candidato y no sólo del pasado a través de su currículum"*. Fuente: https://br.escueladenegociosydireccion.com/business/rr-hh/redes-sociales-imprescindibles-en-el-reclutamiento/

[7] Dunia Talleda, Marc Tudó, Bernat Rodrigo, Alba Nebot: "La evolución del curriculum vitae", *Capital humano: revista para la integración y desarrollo de los recursos humanos*, Año nº 30, Nº Extra 323, 2017, pp. 54-56.

puedan suponer una ventaja a la hora de conseguir el puesto de trabajo[8].

3. LA DIGITALIZACIÓN EN LA SELECCIÓN DE TRABAJADORES

Cuando termina la fase de reclutamiento del candidato, iniciada con la difusión de la oferta de empleo y continuada con la recepción de su información profesional y formativa por medio del CV de una u otra forma, comienza el proceso de selección del personal. Este proceso, realizado por personal especializado establece la vinculación de una persona a la organización convirtiéndose en una actividad de comparación o confrontación, de elección y decisión, de filtro de entrada, y de clasificación.

La selección de personal es un campo aún no totalmente determinado ni se tienen sobre él verdades que se puedan aplicar sin temor al error. En vista de la complejidad psicológica de cada persona, puede haber errores y se puede elegir equivocadamente. Por este motivo psicólogos y empresas que se dedican a asesorías en el reclutamiento están permanentemente en la búsqueda de nuevos elementos que permitan determinar con mayor precisión las capacidades, aptitudes y actitudes de las personas. Para ello es necesario utilizar distintas vías, una de ellas, y que en la actualidad adquiere mucha importancia, es el uso de herramientas digitales que agilizan e incluso colaboran en la objetividad del proceso[9].

Para poder precisar el alcance de las TIC en los procesos de búsqueda de empleo es preciso hacer referencia, en primer lugar, a lo que se conoce como selección 4.0[10]. Este sistema tecnológico, sujeto a las disposiciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico[11], permite, entre otras funciones, la búsqueda de candidatos a través de redes sociales o de buscadores de empleo, configurándose estas técnicas como otra forma de reclutamiento de personal, técnicas de inboud recruiting, nanotecnología, gamificación, el reclutamiento a través de apps del móvil, el uso de algoritmos para seleccionar a los mejores trabajadores, etc. En definitiva un amplio abanico de posibilidades vinculadas a la denominada inteligencia artificial[12].

Estos sistemas se presentan, por un lado, como una alternativa para la selección de personal en las pequeñas y medianas empresas y, por otro, como un medio utilizado también por las propias agencias de intermediación pues su implantación conlleva que se pueda reclutar personal de una forma sencilla y sin realizar una gran inversión económica. Se observa que la aplicación de estos instrumentos es más eficaz que la publicación de ofertas de empleo en prensa ya que, a través de estos mecanismos, los anuncios se transmiten a un número más elevado de personas a la vez que se hace posible el análisis, en un tiempo record, de la aptitud del candidato para un determinado puesto de trabajo vacante. La facilidad que proporcionan las TIC, también para los desempleados, se manifiesta en la posibilidad de acceder a la red incluso desde el propio te-

[8] Climent-Rodríguez, J. A., Navarro-Abal, Y. y Ortega-Campos, E. "El videocurrículum-branding como recurso digital para el desarrollo de competencias de búsqueda de empleo en los futuros egresados". En VV.AA: I Congreso Virtual Internacional sobre Innovación Pedagógica y Praxis Educativa INNOVAGOGÍA 2012; VV.AA. La generación y el potencial de transferibilidad del curriculum vitae en formato audiovisual, *Revista Tecnología, Ciencia y Educación,* núm. 13, 2019, pág. 42. Fuente: https://www.randstad.es/tendencias360/adapta-tu-curriculum-a-la-era-digital/.

[9] Rey, Hilda, C., & Ballesteros, R, Javier A., & Guevara, P, Alonso. (2013). Sistema experto para la selección de personal desarrollador de software. Ingenio Magno. Vol 4, pp. 75-81.

[10] Actualmente los métodos tradicionales para la selección de personal -currículum, referencias, entrevistas personales, test de capacidades cognitivas o aptitudes y pruebas grupales- conviven, de la mano del entorno digital, con las nuevas herramientas con las que cuentan los departamentos de Recursos Humanos.

[11] BOE núm.166, de 12 de julio, de 2002

[12] La inteligencia artificial (IA), es la inteligencia llevada a cabo por máquinas. En ciencias de la computación, una máquina «inteligente» ideal es un agente flexible que percibe su entorno y lleva a cabo acciones que maximicen sus posibilidades de éxito en algún objetivo o tarea.

léfono móvil y consultar las ofertas de empleo publicadas en las redes sociales o a través del llamado boca a boca virtual (los usuarios de internet pueden avisar a otros sobre las posibles ofertas de empleo), para así conocer las posibles vacantes que pueden ofertar las empresas de intermediación laboral.

Sin duda, uno de los aspectos más positivos de este tipo de selección, es que más allá de los años de experiencia, los títulos, etc, el reclutamiento 4.0 le da una gran importancia a competencias, aptitudes y habilidades, lo que permite dar una oportunidad a los empleados para desarrollarse dentro de la compañía. Por otro lado, este tipo de técnicas ahorra mucho tiempo a los profesionales de recursos humanos, que de esta forma tienen acceso a un mayor número de candidatos y a una mayor segmentación de estos, lo que facilita la selección de aquellos candidatos idóneos para el puesto.

En segundo lugar, las TIC también se presentan como herramientas colaboradoras para potenciar y flexibilizar los procesos de búsqueda de empleo. En este sentido, se puede decir que la alta capacidad que tienen las tecnologías informáticas para almacenar y filtrar datos de carácter personal, también se ha trasladado al ámbito de la búsqueda y selección de candidatos al empleo. Así pues, estos mecanismos de recopilación de información personal son utilizados, tanto por las empresas de intermediación públicas y privadas, como por las entidades que realizan su propia selección de personal. Muchos de estos procedimientos, además de ofrecer servicios de registro de datos, se configuran como verdaderas oficinas virtuales de empleo que ofrecen una amplia cartera de servicios para colaborar en la colocación de aquellas personas que estén a la búsqueda de un empleo[13].

[13] García Coca, O.: La protección de datos de carácter personal en los procesos de búsqueda de empleo, Laborum, 2016, p. 69-71.

3.1. Formas de reclutamiento de candidatos basadas en las TICS

La gamificación como herramienta colaborativa en la selección de candidatos supone utilizar mecánicas de juego en contextos no lúdicos para que el que candidato y reclutador puedan convergir en la deseada zona de "winwin"[14]. Es un método de gran atractivo para los candidatos, pues por medio de videojuegos y a través de sus coloridas pantallas, se relaciona la neurociencia y la psicología para encontrar el mejor encaje entre los rasgos cognitivos y emocionales de los potenciales trabajadores y el prototipo de empleado que está buscando la empresa.

Desde el punto de vista de los candidatos, supone un auténtico cambio de paradigma. Se minimiza la frustración de inscribirse a cantidades ingentes de ofertas sin apenas recibir feedback y con escasas posibilidades de éxito, a la par que se reducen las dosis de estrés y nerviosismo de las entrevistas tradicionales que pueden distorsionar las competencias laborales de candidatos válidos. Ahora simplemente se trata de jugar a través de un dispositivo tecnológico que te conectará con ofertas para las que, siempre que esté bien diseñado, tu perfil encajará. Además, en algunos casos los desafíos planteados en estos retos simulan a los que se tendría que enfrentar el trabajador en su futuro entorno laboral, fomentando su preparación en caso de ser contratado[15].

[14] La estrategia de marketing denominada con el nombre inglés «Win-Win», que si tradujéramos al castellano sería "Ganar-Ganar" es aquella estrategia de marketing que tiene como objetivo que todas las partes salgan beneficiadas; entendiéndose como "partes" a empresas, distribuidores, canales de venta y fuerza de ventas y/o consumidores implicados.

[15] Hay empresas que ya han puesto en práctica estas técnicas de gamificación, siendo en la mayoría de los casos una práctica de éxito. Existen entidades que crean aplicaciones en las que los candidatos de empleo se mueven de manera virtual por las oficinas de la empresa, resolviendo juegos y determinadas tareas. A través de una clasificación, los usuarios podían conocer su evolución y luchar por situarse lo más arriba posible. Otra forma de gamificar la selección de personal es simular de forma digital la gestión de la empresa para de esta manera

Todo lo relacionado con el networking online también propicia la colaboración de internet en la búsqueda de candidatos idóneos y aptos para la oferta de empleo que se difunde. La idea y el éxito de esta forma de encuentro de empleo es promover el conocimiento de personas adecuadas que pueden ayudar más en esa tarea, aspecto que se consigue gracias al uso de internet pues, lógicamente, es un hervidero de contactos de muy diversos perfiles. Una idea para lograr esta red de personas es empezar por la gente que ya conoces; los compañeros de trabajo, tus familiares o incluso los amigos del instituto con los que aún tengas contacto. De esta forma se intenta conectar y vincular a empresas que buscan trabajadores con personas que se encuentran en situación de desempleo o de mejora de empleo.

Otra forma de cumplimentar la red de contactos profesionales es la celebración de eventos virtuales, por ejemplo, de coaching, permite a las compañías participantes generar contactos de posibles candidatos para futuras vacantes. Lo ideal es que el candidato de empleo entable conversación y que, incluso, lleve preparado un guion en el que establezca los objetivos de su asistencia al encuentro y las oportunidades de empleo que se puedan presentar[16]. En estos actos pueden llevar una tarjeta de contacto con los datos que quieras facilitar. También es posible interrelacionarse a través de foros y páginas web especializadas en la búsqueda y participar de manera activa en las comunidades que ya hay creadas, busca las que tengan intereses afines a los tuyos, establece conversaciones, comparte contenidos y debate con ellos[17].

El *inboud recruiting* actúa en cuatro fases diferenciadas; en primer lugar, atrae al candidato mostrando la filosofía de trabajo de la empresa; los beneficios de trabajar en ella; su estructura organizativa; lo que aporta a la sociedad; e incluso sus técnicas innovadoras. En segundo lugar y una vez que el demandante de empleo conoce la empresa, si está interesado en entrar a formar parte de la misma la entidad que ofrece empleo, ya sea la intermediadora o la propia empresa, explica de manera detallada las principales oportunidades que ofrece la empresa. Para asegurar la buena marcha de esta fase, los formularios de inscripción a ofertas de empleo deben ser rápidas y fáciles de completar y estar optimizados para móviles. Una vez que el candidato está dentro del proceso de selección, deberá ser informado si avanza o no en el mismo y cuál es el estado de su candidatura, para lo cual se utilizan otros medios complementarios tales como; entrevistas, correos, llamadas, videollamadas. Pasado este trámite, se entraría en la fase final en la que una vez seleccionado, contratado e incorporado a la compañía, la experiencia debe seguir siendo excelente durante el ejercicio de la prestación de servicios[18].

Esta técnica actúa como escaparate para presentar la empresa antes de que los candidatos se postulen a las distintas ofertas de empleo que se ofrecen. Esa exposición también podrá realizarse de forma virtual para conectar con la entidad sin necesidad de desplazarse hasta ella y calibrar en ese momento si le interesa participar y formar parte del proceso de selección. Además, puede ayudar incluso a los demandantes de empleo a visualizarse dentro de la empresa, valorar sus cualidades, aptitudes y las aportaciones que pudiera realizar a esa organización empresarial. Sería interesante que en el propio recorrido virtual pudieran inscribirse en las distintas ofertas de empleo, a la vez que van observando los requisitos de la misma y en qué consistiría la

comprobar las habilidades de los jugadores, así como su estrategia de organización y administración.

[16] GARCÍA COCA, O.: "Las distintas cesiones de datos de carácter personal en la fase previa de contratación de trabajadores", en COLOMER HERNÁNDEZ I. (dir): *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Aranzadi, 2019, pp.733-768.

[17] Fuente:https://www.iebschool.com/blog/networking-profesional-reclutamiento-seleccion/.

[18] Fuente: https://www.randstad.es/tendencias360/inbound-recruiting-el-nuevo-metodo-de-contratacion/.

tarea que van a desempeñar si resultan elegidos[19].

La selección 4.0 también se ha querido aproximar a la nanotecnología como herramienta capaz de realizar una muestra sobre cómo reacciona el cerebro ante determinadas situaciones o estímulos que pueden ocurrir en el día a día de un profesional. Aunque es una forma de reclutamiento de personal todavía pendiente de implantar y explorar, puede ocasionar grandes avances en la selección de los candidatos más idóneos a partir del análisis de una escala manométrica para lo que existen potentes y sofisticadas herramientas (hardware y software) disponibles. Aunque se presenta como un método novedoso y eficaz, cierto es que la inversión por parte de la empresa debe ser mayor al necesitar herramientas tecnológicas avanzadas para realizar un análisis de los datos obtenidos lo más certero posible. Ante este previsible desarrollo, los dirigentes de la política científica-tecnológica de los países más avanzados están desarrollando mecanismos que asienten e impulsen el desarrollo nanotecnológico[20].

3.2. Importancia de las redes sociales para la gestión del talento

Como se ha comentado las redes sociales, concebidas como modelo colaborativo y abierto a la participación de todos los usuarios posibles, se han convertido en un elemento imprescindible a la hora de reclutar potenciales candidatos de empleo[21]. Este sistema supone un gran avance en la selección de demandantes de empleo por la agilización y simplificación que pueden suponer para ese proceso. La navegación por las citadas redes propicia que el intermediador laboral o directamente la empresa pueda conocer información sobre las personas no solo relacionada con su perfil profesional, sino que se aportan otros datos como las habilidades o aptitudes adquiridas, la experiencia laboral en un sector, el vínculo con otros profesionales y amigos, etc[22].

No obstante, aunque se quiera desplazar por la llegada de las redes sociales a los portales de empleo la realidad es bien distinta, ya que sigue siendo un medio en el que los candidatos introducen toda la información profesional y de contacto necesaria[23]. Lógicamente las redes sociales también recogen las ofertas de empleo que se publican en el propio portal, de ahí la vinculación existente entre ambos métodos, pues se permite a los usuarios que desde la red social dónde se difunden esas ofertas accedan a la misma para inscribirse e, incluso, a otras afines a sus intereses profesionales. Por ello se sigue encontrando útil el portal de empleo conectado a una plataforma de difusión tan elevada como la red social.

Acerca del uso de las redes sociales como mecanismo de reclutamiento y búsqueda de candidato existen opiniones encontradas entre los responsables de recursos humanos, ya que consideran que en ocasiones no se trata de un medio tan ágil y que podría producirse una pérdida de tiempo primordial para realizar su tarea, si la investigación sobre el candidato es desmesurada, alejando al profesional de su principal tarea que no es otra que

[19] HOLPE, J. "Incorporate inbound recruiting marketing into your recruitment strategy", *Recruiting & Retaining*, Volume 17, issue 8, 2015, pp.6-7.

[20] SERENO DOMINGO, A. "Nanociencia y nanotecnología: aspectos generales", *Fundación General de la Universidad Autónoma de Madrid*, 2009, pp.6-7.

[21] Adecco (2016), "Informe sobre Redes sociales y Mercado de Trabajo 2016", afirma que en 2016, el porcentaje de empresas que consultaba las redes de los candidatos era ya del 86%, https://adecco.es/wpcontent/uploads/2017/11/Informe-2017-Empleo-y-Redes.-Infoempleo-Adecco.pdf.

[22] MORATO GARCÍA, R.: "El impacto de las redes sociales virtuales en los procesos de selección de trabajadores" Comunicación presentada al X Congreso Europeo de Derecho del Trabajo y de la Seguridad Social, Sevilla, 2011, pp. 10-12, disponible en: http://www.aedtss.com/images/stories/documentos/congresoeuropeocomunicaciones/.

[23] Según GUELBENZU, el portal de empleo "es el punto de captación", donde hay una base de datos de profesionales que, por un lado, aplican a las ofertas de empleo, y por otro, son accesibles para la búsqueda directa por parte de los reclutadores.

contratar nuevos empleados[24]. Tampoco debe establecerse un uso tan generalizado de la red social con esa finalidad de reclutar a los mejores candidatos, ya que este primer ejercicio de filtrado y toma de contacto debe ir acompañado de evaluaciones más profundas que incluyan entrevistas por competen-cias, ejercicios de simulación, role play, cuestionarios de personalidad, peticiones de referencias etc., precisamente para paliar la comisión de errores por parte, por ejemplo, de las consultoras de recursos humanos. El futuro de las consultoras pasa por convertirse, cada vez más, en "socias de talento" para los clientes a lo largo de todo el ciclo de vida del candidato, de tal manera que les ayudemos no solo a incorporar a la persona idónea, provenga de donde provenga, sino también a evaluar, desarrollar y retener a su talento[25].

Otra de las posibilidades que ofrece la selección de personal a través de las redes sociales profesionales es la de obtener datos de los denominados candidatos pasivos, que son aquellos que pueden encajar perfectamente en el perfil que busca la empresa de intermediación pero que no se encuentran en búsqueda activa de empleo. Con ello, el buscar candidatos a través de las redes sociales ha contribuido a que no sólo se puedan encontrar personas desempleadas disponibles, sino a ofrecer oportunidades de empleo más competitivas y más acordes con sus características formativas y profesionales a aquellos trabajadores que tengan intención de cambiar de empleo[26].

Aunque existen, en la actualidad, un gran número de redes sociales, si lo que se pretende es seleccionar personas para trabajar en una determinada empresa, lo lógico es que se acuda a las redes sociales profesionales, siendo las más utilizadas: LinkedIn, Viadeo, Xing, Ziki[27]. Con estos mecanismos se consigue efectividad a coste cero puesto que la inscripción en la mayoría de redes profesionales para buscar candidatos es gratuita. Aunque si se quiere utilizar la red profesional para realizar alguna tarea concreta (por ejemplo, el diseño específico de un plan de selección; buscar candidatos con filtros de búsqueda avanzada para seleccionar personal; poder indagar perfiles distintos de los establecidos en la red de contactos etc.), se puede contratar los servicios premium con un coste que no suele ser elevado.

Entre las ventajas que para candidatos y seleccionadores aporta esta forma de reclutamiento están la de conexión del demandante de empleo con el seleccionador al poder interactuar de forma más directa y, por otra parte, la de acceso de forma realmente sencilla, a los datos de carácter personal que los usuarios exponen en la red social. Para ello, tan sólo es necesaria una conexión a internet y el registro en una concreta red social profesional para poder reunir o visualizar la información sobre un demandante de empleo que tenga un perfil activo en esa red social.

Para que el reclutamiento sea imparcial y objetivo es necesario distinguir entre redes sociales generales y profesionales. Así, aunque LinkedIn está considerada la red social que más se ajusta a lo que se conoce como red social profesional[28], hay otras como Facebook que, aunque su finalidad principal es generar con-

[24] Según el Informe "Redes Sociales y Mercado de Trabajo" de Infoempleo y Adecco de 2016", sólo un 48% de las personas que buscan empleo cree que las empresas las usan para reclutar, pero lo cierto es que la cifra es bastante más elevada; las usan un 84% de las empresas y, además, el 35 % opina que no damos un uso suficiente profesional a las redes sociales.

[25] LUQUERO, M. "Redes sociales y procesos de selección", *Capital humano: revista para la integración y desarrollo de los recursos humanos*, núm. 284, 2014, pág. 20.

[26] GARCIA COCA, O.: *La protección de datos*... op. cit. pp.

[27] La misión de estas redes sociales profesionales consiste en poner en contacto a profesionales de todo el mundo para que sean más productivos y tengan más éxito en el ámbito laboral, por lo que se permite que los usuarios puedan acceder a informaciones laborales incluso de otros países.

[28] ALASTRUEY, R.: *Empleo 2.0*, Editorial UOC, 2009; TELLO DIAZ, L; "Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook", *Revista Científica de Educomunicación*, 2013, pp. 206-208. UNIQUE: "Sobre el uso de las redes sociales y profesionales como fuentes de reclutamiento y selección de personal", *Revista Capital Humano*, núm. 248, 2010, pp. 50-53.

tactos sociales, han comenzado recientemente, como consecuencia del desempleo existente, a crear grupos de búsqueda de empleo. A través de ella se puede consultar información que no queda recogida en los currículums, habilidades personales, aficiones de los empleados y otra información adicional de interés que nos pueda ayudar a cumplimentar el currículum de los candidatos, siempre y cuando sus perfiles estén disponibles. De todas formas, no es el medio adecuado para buscar un determinado profesional, pues lo candidatos pueden tener su cuenta privatizado y además, aunque nos aporte información sobre sus gustos y habilidades, es difícil conocer cómo trabaja sólo con su perfil de Facebook[29].

3.3. Utilización de algoritmos en los procesos de selección de personal

La principal ventaja del uso de estos sistemas es la traslación de modelos matemáticos a las políticas de recursos humanos con el objetivo de lograr una solución clara, rápida, y objetiva en cuanto a su interpretación. Existen diversos algoritmos útiles para los procesos de selección, y este es un nuevo instrumento de la implantación de la inteligencia artificial en los recursos humanos[30].

Para fijar el mecanismo adecuado es necesario establecer algunas instrucciones que variaran según lo que determine la empresa reclutadora, pero generalmente el proceso consiste en introducir una serie de datos personales, a veces incluso una carta, una foto, un correo electrónico y un currículum. La conexión de los algoritmos con otras técnicas digitales de selección, como la gamificación, es más que evidente si tenemos en cuenta que en una segunda fase, al utilizar este método el candidato se enfrenta a una experiencia en la que se le plantea una situación límite, desde sobrevivir en una balsa rodeado de desconocidos tras naufragar, gobernar una isla o gestionar un restaurante. Lo importante no es el juego en sí sino la herramienta que hay detrás, que permite medir patrones de comportamiento humano.

Ese es el propósito principal de trabajar con algoritmos para la selección de personal la facultad de encontrar al candidato perfecto en base a las variables introducidos en la configuración de la propia operación matemática. Una vez conocidos los niveles en que cada candidato posee una determinada cualidad, se procede a su comparación con las cualidades del perfil del puesto de trabajo establecido, lo que debe permitir conocer el grado de adaptación de cada candidato y obtener, en definitiva, un orden de preferencia entre ellos. Todo ello sin olvidar la compatibilidad de las personas, objetivo paralelo a la buena adaptación de los candidatos a los puestos[31].

Ahora bien, el principal problema consiste en la posibilidad de que esos perfiles clasifiquen directa o indirectamente a los trabajadores por categorías discriminatorias. Un riesgo que de acuerdo con los expertos es sumamente elevado. Aunque se prohíba recabar cierta información especialmente sensible de los candidatos al empleo, hay datos que al relacionarlo unos con otros pueden desvelar más información de la realmente necesaria para realizar el proceso de selección.

En suma, el procesamiento digital de datos incrementa exponencialmente las posibilidades de vulneración de los derechos de los trabajadores. Con independencia de que finalmente sea el responsable de recursos humanos el que tome una determinada decisión, el

[29] Fuente: Talent Clue, Los beneficios de reclutar en las redes sociales, pp.7-13; DAGNINO, E.: "Social recruiting: una novità da perfezionare" publicado en *Conquiste del Lavoro*, el 21 de octubre de 2014, disponible en www.bolletinoadapt.it

[30] CANÓS DARÓS, L., CAÑO ALEGRE, C., GONZÁLEZ PÉREZ, B.: Algunos algoritmos de ordenación para el proceso de selección de personal, X Congreso de Ingeniería de Organización: Valencia, 7-8 de septiembre, 2006, págs. 1-2.

[31] VV.AA. "La selección del personal con un algoritmo genético borroso", *InvestigacionesEuropeas de Dirección y Economía de la Empresa* Vol. 2, num.2, 1996, pp. 62-64.

hecho de que lo haga basado en un procesamiento automatizado de datos[32].

3.4. Herramientas informáticas que colaboran en la selección de personal

Las TIC, además de configurarse como mecanismos que pueden llegar a intermediar en el mercado de trabajo, también se presentan como vías de almacenamiento de datos e, incluso, herramientas colaboradoras en la selección de personal. Estos instrumentos tienen transcendencia tanto para acceder a puestos en la empresa pública como en la privada. Aunque, es obvio, que algunas de ellas tienen más repercusión en el ámbito privado sobre aquellas relacionadas con el registro de datos en ficheros automatizados (*cloud computing*).

Es preciso, no obstante hacer referencia a algunos de los instrumentos de informáticos que conforman la llamada Administración Electrónica[33], han creado en el marco de los SEPE y de los SPE autonómicos un sistema de información para poner en relación datos de demandantes de empleo y ofertas de trabajo (SISPE)[34]. Dicho sistema, perteneciente al SNE, permite al SEPE y los SPE autonómicos compartir una información básica y coordinada sobre políticas activas de empleo y prestaciones por desempleo[35]. Lo que se pretende con este sistema informático es combinar la gestión transferida a las CCAA (políticas activas de empleo) y la gestión estatal (prestaciones por desempleo) y que, a su vez, debe posibilitar la coordinación a nivel nacional de los planes de actuación encaminados a fomentar el empleo.

A este efecto, en primer lugar, se establecen unas bases de datos estatales, compartida por todos los SEPE autonómicos en la que se almacenan datos comunes que pueden ser actualizados por las distintas CCAA. En segundo lugar, existen unos sistemas de información de los SE autonómicos, con bases de datos relativos a la CCAA, es decir, el SISPE[36] facilita a la Comunidad Autónoma que pueda desagregar información de las bases de datos estatales cuando sus necesidades lo requieran. Se trata pues, de un modelo de utilización de los datos que garantiza una gestión uniforme y coordinada de los mismos en todas las CCAA[37].

---

[32] Todolí Signes, A. (2019). "Algoritmos para contrataciones y despidos. ¿Son legales las decisiones automatizadas sobre trabajadores?", *Argumentos de Derecho Laboral*, en htpp://https://adriantodoli.com/2019/02/21/algoritmos-para-contrataciones-y-despidos-son-legales-las-decisiones-automatizadas-sobre-trabajadores/

[33] Todo lo relacionado con las actuaciones de la Administración Electrónica está regulado en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE núm. 150 de 23 de junio de 2007).

[34] El SISPE permite integrar la información relativa a la gestión de las políticas activas de empleo y las prestaciones por desempleo que llevan a cabo los Servicios Públicos de Empleo, Estatal y Autonómicos. En un modelo mixto de gestión, en el que tiene que convivir la gestión transferida a las Comunidades Autónomas (políticas activas de empleo) y la gestión estatal (prestaciones por desempleo), y que, a su vez, debe posibilitar la coordinación a nivel nacional de los planes de actuación encaminados a fomentar el empleo, el SISPE hace posible compartir, integrar y coordinar tanto la información propia de cada uno de los Servicios Públicos de Empleo, como las actuaciones y estrategias orientadas a favorecer la inserción laboral y el estudio del mercado laboral español. Fuente: nota informativa del Ministerio de Empleo y Seguridad Social, disponible en http://www.sepe.es/contenidos/inicial/sispe/.

[35] El programa de modernización de los SPE incluye la mejora de los recursos materiales y tecnológicos, un plan estratégico de recursos humanos y una mejora de la gestión de las prestaciones por desempleo. Dicho programa se enmarca dentro de las directrices integradas para el crecimiento y el empleo (2005-2008) de la Estrategia de Lisboa, en concreto la directriz nº 20 que versa sobre la mejora de la respuesta a las necesidades del mercado laboral, disponible en http://eur- lex.europa.eu/.

[36] Los objetivos del SISPE son: promover la libre circulación y la movilidad laboral de los demandantes de empleo; favorecer la igualdad de oportunidades en el acceso al empleo e incrementar la capacidad de cobertura de puestos de trabajo; y compartir la información para mejorar la capacidad de intermediación. De modo que, tendrán que tener acceso a los datos de los demandantes de empleo que sean necesarios para cumplir con estas funciones.

[37] Alujas Ruiz, J.A.: "El Servicio Público de Empleo y su labor como intermediario en el mercado de trabajo en España", *Cuadernos de Ciencias Económicas y Empresariales*, núm. 53, 2007, pp. 31-34; Sánchez-Rodas Navarro, C.: "La orientación e

Cada transacción actualiza directamente la base de datos estatal y asíncronamente, al día también la correspondiente base de datos autonómica. Esta modalidad es unidireccional, es decir las actualizaciones siempre se inician en el sistema estatal y terminan en diferido en el autonómico. También se puede optar por el sistema de información propio de las Comunidades Autónomas, siendo éstas las que optan por implementar y desarrollar su propio sistema de información para dar soporte a la gestión que se les transfiere[38].

Las agencias de colocación tendrán que tener, a su vez, sistemas informáticos compatibles y complementarios del SISPE, produciéndose de esta forma el nacimiento del Espacio Telemático Común como nexo de unión entre la agencia de colocación y el SISPE, en el cual ya se integran los datos aportados por los SEPE y distintos SEP autonómicos. A través de este mecanismo también se deberá presentar una memoria de las actividades desarrolladas por la agencia en el ejercicio anterior, considerando la información relativa a los indicadores de eficacia[39].

Ahora bien, en el ámbito privado, se desarrollan también sistemas que permiten informatizar datos de los demandantes de empleo. Actualmente, existen algunos programas informáticos que colaboran con estas empresas de intermediación privada realizando la tarea de procesamiento y almacenamiento de datos de carácter personal. Dado que el primer paso para la selección de personal es la entrega del CV, habrá que comprobar qué vías utilizan las empresas de intermediación para realizar la tarea de clasificación de CV[40] y el posterior almacenamiento de ese documento. Así pues, estos programas no sólo son útiles, sino que también pueden resultar muy necesarios puesto que, además, ponen en práctica una serie de filtros objetivos como, por ejemplo, pasar la información curricular de aquellos candidatos que cumplan determinados requisitos profesionales, formativos, o de edad, entre otros[41]. Con el uso de estos programas informáticos de selección se clasifican a aquellos candidatos que cumplan los requisitos requeridos, reduciendo, de esta forma, los miles de CV recibidos a cientos o incluso a decenas.

Actualmente, el mercado laboral proporciona herramientas tecnológicas que colaboran en la selección de personal, haciendo una criba de los candidatos atendiendo a su perfil psicológico, siendo quizás el más conocido el sistema experto Sigmund[42], a través del cual se intenta obtener datos cuyo tratamiento automatizado está prohibido (origen racial, nacionalidad, religión, opiniones políticas etc.) mediante unos cuestionarios exhaustivos realizados por psicólogos industriales.

Hoy día, la utilización en algunas empresas de selección de lo que se conoce con el término anglosajón *cloud computing* o computa-

intermediación directa en el empleo", *Revista Temas Laborales*, núm. 125, 2014, pp. 105-109.

[38] Fuente: http://www.sepe.es/contenidos/.

[39] Climent Rodríguez, J. y Navarro Abal, Y.: "Oficinas virtuales de Empleo. El reto de universalizar los servicios públicos de empleo", *Revista Trabajo* núm. 24, 2011, pp. 82-83.

[40] Lee, I., "E-recruiting: Opportunities and challenges", *Information Management*, vol. 19, núm. 3-4, 2006, pp. 24-25; VV.AA: *Manual de selección de personal*, CEP, 2013, pp. 47-51.

[41] La empresa de selección RANDSTAD EMPLEO, utiliza el programa informático Darwin (que es una aplicación para la validación y chequeo de datos, este programa permite hacer una criba curricular por perfiles, de todos los datos incluidos (CV) en el sistema a través de la web de la empresa (Fuente: Randstad Empleo). En MANPOWER ETT utilizan el programa de gestión de datos POWER BASE, para el registro de candidato, búsqueda de los mismos para un determinado empleo, almacenamiento de documentación relacionada con el demandante de empleo etc. (Fuente: MANPOWER ETT).

[42] Sistema que permite determinar rasgos de la personalidad. El Método Sigmund es una herramienta informatizada de evaluación del Potencial, basada en competencias. Consta de 436 preguntas que evalúan 37 diferentes competencias que, a su vez, responden a 10 macrocompetenciaso macrocriterios, en las Dimensiones Profesional, Social y Personal. Tras la realización de la Prueba, el Consultor mantiene una entrevista personal con el Candidato, para proporcionarle feed back explicándole los resultados obtenidos y, al mismo tiempo, ampliando aquellos datos necesarios para completar la información acerca de la candidatura. Como resultado se obtendrán un Gráfico Competencial, un Informe numérico y un Informe Individual con los comentarios del entrevistador, que se entregará al Cliente. (Fuente: Pricewaterhousecoopers).

ción en la nube para la gestión de los recursos humanos y para el almacenamiento de datos es bastante generalizada. Este sistema incluye algunos software tales como; expertHRM®, que incluye módulos como la gestión de nóminas (contratación, retribución y Seguridad Social), control de presencia (asistencia y absentismo), y recursos humanos (definición del organigrama, inventario de personal, desarrollo profesional, planes de carrera y procesos de selección); el IntegRHo que es una aplicación integral de administración de recursos humanos, diseñada con las últimas tecnologías para trabajar en entorno web[43].

El avance de las técnicas de selección digitalizadas por medio de software especializados ha propiciado un gran ahorro en el tiempo dedicado por las empresas a esta gestión, e incluso, en la inversión que supone contratar a empresas externas para que lleven a cabo esta tarea. Por poner un ejemplo la plataforma Evalart[44], dispone de numerosos test para evaluar diversos puestos y competencias. Los mismos se envían por email y los resultados son accesibles a los reclutadores por medio de la plataforma. Esto permite una optimizar los procesos de selección, reduciendo tiempos y costos, además de permitir identificar al mejor talento. De otra parte, con Go You te olvidas de los anuncios pudiendo seleccionar en una base de datos, creada al efecto, al candidato ideal que mejor se ajuste al perfil que estás buscando. Todo ello de una forma rápida, ágil y sencilla.

La base de datos que se crea con Go You permite segmentar a muchos candidatos entorno a distintas posibilidades por: sector, formación, idiomas, situación laboral, lugar de residencia, años de experiencia, tipo de contrato deseado. De esta forma, el cliente obtiene una lista acotada de candidatos que poseen las aptitudes necesarias y se ajustan al perfil que necesita. Es una solución de software bastante completa al permitir, además, realizar búsquedas a través de palabras claves y proporcionar a la empresa de selección una lista acotada de candidatos que poseen las aptitudes necesarias y se ajustan al perfil que necesita[45].

4. IMPACTO DE LA LEGISLACIÓN DE PROTECCIÓN DE DATOS EN LOS PROCESOS DE SELECCIÓN DE TRABAJADORES

Concluido que según las definiciones dadas en la normativa sobre protección de datos los seleccionadores o reclutadores de personal registran y archivan información de los demandantes de empleo, por medio de unos u otros mecanismos, llega el momento de abordar si ese tratamiento sigue las premisas de la legislación que protege la información personal de los mismos. Teniendo en cuenta que los datos que se protegen son aquellos que identifican claramente a una persona física, están exceptuados de esta protección, también en este ámbito, los datos anónimos.

Igualmente, es necesario proyectar las exigencias relacionadas con la protección de datos en relación con otro de los tratamientos que tiene lugar en la intermediación laboral como es, una vez realizada la elección del demandante de empleo más idóneo, la cesión de esos datos al empresario que lo va a contratar o a aquellas empresas externas que pueden, en un determinado momento, colaborar en las tareas relacionadas con la actividad de la empresa intermediadora.

Es por ello que de distintas formas y siguiendo la definición contenida en el RGPD[46]

[43] García Coca, O.: *La protección de datos... op. cit.* pp.78-84

[44] Innovadora plataforma para evaluar a candidatos en línea. permiten a los candidatos a puestos técnicos escribir programas, y posteriormente ser evaluados automáticamente por el sistema.

[45] GoYou: el nuevo concepto de Selección de Perfiles Digitales & IT, en *Blog Social You*, https://blog.socialyou.es/go-you-el-nuevo-concepto-de-seleccion-de-perfiles-digitales-it/

[46] Art. 4.2 RGPD: *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de*

se puede decir que todas las actuaciones que intervienen en la fase previa de contratación de trabajadores, suponen el manejo de datos de carácter personal de los demandantes de empleo. Estas informaciones, en un primer momento, tienen relación con la identificación del propio sujeto; su experiencia formativa y profesional; edad; disponibilidad; etc[47].

4.1. Captación de datos de los demandantes de empleo. Estudio de su pertinencia

El registro de información personal conlleva, inexcusablemente, un tratamiento de datos al introducirse en un fichero automatizado o no. En este caso, lo primero que hay que señalar para comprobar si el responsable del fichero cumple con los principios relativos al archivo de esos datos es la necesidad de su procesamiento para cumplir con los objetivos de selección. Este es el primer escalón para verificar la legalidad de la actuación de los seleccionadores de empleo respecto al uso de los datos que se recogen en los distintos procedimientos de búsquedas de candidatos.

En este sentido, parece obvio que no es necesario conocer y registrar más datos de las realmente necesarias para certificar la aptitud de un candidato respecto al puesto de trabajo. Pero esta obviedad no queda del todo clara cuando el medio para tratar datos está incardinado en la digitalización, ya que aparecen otras informaciones relacionadas que nada tienen que ver con la formación y la profesionalidad del candidato[48].

Por ello y atendiendo al art. 5 del RGPD que establece que los datos serán *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)",* es preciso tomar unas consideraciones respecto a la información captada, sobretodo, por los medios digitales de selección de personal. En primer lugar, cuando presentamos un CV lo primero que pretende el candidato es llamar la atención de la persona que ofrece el empleo, por lo que las nuevas herramientas de expansión del CV, como hemos visto, pueden cumplir con este objetivo, salvaguardando la información personal que contienen. Pero esta innovación trae consecuencias en lo que a la salvaguarda de la información personal se refiere. En algunos casos, ya no se presenta información relevante como puede ser la referida a datos identificativos, formación, puestos desempeñados anteriormente, edad, etc., sino que si se envía un videocurriculum estamos transmitiendo nuestra imagen, que no debe de ser necesaria en este momento del reclutamiento para establecer una primera toma de contacto. A mi modo de entender el problema se plantea no con la visualización de la imagen, que no sería constitutiva de tratamiento, sino con su integración en un fichero que tenga como finalidad principal procesar datos obtenidos de los CVs[49].

---

datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

[47] García Coca, O.: "Las distintas cesiones de datos carácter...", op.cit. pp.733-768

[48] Sin embargo, en sede jurisprudencial se ha admitido la recogida de datos relativos a la intimidad del trabajador si estos son necesarios para un buen desempeño de la actividad laboral, véase; la Sentencia del TSJ de Justicia de Castilla y León de 3 de diciembre de 1996 (AS 1996, 3998): *"...consideró justificadas las preguntas sobre la vida privada y personal de los trabajadores contenidas en un test al que la empresa RENFE sometía al personal de circulación (conductores de puentes grúas, carros trasbordadores carretillas) para evitar accidentes y reducir el índice de peligrosidad en el manejo de maquinaria pesada. Establecería en relación a los test psicológicos que ahondan en aspectos íntimos de la personalidad del trabajador (sociabilidad, inteligencia), tres requisitos que deben reunir las pruebas para respetar el derecho a la intimidad del trabajador: el candidato debe prestar su conformidad a someterse al test, el candidato debe conocer el tipo de test que va tener que desarrollar y cuáles son los objetivos que se persiguen con ello; el psicólogo que corrige el test sólo puede informar al empresario de los datos objetivos del candidato que sean necesarios para el desarrollo del puesto de trabajo al que se aspira".*

[49] Evidentemente hay puestos de trabajo en los que se requiera una determinada imagen y, en esos casos, puede ser

Tampoco se admite el procesamiento de datos para fines que no sean los inicialmente concretados, es decir, cuando una persona inserta sus datos en alguna de las herramientas informáticas que colaboran en la selección de personal, debe conocer cuál es la finalidad de su tratamiento, a través de las clausulas informativas establecidas para ello. En el caso de la recopilación de datos por medio de las plataformas digitales, en ocasiones, no se recogen datos con esa finalidad o, incluso, se busca más información de la necesaria para entrar en el proceso de selección. Si, por ejemplo, se recogen datos del perfil profesional inserto en una red social y se compara con los obtenidos en otras redes que no tengan como objetivo ser un modelo colaborativo para la búsqueda de empleo y si, además, se archivan, no se está cumpliendo con los requisitos de pertinencia y finalidad para el tratamiento.

En este sentido la necesidad de conservación de los datos insertos en las redes sociales estaba regulada ante la falta de regulación de la anterior LOPD en el Dictamen 5/2009 del Grupo del art. 29 sobre las redes sociales en línea, adoptado el 12 de junio de 2009[50]. En el mismo se establecen pautas acerca de la conservación de los datos de las redes sociales cuando los usuarios ya tienen dado de baja su perfil. El Dictamen considera adecuado que los datos, pero únicamente los identificativos, se almacenen durante no más de un año y con la única finalidad de que no vuelvan a registrase en la red social, lo que no tiene mucho sentido pues un usuario, en un determinado momento, puede decidir no formar parte de la red social, por las circunstancias que sean, pero en un futuro se le debería permitir volver a configurar su cuenta en la misma si así lo decide[51].

Como regla general no se podrán tratar datos relacionados con la ideología, por considerarse especialmente protegidos[52] pero, ¿y si tu empresa es de tendencia? ¿sería la gestión de ese dato necesaria? Este aspecto se puede admitir atendiendo a la especial actividad que desarrolla la empresa de tendencia que está intrínsecamente unida a una determinada ideología o pensamiento. Por este motivo, se faculta al empresario de tendencia para llevar a cabo las actuaciones oportunas dirigidas a conocer la aptitud ideológica del candidato para el desempeño de un puesto de trabajo que implique precisamente una tarea ideologizada, a través de la cual llevar a cabo la actividad difusora de la ideología empresarial; no permitiéndosele lógicamente cuando las tareas a realizar no precisen necesariamente de esa identificación del trabajador con el ideario de la empresa. En este supuesto el fin del tratamiento podría estar legitimado para justificar la inclusión del candidato al empleo en una tarea de tendencia[53]. Podría, en casos como este, sacrificarse el derecho a la protec-

adecuado y necesario registrarla junto a la información personal presentada en el CV, pero habrá otros en los que el tener una imagen concreta no sea un requisito esencial ni restrictivo para continuar en el proceso, por lo que debería archivarse por separado.

[50] Este documento está disponible en http://ec.europa.eu/justice/policies/privacy/. Existen otros trabajos y documentos sobre el tema, utilizados para la redacción del Dictamen, como es el caso del Memorándum de Roma, disponible en: http://www.datenschutz- berlin.de, adoptado en marzo de 2008 por el Grupo de Trabajo internacional de Berlín sobre protección de datos en las telecomunicaciones. Este Memorándum analiza los riesgos que para la intimidad y la seguridad presentan las redes sociales y proporciona directrices a los reguladores, proveedores y usuarios.

[51] García Coca, O.: *La protección de datos... op. cit.* pp. 127-128.

[52] Art. 9.1 b) RGPD: "Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física". Esta prohibición de tratamiento esta excepcionada 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, 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".

[53] García Salas, A.I.: "Limitaciones al derecho a la intimidad: necesidad de la empresa de obtener datos sensibles del

ción de datos del candidato pues como recuerda la Sentencia núm. 77/1985 del Tribunal Constitucional de 27 de junio: *"la facultad de selección del empresario no puede ni debe limitarse a comprobar la simple y mera capacidad del aspirante; se trata además de elegir a la persona más idónea para la concreta misión a la que será destinado el trabajador»*.

De otra parte, los medios de inteligencia artificial suponen una amenaza para la protección de datos pues pueden procesar más datos de los realmente necesarios para llevar a cabo con éxito el proceso de selección de personal. Parece que la normativa sobre protección de datos no puede responder a algunas cuestiones al respecto. Obviamente al usar esos mecanismos para reclutar a trabajadores es preciso hacer algunas matizaciones respecto a la finalidad del tratamiento de los datos archivados en esos sistemas. La aplicación del principio de minimización de datos es difícil porque colisiona directamente con el uso de la tecnología, en lo que se refiere a la toma automatizada de decisiones a la hora de elegir al candidato más adecuado. Son tecnologías que tienen una gran capacidad de interrelacionar informaciones muy variadas no sólo relacionadas con la capacidad profesional, sino con otras como la situación económica, salud, preferencias personales, comportamientos etc., que no tienen que observarse para medir la capacidad y aptitud profesional. Por ello, en el caso de que se registrasen tenían que almacenarse en ficheros con distintos fines y especiales tratamientos, sobre todo en lo que a los datos de la salud se refiere[54].

La actualización de la información contenida en los ficheros de gestión de los procesos de selección es otra de las obligaciones que tiene el responsable del fichero para el mantenimiento y conservación de los datos[55]. Para las tareas relacionadas con los recursos humanos y el reclutamiento de candidatos es esencial que la información esté actualizada y que sea exacta para que puedan tener acceso a las ofertas y se tengan en cuenta sus mejoras en lo que a su formación y experiencia profesional se refiere. Respecto al período de conservación se estima que la retención habitual es de 6-12 meses tras los cuales un currículum puede ser no vigente. Tras ese periodo de retención, no existe motivo de conservación y por ello inicialmente se destruirían.

Sin embargo, el caso de los datos de los perfiles seleccionados, en cambio, es diferente pues en tanto en cuanto el trabajador forma parte de la plantilla la información de su perfil se conservaría. Si el candidato forma parte de una bolsa de empleo, para la búsqueda continua de ofertas, o bien de una ETT, a disposición de los trabajos eventuales que surjan, el periodo de retención sería indefinido, hasta el momento en que el candidato decida darse de baja.

4.2. El reforzamiento del principio de consentimiento

A raíz de la promulgación y entrada en vigor del RGPD se han establecido algunas directrices respecto a la forma de prestar el consentimiento[56] con la intención de reforzar-

trabajador", en *Necesidades empresariales y derechos fundamentales de los trabajadores*, Lex Nova, 2016.

[54] Es esencial por tanto respetar lo dispuesto en el artículo 22 del RGPD que otorga a todo interesado el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos en él o le afecte significativamente.

[55] Considerando 39 del RGPD: *"Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".*

[56] Art. 4.11 del RGPD: "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara*

lo y evitar así, tratamiento de datos en los que no medie el asentimiento de los titulares de la información. Estas pautas están dirigidas a preservar que el consentimiento sea libre, voluntario, inequívoco e informado.

En lo que a la utilización de medios tecnológicos se refiere para tratar datos de los demandantes de empleo se refiere se puede cumplir con esta forma de consentir marcando una casilla de un sitio web en internet, escogiendo parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. No se admite en la nueva regulación la prestación de un consentimiento tácito, indicando además que tendrán que otorgarse para cada una de las finalidades de tratamiento de datos que se vayan a realizar.

Otra de las garantías previstas en la nueva normativa sobre protección de datos es la prestación del consentimiento informado. En este caso el titular de la información se considerará informado, cuando conozca como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. Por tanto, resultará necesario que la información sea facilitada al interesado antes del tratamiento, en caso contrario, el tratamiento no podrá ser considerado lícito.

Ahora bien, en cuanto a la libertad para asentir[57] se establece que éste no se considerará libremente prestado cuando el interesado no goce de verdadera o libre elección, o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno. Para ello debe establecerse un equilibrio entre el titular del dato y el responsable del tratamiento para no generar un consentimiento viciado[58]. El desequilibrio puede apreciarse cuando, por ejemplo, estamos sometidos en un proceso de selección interno de una empresa que ofrece empleo. En este supuesto, existe un riesgo real de no dar un consentimiento de forma libre ante el miedo de ser excluido del proceso de selección, por lo que no parece que exista una voluntad de consentir libremente.

Por último también en el RGPD se establece una excepción al principio de consentimiento relativa al tratamiento de datos necesario para mantener una relación precontractual como pudiera ser la relacionada con cualquier fase previa de contratación[59]. Esta modulación del consentimiento puede ser necesaria para lograr la finalidad del proceso de selección, pero sería interesante atender a la interpretación de necesariedad[60] relativa al tratamiento sin consentimiento, puesto que en muchos casos los candidatos no van a conseguir el empleo, por un motivo u otro, y sus datos ya han sido registrados, conformando un apartado que pudiera considerarse lista negra por no

acción afirmativa, el tratamiento de datos personales que le conciernen".

[57] El Grupo de Trabajo del Artículo 29 -en su Dictamen 15/2011-, ha expresado que tal libertad consiste que «*el interesado puede hacer una elección real y no haya ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta. Si las consecuencias del consentimiento socavan la libertad de elección de la persona, el consentimiento no es libre*».

[58] Considerando 43 del RGPD: *"Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento".*

[59] Art. 6.2 RGPD: "*el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*".

[60] García Murcia, J. y Rodríguez Cardo, I.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216, 2019.

cumplir los requisitos para ese puesto aunque su validez podría no cuestionarse para otros[61].

4.2.1. La información como requisito indispensable para consentir

El fortalecimiento del principio de información[62] como medio para garantizar un consentimiento preciso y determinado ha exigido que, también, los procedimientos de búsqueda de empleo se adapten a esta nueva realidad. La información que el responsable del tratamiento debe facilitar a los interesados, tanto respecto a las condiciones de los tratamientos que les afecten como en las respuestas a los ejercicios de derechos, deberá proporcionarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo[63], además será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Se admite, en algunos supuestos, que sea el propio titular del dato el que decida que se le informe verbalmente, siempre que se demuestre la identidad del interesado por otros medios.

Por ello, si se van a registrar datos utilizando los distintos mecanismos de reclutamiento se hace preciso llevar a cabo una serie de actuaciones por parte de los responsables del tratamiento. Así, por ejemplo, si *se* utilizan cuestionarios u otros impresos digitales para la recogida de datos de candidatos deberán figurar en los mismos, de forma claramente legible, la información mencionada. Puede ocurrir que los datos se reciban a través de comunicaciones escritas, solicitadas o no, en caso de que vayan a ser utilizados en procesos de selección y debido a la imposibilidad de informar con anterioridad, deberá informarse al candidato de todos los extremos señalados acerca del tratamiento que se vaya a realizar mediante cualquier medio que acredite su notificación (correo electrónico, llamada telefóni-

[61] La Sala Primera del Tribunal Supremo, en sentencia nº 609/2015 de 12 de noviembre de 2015 (Rec. 899/2014; Ponente: señor SARAZÁ JIMENA) (ver enlace más abajo), ha condenado a a la empresa Construcciones de las Conducciones del Sur (Cotronic) por vulneración del derecho a la protección de los datos personales y del derecho al honor de un trabajador, por comunicar la causa de su despido a otra compañía (Telefónica) con el fin de incluirlo en una *lista negra*, que dificultó la búsqueda de un nuevo empleo.

[62] Art. 13 RGPD: *"Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; L 119/40 ES Diario Oficial de la Unión Europea 4.5.2016 d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado".*

[63] Art. 11 LOPDGDD: *«1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. 2. La información básica a la que se refiere el apartado anterior deberá contener, al menos: a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento. c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679. Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679. 3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también: a) Las categorías de datos objeto de tratamiento. b) Las fuentes de las que procedieran los datos».*

ca, correo postal, …), debiéndose conservar la notificación realizada hasta la finalización del proceso de selección o mientras se conserven lo datos personales del candidato-

Si la empresa prevé la recogida de información a través de medios electrónicos o formularios webs, se incluyen en los mismos un *checklist* en el que se pone un texto tipo a *«he leído y acepto la política de privacidad de este sitio web»* (con enlace al texto legal completo). El usuario deberá marcar el *checklist* para poder enviar sus datos personales a través de la web y supuestamente con esta acción debe estar informado acerca del tratamiento de su información personal que vaya a realizar el intermediador laboral[64].

Este derecho a la información funciona, sin duda, como una garantía para los trabajadores puesto que se les tendrán que informar también sobre los derechos que tienen respecto de los datos suministrados y ante quién puede ejercerlos. Así, la política de privacidad de las empresas o plataformas de selección constituyen un mecanismo idóneo para dar la información relativa al tratamiento de datos, así como la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, sin dejar atrás el tan cuestionado derecho al olvido que es fundamentarlo ejercerlo para limpiar en algún momento la reputación online[65].

4.2.2. Materialización del consentimiento informado en los procesos de selección

Al hilo de lo dicho anteriormente podemos distinguir dos fases dentro de las relaciones precontractuales, una de ellas sería el recibimiento del currículum y, la otra la se produce en el desarrollo del proceso de selección. En ambos casos se presume que el interesado otorga el consentimiento para el tratamiento de sus datos para los fines de un posible reclutamiento, sin embargo, existen una serie de buenas prácticas empresariales que pueden blindar de mayor seguridad jurídica a dicho consentimiento implícito. En primer lugar, sería aconsejable que cuando la empresa reciba un currículum por cualquier medio, remita una respuesta al remitente de la confirmación de la recepción y en la que se especifique que la información personal contenida en el currículum tan solo será usada con fines de selección de personal.

Si el envío se realiza por una plataforma web, se podría implantar un sistema de respuesta automática para la confirmación de la recepción. También cabe la posibilidad que la entrega del currículum se limite a la cumplimentación de un formulario, ya sea, online o en físico. En ese caso el formulario web debe garantizar la protección de datos recogiendo solamente los datos necesarios e informando acerca de su tratamiento y utilización. No obstante, es preciso mencionar que no es lícito solicitar datos de carácter personal que puedan originar discriminación en un proceso de selección o que no sean imprescindibles para valorar la aptitud profesional[66], como, por ejemplo; edad, estado civil, religión, política, etc. Por otro lado, debemos mencionar aquí que la obtención de estos datos actualmente no es tarea difícil para el seleccionador, debido a las redes sociales, ya que, se está haciendo práctica común investigar a los solicitantes en sus perfiles de internet, por lo que cada vez adquiere más importancia conservar cierta re-

[64] García Coca, O.: "Las distintas cesiones de datos…" op. cit. pp. 733-768.

[65] Sempere Navarro, A.V.: "Contrato laboral y tecnologías novedosas", *Actualidad Jurídica Aranzadi* núm. 912, 2015; García Coca, O.: *La protección de datos…*, op.cit.pág.172.

[66] Sentencia de la Audiencia Nacional de 28 de enero de 2014 (AS 2014\231) establece; *"Teniendo en cuenta lo que se acaba de indicar, la comunicación de los números de teléfono móvil y dirección de correo electrónico requerirá el consentimiento de los interesado a menos que la misma pueda ampararse en alguno de los supuestos excepcionados por el citado artículo 6.2, y ninguno de los cuales parece concurrir en el supuesto contemplado, por lo que la empresa no puede imponer a los trabajadores que le faciliten los referidos datos porque ello sería contrario a la Ley 15/1999"*.

putación online que no perjudique los aspectos relacionados con el ámbito laboral[67].

Si se analiza la prestación del consentimiento a través de buscadores webs o insertando datos en las redes sociales de empleo, por ejemplo, se observa como la aceptación de la política de privacidad no debe significar que el titular de los datos da su conformidad para que éstos sean cedidos o tratados ya que se considera que esta forma de dar el consentimiento no expresa de manera suficiente su voluntad, pues realmente no se le está informando del tratamiento que se le va a dar a esa información personal. Así pues, esta forma de prestar el consentimiento no puede ser considerada válida en el sentido de lo exige la normativa sobre protección de datos.

Además, los mecanismos relacionados con los sistemas de inteligencia artificial que archivan informaciones de diversa índole deberían justificar que necesitan esos datos para realizar el proceso de selección, ya que si no lo hacen no se podrían beneficiar de la excepción del consentimiento contenida en la normativa sobre protección de datos de carácter personal. De hecho, en el caso de los algoritmos se ponen en relación mucha información personal y el RGPD ha establecido que la elaboración de perfiles automatizados[68] como único medio de valoración para tomar una decisión, sin que haya intervenido ninguna persona sólo es admitido en dos situaciones: cuando la decisión es necesaria (es decir, no debe haber ninguna otra manera de lograr el mismo objetivo) para celebrar o ejecutar un contrato; o cuando se ha consentido explícitamente.

En ambos casos, la decisión adoptada debe garantizar los derechos y libertades del candidato al empleo. La empresa u organización debe, como mínimo, informar acerca del derecho a obtener intervención humana y establecer los requisitos de procedimiento obligatorios[69].

En segundo lugar y, haciendo referencia a la segunda fase, perteneciente al proceso de selección, se trata de una fase en la que la empresa a través de entrevistas, o dinámicas de grupo, trata de recabar información detallada sobre las capacidades del candidato, lo que se traduce en la obtención de más datos personales. En esta fase se deberá informar al candidato que el tratamiento de sus datos personales está destinado exclusivamente al proceso de selección. Además, la información proporcionada debe ser detallada, se incluirá, por ejemplo, la identificación del encargado del tratamiento, los derechos que le asisten, como la supresión de sus datos al final del proceso.

Por otro lado, en el caso de que la empresa quisiera conservar los datos del candidato para incluirlos en una bolsa de trabajo o para enviarlo a otra empresa del grupo, en la que pueda encajar su candidatura, deberá solicitar el consentimiento del candidato, ya que, finalizado el proceso de selección decae la licitud del tratamiento. Finalmente cabe la posibilidad que una vez finalizado el proceso de selección se solicite a la empresa la prueba de que efectivamente cumplió con el deber de información, por este motivo, es aconsejable que estas actuaciones queden documentadas[70].

---

[67] ORTEGA JIMÉNEZ, A.: "Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de datos de la UE", *Revista Española de Derecho del Trabajo*, núm. 216/2019.

[68] Art. 4.4 RGPD: *"elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física".*

[69] Por su parte, el considerando 71 del RGPD, de modo similar al apartado primero del artículo 22 del mismo Reglamento, establece que el interesado tendrá derecho a no ser objeto de una decisión que conllevé la evaluación de aspectos personales que le conciernen y que se ampare de modo exclusivo en el tratamiento de forma automatizada8, produciendo efectos jurídicos en dicho interesado o afectando le de un modo significativo de una forma semejante.

[70] ORTEGA JIMÉNEZ, A.: "Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo reglamento general de protección de los datos de la UE", *Revista Española de Derecho del Trabajo*, núm. 216/2019.

4.3. Algunas notas acerca de las cesiones de datos en los procesos de búsqueda de empleo[71]

Ahora bien, como se ha comentado la inserción de datos en las plataformas digitales de empleo y en los denominados sistemas de selección 4.0 implica que la información pueda estar siendo cedida a un tercero de un país extranjero. En estos casos si esa cesión tiene ese propósito relacionado con la búsqueda de empleo que, ciertamente, es la intención que tiene el usuario al incluir su información personal y profesional en la herramienta tecnológica que fuere, se estaría aceptando esta premisa legal. El problema se plantea cuando las comunicaciones se producen a países que no cuentan con un sistema equivalente de protección. Para estos casos la propia normativa europea sobre protección de datos explica de forma detallada cómo deberán de realizarse esas cesiones para cumplir con un nivel adecuado de protección estableciendo garantías que justifican esa protección e incluso la autorización de la AEPD si esas garantías tan sólo se han podido certificar a través de cláusulas contractuales entre el responsable o el encargado y el responsable, y el encargado y subencargado, que no hayan sido adoptadas por la Comisión Europea o de disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados[72].

La importancia que han adquirido las redes sociales en las fases previas de contratación como medio que facilita la incorporación de los desempleados al mercado de trabajo, debido al acceso que tienen las empresas oferentes de empleo a multitud de datos profesionales de los potenciales candidatos. No obstante, su funcionalidad puede contribuir a la conservación de los datos de forma demasiado prolongada en el tiempo, por ese motivo el art. 94 de la LOPDGDD[73] regula el *"Derecho al olvido en servicios de redes sociales y servicios equivalentes"*, recogiendo el derecho de toda persona a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes, cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información[74].

Como novedad se reconoce al interesado la portabilidad de los datos, es decir, el derecho a recibir los datos personales proporcionados a un responsable, *«en un formato estructurado, de uso común y lectura mecánica»*. Pero esto no se queda aquí, porque estos datos se podrán transmitir, a su vez, a otro responsable. Sobre esta posibilidad de portar datos también tendrá que ser informado el titular del dato. Cuando el titular de la información solicite esta portabilidad el responsable facilitará información a sus

[71] Véase, GARCÍA COCA, O.: "Las distintas cesiones…", op.cit. 733-768.

[72] Fuente: https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html

[73] Art. 94 1 y 2 LOPDGDD: *«1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes. 2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información».*

[74] Por primera vez reconocido en la STJUE de 13 de mayo de 2014 de la Gran Sala del TJUE para el asunto C-131/12 Google España. Esta sentencia supuso que el interesado puede solicitar que se bloqueen en las listas de resultados de los buscadores, los vínculos que conduzcan a informaciones que le afecten y que resulten obsoletas, incompletas, erróneas, falsas o irrelevantes y no sean de interés público, entre otras razones.

actuaciones, sin dilación indebida y, en cualquier caso, en el plazo de un mes desde la recepción, el período puede ampliarse a un máximo de tres en los casos complejos. En este caso, será necesario informar al interesado de las razones de la demora. Lo que sí que queda claro es que el responsable no puede dejar una solicitud sin respuesta. Entre las premisas informativas sobre el tratamiento de datos no se incluye la obligación de advertir las posibles transferencias internacionales de datos que se puedan realizar.

BIBLIOGRAFIA

ALASTRUEY, R.: *Empleo 2.0*, Editorial UOC, 2009.

ALUJAS RUIZ, J.A.: "El Servicio Público de Empleo y su labor como intermediario en el mercado de trabajo en España", *Cuadernos de Ciencias Económicas y Empresariales*, núm. 53, 2007

CANÓS DARÓS, L., CAÑO ALEGRE, C., GONZÁLEZ PÉREZ, B.: Algunos algoritmos de ordenación para el proceso de selección de personal, X Congreso de Ingeniería de Organización: Valencia, 7-8 de septiembre, 2006.

CLIMENT-RODRÍGUEZ, J. A., NAVARRO-ABAL, Y. Y ORTEGA-CAMPOS, E. "El videocurrículum-branding como recurso digital para el desarrollo de competencias de búsqueda de empleo en los futuros egresados"en VV.AA: I Congreso Virtual Internacional sobre Innovación Pedagógica y Praxis Educativa INNOVAGOGÍA 2012.

CLIMENT-RODRÍGUEZ, J. A., NAVARRO-ABAL. Y.: "Oficinas virtuales de Empleo. El reto de universalizar los servicios públicos de empleo", *Revista Trabajo* núm. 24, 2011.

DUNIA TALLEDA, MARC TUDÓ, BERNAT RODRIGO, ALBA NEBOT: "La evolución del curriculum vitae", *Capital humano: revista para la integración y desarrollo de los recursos humanos*, Año nº 30, Nº Extra 323, 2017.

GARCÍA COCA, O. La protección de datos de carácter personal en los procesos de búsqueda de empleo, Laborum, 2016.

GARCÍA COCA, O.: "Las distintas cesiones de datos de carácter personal en la fase previa de contratación de trabajadores", en COLOMER HERNÁNDEZ I. (dir): *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Aranzadi, 2019.

GARCÍA MURCIA, J. Y RODRÍGUEZ CARDO, I.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo*, núm. 216, 2019.

GARCÍA SALAS, A.I.: *Necesidades empresariales y derechos fundamentales de los trabajadores*, Lex Nova, 2016.

HOLPE, J. "Incorporate inbound recruiting marketing into your recruitment strategy", *Recruiting & Retaining*, Volume 17, issue 8, 2015.

LEE, I., "E-recruiting: Opportunities and challenges", *Information Management*, vol. 19, núm. 3-4, 2006,

LUQUERO, M. "Redes sociales y procesos de selección", *Capital humano: revista para la integración y desarrollo de los recursos humanos*, núm. 284, 2014.

MORATO GARCÍA, R.: "El impacto de las redes sociales virtuales en los procesos de selección de trabajadores" Comunicación presentada al X Congreso Europeo de Derecho del Trabajo y de la Seguridad Social, Sevilla, 2011

ORTEGA JIMÉNEZ, A.: "Cuestiones prácticas laborales en materia de protección de datos de carácter personal tras el nuevo Reglamento General de protección de datos de la UE", *Revista Española de Derecho del Trabajo*, núm. 216/2019.

RUBIO, A. *Ganarse el puesto y superar con éxito el período de prueba*, Díaz de Santos, 2008.

SÁNCHEZ-RODAS NAVARRO, C.: "La orientación e intermediación directa en el empleo", *Revista Temas Laborales*, núm. 125, 2014.

SEMPERE NAVARRO, A.V.: "Contrato laboral y tecnologías novedosas", *Actualidad Jurídica Aranzadi* núm. 912, 2015.

SERENO DOMINGO, A. "Nanociencia y nanotecnología: aspectos generales", *Fundación General de la Universidad Autónoma de Madrid*, 2009.

TELLO DÍAZ L; "Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook", *Revista Científica de Educomunicación*, 2013.

UNIQUE: "Sobre el uso de las redes sociales y profesionales como fuentes de reclutamiento y selección de personal", *Revista Capital Humano*, núm. 248, 2010

VV.AA. "La generación y el potencial de transferibilidad del curriculum vitae en formato audiovisual", *Revista Tecnología, Ciencia y Educación,* núm. 13, 2019.

VV.AA. "La selección del personal con un algoritmo genético borroso", *Investigaciones Europeas de Dirección y Economía de la Empresa* Vol. 2, num.2, 1996

RESUMEN La selección de trabajadores se sigue presentando como elemento primordial para una correcta inserción del trabajador en el mercado de trabajo. Además de ser una herramienta que colabora en el acercamiento a los distintos tipos de candidatos para poder valorar cual es el que mejor se adapta a las necesidades de la empresa, si se plantea bien puede considerarse como un mecanismo que evita las colocaciones arbitrarias y discrecionales por parte del empresario. Lógicamente, los sistemas de selección han ido experimentando cambios, cada vez más acentuados, para adaptarse a las necesidades de un mercado de trabajo estigmatizado por la digitalización y por técnicas que generen inmediatez y agilidad, también en los momentos previos a la contratación de trabajadores. Ante esta situación se puede decir que el aumento de usos de sistemas tecnológicos ha ayudado bastante en la selección de personal, pero también ha interferido en la salvaguarda del derecho a la protección de datos de carácter personal, pudiendo el titular perder el dominio de su información personal si no se cumplen, de forma diligente, las indicaciones y obligaciones de la normativa sobre protección de datos.

A pesar de que la promulgación del Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, por el que se deroga la Directiva 95/46/CE[a] y de la transposición del mismo a nuestro derecho interno por medio de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[b], ha mejorado algo el panorama de desprotección generado en el ámbito de las relaciones de trabajo respecto a los datos, en este caso, de los demandantes de empleo cierto es que, aún existen algunas lagunas respecto al tratamiento de esa información. Es por ello que se pretende hacer un recorrido por los medios de captación de datos de candidatos que ofrecen su información personal a las distintas empresas que proponen empleos o a todas aquellas que actúan como intermediarias, según lo establecido en el art. 32 de la Ley de Empleo[c].

Es más que evidente que cualquier método de selección de trabajadores, de una u otra forma, tratan datos de carácter personal de los demandantes de empleo si se atiende a la definición de los mismos dada en el RGPD[d] y, por tanto, deben cumplir las premisas legales para no contravenir ni perjudicar a los demandantes de empleo. En ese sentido, la creación de esos ficheros con datos constituye lo que se denomina por la norma tratamiento de datos, independientemente de que se encuentren en soporte físico o telemático. En la mayoría de los casos se produce una digitalización de la información, no sólo porque se recogen y archivan a través de plataformas basadas en sistemas de selección 4.0, sino también porque los propios seleccionadores de personal crean bases de datos informatizadas a raíz de los datos que les transmiten en formato papel.

[a] DOUE L119/1 de 4 de mayo de 2016.

[b] BOE núm. 294 de 6 de diciembre de 2018.

[c] Art. 32 Ley de Empleo: *"A efectos del Sistema Nacional de Empleo, la intermediación en el mercado de trabajo se realizará a través de: a) Los servicios públicos de empleo. b) Las agencias de colocación. c) Aquellos otros servicios que reglamentariamente se determinen para los trabajadores en el exterior".*

[d] Art. 4.1 RGPD: *"datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"*

Ante esta situación se hace necesario hacer un análisis desde dos perspectivas; de un lado, la forma de captación, registro y selección; y de otro, las consecuencias que ese modo de procesar datos de los demandantes de empleo conlleva para el derecho a la protección de datos de carácter personal. También alcanza gran notoriedad las cesiones de datos que realizan todos los sujetos que intervienen en los procesos de selección de trabajadores. En este punto es importante tratar todo lo relacionado con aquellas comunicaciones de datos que se producen en las plataformas digitales, si estas son gestionadas por empresas que no se encuentran ubicados en los países que la norma considera que tienen un nivel equivalente de protección, en lo que a los datos personales se refiere.

Para realizar este estudio se han analizado las técnicas de selección desde la óptica de los departamentos de recursos humanos para intentar dar una visión lo más concreta posible sobre cómo la digitalización de los procesos de reclutamiento y selección de trabajadores ha llegado a ellos, y que mecanismos son los que más se utilizan y tienen mejores resultados. Una vez realizado este análisis, como se ha comentado, se informa acerca de las consecuencias de la utilización de esos sistemas, teniendo en cuenta lo recogido en la normativa sobre protección de datos, así como lo contenido en otras resoluciones de instituciones que dan respuesta a problemas relacionados con este derecho.

En definitiva, el tratamiento de datos de los demandantes de empleo debe estar protegido por las premisas del RGPD y la LOPDGDD, aunque sería necesaria una regulación más específica que resolviera y diera respuesta a los supuestos que se plantean en las relaciones de trabajo entorno a la salvaguarda de la información personal de los candidatos de empleo. En este punto, algo se ha mejorado con la nueva regulación, pero ni mucho menos ha servido para despejar interrogantes y tratar estos datos personales conforme a las pautas legalmente establecidas.

Palabras clave: Información personal; digitalización; selección; empleo; protección de datos.

ABSTRACT The selection of workers continues to be presented as a fundamental element for the correct insertion of the worker in the labor market. In addition to being a tool that collaborates in the approach to the different types of candidates to be able to assess which is the one that best suits the needs of the company, if it is well considered it can be considered as a mechanism that avoids arbitrary and discretionary placements. part of the entrepreneur. Logically, the selection systems have been undergoing changes, increasingly accentuated, to adapt to the needs of a labor market stigmatized by digitalization and techniques that generate immediacy and agility, also in the moments before hiring workers. Given this situation, it can be said that the increase in the use of technological systems has helped a lot in the selection of personnel, but it has also interfered in the safeguarding of the right to the protection of personal data, and the holder may lose the domain of his information personnel if the instructions and obligations of the data protection regulations are not met diligently.

Despite the promulgation of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 regarding the protection of natural persons with regard to the processing of personal data and the free movement of this data, which repeals Directive 95/46 / EC[a] and its transposition into our domestic law through Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights[b], The lack of protection generated in the field of labor relations with respect to the data has improved somewhat, in this case, it is true that there are still some gaps regarding the treatment of this information. That is why it is intended to take a tour of the means of collecting data from candidates who offer their personal information to the different companies that propose jobs or to all those that act as intermediaries, as established in art. 32 of the Employment Law[c].

It is more than evident that any method of selecting workers, in one way or another, treat personal data of job seekers if they meet the definition of the same given in the RGPD[d] and, therefore, must comply with the premises legal not to contravene or harm job seekers. In that sense, the creation of these files with data constitutes what is called by the data processing standard, regardless of whether they are in physical or telematic support. In most cases, the information is digitized, not only because they are collected and archived through platforms based on 4.0 selection systems, but also because the personnel recruiters themselves create computerized databases based on the data that transmit them in paper format.

Given this situation it is necessary to make an analysis from two perspectives; on the one hand, the form of capture, registration and selection; and on the other, the consequences that this way of processing data of job seekers entails for the right to the protection of personal data. The transfer of data made by all the subjects involved in the selection processes of workers also reaches great notoriety. At this point it is important to deal with everything related to data communications that occur on digital platforms, if they are managed by companies that are not located in countries that the standard considers to have an equivalent level of protection, in terms of which refers to personal data.

[a] DOUE L119/1 de 4 de mayo de 2016.

[b] BOE núm. 294 de 6 de diciembre de 2018

[c] Art. 32 Employment Law: *"For the purposes of the National Employment System, intermediation in the labor market will be carried out through: a) Public employment services. b) Employment agencies. c) Those other services that are determined by regulation for workers abroad ".*

[d] Art. 4.1 RGPD: *"personal data": all information about an identified or identifiable natural person ("the interested party"); An identifiable natural person shall be deemed to be any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of identity. physical, physiological, genetic, psychic, economic, cultural or social of said person".*

To carry out this study, the selection techniques have been analyzed from the perspective of the human resources departments to try to give a vision as concrete as possible about how the digitalization of the recruitment and selection processes of workers has reached them, and what mechanisms They are the most used and have better results. Once this analysis has been carried out, as mentioned, the consequences of the use of these systems are informed, taking into account what is included in the data protection regulations, as well as what is contained in other resolutions of institutions that respond to Problems related to this right.

In short, the data processing of job seekers must be protected by the premises of the GDPR and the LOPDGDD, although a more specific regulation would be necessary to solve and respond to the assumptions that arise in the labor relations around the Safeguarding the personal information of job candidates. At this point, something has been improved with the new regulation, but it has not served to clear questions and treat this personal data according to the legally established guidelines.

Keywords: Personal information; digitalization; selection; employment; data protection.

Sistema de denuncias y protección de datos personales

Breaches procedures and data protection

ROSARIO CRISTÓBAL RONCERO*

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantías de los Derechos digitales (en adelante, LOPD) se dicta para adaptar el ordenamiento jurídico español al Reglamento UE 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[1].

Esta Ley, además de regular los derechos a la intimidad y uso de dispositivos digitales en el ámbito laboral (art. 87), a la desconexión digital en el ámbito laboral (art. 88), a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo (art. 89), a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral (art. 90) y los derechos digitales en la negociación colectivo, introduce un sistema de información de denuncias internas, a cuyo tenor se establece una especial protección para los denunciantes que también va a desplegar efectos en el ámbito laboral. Estos sistemas de recepción y conocimiento de infracciones se encuadran bajo las exigencias de la legislación aplicable en materia de protección de datos, siempre que traten denuncias referidas a normas, fundamentos o principios, cuyo incumplimiento tenga consecuencias efectivas sobre la pervivencia de la relación contractual entre la empresa y el denunciado.

El art. 24 LOPD regula un sistema de denuncias internas desde la perspectiva del derecho de protección de datos personales, referido a los límites de acceso a los datos de las personas, la confidencialidad del tratamiento o la limitación temporal en orden a la conservación de las denuncias.

Recientemente, se ha regulado la protección a los denunciantes (*whistelblowing)* en el ámbito de la Unión Europea. En efecto, la Directiva UE2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre, relativa a la protección de las personas que informan sobre infracciones del Derecho de la Unión (en adelante, DPII) configura, de forma profusa, un sistema de canales de denuncia, externo e interno, que protege la confidencialidad, el anonimato y la no represalia del denunciante[2]. La Directiva entró en vigor el pasado 17 de diciembre, si bien el plazo de

* Profª Titular de Derecho del Trabajo y de la Seguridad Social. Universidad Complutense de Madrid.

[1] DOUE núm. 119, de 4 de mayo de 2016.

[2] Siguiendo las Resoluciones del Parlamento Europeo de 20 de enero sobre la Función de los denunciantes en la protección de los intereses financieros de la Unión y la de 24 de octubre de 2017 sobre Medidas legítimas para la protección de los denunciantes de infracciones que actúan en aras del interés público, en abril de 2018 la Comisión europea presentó la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas que informen sobre infracciones del Derecho, que llevan después a la aprobación de la Presente Directiva.

trasposición a nuestro Ordenamiento concluye el 17 de diciembre de 2021. Por tanto, los Estados Miembros disponen de dos años para adaptar, con amplio margen, sus legislaciones internas al contenido mínimo previsto por la Directiva.

Estamos, pues, ante una norma esperada, un elemento más en el engranaje normativo que el legislador comunitario –pero también, el nacional– propone para articular la obligación de establecer canales de denuncia y a su vez medidas que garanticen la protección de los denunciantes. La principal virtualidad de la Directiva es que, con su sola existencia, despeja los debates sobre los cauces del sistema de denuncia, aportando luz en un contexto absolutamente necesitado de seguridad jurídica. Se busca, en definitiva, reforzar la protección del *whistelblower* y el ejercicio del derecho a la libertad de expresión e información reconocido en al art. 10 CEDH y en el art. 11 de la Carta de los Derechos Fundamentales y con ello se aspira a incrementar su actuación "en el descubrimiento de prácticas ilícitas o delictivas que tengan un impacto en el derecho de la Unión Europeo, sus políticas o presupuesto"[3].

En conclusión, esta Directiva contribuye a una mejor implementación del Derecho de la Unión Europea con un alcance muy amplio en el ámbito del *compliance*, si bien nosotros abordaremos de forma específica las medidas de protección del informante en el ámbito laboral.

1. ÁMBITO DE PROTECCIÓN

El Capítulo I recoge las reglas de configuración sobre el alcance material y el ámbito personal de los "denunciantes" que informan sobre infracciones del Derecho de la Unión.

Asimismo, en este Capítulo se disponen las definiciones que se ofrecen en el marco de esta Directiva, en aras de determinar y garantizar la protección de los sujetos con ocasión de su actuación en el marco del *whistleblowing*. Muchas de estas definiciones son nuevas y algunas desconocidas para nuestro ordenamiento jurídico laboral. Sin duda, debe agradecerse la voluntad del legislador europeo por facilitarnos luz para entender el ámbito de aplicación y protección de los informantes y, sobre todo, el alcance de sus garantías en el ejercicio y desarrollo de las relaciones laborales.

1.1. Ámbito de aplicación material

El art. 2 de la Directiva establece y define el ámbito de aplicación material a través de la delimitación de las infracciones. Así, se consideran infracciones del Derecho de la Unión "las acciones u omisiones que sean ilícitas y que estén relacionadas con los ámbitos de actuación de la Unión o que desvirtúen su objeto o finalidad"[4]. En concreto, se precisan los siguientes: contratación pública; servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo; seguridad de los productos; seguridad del transporte; protección del medio ambiente; protección contra las radiaciones y seguridad nuclear; seguridad de los alimentos y los piensos, salud animal y bienestar de los animales; salud pública; protección de los consumidores; y protección de la intimidad y los datos personales, y seguridad de las redes y los sistemas de información [art. 2.1 a) Directiva].

[3] L. Bachmaier Winter: "*Whistelblowing* europeo y compliance: la Directiva EU de 2019 relativa a la protección de las personas que reporten infracciones del Derecho de la Unión", *Diario La Ley*, núm. 9527, 2019, p. 3.

[4] El ámbito de la Directiva también se extiende a infracciones que afecten a los intereses financieros de la Unión, tal y como se definen en el artículo 325 del Tratado y tal y como se concretan en la correspondientes medidas de la Unión; e infracciones relativas al mercado interior (art. 26.2. TFUE), incluidas las infracciones de las normas en materia de competencia y ayudas estatales; y también en relación con actos que infrinjan las normas del impuesto sobre sociedades o con disposiciones cuya finalidad deba obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades [art. 2.1 a) Directiva].

Además, la Directiva se extiende a "todos aquellos ámbito no regulados en el marco de instrumentos sectoriales específicos que deben ser completados por la presente Directiva, de tal modo que sean conformes con las normas mínimas previstas en ellas" (Considerando 20). En este sentido, cabe plantearse si dentro del ámbito de la Directiva quedaría protegido la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual y el acoso por razón de sexo" [art. 4.2 e) ET]. Como tendremos oportunidad de analizar, las represalias, por el hecho de la denuncia, se deben considerar como vulneración de un derecho fundamental. En este contexto, el acoso en sus distintas formas ocupa un lugar preferente de protección, sobre todo, cuando el trabajador se sienta discriminado, vejado o acosado por el empresario, por sus superiores, por otros trabajadores o por terceros, como consecuencia de la denuncia de irregularidades o por la denuncia del propio acoso[5].

El ámbito de aplicación de la Directiva no afecta, sin embargo, al ejercicio de los derechos de los trabajadores a consultar a sus representantes o sindicatos, ni a las medidas perjudiciales injustificadas derivadas de tales consultas ni a la autonomía de los interlocutores sociales a celebrar convenios colectivos (art. 3.4 DPII)[6].

1.2. Ámbito de aplicación personal

Uno de los aspectos más complicados que presenta la Directiva por la extensión de su alcance subjetivo, es el que tiene que ver con la determinación y concreción del ámbito de aplicación personal.

En efecto, se protege no sólo a los denunciantes del sector público sino también a los del sector privado, que comuniquen o revelen públicamente información sobre infracciones del Derecho de la Unión, que se hayan conocido en un contexto laboral, siempre que tuvieran motivos razonables para creer que la revelación era veraz en el momento de la denuncia[7]. En este sentido, se precisa que se aplicará, como mínimo a:

– las personas que tengan la condición de trabajadores en el sentido del artículo 45. 1 TFUE. Respecto del concepto comunitario de trabajador, hay que subrayar, en consonancia con la jurisprudencia del TJUE, que se incluye a los trabajadores por cuenta ajena en el sentido del art. 1.1 ET, ya sean a trabajadores con contrato indefinido, temporal, a tiempo completo o a tiempo parcial, pero también se consideran incluidas dentro del concepto de trabajador las relaciones laborales atípicas mediante la técnica de las relaciones laborales especiales, así como los funcionarios, empleados del servicio público y cualquier otra personas que trabaje en el sector público[8].

[5] En el derecho alemán esta garantía viene, específicamente, establecida en el § 16. 1 de la *Allgemeines Gleichbehandlungsgesetz*, AGG, Ley alemana de Igualdad de trato, que prevé una "garantía de indemnidad en sentido estricto que sanciona con nulidad por discriminatorio las represalias frente a las quejas de todo tipo formuladas en relación con el principio de igualdad de trato", en R. CRISTÓBAL RONCERO: Igualdad de mujeres y hombres: Un estudio de Derecho comparado", *REDT* 2010, núm. 147, p. 548. En nuestro país, el art. 48 de la Ley 2/2007 para la Igualdad efectiva de mujeres y hombres " obliga a las empresas a arbitrar procedimientos específicos para la prevención del acoso sexual y por razón de sexo y para dar cauce a la denuncias o reclamaciones que puedan formular quienes hayan sido objeto del mismo".

[6] Ni tampoco a la protección del secreto médico y del secreto profesional en la relación cliente-abogado, el secreto de las deliberaciones judiciales y las normas sobre protección y confidencialidad establecidas a nivel nacional en la ley de enjuiciamiento criminal (art. 3.3 DPII)

[7] Este requisito se construye sobre un triple presupuesto: 1.-Salvaguarda frente a denuncias malintencionadas, frívolas o abusivas para garantizar que quienes, en el momento de denunciar, comuniquen deliberada y conscientemente información incorrecta o engañosa no gocen de protección; 2.– El denunciante que comunique informaciones inexactas sobre infracciones por error cometidos de buena fe no queda exento de protección; 3.– Irrelevancia de los motivos de los denunciantes al denunciar, en todo caso deben gozar de protección (considerando 32).

[8] En efecto, el concepto de trabajador en el ámbito del Derecho de la Unión Europea se apoya en la *vis attractiva* del Derecho del Trabajo que alcanza a los funcionarios "laboralizando su relación", en A. MONTOYA MELGAR: *Tendencias actuales del Derecho del Trabajo*, Ed. CEU, 2014, pág. 7.

– las personas que tengan la condición de trabajadores no asalariados, en el sentido del artículo 49 del TFUE; se incluye a los autónomos, voluntarios, trabajadores en prácticas sin remuneración, proveedores de servicios y "facilitadores" y personas relacionadas con los denunciantes que puedan sufrir represalias en un contexto laboral y las entidades jurídicas que sean propiedad del denunciante paras las que trabaje o mantenga cualquier otro tipo de relación laboral que asisten al denunciante.

– los accionistas y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;

Además, el ámbito de aplicación y protección de la Directiva se extiende a sujetos que no entran dentro de la categoría de trabajador. Alcanza a denunciantes que comunican o revelan información sobre infracciones obtenidas en el marco de una relación laboral extinguida, así como también al informante que denuncia infracciones obtenidas durante el proceso de selección de negociación precontractual. En definitiva, se aplica a trabajadores cuyo contrato de trabajo se ha extinguido o todavía no ha comenzado (art. 4 DPII).

Con ello, el legislador europeo otorga protección jurídica a todos aquellos que puedan ser objeto de represalias en el ámbito de las relaciones laborales *stricto sensu* o en el ámbito de la función pública, extendiéndose, además, a la protección a terceros personas jurídicas, físicas, como: familiares, compañeros de trabajad y "facilitadores", que por su vinculación con el denunciante pueden ser objeto de represalias (art. 4 DPII).

Por lo que se refiere a la protección y apoyo a los informantes, aquélla se vinculó, en un principio, a la actuación de buena fe del denunciante. Recuérdese que, a los efectos de la Directiva, el denunciante es "una persona física que comunica o revela públicamente información sobre infracciones obtenidas en el contexto de sus actividades laborales".

En la práctica resulta difícil deslindar si la denuncia está motivada por un interés público o personal. De hecho, la Directiva 2019/1937 elimina el requisito de la buena fe en la protección a los *whistleblowers*, de forma que las medidas de protección se aplican a los denunciantes que "tengan motivos fundados para pensar que la información notificada es veraz en el momento de la denuncia y que es susceptible de protección. Por tanto, las razones que llevan al informante a canalizar una denuncia se tornan irrelevantes, "siempre que los hechos denunciados sean ciertos o el denunciante estuviera en la creencia razonable de que lo eran"[9].

En definitiva, la Directiva amplía las garantías a una serie sujetos, con mayor o menor vinculación en el contexto laboral, para asentar las bases mínimas de protección a todos los concernidos y afectados por la información de infracciones del Derecho de la Unión.

2. CANALES DE DENUNCIA

La obligación de establecer canales de denuncia constituye uno de los pilares fundamentales sobre los que se asienta el espíritu de la Directiva sobre protección de las personas que informen infracciones del Derecho de la Unión Europea. En primer lugar, se establece el canal de denuncia interna, es decir, se invita a los informantes para que acudan a este medio como vía preferente para tratar la infracción dentro de la organización y sin riesgo a represalias; y en segundo lugar, se propone, el sistema de denuncia externas, como mecanismo subsidiario que persigue idénticos objetivos y garantías, si bien con posible repercusión *ad extram* de lo acontecido en la empresa. Es relevante advertir, no obstante, que no existe deber de denuncia, pero sí se obliga a la creación e implantación de estos cauces y a que se confiera, en todo caso, protección al denunciante.

[9] J.R. MERCADER UGUINA: *Protección de datos en la relaciones laborales*, Ed. Francis Lefebvre, Madrid, 2018, p. 165.

Como principio general para la detección y prevención de infracciones del Derecho de la Unión Europea se pretende que la información pertinente llegue de manera rápida a quienes están más próximos a la fuente del problema y tienen más posibilidades de investigarlo y competencias para remediarlo.

El art. 24 LOPD regula también los sistemas de denuncias –aunque en nuestro ordenamiento jurídico sólo se refiere a los internos– para conocer la realización de posibles irregularidades dentro de la empresa no sólo desde la perspectiva de la protección de datos, pues alcanza también a las medidas que se adopten para garantizar y salvaguardar dicha protección. En efecto, estos canales permiten que la organización empresarial o a la entidad pública actúe e intervenga con un doble objetivo: por un lado, conocer de forma inmediata las infracciones cometidas, y por otro, para detectar los fallos en la prevención y reaccionar con celeridad frente a las irregularidades e infracciones.

Las entidades jurídicas de los sectores públicos y privados tienen potestad para implantar la creación y seguimiento de canales de denuncias internos (art. 8 DPI).

Mientras que la Directiva comunitaria dispone la obligación de instaurar estos sistemas en las empresas privadas que tenga 50 empleados o más y en todas las entidades públicas con la salvedad de exención a los municipios "pequeños" –menos de 10.000 habitantes– y entidades con menos de 50 empleados, el art. 24 LOPD se limita a disponer su licitud sin establecer una obligación específica de organizar e incorporar estos canales ni en el ámbito privado (art. 24.1) ni en las Administración públicas (art. 24.5)[10]. En este sentido, nuestro ordenamiento jurídico tendrá que adoptar las medidas necesarias para garantizar la obligatoriedad de imposición de los sistemas de denuncia en uno y en otro caso. Para ello, habrá que imponer a los empresarios la obligación de implantar canales de denuncia objetivos y fiables, de forma que "la información recogida y tratada se trasmita solo a las personas responsables de la investigación" y, en todo caso, se garantice la adopción de las medidas necesarias para realizar el seguimiento e investigación de los hechos denunciados[11].

La directiva regula tres tipos de canales de denuncia de infracciones: 1) internos, dentro de una entidad jurídica pública o privada, 2) externos, dependientes de las autoridades competentes que designen los Estados miembros y 3) la revelación pública, consistente en la puesta a disposición del público de información sobre infracciones.

1.– Canales de denuncia internos en una entidad jurídica pública o privada

Los canales de denuncia internos deben implantarse previa consulta con los interlocutores sociales, cuando así lo establezca el derecho nacional (art. 8 DPII). Nada dice el art. 24 LOPD a este respecto, pero cabe augurar su necesaria participación en el diseño y configuración de estos sistemas.

En efecto, entre las competencias que el legislador estatutario otorga a la representación de los trabajadores en la empresa se encuentra la de su intervención en los procesos de consulta y negociación. Una posible opción es que se configure y se organice el canal de denuncias mediante negociación colectiva o acuerdo de empresa o, en su defecto, a través

[10] Se impone una obligación de mínimos. Por tanto, la Ley que transponga el contenido de la Directiva podrá impulsar o directamente establecer la obligación de creación de estos sistemas de denuncias e incluso extenderlo, a empresas de menor tamaño estableciendo requisitos menos exigentes que la propia Directiva, pero "siempre garantizando la confidencialidad y el seguimiento diligente de la denuncia" (considerando 49)

[11] En cierto, modo el párrafo 4º del art. 23 LOPD ya precisa que se deben adoptar las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.

de la decisión del empresario previa consulta con los representantes legales en la empresa.

Para conseguir su eficacia real, la consulta debería permitir a los representantes de los trabajadores sobre la base de la información recibida reunirse con el empresario, contrastar sus puntos de vista y opiniones con objeto de poder llegar a un acuerdo sobre la implantación y configuración de los canales de denuncia.

En todo caso, su actuación se debe garantizar conforme al deber de buena fe con vistas a la consecución de un acuerdo y al de de confidencialidad en relación con la información que, en legítimo interés de la empresa, del centro de trabajo o de los informantes les haya sido expresamente comunicada con carácter reservado. En este sentido, se ha pronunciado el Tribunal Constitucional, en su sentencia de 11 de noviembre de 2002[12], al declarar que ningún tipo de documento entregado por la empresa al Comité podrá ser utilizado ni fuera del ámbito estricto de aquélla ni tampoco para fines distintos de los que motivaron su entrega. Y, añade el Alto Tribunal, que tal obligación "subsistirá incluso tras la expiración del mandato e independientemente del lugar en que se encuentren de conformidad con lo establecido en el art. 65.2 y 65.3 ET"[13].

Ahora bien, este deber de sigilo debe cohonestarse con la obligación de la representación legal de los trabajadores de informar a sus representados en todos los temas y cuestiones señalados en el art. 64.7.e) ET en cuanto directa o indirectamente tengan o puedan tener repercusión en las relaciones laborales[14], tal y como señala el texto de la propia Directiva.

Un aspecto relevante de la Directiva 2019/1037 es que, además de obligar a que se establezcan procedimientos internos de denuncia, exige la consignación de un contenido mínimo en estos canales de denuncia. En efecto, se establecen unas exigencias mínimas que deben cumplir todos los Estados miembros[15] y que, en cierta medida, favorecen la eficacia de este sistema de protección de las personas que informen sobre derechos de la Unión Europea. En este sentido, se han propuesto como posibles requisitos, entre otros: "el apoyo por parte de la dirección; la información previa a los destinatarios del mecanismo, la accesibilidad, proporcionalidad y documentación del sistema, la independencia del órgano de gestión, sistema de infracciones y sanciones y la protección del denunciante o informador"[16]. En concreto, la Directiva establece que deberán incluir, al menos, las siguientes exigencias:

a) Confidencialidad.– Los canales para recibir denuncias deben estar diseñados y gestionados de forma que se garantice, en todo caso, la confidencialidad de la identidad del denunciante y/o de cualquier tercero que se mencione en la denuncia. En este sentido, el deber de confidencialidad debe alcanzar también a los no afectados, de forma

[12] STC 213/2002 (RTC 2002, 213)

[13] Sin embargo, la empresa no estará obligada, si bien de manera excepcional, a comunicar aquellas informaciones específicas relacionadas con secretos industriales, financieros o comerciales cuya divulgación pudiera, según criterios objetivos (STS 13-02-1989 y STSJ Castilla La Mancha 24-11-2005, rec. 1588/05), obstaculizar el funcionamiento de la empresa o del centro de trabajo u ocasionar graves perjuicios en su estabilidad económica, aunque la excepción mencionada no abarca aquellos datos que tengan relación con el volumen de empleo en la empresa (art. 65.4 ET). Por consiguiente, cuando la representación legal de los trabajadores acredite la pertinencia de la documentación complementaria, la empresa solo podrá negarse a su aportación, cuando concurran las circunstancias mencionadas, cuya prueba le corresponderá, de conformidad con lo dispuesto en el art. 217.3 LEC, salvo que se trate de datos relacionados con el volumen de empleo de la empresa. La negativa infundada a aportar documentación pertinente constituye falta grave, de conformidad con lo dispuesto en el art. 7.7 RDL 5/2000, aunque podría llegar a calificarse como falta muy grave (art. 8.3 RDL 5/2000), de acreditarse, que dicha decisión empresarial impidió que el período de consultas alcanzase sus fines (STC 213/2002).

[14] STSJ Murcia 23-07-2001, rec.617/01, resol. 1107/01. En: https://app.vlex.com/#vid/17456032.

[15] Lo que contribuirá a un mayor alcance de las denuncias y a una esperada uniformidad de sistemas dentro de la UE.

[16] J.F. Lousada Arochena: "Sistemas de denuncias internas (*whistleblowing*) y derechos fundamentales en el trabajo", *Trabajo y Derecho,* núm. 52, 2019, pág.3.

que su acceso a la información sea del todo imposible al tratarse de personal "no autorizado".

b) Comunicación escrita.– Se debe comunicar al denunciante, por escrito y con acuse de recibo, la recepción de la denuncia en un plazo de siete días.

c) Información, clara y fácil, sobre los procedimiento de denuncias a los posibles denunciantes que deben incluir no solo la existencia y/o conocimiento de esta vía de actuación, sino también las forma y procedimiento de acceso y utilización.

d) Órgano de gestión y seguimiento de la denuncia.– Para el desempeño de estas funciones se puede designar a un tercero externo o a un departamento, nombrado a tal efecto por la empresa, para entender de cuantas cuestiones les sean atribuidas. En principio, tienen señaladas competencias "ordinarias" o "simples", como son: la recepción de la denuncia, la comunicación con el denunciante, la solicitud de información adicional, y en todo caso, la contestación de la denuncia, que debe realizarse en un plazo razonable. A estos efectos, se distinguen dos plazos diferentes en función de si ha habido acuse de recibo o no. En caso afirmativo, la contestación no podrá ser "superior a tres meses a partir del acuse de recibo", y si éste no se remitió, será también "de tres meses, pero a partir del vencimiento del plazo de siete días después de hacerse la denuncia".

Además, el sistema de denuncias, consecuencia del carácter de confidencialidad del que se le ha dotado, ha dado origen a una modalidad especial de competencia, que puede llamarse "competencia reforzada", en virtud de la cual a la persona o departamento designados se les exige, además, un seguimiento diligente de la denuncia, incluso anónima, cuando así lo establezca el Derecho nacional.

La Directiva, al igual que sucede durante el seguimiento de la denuncia reforzada y diligente, deja a la discrecionalidad de los Estados miembros la aceptación o no de denuncias anónimas (art. 5.2. DPII). En todo caso, podrán presentarse por escrito en formato electrónico o en papel o de palabra, por vía telefónica, grabadas o no grabadas, o en reuniones presenciales con la personas o departamento designados para gestionar y seguir la denuncia, cuando así lo solicite el informante (art. 9.2 DPII).

En relación con la aceptación denuncias anónimas, el art. 24 LOPD acepta la licitud de canales que aceptan y tramitan denuncias en las que se desconoce la identidad del informante. Por tanto, se garantiza el anonimato del denunciante sin que esta previsión legal quede exenta de problemas jurídicos detectados por la doctrina científica y por la práctica judicial.

2.– Canales de denuncia externos, dependientes de las autoridades competentes que designen los Estados miembros

Aunque se incentiva el uso de canales internos, es también posible presentar la denuncia a través de un sistema externo. Varias son las razones que se encargan de establecer precisiones sobre la posibilidad de optar por este canal. En primer lugar, la ausencia de implantación de un sistema interno de denuncias en la empresa o en la institución pública. En segundo lugar, la falta o insuficiencia de funcionamiento apropiado del sistema interno de la organización. En tercer lugar, las deficiencias en el desarrollo del procedimiento por inobservancia de los requisitos formales– por ejemplo, diligencia debida el seguimiento, adopción de medidas en el plazo establecido– y en fin, porque exista verdadero temor a represalia, al no poder esperar razonablemente que los canales internos funcionen de forma adecuada.

El capítulo III de la Directiva 2019/1937 (arts. 10-14 DPII) se ocupa de la regulación de los canales externos; exige, en todo caso, que sean independientes y autónomos, y garanti-

cen la exhaustividad, integridad y confidencialidad de la información (art. 12 DPII).

Al igual que sucede con los canales de denuncia internos, la Directiva incluye un contenido mínimo para el adecuado funcionamiento del sistema y, además, requiere que el personal que los gestione tenga formación específica. Por lo demás, las exigencias mínimas que deben reunir los procedimientos de denuncias externas son muy similares a las exigidas para los procedimientos externos: confidencialidad; comunicación escrita; información, clara y fácil; y designación de órganos de gestión y seguimiento de la denuncia.

Sin perjuicio de las razones que favorecen la opción de los canales de denuncia internos frente a los externos, el recurso a los procedimientos de denuncia externos no quedan supeditados al requisito previo de haber acudido, con anterioridad, a los canales internos, por lo que el denunciante podrá escoger si utiliza los cauces internos o formula la denuncia directamente ante un órgano externo (art. 10 DPII)

Como regla general, a la empresa le interesará que se acuda a los canales de denuncia internos y evitar las denuncias externas "por temor al riesgo reputacional". En este sentido, la Directiva también muestra preferencia por que se recurra, cuando sea posible y adecuado, a los canales internos con el fin de contribuir a fomentar la cultura de buena gobernanza y responsabilidad social. En efecto, la Directiva señala que "debe animarse a los denunciantes a utilizar en primer lugar los cauces internos e informar a su empleador (…), en particular, cuando piensen que la infracción puede resolverse de manera efectiva dentro de la organización, y siempre que el denunciante considere que el cauce interno no presenta riesgo de represalias"[17].

Ahora bien, esto no significa que el denunciante deba valorar en cada supuesto el riesgo de represalias para decidir si acude directamente a la vía externa o a los cauces de denuncia internos; ni tampoco cabe deducir que si acude directamente al cauce externo, esta decisión deba incidir en las medidas de protección que se le han de garantizar en todo caso[18]. Por tanto, el informante es libre de optar por una vía u otra. No obstante, el legislador le recuerda la buena práctica empresarial y sobre todo, la preferencia de opción por el canal interno si la infracción puede ser resuelta a través de esta vía (art. 7.1 DPII)

3.– La revelación pública

La revelación pública constituye la tercera vía de denuncia que dispone la Directiva 2019/1937. Está regulada en el Capítulo IV, en concreto, en el art. 15. Consiste en la puesta a disposición del público de información sobre infracciones. Cierto es que este supuesto puede quedar más alejado del ámbito de las relaciones laborales en la empresa privada no así de la instituciones públicas; de hecho, constituye un canal adicional de protección de las personas que informe sobre infracciones del Derecho de la Unión Europea.

Se puede acudir a la revelación pública, cuando se haya denunciado primero por canales internos o externos y la "persona informante" tenga motivos razonables para pensar:

- Que no se hayan tomado medidas al respecto en el plazo previsto para la contestación
- Que la infracción constituye un peligro inminente o manifiesto para el interés público, por ejemplo: situación de emergencia o riesgo de daños irreversibles.
- Que exista, en caso de denuncia externa, un riesgo de represalias o haya pocas probabilidades de que

[17] Considerando 47 Directiva 2019/1937.

[18] L. Bachmaier Winter: "Whistelblowing europeo y compliance: la Directiva EU de 2019 relativa a la protección de las personas que reporten infracciones del Derecho de la Unión", *cit.*, p. 9.

se dé un tratamiento efectivo a las circunstancias particulares del caso. Por ejemplo, que puedan ocultarse o destruirse las pruebas o que una autoridad esté en connivencia con el autor de la infracción o implicada en la infracción.

Este procedimiento no será de aplicación cuando una persona revele información directamente a la prensa con arreglo a las disposiciones nacionales específicas por las que establezca un sistema de protección relativo a la libertad de expresión e información.

3. PROTECCIÓN AL TRABAJADOR QUE DENUNCIA INFRACCIONES O IRREGULARIDADES EN EL ÁMBITO DE TRABAJO

Antes de que se apliquen las medidas de protección frente a posibles desagravios del trabajador por haber informado de determinadas irregularidades en el seno de la empresa o de la administración pública, el denunciante está obligado a creer en la veracidad de los hechos que denuncia y a proceder a la denuncia a través de los cauces previstos para ello (canal interno o externo, principalmente). El resultado positivo de estas comprobaciones acredita el cumplimiento del procedimiento de información por parte del denunciante, lo que permite que se activen las medidas de protección para prohibir todo tipo de represalias.

La principal medida de protección es la confidencialidad de la identidad del informante, salvo que exista consentimiento expreso por su parte (art. 16.1.DPII) o que la revelación de su identidad constituya una obligación necesaria y proporcionada en el marco de un proceso judicial. En este sentido, se exige que el sistema de denuncias garantice que sólo el órgano destinatario acceda a su identidad; precisamente para preservarla pero, sobre todo, para evitar que se tomen represalias frente al informante.

En efecto, el hecho de que un trabajador informe de cualquier irregularidad conlleva el tratamiento de los datos personales, de modo que se debe garantizar, por una parte, que la información recogida y tratada se transmita exclusivamente a las personas responsables de la investigación, y por otra, que se adopten las medidas necesarias para realizar el seguimiento e investigación de los hechos denunciados[19].

Por tanto, los sujetos que reciban esta información (personas o departamento designado al efecto), deben asegurar 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. El art. 24. 4 LOPD añade, a este respecto, que los datos personales deben conservarse en el sistema de denuncias por el tiempo imprescindible "para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados". En todo caso, transcurridos tres meses desde de la introducción de los datos, se debe proceder a supresión del sistema de denuncias[20].

Además del deber de confidencialidad, los denunciantes deben estar protegidos frente a todo tipo de represalias, ya sean directas o indirectas, que se tomen, alienten o toleren por el empresario, clientes o destinatarios de servicios y personas que trabajen por cuenta o en nombre de éstas, incluidos los compañeros de trabajo y directivos de las misma organización o de otras organizaciones en las que el denunciante esté en contacto en contexto de sus actividades.

El Capítulo VI de la Directiva 2019/1937 recoge las medidas de protección del informante en el ámbito laboral. Siguiendo la Recomendación del Consejo Europeo sobre

[19] S. Rodríguez Escanciano: *Derechos laborales digitales: garantía e interrogantes*, Ed. Aranzadi, 2019, pag. 115.

[20] "Salvo que la finalidad de la conservación sea dejar evidencia funcionamiento del modelo de prevención de la comisión de delito por la persona jurídica" (art. 24. 4 LOPD).

whistelblowers[21], se proponen, entre otras, las siguientes medidas: prohibición de represalias (art. 19), medidas de apoyo (art. 20), medidas de protección frente a represalias (art. 21), medidas para la protección de las personas afectadas (art. 22) y sanciones.

En definitiva, se establece una suerte de indemnidad que trata de garantizar una protección cualificada al trabajador que denuncia una irregularidad en el seno de la empresa. En este sentido, el legislador europeo se esfuerza por identificar todas aquellas situaciones que pudieran suponer un trato desfavorable para el trabajador, cuando la decisión disciplinaria del empresario sea consecuencia de la denuncia del trabajador.

Se incluyen tanto la amenaza de represalia como la tentativa de represalia, en forma de: a) suspensión, despido, destitución o medidas equivalentes; b) degradación o denegación de ascensos; c) cambio de puesto de trabajo, cambio de ubicación del lugar de trabajo, reducción salarial o cambio del horario de trabajo; d) denegación de formación; e) evaluación o referencias negativas con respecto a sus resultados laborales; f) imposición de cualquier medida disciplinaria, amonestación u otra sanción, incluidas las sanciones pecuniarias; g) coacciones, intimidaciones, acoso u ostracismo; h) discriminación, o trato desfavorable o injusto; i) no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; j) no renovación o terminación anticipada de un contrato de trabajo temporal; k) daños, incluidos a su reputación, en especial en los medios sociales, o pérdidas económicas, incluidas la pérdida de negocio y de ingresos; l) inclusión en listas negras sobre la base de un acuerdo sectorial, informal o formal, que pueda implicar que en el futuro la persona no vaya a encontrar empleo en dicho sector; m) terminación anticipada o anulación de contratos de bienes o servicios; n) anulación de una licencia o permiso; o) referencias médicas o psiquiátricas.

Desde la perspectiva europea se ofrece una protección amplia y adecuada, que debe vincularse a la exigencia general de que las represalias por el hecho de la denuncia se consideren una vulneración de un derecho fundamental o libertad pública[22]. En este sentido, consideramos que todos los actos "de represalia", consecuencia de la información de irregularidades transmitida por el denunciante, deberían reputarse nulos y sin efecto, tanto si consisten en decisiones unilaterales del empresario o como si proceden de un tercero del "contexto laboral". En esta línea el Tribunal Constitucional, en su STC 146/2019, de 25 de septiembre, declara vulnerado el derecho a la libertad de expresión del trabajador que es despedido disciplinariamente por criticar la gestión empresarial del centro de trabajo en el que prestaba servicios. Distingue entre el derecho a expresar y difundir libremente los pensamientos ideas y opiniones, del derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión [art. 20.1 a) y d) CE].

El Alto Tribunal nos recuerda su doctrina consolidada sobre el derecho que garantiza la libertad de expresión, cuyo objeto son los pensamientos, ideas y opiniones (concepto amplio que incluye las apreciaciones y los juicios de valor) y el derecho a comunicar información, que se refiere a la difusión de aquellos hechos que merecen ser considerados noticiables. Tal distinción entre pensamientos, ideas y opiniones, de un lado, y comunicación informativa de hechos, de otro, tiene una importancia decisiva para determinar la legitimidad del ejercicio de esas libertades, pues, «mientras los hechos son susceptibles de prueba, las opiniones o juicios de valor, por su misma naturaleza, no se prestan a una demostración de exacti-

[21] Protecting Whistleblowers, Council of Europe, Recommendation, CM/Rec(2014), en: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806fffd1

[22] J.F. Lousada Arochena: "Sistemas de denuncias internas (*whistleblowing*) y derechos fundamentales en el trabajo", *cit.*, pág 9.

tud, y ello hace que al que ejercita la libertad de expresión no le sea exigible la prueba de la verdad o diligencia en su averiguación, que condiciona, en cambio, la legitimidad del derecho de información» (FJ 4º STC 146/2019).

Por todo ello, el TC centra su enjuiciamiento en el marco del derecho a la libertad de expresión y rechaza la interpretación del derecho fundamental realizada por TSJ del País Vasco que, "al haber exigido que la crítica realizada no trascendiera más allá de la empresa, despojó al trabajador de la libertad de expresión que le reconoce el art. 20.1 a) CE, haciendo que tal derecho cediera ante un deber de lealtad entendido en términos absolutos de «sujeción indiferenciada del trabajador al interés empresarial» (SSTC 4/1996, de 16 de enero, FJ 4, y 227/2006, de 17 de julio, FJ 5) (FJ 6º STC 146/2019).

Ahora bien, la prohibición de represalia frente al denunciante no debe impedir la adopción de las medidas disciplinarias cuando la investigación interna determine que la comunicación sea falsa y que la persona que la ha realizado ha actuado de mala fe[23].

Así, lo ha entendido el TSJ de Andalucía, en sus sentencia de 15 de marzo de 2018, al no reconocer la vulneración del derecho a la indemnidad por la sanción a un trabajador que no cumple con una orden reiterada de la empresa para justificar irregularidades anunciadas por él y presuntamente cometidas por otros miembros de la empresa con repercusiones sobre su bienestar emocional[24].

Como se ha señalado, la norma no exige que el denunciante actúe de buena fe, pero requiere que éste afirme o crea en la veracidad de las irregularidades denunciadas. El hecho de que el trabajador haya mantenido una aptitud obstativa para verificar las irregularidades por él informadas, quiebran la protección frente a represalias y le excluye, por tanto, de la aplicación de la garantía de indemnidad. En efecto, la divulgación de informaciones, aún siendo veraces, no puede realizarse con el ánimo exclusivo de "vilipendiar, humillar o insultar a las personas de forma innecesaria o gratuita, o *con el ánimo de* inferir intencionalmente un daño moral o material al empleador"[25].

Salvo error u omisión por nuestra parte no hemos encontrado jurisprudencia del Tribunal Supremo que haya examinado las represalias frente a las denuncia del trabajador *(whistleblowing)* como vulneración de un derecho fundamental[26]. Sin embargo, hemos revisado con resultados positivos la doctrina judicial de algunos Tribunal Superiores de Justicia que estiman la existencia de vulneración de los derechos fundamentales del trabajador por denuncia de irregularidades.

– Este es el caso de la STSJ de Madrid, de 15 de febrero de 2019, que reconoce la existencia de acoso moral *(whiselblowers)* a un

[23] S. Rodríguez Escanciano: *Derechos laborales digitales: garantía e interrogantes, cit.*, pag. 116.

[24] STSJ Andalucía 15 marzo 2018 (rec 1935/2017).

[25] J.F. Lousada Arochena: "Sistemas de denuncias internas (*whistleblowing*) y derechos fundamentales en el trabajo", *cit.*, pág 10.

[26] En todo caso, la doctrina laboralista advirtió en la STC 6/1998, de 21 de enero, una recepción de la figura del *whistleblower* y de la necesidad de protección que ésta requiere, en S. Del Rey Guanter: *Libertad de expresión e información y contrato de trabajo: un análisis jurisprudencial,* Ed. Civitas, Madrid, 1994, p. 100-102. En efecto, se apuntan muchos de los requisitos que ahora exige la Directiva comunitaria, a saber: a) relevancia pública de la información que, en el caso de las administraciones públicas, e extiende a cualquier tipo de irregularidad; b) diligencia en la verificación de los hechos denunciados, y en fin, c) no se exige que la divulgación de la información esté sujeta a un procedimiento formal, ni tampoco se exige que el denunciante acuda los órganos administrativos o judiciales competentes. En este caso, sí se observa un cambio, pues ahora es necesario que los denunciantes acudan a los sistemas de denuncia previstos (interno o externos) para que no se adopten represalias hacia al trabajador. Otro sector de la doctrina ahonda en esta línea, al entender que la STC 204/1997, de 25 de noviembre y la precedente STC 6/1998, de 21 de enero, "trasponen al derecho español una figura de procedencia norteamericana, *whistleblower* o denunciante, en J. Gorrelli Hernández, T. Igartúa Miro: "La liberta de información y contrato de trabajo. El problema de sus límites. A propósito de la STC 57/1999, de 12 de abril", *Revista Doctrinal Aranzad Social, Vol. BIB, 1999/343.*

tripulante de cabina de una compañía aérea por el colectivo de pilotos. Conviene recordar y repasar por su trascendencia y alcance para el tema que nos ocupa, los hechos que dan lugar a la vulneración de derechos fundamentales y al reconocimiento de una indemnización al trabajador en conceptos de daños y perjuicios.

El día 8 de enero de 2017 en el vuelo de la compañía aérea el actor presencia la comisión por el comandante de vuelo de dos irregularidades que afectan sustancial y gravemente a la seguridad del vuelo. En su condición de sobrecargo deja constancia al comandante de la irregularidad y de la más absoluta disconformidad de toda la tripulación ante las mismas. El otro comandante que irregularmente viaja en cabina de vuelo y que no forma parte de la tripulación de ese vuelo con dos de sus hijos y con otro menor en trasportín situado en galley trasero junto a puerta en asiento exclusivo de tripulación de forma agitada y agresiva le indica que debe acatar órdenes.

El actor denuncia la irregularidad el mismo día 8 de enero de 2017 marcando expresamente la casilla "request confidentiality", es decir, solicita confidencialidad. En el indicado modelo consta su nombre. El 23 de febrero de 2017 la empresa abre pliego de cargos al comandante del vuelo por las irregularidades cometidas en el vuelo del 8 de enero de 2017 como responsable de la seguridad de todos los miembros de la tripulación y le suspende por falta leve con 1 día de empleo y sueldo. A partir de aquí se desata una campaña de persecución contra el demandante por el colectivo de pilotos a través de whatsapps y otros medios llegando a decirle que no le iban a pasar ni una, que no querían que accediera a la cabina de tripulación, que no querían coincidir con él, que "Usted no puede pasarnos la comida, ni las bebidas, ni siquiera destapar la comida".

El 25 de julio de 2017 se informa al actor de la activación del procedimiento de actuación por acoso moral con las siguientes actuaciones: "1. investigación de los hechos denunciados que durará el tiempo estrictamente necesario para el esclarecimiento de los mismos. 2. Citarle para que comparezca en la fecha que se le dará a conocer próximamente, en el Servicio Médico de la Empresa, a fin de evaluar los daños que el supuesto acoso haya podido o pueda potencialmente ocasionarle". El actor no pasó el reconocimiento para evaluar su estado de salud al estar en incapacidad temporal.

El 28 de septiembre de 2017, una vez concluidas las investigaciones, se le comunica por la demandada que no se ha detectado indicio racional alguno de acoso laboral, lo que ponemos en su conocimiento a los efectos que resulten oportunos, dando por resuelto el protocolo de acoso laboral o "mobbing"" con esa fecha.

El informe pericial recoge la presencia en el actor de una sintomatología cronificada y recurrente que se concreta en una serie de síntomas que aparecen en las pruebas aplicadas con síntomas psicosomáticos en forma de palpitaciones, ardores de estómago y molestias gástricas y dolor precordial, trastorno por estrés postraumático.

El Tribunal Superior de Justicia de Madrid considera una forma específica de acoso moral "aquel que sufren las personas que denuncian las irregularidades y/o disfunciones de un superior, sistema u organización (conocido como *whistleblower*)" pues, en muchas ocasiones, van a ser represaliadas por el sistema o por el grupo al que el superior pertenece. El que "informa" porque considera un deber, o simplemente cumple con el deber establecido de alertar y denunciar las acciones de sus compañeros de trabajo y/o superiores que representan una grave irregularidad o peligro sustancial y específico para la seguridad o la salud, se convierten con frecuencia en víctimas de represalias. En estos casos, el acoso va destinado a silenciar al que no participa del mismo juego que los demás y a represaliar al que ha hablado. Lo que le ocurre a un whistleblower es de todo punto equiparable al acoso moral. De ahí la necesidad de su protección a través de una confidencialidad estricta.

Como señala el propio TSJ, no se tiene una protección general de whistleblower, pero conviene en "que una mínima e indispensable ética organizacional y de prevención del riesgo psicosocial debe llevar a la protección del denunciante por cuanto la denuncia supone un beneficio tanto para la organización como para la sociedad en su conjunto al poner de manifiesto y sacar a la luz problemas que deben ser resueltos y respecto de los cuales muy pocas personas están dispuestas a hacer algo, especialmente cuando la irregularidad es cometida por algunos de los miembros de un grupo con poder y mando (en este caso el colectivo de pilotos)"[27].

El actor cumplió su deber y obligación de informar, requiriendo expresamente de su empleador protección específica por confidencialidad *(request confidentiality)*, depositando de buena fe confianza plena en la empresa [art. 5 a) ET], es decir, en la confianza legítima de que se preservaría la confidencialidad que la empresa, con toda evidencia, no garantizó adecuadamente en ningún momento. Por todo ello, y a juicio del Tribunal Superior de Justicia de Madrid, es indiferente quién llevó a cabo la filtración porque es la empresa la responsable frente al trabajador denunciante de preservar su confidencialidad y de garantizar que como consecuencia de la denuncia no sufra perjuicio alguno [art. 4.2.d) y e) ET].

Al igual que es responsable la empresa de la custodia y protección de los datos personales sin perjuicio de la acción que, en su caso, corresponda contra el filtrador[28]. Por tanto, el actor se ha visto sometido a violencia psicológica en el trabajo y fuera de él como consecuencia también del trabajo al no haber preservado la empresa la confidencialidad, violencia que se ha ejercido de forma sistemática y recurrente durante un tiempo prolongado, con la finalidad de destruir sus redes de comunicación, destruir su reputación, perturbar el ejercicio de sus labores y lograr finalmente que termine abandonando el lugar de trabajo, lo que ya ha acontecido siquiera temporalmente al causar incapacidad temporal[29].

Por todo ello, el Tribunal Superior de Justicia de Madrid entiende que nos encontramos ante un supuesto de *whistelblowing*. El denunciante solicitó confidencialidad en la denuncia de irregularidades, aquélla no se garantizó en ningún caso; y además, supuso

[27] La pérdida del beneficio o contemplar al denunciante como un peligro es la causa de la represalia y el acoso. Al respecto sirva de ejemplo el documento interno de la OIT para su personal titulado "La ética en la oficina: la protección de los funcionarios que denuncian irregularidades" destinado a la protección de los funcionarios que consideran que fueron objeto de represalias por haber denunciado casos de falta grave o por haber colaborado en una auditoría o una investigación. En determinados sectores, como es el de la seguridad en la aviación civil, existen normas específicas que tratan de favorecer la denuncia y proteger al denunciante. Tal es el caso del Reglamento (UE) nº 376/2014 relativo a la notificación de sucesos en la aviación civil. De forma expresa los considerandos de la norma exponen que la persona física que notifique un suceso que afecte a la seguridad debe estar adecuadamente protegida, careciendo la notificación de sucesos de la identificación y los datos del notificante, sin que quede registro en las bases de datos (STSJ 15-02-2019, Rec. 824/2018).

[28] Entender lo contrario llevaría a considerar que si la empresa no conoce el origen de la filtración o de cualquier irregularidad que en su seno se cometa deviene irresponsable de todo punto lo que escapa a la más elemental lógica de la responsabilidad empresarial. No es de recibo, por tanto, la afirmación judicial de que el actor no prueba que la empresa tuviera conocimiento del autor de las filtraciones, porque lo decisivo es que no preservó adecuadamente la confidencialidad, es decir, no protegió adecuadamente al trabajador en el origen de un riesgo laboral (art. 15.c LPRL). Este riesgo viene representado por la denuncia actuación que, por sí sola, se erige como un evidente riesgo laboral para la seguridad y la salud del trabajador por cuanto, formulada la denuncia, existe la posibilidad de que el trabajador sufra un determinado daño derivado del trabajo de producción racionalmente probable en un futuro inmediato y susceptible de causar un daño grave para su salud (art. 4.2º, 4º y 5º LPRL), en STSJ 15-02-2019, Rec. 824/2018.

[29] La expresión de esta violencia psicológica ha tenido lugar a través de diversos comportamientos hostiles de distinta naturaleza tanto contra su reputación como contra su dignidad con el objeto de crear estigma. Descriptivo al respecto es la declaración escrita del comandante donde explica cómo se niega a compartir mesa con el actor de forma reiterada, que pueda manipular la comida, y la caracterización del demandante como un buscador de problemas e, incluso, manipulador de situaciones para buscar blindajes laborales. El TSJ da credibilidad por la metodología utilizada al informe pericial y cuantifica la indemnización en 60.000 euros utilizando como parámetro analógico la LISOS, en STSJ 15-02-2019, Rec. 824/2018.

la pérdida de su reputación y confianza en el desarrollo de su relación de trabajo. De ahí que el Tribunal calificara las represalias por el hecho de la denuncia como vulneración de un derecho fundamental.

– En sentido similar, se pronuncia también el Tribunal Superior de Justicia de Madrid, en su sentencia de 15 de marzo de 2019, aunque ahora en un supuesto circunscrito a un caso de acoso sexual, ambiental reiterado y generalizado en el trabajo por un superior jerárquico, que se canaliza a través de una primera denuncia genérica e indeterminada y formulada ante un canal externo, gestionado también de forma externa a la empresa.

El TSJ revoca la sentencia de instancia y declara la procedencia del despido estimando el recurso de la empresa[30]. A juicio de la Sala de suplicación, se trata de una falta continuada y oculta como consecuencia de la situación personal del demandante en la empresa de la que por consiguiente se prevale, que responde a una conducta prolongada en el tiempo manifestada a través de una pluralidad de hechos y comportamientos repetidos, dotados de una unidad que se corresponde con el mismo tipo de infracción.

En el presente supuesto, a criterio del Tribunal Superior de Justicia, nos encontramos ante la imputación de un acoso sexual ambiental llevado cabo por la persona que ostenta la máxima responsabilidad y representa, en consecuencia, los valores de la dirección y de la mercantil demandada. La propia naturaleza de la imputación impide el registro sistemático y minucioso de cada uno de los hechos que integran la conducta, a la sazón continuada. Así, entiende el Tribunal que resulta prácticamente impensable exigir a las trabajadoras que lleven a cabo un registro diario de cada uno de los comentarios inapropiados que reciben a los efectos de conformar, si es el caso, una denuncia de acoso sexual ambiental. Varios son los argumentos que se señalan en la sentencia y fundamentan tal situación de discriminación y las dificultades de su denuncia, entre otras:

– "Las relaciones humanas, entre ellas las laborales, se deben desarrollar y normalmente se desarrollan en los límites de la confianza, el respeto y la igualdad.

– La sutileza de muchos de los comportamientos de acoso y su ambigüedad buscada incluso de propósito, impide que el afectado procese inmediatamente y sin duda la violencia del comportamiento del que está siendo objeto, que normalmente se cuestiona por temor a la incomprensión.

– De la misma forma impide la reacción inmediata, probablemente en la esperanza de que son hechos aislados, por no hablar de la dificultad de reacción cuando el que la lleva a cabo representa la máxima autoridad empresarial lo que constituye una agravante.

– Por el contrario, es la repetición, la constancia, la actuación sobre multiplicidad de sujetos pasivos la que genera el daño, el efecto indeseado, humanamente y jurídicamente reprobable y que en un momento dado elimina la sutileza y la ambigüedad, esto es, la duda de la violencia que es objeto de denuncia.

Por ello, a juicio del TSJ de Madrid, resulta evidente la dificultad y casi imposibilidad del registro de hechos y fechas en supuestos como el presente pues, de exigirse, se impediría la

[30] A la vista de que la primera denuncia es genérica e indeterminada y formulada ante un canal externo gestionado también de forma externa a la empresa, no entra en juego el mecanismo de la prescripción del art. 60 del ET, que ha resultado así infringido por la sentencia de instancia Además, es necesario reiterar que, en modo alguno, las denuncias pueden ser medio de prueba de infracciones laborales que, desde luego, requerirán de una labor investigadora más seria por la propia entidad antes de proceder a las imposición con las garantías previstas en el art. 58 ET y en el convenio que resulte de aplicación, en S. RODRÍGUEZ ESCANCIANO: *Derechos laborales digitales: garantía e interrogantes, cit.*, pag. 116.

persecución de esos "pequeños" actos violentos cotidianos que pueden parecer incluso "normales" para algunas personas y en algunos contextos, que empiezan con sencillas faltas de respeto y que poco a poco aumentan en intensidad especialmente si el grupo social en el que aparecen no reacciona, pues es entonces cuando los actos progresivamente se conviertan en verdaderas conductas violentas susceptibles de generar graves consecuencias. En fin, en las circunstancias expuestas, exigir aquel registro minucioso penalizaría la reacción del grupo que ha sido, en definitiva, el motor de la denuncia del Presidente del Comité de Empresa.

El actor ha llevado a cabo acoso sexual físico al besar en el cuello[31]; también ha llevado a cabo acoso sexual de palabra al comentar sus fantasías sexuales[32] o realizar comentarios sobre lo bien que les sientan los pantalones o la ropa que visten las trabajadoras[33]. Estos actos son ejemplos de un comportamiento degradante continuo y son considerados como conducta violenta en el trabajo (Acuerdo Marco sobre violencia y acoso en el trabajo). Constituyen acoso sexual y, como tales, sin más precisiones, son reputados como falta muy grave habiendo decidido la empresa la sanción de despido en uso de un poder de elección no revisable judicialmente. Sin duda inciden en la dignidad y degradan a la mujer y el ambiente laboral. El hecho de que el ambiente de trabajo sea aún así normal[34] no constituye un obstáculo porque lo decisivo es que el factor que incide en el ambiente sea degradante, no que el ambiente esté ya degradado.

Y, efectivamente, es degradante al constituir las conductas descritas factores susceptibles de deteriorar o degradar el ambiente laboral al afectar negativamente las acciones de acoso sexual del máximo responsable empresarial en España de forma directa o indirecta, voluntaria o involuntariamente, a la calidad ambiental laboral de la empresa demandada en cualquiera de sus grados.

Como señala el Acuerdo Marco sobre el acoso y la violencia en el trabajo "el respeto mutuo de la dignidad a todos los niveles en el lugar de trabajo es una de las características esenciales de las organizaciones exitosas. Por eso son inaceptables el acoso y la violencia… en todas sus formas… que puede tener graves consecuencias sociales y económicas. Tanto el Derecho de la UE como el nacional establecen el deber de los patronos de proteger a los trabajadores contra el acoso y la violencia en el lugar de trabajo".

En fin, concluye el Tribunal Superior de Justicia de Madrid que "la política de tolerancia cero hacia este tipo de conductas, plasmada de la misma forma en el Convenio, determina la declaración de procedencia del despido y la consiguiente corrección del proceder empresarial en aplicación del art. 54.g) ET, 16.m del Acuerdo y 57.m del Convenio de aplicación."

-Además de la identificación de la existencia de vulneración de los derechos fundamentales del trabajador por denuncia de irregularidades, resulta interesante también que se contemple como represalia los daños reputacionales "en especial, en los medios sociales que pueda ser objeto el *whistleblowers*", así como las denominadas "listas negras" que impliquen el denunciante no pueda volver a trabajar en un determinado sector.

Tal es el caso de la STS, Sala Primera, de 12 de noviembre de 2015[35], en la que incorpora un criterio de interés, tras analizar los efectos de la inclusión de un trabajador en una "lista negra" que le vetaba para trabajar para empresas del sector de las telecomunicaciones.

En efecto, el demandante, trabajador de una empresa subcontratista de Telefónica, fue despedido acusado de haber cobrado a un cliente por un servicio que debía ser gratuito.

[31] Hechos probados octavo y décimo.
[32] Palabras textuales: "hacer un trío o tocar los pechos".
[33] Hechos probados octavo y décimo.
[34] Hechos probado noveno.
[35] Sentencia nº 609/2015.

Demandó a su empresa por dicho despido, que fue declarado improcedente por la jurisdicción social por no quedar acreditados los hechos imputados y la empresa optó por indemnizarle y extinguir la relación laboral. Posteriormente, el trabajador realizó varios procesos de selección y cuando iba a ser contratado por una empresa del mismo sector, ésta le manifestó que no podía contratarle, por haber sido incorporado a un fichero de "personal conflictivo" por los hechos que motivaron su despido –a pesar de que el Juzgado no los considerara probados[36].

Finalmente, el Tribunal Supremo ha considerado que efectivamente se había producido la vulneración de su derecho al honor y a la protección de datos (reconocidos en el art. 18 CE) –no así a su propia imagen–, y condena a la empresa a abonar la suma de 30.000 euros. El Tribunal estima la demanda basándose en que la prueba de que efectivamente existía tal "lista negra" resultaba prácticamente imposible para el trabajador. De hecho, además de los indicios derivados de los fallidos procesos de selección, la única prueba que pudo aportar en el juicio fue la testifical de un miembro del comité de empresa de Telefónica que mostró su convencimiento de que "existía ese fichero de trabajadores vetados".

Sin embargo, el Tribunal considera que, tratándose de un procedimiento de vulneración de derechos fundamentales, y habida cuenta de la existencia de tales "indicios razonables", la carga de la prueba debe recaer en la empresa que supuestamente incluyó sus datos en la "lista negra", que debería haber tratado de demostrar en el acto de juicio –cosa que no hizo– que cuando notificó a Telefónica la extinción de la relación laboral con el trabajador (comunicando para ello sus datos de carácter personal), no incluyó ningún otro tipo de información sobre los hechos que motivaron el despido.

Desde el punto de vista de la normativa de protección de datos, el Tribunal considera que la cesión de datos realizada para la formación de la "lista negra" fue ilícita, ya que a) no contó con el consentimiento del afectado; b) no resultaba amparada en ninguna de las excepciones del artículo 11.2 LOPD; c) no respetaba el principio de calidad de los datos –los datos cedidos no eran veraces, al no haber sido considerados por el Juzgado de lo Social como acreditados–; y d) no se lo concedió la posibilidad de ejercitar los derechos acceso, rectificación, cancelación y oposición. Además, para el Tribunal, esta infracción de la normativa de protección de datos produjo, a su vez, una vulneración del derecho al honor del demandante, ya que los datos comunicados no cumplían el requisito de veracidad y afectaban negativamente a su reputación.

Desde el punto de vista del Derecho del Trabajo, el Tribunal no cuestiona en esta sentencia la competencia de la jurisdicción civil para conocer de la acción interpuesta. Ahora bien, cabe entender que si la demanda se interpusiese a la luz de la LRJS, la competencia sería, a buen seguro, de la jurisdicción social.

La Sala Primera tampoco entra a valorar aquí ni si el consentimiento prestado por el ex trabajador hubiese sido válido en este contexto, ni tampoco qué hubiese sucedido en el supuesto de que los hechos imputados en la carta de despido hubieran resultado acreditados y el despido hubiese sido declarado procedente.

Por último, se contempla también la asistencia al *whistleblower* en los procesos frente a las represalias, incluida la asistencia jurídica gratuita si procede, la protección frente a acusaciones de revelación de información confidencial, así como la obligación de inversión de carga de la prueba. Asimismo, se incluyen medidas de apoyo financiero y psicológico al denunciante (art. 20 DPII)[37].

[36] Como consecuencia de ello, el trabajador demandó a su anterior empleador solicitando una indemnización de más de 600.000 euros por la vulneración de sus derechos de honor e imagen, así como a la protección de datos personales.

[37] Asimismo, y para lograr la protección efectiva del *whistleblower* y favorecer que se recurra a los canales de

4. A MODO DE CONCLUSIÓN

Es pronto para valorar la incidencia de la Directiva 2019/1937 en el marco de la protección de datos y el contexto laboral. Habrá que esperar a la norma de transposición que desarrolle los mínimos establecidos para garantizar una cultura de cumplimiento y lucha contra la represión de la información de las irregularidades.

En todo caso, la detallada regulación de los canales de denuncia y, a su vez, la minuciosa configuración de las medidas de protección para el *whistleblower* ofrece una respuesta razonable y proporcionada para aquéllos que deban hacer uso de estos sistemas de información para denunciar infracciones en el ámbito laboral.

El art. 17 ET recoge una garantía de indemnidad amplia, reputando nulas las órdenes del empresario que supongan un trato favorable de los trabajadores como reacción ante una reclamación efectuada en la empresa o ante una decisión administrativa o judicial destinada a exigir el cumplimiento del principio de igualdad de trato y no discriminación.

Sería deseable que la Ley de transposición de la Directiva acogiera un precepto legal que garantizara al trabajador el derecho a no sufrir perjuicio alguno por el hecho de formular denuncias o quejas de anomalías o irregularidades de la empresa. Esta obligación se podría exigir al empresario, siempre que la empresa hubiera habilitado un adecuado sistema de canal denuncia, en el que se asegure tanto la confidencialidad del denunciante como la garantía de no sufrir represalias por presenta una queja o denuncia.

denuncia de irregularidades, se contemplan sanciones frente a aquellas entidades que a) impidan o intenten impedir la presentación de denuncias, b) adopten medidas de represalia frente a los informantes, c) promuevan procedimientos temerarios contra los informantes, d) incumplan el deber de mantener la confidencialidad de la identidad de los informante (art. 23 DPII).

RESUMEN La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantías de los Derechos digitales se dicta para adaptar el ordenamiento jurídico español al Reglamento UE 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Esta Ley introduce un sistema de información de denuncias que establece una especial protección para los denunciantes que va a desplegar efectos en el ámbito laboral. Estos sistemas de recepción y conocimiento de infracciones se encuadran bajo las exigencias de la legislación aplicable en materia de protección de datos, siempre que se traten denuncias referidas a normas, fundamentos principios, cuyo incumplimiento tenga consecuencias efectivas sobre la pervivencia de la relación contractual entre la empresa y el denunciado.

El art. 24 LOPD regula un sistema de denuncias internas desde la perspectiva del derecho de protección de datos personales, referido a los límites de acceso a los datos de las personas, la confidencialidad del tratamiento o la limitación temporal en orden a la conservación de las denuncias.

La Directiva UE2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre, relativa a la protección de las personas que informan sobre infracciones del Derecho de la Unión configura, de una forma mucho más profusa, un sistema de canales de denuncia, externas e internas, que protege la confidencialidad, anonimato y no represalia del denunciante.

Estamos, pues ante una norma esperada, un elemento más en el engranaje normativo que el legislador comunitario –pero también, el nacional– propone para articular la obligación de establecer canales de denuncia y a la vez prevé medidas de protección que deben garantizarse en el marco del *whistelblowing*.

Su principal virtualidad es que, con su sola existencia, despeja los debates sobre los cauces del sistema de denuncia, aportando luz en un contexto absolutamente necesitado de seguridad jurídica. Se busca reforzar la protección del *whistelblower* y el ejercicio del derecho a la libertad de expresión e información, reconocidos en el art. 10 Carta Europea de Derechos Humanos y en el art. 11 de la Carta de Derechos Fundamentales.

Se delimitan las reglas de configuración del ámbito de aplicación, es decir, se delimitan las infracciones, así como también el ámbito personal de los denunciantes. Se protege no sólo a los denunciantes del sector privado, sino también del sector público, que comuniquen o revelen públicamente información sobre infracciones del Derecho de la Unión, que se hayan conocido en un contexto laboral, siempre que tuvieran motivos razonables para creer que la información era veraz en el momento de la denuncia.

Las denuncias deben articularse a través de unos sistemas establecidos al efecto. Se prevén tres tipos de canales: internos, dentro de una entidad jurídica pública o privada; 2) externos, dependientes de las autoridades que se designen en cada Estados miembros, y con los que la empresa tendrá cierta prevención, sobre todo, por temor "a perder la reputación" y 3) la revelación pública, que consiste en la puesta a disposición del público de información sobre infracciones.

Con este sistema de denuncias habrán de tenerse muy presente las medidas de protección del denunciante. La primera es la confidencialidad, es decir, los canales de denuncia deben estar diseñados y gestionados de tal forma que este deber debe alcanzar también a los no afectados, para que su acceso a la información sea del todo imposible al tratarse de personal "no autorizado", pero también se deben establecer garantías frente a posibles represalias en el ámbito laboral. No obstante, antes de que se apliquen las

medidas protectoras frente a posibles desagravios del trabajador por haber informado de determinadas irregularidades en la empresa, debe comprobarse que el denunciante cree en la veracidad de los hechos que denuncia y que procede a través de los cauces adecuados. Los informantes deben estar protegidos frente a todo tipo de represalias, ya sean directas o indirectas, que se tomen por el empresario, clientes incluso compañeros de trabajo. Se propone: la prohibición de represalias, medidas de apoyo, medidas de protección frente a represalias, medidas para la protección de las personas afectadas y sanciones. En definitiva, se establece una suerte de indemnidad que trata de garantizar una protección cualificada al trabajador que denuncia una irregularidad en el seno de la empresa.

Ahora bien la prohibición de represalia frente al denunciante no debe impedir la adopción de las medidas disciplinarias cuando la investigación determine que la comunicación sea falsa y que la persona que la ha realizado ha actuado de mala fe.

En todo caso, la prohibición frente a represalias debe tramitarse como vulneración de un derecho fundamental del trabajador y tales medidas deberían reputarse nulas y sin efecto. Aunque todavía no se ha pronunciado el Tribunal Supremo sobre el particular, sí que hemos revisado con resultados positivos la doctrina judicial de algunos Tribunales Superiores de Justicia que estiman la existencia de vulneración de derechos fundamentales del trabajador por denuncia de irregularidades. En este sentido, la doctrina del Tribunal Constitucional ha confirmado la recepción de la figura del *whistelblower* y la necesidad de protección que ésta requiere.

Todavía es pronto para valorar la incidencia de la Directiva 2019/1937 en el marco de la protección de datos y el contexto laboral. Habrá que esperar a la norma de transposición que desarrolle los mínimos establecidos para garantizar una cultura de cumplimiento y lucha contra la represión de la información de las irregularidades. En todo caso, es una estupenda oportunidad para que el legislador español promueva una regulación detallada y completa sobre *whistleblowing* a tenor de la doctrina que sobre este particular está construyendo el Tribunal Constitucional.

Palabras clave: Tecnologías; informantes; Canal de denuncias; confidencialidad; derecho fundamental; prohibición de represalias

ABSTRACT The Law 3/2018 of 5th December about the protection of personal data and guarantees of digital rights is approved to adapt the Spanish legal system to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) This Law introduces a reporting information channel or system that establishes special protection for whistleblowers that will display effects in the workplace

This Law introduces confidential and secure reporting channels and by ensuring that whistleblowers are protected effectively against retaliation, even in the work-related context. Specifically, art. 24 Law about the protection of personal data and guarentees of digital rights regulates an internal reporting channel from the perspective of data protection, referring to the limits of access to people's data, the confidentiality of the treatment or the temporary limitation in order to preserve internal reporting

Recently, it has adopted the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law sets up a system of reporting channels, external and internal, that protects the confidentiality, anonymity and non-retaliation of the reporting person.

This Directive is an expected norm, one more element in the normative gear that the community legislator – but also our national one – proposes to articulate the obligation to establish reporting channels and provides protection measures that must be guaranteed within the framework of the *whistelblowing*. Its main virtuality is that it clears the debates on the reporting channels finding out ways of solution in a context which requires legal certainty. It´s try to strengthen the protection of the whistelblower and the exercise of the right to freedom of expression and information, recognized in art. 10 European Charter of Human Rights and in art. 11 of the Charter of Fundamental Rights

The rules of configuration of the scope of application are defined, as well as the personal scope of the reporting persons. It wil be apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context about violations of Union Law, including reasonable suspiciones, whic ocured or are very likely to occur ein the organisation in which reportung person Works or has worked or in another organisation with which the reporting person i sor was in contact through his or her work, and about attempts to conceal such breaches.

Information on breaches must be articulated through reporting channels established for this purpose. Three types of channels are planned: internal reporting channel, within a public or private legal entity; 2) external reporting channel, dependent on the authorities competent are designated in each Member States, and with whom the company will have some prevention, especially for fear "to lose reputation" and 3) public disclosure, which consists in putting public provision of information on breaches.

With this reporting system the reporting person should enjoy the protection against retaliation provided by this Directive. The first is confidentiality, that is, the reporting channels must be designed and managed in such a way that this duty must also reach those not authorised staff members competent to receive or follow up on reports, because they are "unauthorized" personnel; but it should be established guarantees possible retaliation in the work-related context that, in any case, must be processed as a violation of a fundamental right of the worker, in fact such measures should be considered void and without effect.

However, before the protective measures are applied to prohibit any form of realiation against reporting persons for having reported certain irregularities in the company, it must be verified that the informan believes in the veracity of the facts he denounces and that he proceeds through the appropriate channels Informants must be protected against all types of realiation, whether direct or indirect, that are taken by the employer,

clients or third persons who are connected with the reporting persons. The proposal are: prohibition of retaliation, measures of support, measures for protection against retaliation, measures for the protection of concerned persons and penalties sanctions. In short, a kind of indemnity is established that tries to guarantee a qualified protection to the worker who informas on breaches within a privat or public company.

The prohibition of retaliation against reporting persons should not prevent the adoption of disciplinary measures when the investigation determines that the communication is false and that the person who has informed about it has acted in bad faith.

The prohibition of retaliation must be processed as a violation of a fundamental right and such measures should be considered void

Although the Supreme Court has not yet ruled on the matter, we have reviewed with positive results the judicial doctrine of some Superior Courts of Justice, that consider the existence of a violation of fundamental rights of the worker for reporting information on breaches. In this sense, the doctrine of the Constitutional Court has confirmed the reception of the figure of the *whistelblower* and the need for protection that it requires.

It is early to analyse the impact of Directive 2019/1937 in the framework of data protection and on the work-related context. We will have to wait for the transposition regulation that develops the minimum established to guarantee the protection of persons who report breaches of Union law. In any case, it´s a great opportunity for the Spanish legislator to adopt a complete and detailed regulation on whistleblowing, according to the doctrine that the Constitutional Court is building on this particular.

Keywords: Technologies; information on breaches; reporting channels-confidentiality; fundamental right; prohibition of retaliation

Facultades empresariales y garantías del trabajador en relación con el uso de dispositivos digitales en el ámbito laboral

Employer measures and workers' rights regarding the use of computers and digital media in the workplace

FEDERICO NAVARRO NIETO*

1. LA PROTECCIÓN DE LA *PRIVACY* DEL TRABAJADOR: LA EVOLUCIÓN DESDE UNA CULTURA CONTRACTUALISTA A UNA VISIÓN CONSTITUCIONALMENTE ORIENTADA

Las nuevas tecnologías y los medios digitales no sólo facilitan el control de la actividad laboral, también refuerzan exponencialmente la capacidad de vigilancia y control de la persona del trabajador, de su imagen e intimidad, de sus comunicaciones, y de sus datos personales[1]. El Dictamen 2/2017 del Grupo de Trabajo 29 de la UE, *sobre el tratamiento de datos en el trabajo* (17/ES, WP 249), recuerda que, con las actuales tecnologías, "Si el tratamiento no tiene límites y no es transparente, existe un alto riesgo de que el interés legítimo de los empresarios en la mejora de la eficiencia y protección de los activos de la empresa se convierta en un control injustificado e intrusivo" (p. 10).

En el plano jurídico, el control empresarial de la actividad laboral del trabajador, amparada genéricamente en el art. 20.3 ET, como concreción del derecho empresarial de organización del trabajo en la empresa y de la libertad de empresa (art. 38 CE), ha supuesto un sólido respaldo a las facultades empresariales de control de la actividad laboral mediante medios de videovigilancia en el lugar de trabajo e instrumentos de control de los medios digitales empresariales puestos a disposición del trabajador.

El control empresarial de los dispositivos digitales facilitados al trabajador por la empresa (ordenador, cuenta de correo electrónico, teléfono móvil, tablet) puede plantear situaciones que afectan al derecho a la intimidad o a la protección de datos de los trabajadores, cuando la vigilancia afecta a la «navegación» por Internet o a determinados archivos personales del ordenador, y al secreto de las comunicaciones, en el caso particular de control sobre el correo electrónico o el móvil.

En términos generales, el tratamiento normativo de esta temática se ha caracterizado históricamente por una regulación jurídica

* Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de Córdoba.

[1] Cfr. F. VALDÉS DAL-RÉ, "*Nuevas tecnologías y derechos fundamentales de los trabajadores*", en *Derecho de las Relaciones Laborales*, nº 2, febrero 2019, p. 130.

escasa e imprecisa y por el casuismo judicial[2]. No obstante, en las últimas décadas contamos con documentos elaborados en el ámbito internacional o de la UE donde se contemplan los parámetros que deben de servir de equilibrio en los intereses en juego en la temática y que justifican el sacrificio de la privacidad del trabajador (existencia de un fin legítimo, trasparencia informativa y proporcionalidad y minimización del control)[3], hoy plasmados normativamente en los principios recogidos en el art. 5 del Reglamento (UE) 2016/679, *relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (RGPD).

Históricamente, la escasa normativa nacional e internacional sobre tutela del uso laboral de medios digitales conduce a que el alcance de su protección haya quedado supeditado a la interpretación judicial, muy basada en el caso concreto, donde por ello la doctrina jurisprudencial no puede desligarse de los concretos casos abordados[4].

En un escenario normativo tradicionalmente deficitario en la regulación de los derechos inespecíficos en el ámbito laboral[5], nuestra temática es un ejemplo donde el conflicto entre los poderes organizativos empresariales y los derechos fundamentales del trabajador acaba decantándose por la primacía de una "lógica contractual" y una "lógica organizativa", salvo en las formas más arbitrarias de ejercicio del poder empresarial[6]. Bien es cierto que también en la temática en estudio se ha echado en falta, de cara a un juicio ponderado, la consideración de la mala fe de quien invoca el derecho a la *privacy*[7].

Pero no puede ignorarse que, en términos generales, respecto de los derechos fundamentales inespecíficos, la jurisprudencia constitucional desde hace años ha sentado las bases para asegurar la operatividad de tales derechos en el lugar de trabajo[8]; ni se puede ignorar tampoco, específicamente en relación con la protección de la *privacy* del trabajador, donde en los últimos años se avanza desde una cultura jurídica contractualista a otra consti-

[2] De la normativa internacional destacamos, en el ámbito del Consejo de Europa, el art. 8 CEDH y el Convenio nº 108, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, de 1981. En el ámbito de la UE, hay que destacar la Directiva 95/46/CE, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Finalmente, en nuestro derecho interno el enfoque normativo se ha circunscrito al art. 20.3 ET.

[3] OIT, *Protección de los datos personales de los trabajadores. Repertorio de recomendaciones prácticas de la OIT*. 1997. En el ámbito de la UE, Grupo de Trabajo del Artículo 29, Dictamen 8/2001, sobre el tratamiento de datos personales en el contexto laboral (WP48), Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo (WP55) de 2002 y Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (WP 249). Este último documento concluye que es legítimo el interés empresarial como fundamento del control (la necesidad de proteger la red y los datos personales de los trabajadores y clientes que allí se guardan contra el acceso no autorizado o la fuga de datos, controlar automáticamente los correos electrónicos salientes, con el fin de prevenir la transmisión no autorizada de datos protegidos), pero se insiste en que es necesario que se garantice un principio de transparencia y proporcionalidad (p. 16).

[4] Se ha dicho, por ejemplo, de la jurisprudencia del TEDH que "las circunstancias particulares del caso concreto suelen adquirir tal relevancia en la doctrina formulada, que no es posible hacer una lectura de la misma desligada de tales circunstancias". Cfr. F. Pérez de los Cobos Orihuel, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado*, Consejo de Europa. Estudio, octubre 2018, p. 6.

[5] Remito a J.L. Goñi Sein, "*Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?*", en AEDTSS, *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*, Ed. Cinca, 2014, p. 28 y sigs.

[6] Cfr. J.L. Goñi Sein, "*Los derechos fundamentales inespecíficos en la relación* laboral…", *cit.* p. 56. Con una visión crítica, desde esta perspectiva, de la doctrina constitucional española (SSTC 241/2012 y 170/2013) puede verse F. Valdés Dal-Ré, "*Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa*", en *Revista de Derecho Social*, nº 79, p. 28 y sigs. Una perspectiva crítica que el autor considera trasladable al conjunto de los ordenamientos europeos. Cfr. del mismo, "*Nuevas tecnologías y derechos fundamentales…*", *cit.* pp. 130-131.

[7] Cfr. F. Pérez de los Cobos Orihuel, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado*, *cit.*, p. 46.

[8] J.L. Goñi Sein, "*Los derechos fundamentales inespecíficos en la relación* laboral…", *cit.* p. 33-35.

tucionalista[9]. En esta evolución reciente juega un papel de vanguardia el TEDH que, al hacer efectiva la garantía de la *privacy* contenida en el art. 8 CEDH, "repropone" en términos nuevos la dialéctica entre el poder de vigilancia del empresario y el respeto a la privacidad y el secreto de las comunicaciones del trabajador[10]. También un nuevo enfoque es perceptible en nuestra jurisprudencia constitucional, que amplía el escenario de los derechos fundamentales del trabajador en juego (del derecho a la intimidad y al secreto de las comunicaciones al derecho a la protección de datos) y sitúa en primer plano, como canon de razonamiento, el juicio de proporcionalidad. Como el mismo TEDH reconoce recientemente, los criterios de proporcionalidad establecidos por la jurisprudencia del TC "son próximos a los que él [el TEDH] ha mantenido en su jurisprudencia"[11]. Como trataré de poner de manifiesto en el presente estudio, se puede decir que la jurisprudencia del TEDH y del TC muestran una tendencia hacia la convergencia de la tutela de la privacidad del trabajador, que abarca la protección de datos, de la intimidad y del secreto de las comunicaciones[12].

La tutela del trabajador frente al control empresarial de los medios digitales ha sido enfocada inicialmente desde el ámbito del derecho a la intimidad y el secreto de las comunicaciones (art. 18.1 y 3 CE). Un avance sustancial se produce con la ampliación de la tutela laboral a través del derecho a la protección de datos, donde cobra particular relevancia la doctrina del TEDH, que pone el acento en la imbricación entre el derecho a la intimidad y a la protección de datos, favoreciendo una interpretación ampliatoria del derecho a la vida privada (STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros)*. En el caso español contamos con una doctrina constitucional de primer orden a partir de la STC 29/2013.

La jurisprudencia del TEDH y nuestra jurisprudencia interna legitiman el poder empresarial de control de los medios digitales puestos a disposición del trabajador por la empresa, y efectúan el enjuiciamiento de la injerencia empresaria a partir de dos criterios interpretativos, la expectativa de privacidad y el principio de proporcionalidad. El primer criterio ha sido considerado central para valorar el conflicto de intereses y derechos, y a él se ha vinculado el principio de trasparencia informativa (la información sobre el uso de los medios digitales y los dispositivos de control al efecto). Pero ello no ha privado de valor al criterio clásico del juicio de proporcionalidad, hasta el punto de venir a ocupar actualmente el centro de gravedad del tratamiento jurisprudencial. Ilustra claramente esta evolución la STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, que observa que "la exigencia de trasparencia y el derecho a la información que se deriva del mismo reviste un carácter fundamental", aunque el canon de razonamiento a seguir implica que "la información ofrecida a la persona sometida a la vigilancia y su amplitud no es sino uno de los criterios a tener en cuenta para apreciar la proporcionalidad de tal medida" (ap. 131). Como veremos, los tribunales, a pesar de no existir un conflicto de derechos, debido a la constatación de la inexistencia de una expectativa razonable de confidencialidad, entran a enjuiciar la naturaleza y el alcance del control empresarial a la luz del juicio de proporcionalidad[13], en sintonía con el test de legitimidad delimitado por la jurisprudencia del TEDH.

[9] J.L. Goñi Sein, "*Los derechos fundamentales inespecíficos en la relación* laboral…", *cit.* p. 55 y sigs.

[10] J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional*", en *Trabajo y Derecho*, nº 40, 2018, p. 14.

[11] STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, Asuntos nº 1874/13 y 8567/13, ap. 132.

[12] J.L. Goñi Sein, "*Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016*", en *Revista de Derecho Social*, nº 78, pp. 31-33

[13] Llaman la atención sobre esta paradoja, A. Desdentado Bonete y E. Desdentado Daroca, "*La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del*

Desde este enfoque, la jurisprudencia del TEDH y de nuestros tribunales coinciden en una evolución hacia la clarificación de los parámetros que justifican el sacrificio de la privacidad del trabajador (existencia de un fin legítimo, trasparencia informativa y proporcionalidad y minimización del control). Además, la intensidad en la valoración de estos parámetros, esencialmente el principio de proporcionalidad en sentido estricto, depende del tipo de medida de control empresarial, pudiendo distinguirse, por el mayor impacto en los derechos fundamentales del trabajador, la audio o la videovigilancia (en este caso pudiendo graduarse por el ámbito al que se dirige la misma) y la interceptación de comunicaciones, supuestos que se diferencian del control de medios digitales de trabajo, que cuentan con la consideración de instrumentos de trabajo de propiedad empresarial. Así lo constatamos en la doctrina del TEDH sobre la aplicación del test de legitimidad del control empresarial (STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*).

Esta orientación actualmente cristaliza en la normativa de protección de datos, donde se han producido avances sustanciales con el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, *de Protección de Datos Personales y garantía de los derechos digitales* (LOPD). La legislación vigente es relevante porque, conforme al art. 8.2 CEDH, las injerencias en la privacidad del trabajador serán legítimas "en tanto en cuanto esta injerencia esté prevista por la ley"; pero hay que subrayar también la importancia de la jurisprudencia, que abordamos a continuación, porque en el concepto de "la ley" de la norma citada debe incluirse la jurisprudencia del TEDH, la doctrina de del TC y de la jurisdicción ordinaria[14].

2. DEL CRITERIO DE LA EXPECTATIVA DE PRIVACIDAD AL JUICIO DE PROPORCIONALIDAD

2.1. La jurisprudencia del Tribunal Supremo en relación con el uso de dispositivos digitales en el ámbito laboral

En España, ante un enfoque normativo muy esquemático hasta tiempos recientes (art. 20.3 ET), la problemática creciente en nuestra temática es abordada por la jurisprudencia, que arranca con la doctrina del TS en la primera década del 2000, caracterizada por un enfoque desde la perspectiva del derecho a la intimidad (art. 18.1 CE) y del derecho al secreto de las comunicaciones (art. 18.3 CE).

Un dato esencial que singulariza el canon de razonamiento en el control empresarial de los dispositivos digitales puestos a disposición del trabajador es la consideración del ordenador como un instrumento de trabajo, cuyo uso queda sometido al poder de control y vigilancia empresarial. Este enfoque es firme en nuestra jurisprudencia desde la STS 26-9-2007, rec. 966/2006, que considera que el control de los ordenadores se justifica, por un lado, "porque en él se cumple la prestación laboral y, por tanto, ha de comprobar si su uso se ajusta a las finalidades que lo justifican, ya que en otro caso estaría retribuyendo como tiempo de trabajo el dedicado a actividades extralaborales". Por otro lado, también se justifica el control por la necesidad de coordinar y garantizar la continuidad de la actividad laboral en los supuestos de ausencias de los trabajadores (pedidos, relaciones con clientes...), por la protección del sistema informático de la empresa, y por la prevención de responsabilidades que para la empresa pudieran derivar también algunas formas ilícitas de uso frente a terceros. Esta justificación causal del control empresarial, como veremos, ha cristalizado en el actual art. 87 LOPD. Este enfoque es avalado por la doctrina del TEDH. Como indica la STEDH 22-2-2018, *asunto Libert*, ap. 46, el empresario "legítimamente puede querer

uso laboral del ordenador", en *Revista de Información Laboral*, nº 1/2018 (Base Aranzadi, BIB 2018, 6059), p. 5 del documento electrónico.

[14] Cfr. F. Pérez de los Cobos Orihuel, *El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado, cit.* p. 37.

asegurarse de que sus empleados utilizan los equipos informáticos puestos a su disposición para el desempeño de sus funciones, conforme a sus obligaciones contractuales y a la reglamentación aplicable".

A partir de este dato la jurisprudencia ordinaria construye su canon de enjuiciamiento sobre dos criterios interpretativos, la existencia de una expectativa razonable de privacidad y el principio de proporcionalidad del control empresarial. Como vamos a ver, a pesar de la centralidad del primer criterio (que condiciona la tutela del derecho a la intimidad y al secreto de las comunicaciones), el criterio de proporcionalidad lleva a los tribunales a entrar en la valoración de la intensidad del control empresarial (las características de la monitorización de los ordenadores, la información que se extrae de la navegación del trabajador por internet, el alcance del control de la mensajería electrónica).

En la STS 26-9-2007 se estima que la medida adoptada por la empresa de recogida de información más allá del objetivo inicial de verificar fallos técnicos en un ordenador, sin previa advertencia sobre el uso y sobre posibles controles del ordenador, supuso una lesión al derecho a la intimidad del trabajador. Se parte de que, en el uso por el trabajador de los medios informáticos facilitados por la empresa, pueden producirse conflictos que afectan a la intimidad de los trabajadores, "tanto en el correo electrónico, en el que la implicación se extiende también al secreto de las comunicaciones, como en la denominada "navegación" por Internet y en el acceso a determinados archivos personales del ordenador".

Para el TS, "aunque el trabajador tiene derecho al respeto a su intimidad, no puede imponer ese respeto cuando utiliza un medio proporcionado por la empresa en contra de las instrucciones establecidas por ésta para su uso y al margen de los controles previstos para esa utilización y para garantizar la permanencia del servicio". Sin embargo, la tolerancia empresarial puede generar una expectativa razonable de privacidad, planteándose en este caso un conflicto entre el derecho a la privacidad del trabajador y el poder de control empresarial, que debe resolverse mediante el principio de proporcionalidad. La sentencia observa que los conflictos surgen porque "existe una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa", y porque esa utilización personalizada "se produce como consecuencia de las dificultades prácticas de establecer una prohibición absoluta del empleo personal del ordenador –como sucede también con las conversaciones telefónicas en la empresa– y de la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa".

Dicha expectativa de privacidad en favor del trabajador queda neutralizada si la empresa establece previamente las reglas de uso de los medios digitales, con aplicación de prohibiciones absolutas o parciales, e informa a los trabajadores de que va a existir un control y de los medios que se emplearán en orden a comprobar la corrección de los usos. La expectativa razonable de privacidad, en suma, queda condicionada en su existencia y alcance por la existencia o no de reglas de uso y de información al trabajador sobre posibles controles de los medios digitales. Esta doctrina se reitera en la STS 8-3-2011, Rec. 1826/2010[15].

[15] En el asunto, el trabajador es despedido por motivos disciplinarios, por falta muy grave. La empresa realizó un procedimiento de auditoria interna en las redes de información con el objeto de revisar la seguridad del sistema y detectar posibles anomalías en la utilización de los medios puestos a disposición de los empleados. Se comprobó que desde el ordenador utilizado por los jefes de turno de mantenimiento (uno de los cuales es el trabajador despedido) se accedió a internet en horas de trabajo con visitas a páginas referidas al mundo multimedia-vídeos, piratería informática, anuncios, televisión, contactos, etc. La gran mayoría de esas visitas se produjeron en los turnos de trabajo del trabajador y en tramos horarios en los que aquél estaba en el despacho. En el caso, indica el TS que no consta que la empresa hubiera establecido previamente algún tipo de reglas para el uso de dichos medios, ni tampoco que se hubiera informado a los trabajadores de que se iba a proceder al control y de los medios a aplicar en este caso.

La STS Sala General 6-10-2011, rec. 4053/10, afianza el criterio de que una prohibición empresarial de uso personal neutraliza la expectativa de privacidad para el trabajador. En el asunto, que concluye con el despido disciplinario de la trabajadora, la empresa entregó a todos los trabajadores una carta en la que se comunicaba que quedaba terminantemente prohibido el uso de medios de la empresa (ordenadores, móviles, internet, etc.) para fines propios, tanto dentro como fuera del horario de trabajo. La empresa decidió hacer una comprobación sobre el uso de sus medios de trabajo para lo que procedió a la monitorización de los ordenadores de varias trabajadoras.

Para el TS, la cuestión clave –"admitida la facultad de control del empresario y la licitud de una prohibición absoluta de los usos personales"– consistía en determinar si existe o no un derecho del trabajador a que se respete su intimidad cuando, en contra de la prohibición del empresario o con una advertencia expresa o implícita de control, utiliza el ordenador para fines personales. Para el TS, "la clara y previa prohibición de utilizar el ordenador de la empresa para cuestiones estrictamente personales" debe conducir a afirmar que "si no hay derecho a utilizar el ordenador para usos personales, no habrá tampoco derecho para hacerlo en unas condiciones que impongan un respeto a la intimidad o al secreto de las comunicaciones, porque, al no existir una situación de tolerancia del uso personal, tampoco existe ya una expectativa razonable de privacidad y porque, si el uso personal es ilícito, no puede exigirse al empresario que lo soporte y que además se abstenga de controlarlo". Estamos ante un claro razonamiento desde el criterio de la existencia de una expectativa de privacidad.

Desde este enfoque, además, la STS 6-10-2011 introduce una importante novedad en esta doctrina ya asentada, puntualizando que la prohibición de uso personal y las advertencias sobre posibles controles de los medios digitales no son dos requisitos acumulables, esto es, la prohibición absoluta lleva implícita la posibilidad de controles de uso de los medios digitales. El TS en esta sentencia estima que no existe contradicción con la STS 26-9-2007, porque en el supuesto planteado en ésta no existía prohibición de uso personal del ordenador ni advertencia de control, a diferencia del caso abordado en 2011. De manera que "lo decisivo a efectos de considerar la vulneración del derecho fundamental, es que "la tolerancia" de la empresa es la que "crea una expectativa de confidencialidad" y, por ende, la posibilidad de un exceso en el control llevado a cabo por el empleador que vulnere el derecho fundamental de la intimidad del trabajador. Pero si hay prohibición de uso personal deja de haber tolerancia y ya no existirá esa expectativa, con independencia de la información que la empresa haya podido proporcionar sobre el control y su alcance". Este enfoque, sin embargo, margina el derecho del trabajador a la protección de datos, y una de sus principales garantías, el derecho de información previa, en contradicción con la STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, como veremos. El voto particular a la sentencia precisamente considera que estamos ante dos requisitos acumulables. De forma que en el caso se viola la expectativa de privacidad porque, aunque se comunicó por escrito la prohibición del uso con fines particulares de los medios digitales, no se informó que iba a existir un control, y los medios que iba a utilizar para comprobar la corrección del uso del ordenador.

Pero la sentencia, además, introduce otro enfoque en su enjuiciamiento. Al mismo tiempo que valora el asunto desde la perspectiva de la existencia de una expectativa de privacidad, la sentencia se detiene en valorar las características del control efectuado por la empresa. Se observa en este sentido que se trataba de un sistema "pasivo", poco agresivo, que no permitía acceder a los archivos del ordenador que están protegidos por contraseñas de cada uno de los usuarios. Se procedió a visualizar el proceso de monitorización del ordenador de una de las trabajadoras en presencia de ésta, de las dos personas que habían procedido a la monitorización, de representantes

de la empresa y de los trabajadores y de otros dos trabajadores. En realidad, lo que hace el TS en esta sentencia es modificar su criterio de razonamiento con respecto a sentencias anteriores. La neutralización del principio de privacidad no impide al órgano judicial valorar las características de la intromisión empresarial bajo el prisma del principio de proporcionalidad. Se puede decir que la Sala General relativiza el principio de trasparencia, evaluándolo junto a otros criterios dentro del juicio de proporcionalidad, verificándose la existencia de un fin legítimo y la proporcionalidad y minimización del control efectuado por la empresa.

En el caso de la STS 8-2-2018, rec. 1121/2015, no se estima violado el derecho a la intimidad del trabajador por el hecho de que la empresa decida examinar su correo electrónico profesional, tras el hallazgo casual de documentos que ponen de manifiesto una actuación irregular del mismo en su relación con proveedores. Consta en el caso que los empleados, cada vez que acceden con su ordenador a los sistemas informáticos de la compañía, y de forma previa a dicho acceso, deben de aceptar las directrices establecidas en la Política de Seguridad de la Información de la empleadora, en la que se señala que el acceso lo es para fines estrictamente profesionales, reservándose la empresa el derecho de adoptar las medidas de vigilancia y control necesarias para comprobar la correcta utilización de las herramientas que pone a disposición de su empleados. La sentencia concluye que no existe una tolerancia del uso personal de los medios digitales, ni por tanto de expectativa de intimidad para el trabajador. Pero esta sentencia añade en su juicio que el control empresarial lo fue mediante un ponderado examen del correo electrónico (se examinó el contenido de ciertos correos electrónicos de la cuenta de correo corporativo del trabajador, pero no de modo genérico e indiscriminado), utilizando el servidor de la empresa y parámetros de búsqueda informática orientados a limitar la invasión en la intimidad, lo que "evidencia que se han respetado escrupulosamente los requisitos exigidos por la jurisprudencia constitucional y se han superado los juicios de idoneidad, necesidad y proporcionalidad".

Por tanto, en la doctrina del TS, a partir de la delimitación de los usos autorizados y prohibidos (y por tanto de las expectativas de privacidad del trabajador), la legitimidad de los controles empresariales debe valorarse a partir de un juicio de proporcionalidad, dentro del cual se incluye el criterio de la trasparencia informativa. Esto nos ayuda a entender el *modus operandi* del TS en estas sentencias, donde, a pesar de la inexistencia de una expectativa de confidencialidad, y por tanto de conflicto con el derecho a la intimidad, el mismo TS enjuicia los supuestos tal como si el conflicto existiese, aplicando el juicio de proporcionalidad.

La doctrina de suplicación se acoge a esta doctrina del TS. En primer lugar, se considera que el trabajador tiene una expectativa razonable de confidencialidad, según la cual puede realizar un uso moderado, con fines privados, de los dispositivos digitales facilitados por la empresa, como herramientas de trabajo[16]. En segundo lugar, la expectativa razonable de confidencialidad puede neutralizarse por el empresario mediante la prohibición expresa del uso para fines privados de los dispositivos digitales, facilitados por la empresa. En este caso, la intimidad deja de ser alegable frente a intromisiones empresariales[17].

[16] La STSJ Islas Canarias 3-4-2017, rec. 743/2016, concluye que el uso del correo electrónico y demás instrumentos de comunicación empresarial para fines particulares es lícito, aunque no haya sido pactado, siempre y cuando se cumplan las siguientes condiciones: a) que se haya puesto a disposición del trabajador por la empresa el instrumento de comunicación informática por motivos laborales; b) que no se perturbe la actividad normal de la empresa mediante el uso privado; c) que no se vea perjudicado el uso específicamente productivo del instrumento; y d) que no suponga un gravamen económico para la empresa por su uso. De manera que "la prohibición del uso para fines privados del instrumento de comunicación en tales condiciones podría vulnerar el derecho a la libertad individual de expresión y comunicación de los trabajadores".

[17] STSJ Andalucía 3-5-2018, rec. 2195/17. La STSJ Islas Canarias 3-4-2017, citada en la nota anterior, observa que "si la empresa prohíbe el uso de estos medios para fines particulares, la prohibición determina que ya no exista una situación de to-

En tercer lugar, en suplicación se exige una información previa, clara y completa del alcance de la prohibición de usos personales, así como de la extensión y la naturaleza de la vigilancia llevada a cabo por su empleador. Para la STSJ Asturias 14-11-2017, rec. 1895/17, dichas exigencias no se cubren con afirmaciones sobre prohibiciones generales como las plasmadas en las comunicaciones de la empresa a los trabajadores[18]. En el caso de la STSJ Comunidad Valenciana 19-11-2018, rec. 2490/18, la trabajadora no fue informada previamente, como exigía el protocolo empresarial, de la instalación en su ordenador de un programa informático "espía" que monitorizaba y registraba toda su actividad de navegación en internet, su mensajería electrónica y la consulta de archivos informáticos[19]. La sentencia concluye que dicha medida de vigilancia fue utilizada por el empresario sin adoptar las garantías previstas en el protocolo, y por tanto incumpliendo su obligación de información previa y clara sobre las medidas de control.

En esta línea, el hallazgo de irregularidades en el ordenador del trabajador con motivo de una revisión de seguridad del sistema, de control y eliminación de virus, es ilícita cuando no se cumple con la exigencia de una información previa. En el caso de la STSJ Islas Canarias 3-4-2017, rec. 743/2016. en lugar de limitarse al control y eliminación del virus, se siguió con el examen del ordenador para entrar y examinar archivos cuyo control no puede considerarse que fuera necesario para realizar la reparación interesada (fotografías personales, descargas de internet, rastros de navegación y dispositivos ajenos a la empresa). De esta forma, no cabe entender que estemos ante un hallazgo casual, pues se ha ido más allá de lo que la entrada regular para la reparación justificaba. Por ello, la medida adoptada por la empresa sin previa advertencia sobre el uso y el control del ordenador, supone una lesión a la intimidad de la trabajadora despedida[20].

La debida información se entiende cumplida si la prohibición se contempla en el convenio colectivo, en el contrato de trabajo o en la normativa sobre las técnicas de información y comunicación de la empresa (STSJ Andalucía 28-3-2019, rec. 744/18).

En cuarto lugar, aunque la información previa elimina la expectativa de privacidad, sin embargo, el control que ejerce la empresa sobre los medios digitales del trabajador se somete al principio de proporcionalidad. La STSJ Comunidad Valenciana 19-11-2018, rec.

lerancia con el uso personal del ordenador y que tampoco exista lógicamente una expectativa razonable de confidencialidad. En estas condiciones el trabajador afectado sabe que su acción de utilizar para fines personales el ordenador no es correcta y sabe también que está utilizando un medio que, al estar lícitamente sometido a la vigilancia de otro, ya no constituye un ámbito protegido para su intimidad". En el asunto, no consta que existiera por parte de la empresa ningún instrucción u orden en contrario, ni que la demandante llevara a cabo dicha conexión con ocultamiento, lo que viene a indicar que lo utilizaba mayormente para cuestiones de trabajo, sin perjuicio de que en su interior hubiera datos (fotos, video, etc) personales y que al conectarse al sistema de la empresa le hubiera podido traspasar un virus.

[18] En el asunto, la sentencia declara probado que la empresa advertía a sus trabajadores que "está terminantemente prohibido utilizar los ordenadores para labores que no sean exclusivamente relacionadas con el ámbito laboral" y alude a la declaración de varios trabajadores sobre el envío por la demandada cada cierto tiempo de "correo electrónico a todos los usuarios de las herramientas y aplicaciones informáticas de la empresa de aviso y recordatorio de que el ordenador solo se podía utilizar para usos profesionales, que incluso hubo advertencias de inspección para comprobar el uso que realizaban".

[19] Conforme al protocolo empresarial, la empresa "se reserva el derecho de revisar, cuando la defensa del patrimonio de la empresa y el de los demás trabajadores así lo exija, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a internet iniciada por los usuarios de la red corporativa y los mensajes de correo electrónico de éstos, siempre en presencia de dichos/s usuario/s y de su representante o de otro trabajador si ello no fuera posible, y los archivos LOG del servidor, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la empresa como responsable civil subsidiario". Sin embargo, la empresa procedió a instalar un programa espia en todos los ordenadores de la empresa para monitorizar y registrar toda la navegación por internet, sin comunicarlo, previamente al representante de los trabajadores. Dicho programa pasa desapercibido para el usuario y captura todo lo que hay en el ordenador.

[20] Igualmente, STSJ Islas Canarias 6-6-2017, rec. 12/17.

2490/18, citada anteriormente, estima que, aparte de una información previa insuficiente, la empresa no ha probado la existencia de un motivo concreto y legítimo que justifique el establecimiento de un sistema de vigilancia para monitorizar y registrar toda la navegación por internet y los correos electrónicos de la trabajadora. Por otra parte, tampoco es proporcional al objetivo genérico expresado en el protocolo empresarial: la defensa del patrimonio de la empresa y el derecho de otros trabajadores. Este objetivo puede alcanzarse con métodos menos intrusivos que el acceso al contenido de las comunicaciones y archivos de la demandante, como la exclusión de conexiones a determinadas páginas web o el control del tráfico en internet o de la mensajería electrónica, pero no el de su contenido.

2.2. La doctrina del Tribunal Constitucional en el uso de medios digitales laborales

La doctrina constitucional en su canon de razonamiento básicamente se alinea con la doctrina del TS descrita. El TC estima, en primer lugar, que el uso de los medios digitales por el trabajador, y en particular el control de sus comunicaciones vía correo electrónico, están protegidas por el derecho a la intimidad (art. 18.1 CE) y el secreto de las comunicaciones (art. 18.3 CE). En las dos sentencias que constituyen la referencia en la doctrina constitucional (SSTC 241/2012 y 170/2013) se denuncia la violación de tales derechos fundamentales.

El TC ha puesto de manifiesto que "el cúmulo de información que se almacena por su titular en un ordenador personal –entre otros datos sobre su vida privada y profesional– forma parte del ámbito de la intimidad constitucionalmente protegido; también que el ordenador es un instrumento útil para la emisión o recepción de correos electrónicos, pudiendo quedar afectado el derecho a la intimidad personal en la medida en que estos correos o email, escritos o ya leídos por su destinatario, quedan almacenados en la memoria del terminal informático utilizado" (STC 170/2013, FJ 5, con cita de la STC 173/2011, FJ 3). Por otro lado, también considera el TC que la injerencia en los archivos de las comunicaciones de los trabajadores mediante el acceso al ordenador en que están depositados es un supuesto con relevancia constitucional al amparo del art. 18.3 CE, como vamos a ver.

En segundo lugar, el TC resuelve el conflicto de intereses realizando una ponderación de bienes constitucionalmente relevantes a partir de la configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin. Al igual que lo hace la jurisprudencia del TS, el TC reconoce la facultad empresarial de prohibición del uso personal de los medios digitales puestos a disposición del trabajador, lo que elimina toda expectativa de privacidad y excluye la tutela del derecho a la intimidad o al secreto de las comunicaciones. En supuestos donde la empresa sólo autoriza al trabajador el uso profesional de los medios digitales de trabajo "el poder de control de la empresa sobre las herramientas informáticas de titularidad empresarial puestas a disposición de los trabajadores podía legítimamente ejercerse, ex art. 20.3 LET, tanto a efectos de vigilar el cumplimiento de la prestación laboral realizada a través del uso profesional de estos instrumentos, como para fiscalizar que su utilización no se destinaba a fines personales o ajenos al contenido propio de su prestación de trabajo" (STC 241/2012, FJ 5[21]). Se subraya que la pro-

[21] En la STC 241/2012, la empresa para la que presta servicios la trabajadora despedida accede a los ficheros informáticos en que quedaban registradas las conversaciones mantenidas por aquella con otra compañera a través de un programa de mensajería instalado por ellas mismas en un ordenador de uso común y sin clave de acceso. La sentencia estimará que no existe una expectativa razonable de privacidad, y por tanto no cabe apreciar afectación del derecho a la intimidad, desde el momento en que la empresa había prohibido expresamente a los trabajadores instalar programas en el ordenador, y, por otro lado, las trabajadoras instalaron dichos programas en el disco del ordenador, en el cual podían ser leídas por cualquier otro

hibición expresa por la empresa del uso personal de los medios digitales (la instalación de programas personales en el ordenador) "en modo alguno aparece como arbitraria en tanto que se enmarca en el ámbito de las facultades organizativas del propio empresario" (STC 241/2012, FJ 6). La STC 241/2012, como vemos, es un claro exponente de la primacía del criterio de la expectativa de privacidad que considero en clara contradicción con la doctrina de la STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*.

En tercer lugar, el canon de razonamiento parte, como vemos, de la premisa de la existencia o no de una expectativa de privacidad, pero, al igual que hemos visto en la doctrina del TS, ello no es excluyente de la valoración de las características de la injerencia empresarial a la luz del principio de proporcionalidad.

En el caso de la STC 170/2013, la empresa, sin información previa al trabajador, fiscalizó los contenidos de los correos electrónicos del ordenador que la empresa facilitó al aquel, de los que se deducía una actuación laboral irregular del mismo (transmisión a terceros de información reservada de la empresa). Existe una implícita prohibición convencional del uso extralaboral del correo electrónico y su consiguiente limitación a fines profesionales (dentro del régimen disciplinario del convenio), lo que desde luego no se puede considerar como información expresa y calara a los trabajadores al respecto. Como quiera que sea, entiende la sentencia que, al no existir una expectativa de privacidad, dada la prohibición, no es alegable el derecho a la intimidad (art. 18.1 CE). Por otra parte, el TC estima que la remisión de mensajes enjuiciada se llevó a cabo a través de un canal de comunicación que, conforme a las previsiones legales y convencionales, se hallaba abierto al ejercicio del poder de inspección reconocido al empresario; con lo que quedaba fuera de la protección constitucional del art. 18.3 CE.

Pero en esta sentencia, el TC procede también mediante un juicio de proporcionalidad. Tras la valoración de las exigencias de justificación (existencia de sospechas), idoneidad (verificar la revelación de información empresarial a terceros), necesidad (el texto de los correos era prueba necesaria) y proporcionalidad en sentido estricto (control con garantías, ceñidos a los correos reveladores de la actuación del trabajador, que se limitan a la información relativa a la empresa), concluye que, "una vez ponderados los derechos y bienes en conflicto", el Tribunal considera que "la conducta empresarial de fiscalización ha sido conforme a las exigencias del principio de proporcionalidad" (FJ 5, c). Desde esta perspectiva podemos decir que la doctrina constitucional entronca con la más reciente doctrina del TEDH, que pasamos a ver.

2.3. La doctrina del TEDH: la centralidad del juicio de proporcionalidad

La doctrina del TEDH referida al art. 8 CEDH es una referencia central para los supuestos de control empresarial de los medios digitales a disposición del trabajador, ofreciendo una interpretación expansiva del alcance del derecho a la privacidad del trabajador.

El TEDH favorece una interpretación ampliatoria del derecho a la vida privada[22]. Es

usuario, pudiendo trascender su contenido a terceras personas; como ocurrió en el caso al tener conocimiento la dirección de la empresa, lo que determinó la eliminación de la privacidad de sus conversaciones.

[22] Este derecho "no se presta a una definición exhaustiva" (STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, ap. 70). El Tribunal reconoce que toda persona tiene derecho a una vida privada, lejos de la injerencia no deseada de otros y considera que sería demasiado restrictivo limitar la noción de "vida privada" a un "círculo íntimo"; así, el artículo 8 garantiza un derecho a la "vida privada" en sentido amplio, que incluye el derecho a realizar una "vida privada social", es decir, la posibilidad de que el individuo desarrolle su identidad social (STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, ap. 70). Esta identidad social puede incluir actividades de naturaleza comercial, profesional o laboral. Sobre el alcance del concepto de vida privada en la jurisprudencia del TEDH, cfr. F. Pérez de los Cobos Orihuel, *El*

firme la consideración de que el concepto de "vida privada" puede incluir actividades profesionales; de hecho, se subraya que "es en el marco de la vida laboral donde la mayoría de la gente tiene muchas, si no la mayoría, de las oportunidades para fortalecer sus lazos con el mundo exterior" (STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, ap. 71). Y en este contexto laboral, deben ser examinadas a la luz del art. 8 CEDH las prácticas empresariales de vigilancia de dispositivos digitales a disposición del trabajador, la interceptación de las comunicaciones por esta vía (a través del correo electrónico), e igualmente el acceso y recopilación de datos personales contenidos en dichos dispositivos (por ejemplo, mediante el seguimiento del uso que hace el trabajador de internet) (STEDH (Gran Sala) *asunto Barbulescu*, ap. 72).

En particular, el TEDH, desde la STEDH 25-6-1997, *asunto Halford contra Reino Unido*, avanza hacia una interpretación amplia de la noción de "correspondencia" amparado por el art. 8 CEDH, afirmando un concepto funcional y no literal de la noción que incluye la comunicación individual a través de cualquier soporte, y las comunicaciones realizadas desde el ámbito profesional o laboral. De esta forma, el TEDH concluye que la noción de "correspondencia" del art. 8.1 CEDH se aplica al envío y recepción de mensajes, incluso desde el ordenador de la empresa empleadora (STEDH 3-4-2007, *asunto Copland contra Reino Unido*, ap. 41 y 45; STEDH 5-9-2017, *asunto Barbulescu*, ap. 74).

Respecto del uso por el trabajador de los medios digitales de la empresa, el TEDH sienta la siguiente doctrina. En primer lugar, se afirma la doctrina de una expectativa razonable de privacidad como canon de valoración de la legitimidad de las facultades empresariales de control de la actividad laboral. Sin embargo, no basta con indicaciones generales por la empresa sobre el uso laboral de los medios digitales, sino que es necesaria una indicación previa, clara y precisa sobre los usos permitidos y los controles al respecto, a partir de donde se delimita la expectativa de privacidad del trabajador[23]. En segundo lugar, y no menos relevante, para el TEDH el poder de control y las injerencias en el uso por el trabajador de los medios digitales se somete necesariamente a un juicio de proporcionalidad. La STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, configura un canon de garantías sobre la aplicación del juicio de proporcionalidad en relación con el derecho a la privacidad del trabajador en su actividad laboral (art. 8 CEDH). Esta sentencia referirá dicho canon en concreto al control de las comunicaciones electrónicas del trabajador[24]. Posteriormente, la STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, va a aplicar dicho canon de garantías a los instrumentos de videovigilancia en el lugar de trabajo[25]. Se puede decir que el test

derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado, *cit.* p. 8 y sigs.

[23] M.E. Casas Bahamonde, en su análisis de la sentencia, estima que la obligación de información previa es la gran aportación del TEDH en el *asunto Barbulescu*. Trasladando esta doctrina a nuestro derecho interno supondría que "esa información previa es contenido de los derechos fundamentales a la intimidad, al secreto de las comunicaciones, a la propia imagen y a la protección de datos de carácter personal (art. 18.1, 3 y 4 CE)". Cfr, de la autora, "*Informar antes que 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*", *en Derecho de las Relaciones Laborales*, nº 2, 2018, p. 115.

[24] En concreto, la STEDH (Gran Sala) 5-9-2017 revoca la STEDH (Sección 4ª) 12-1-2016, y declara que en el asunto se ha producido una violación del art. 8 del CEDH. En el caso se aborda la injerencia en el contenido de la correspondencia electrónica. En la sentencia el control se realiza sobre el medio electrónico corporativo del trabajador (una cuenta de Yahoo Messenger). A través de esta cuenta se canalizan las comunicaciones profesionales, pero también se intercambiaron comunicaciones de carácter personal con su novia y su hermano, algunas de estas comunicaciones eran íntimas.

[25] La STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, revoca la dictada por la Sección 3ª del TEDH de 9-1-2018 y declara que en el asunto no se ha producido una violación del art. 8 del CEDH. El supuesto se refiere a la instalación de medios de videovigilancia encubierta o secreta de las cajeras de un supermercado. En la sentencia se estima la justificación que los tribunales españoles otorgan a la videovigilancia (el interés legítimo empresarial en identificar a los responsables de las importantes pérdidas detectadas y sancionarles), considera

de legitimidad diseñado por el TEDH tiene un alcance general respecto de los medios de vigilancia empresarial[26], que incluye el uso por el trabajador de los dispositivos digitales.

Refiriéndose a la doctrina de una expectativa razonable de privacidad, la STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, fija una premisa relevante, que la mera prohibición no justifica el sacrificio puro y duro de la privacidad de las comunicaciones del trabajador. Dicho en otros términos, el que no haya una expectativa de privacidad no legitima un poder absoluto y sin restricciones del control empresarial. Indica la sentencia: "No está claro que las normas restrictivas de la empresa empleadora dejaran al demandante con la expectativa razonable de privacidad – una expectativa que queda por determinar. Sin embargo, las instrucciones de una empresa no pueden anular el ejercicio de la privacidad social en el puesto de trabajo. El respeto a la privacidad y confidencialidad de las comunicaciones sigue siendo necesario, aunque pueden limitarse dentro de las medidas de necesidad" (ap. 80). Es destacable en esta asunto que la empresa había prohibido expresamente el uso personal de los medios electrónicos corporativos (la previsión se contiene en el reglamento interno de la empresa, que el empleado conoce, y en una nota informativa posterior, que también es de conocimiento del trabajador), pero el TEDH considera en esta sentencia que no queda claro que, *además*, se advirtiera con antelación del alcance del control empresarial, que afectó incluso a las comunicaciones privadas del trabajador, ni consta que se justificara la razón por la que se realizó este control específico, no siendo suficiente con justificaciones en abstracto.

Pero la sentencia no niega abiertamente la hipótesis de una política empresarial de prohibición del uso personal de los medios electrónicos, y en todo caso reconoce la legitimidad de las injerencias empresariales en el secreto de las comunicaciones en determinadas circunstancias. En esta línea, la posterior STEDH 22-2-2018, *asunto Libert*, considera que "los archivos creados por el empleado con la ayuda de la herramienta informática puesta a su disposición por el empleador para el desempeño de su trabajo se suponen de carácter profesional, por lo que el empleador tiene derecho a abrirlos en su ausencia, excepto si están identificados como personales" (ap. 49)[27].

Lo que la sentencia *Barbulescu* pretende subrayar es que, incluso existiendo una prohibición empresarial absoluta, es necesario que el control empresarial del uso de los dispositivos digitales por el trabajador respete el test de legitimidad o el juicio de proporcionalidad. El test de legitimidad elaborado por el TEDH revaloriza el papel de este canon tradicional respecto del art. 8 CEDH. Se trata de criterios que, por lo demás, ya están presentes en la re-

razonables las medidas de videovigilancia adoptadas, y concluye que la videovigilancia oculta puede ser legítima conforma a un juicio de proporcionalidad, al margen de exigencias de trasparencia informativa.

[26] En este sentido, J.L. Goñi Sein, "*La protección de las comunicaciones electrónicas del trabajador…*", *cit.* p. 14.

[27] En el caso de la STEDH 22-2-2018, *asunto Libert*, el Tribunal declara inexistente una violación del art. 8 CEDH. En el asunto, el empleador abrió archivos personales almacenados en el disco duro del ordenador profesional del trabajador, sin información previa y en su ausencia. Según la legislación francesa, el empleador puede abrir los archivos profesionales almacenados en el disco duro de los ordenadores que pone a disposición de sus empleados para el desempeño de sus funciones, pero no puede, "excepto riesgo o acontecimiento especial", abrir archivos identificados como personales. Únicamente podrá proceder a la apertura de los archivos identificados como personales en presencia de los empleados afectados o después de que hayan sido debidamente informados. Estas son reglas seguidas por los tribunales franceses en el enjuiciamiento del caso. En particular se aplicó la regla jurisprudencial interna conforme a la cual el empleador, en principio, no puede abrir los archivos identificados por el empleado como "personales". Sin embargo, en el caso el trabajador no respetó la regla del manual del usuario para la utilización de los sistemas informativos de la empresa, que indica específicamente que las "informaciones de carácter privado deben estar claramente identificadas como tales". Sin embargo, el trabajador identificó los archivos como "personales" y no como "privados", lo que permitió presumir el carácter profesional de tales archivos y por tanto la legitimidad de la injerencia empresarial en los mismos (ap. 52). El Tribunal recuerda que es necesario considerar "las decisiones impugnadas a la luz del conjunto de la causa" (ap. 53).

gulación en la materia, como ponen de manifiestos los sucesivos dictámenes del Grupo de Trabajo del Artículo 29 (GT29), refiriéndose a la Directiva 95/46/CE y el RGPD 2016/679[28].

El test de legitimidad, como vía de concreción del juicio de proporcionalidad, es sintetizado por la STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, a partir de los siguientes factores: i) si ha existido información previa sobre la medida empresarial de control (principio de trasparencia); ii) la existencia de motivos legítimos (justificación de la injerencia); iii) las características de las medidas empresariales y el grado de injerencia en la vida privada del trabajador; en este sentido debe valorarse si eran posible o no medidas menos intrusivas para alcanzar dicho fin; iv) la coherencia del uso que el empresario ha hecho de las medidas de control respecto de la finalidad que las justificó; v) la existencia de garantías adecuadas, como la información ofrecida, la traslación de la información a un organismo independiente o la posibilidad de reclamaciones. En la aplicación del test de legitimidad será fundamental considerar el ámbito en que se concreta el control empresarial (audio o videovigilancia, monitorización de las comunicaciones del trabajador, control del uso de los medios digitales de trabajo y en particular de su correo electrónico).

Conforme al test de legitimidad, en primer lugar, se considera esencial respetar un criterio de trasparencia, de forma que el empleado ha debido ser informado de la posibilidad del empleador de adoptar medidas de control y su aplicación. En el *asunto Barbulescu*, la Gran Sala puntualiza, en relación con el control de las comunicaciones del trabajador, que "la advertencia debe ser, en principio, clara en cuanto a la naturaleza de la supervisión y antes del establecimiento de la misma" (ap. 120, i). Cabe deducir del principio de transparencia que no es posible amparar en genéricas prohibiciones absolutas iniciales la legitimidad de controles ocultos del correo electrónico por inexistencia de expectativa de privacidad. De hecho, en esta sentencia se estima que los órganos jurisdiccionales nacionales no consiguieron, por un lado, comprobar, concretamente, si el empleador había notificado previamente al demandante la posibilidad de que sus comunicaciones iban a ser controladas y, por otro, no comprobaron igualmente si se le había informado de la naturaleza y alcance de la vigilancia a que iba a ser sometido, así como del grado de intrusión en su vida privada y en su correspondencia.

Hay que advertir, sin embargo, que en la STEDH 22-2-2018, *asunto Libert*, el Tribunal relativiza el papel de las garantías de transparencia de la política empresarial de vigilancia en el tratamiento de datos: la notificación previa y clara al trabajador de la posibilidad de un control de los archivos del ordenador; la información previa sobre la naturaleza y alcance de la vigilancia a que podía ser sometido, así como del grado de intrusión en su vida privada.

Por su parte, la STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, recuerda que "la exigencia de trasparencia y el derecho a la información que se deriva del mismo reviste un carácter fundamental" e implica, en principio, la necesidad de informar previamente y con claridad (ap. 131); pero entiende el TEDH que es posible justificar la ausencia de información previa cuando exista "un imperativo preponderante relativo a la protección de intereses públicos o privados importantes" (ap. 133). Entiende la Gran Sala que el canon de razonamiento a seguir implica que "la información ofrecida a la persona sometida a la vigilancia y su amplitud no es sino uno de los criterios a tener en cuenta para apreciar la proporcionalidad de tal medida" (ap. 131).

En segundo lugar, conforme al test de legitimidad, debe existir una justificación para

[28] GT29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, 17/ES, WP 249, que complementa y sintetiza las publicaciones anteriores del GT29: el Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral (WP48) y el Documento de trabajo relativo a las comunicaciones electrónicas en el lugar de trabajo (WP55) de 2002.

el control empresarial. Conforme al art. 8.2 CEDH, la garantía de protección de "los derechos y las libertades de los demás" pueden referirse a los del empleador, "que legítimamente puede querer asegurarse de que sus empleados utilizan los equipos informáticos puestos a su disposición para el desempeño de sus funciones, conforme a sus obligaciones contractuales y a la reglamentación aplicable" (STEDH 22-2-2018, *asunto Libert*, ap. 46). En el *asunto Barbulescu*, la Gran Sala estima legítimos ciertos objetivos, aunque nunca en abstracto, como la necesidad de evitar una vulneración en los sistemas informáticos de la empresa, evitar el cuestionamiento de la responsabilidad de la empresa en caso de actividad ilegal en el espacio virtual, así como la divulgación de sus secretos comerciales (ap. 134). En el caso abordado, el TEDH concluye que los tribunales nacionales mencionan estos objetivos en términos teóricos, ya que no se acusó concretamente al demandante de exponer a la empresa a ninguno de esos riesgos (ap. 134). Por otro lado, la sentencia subraya que la justificación requerida debe ponerse en relación con la naturaleza y alcance del control empresarial e indica que en el caso abordado "la vigilancia del contenido de las comunicaciones … requiere justificaciones más fundamentadas" (ap. 120, iii).

En tercer lugar, el test exige el respeto del principio de proporcionalidad y de minimización. Este criterio debe tomar en consideración el tipo de medida adoptada y sus características, que deben regirse por el principio de minimización (limitada a lo necesario para el fin pretendido). En el asunto *Barbulescu* se estima que, en el caso del control de las comunicaciones del trabajador, deben tomarse en consideración distintos aspectos. El principio de proporcionalidad será de distinta intensidad si el control se limita al flujo de comunicaciones o incluye también el de su contenido. También se debería tener en cuenta si la supervisión de las comunicaciones se ha realizado sobre la totalidad o sólo una parte de ellas y si ha sido o no limitado en el tiempo y el número de personas que han tenido acceso a sus resultados (ap. 133, iv).

3. EL TRATAMIENTO DEL USO DE DISPOSITIVOS DIGITALES EN EL ÁMBITO LABORAL EN LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS

3.1. Los parámetros normativos del art. 87 LOPD

El RGPD (Reglamento (UE) 2016/679) y la LOPD (Ley Orgánica 3/2018) constituyen el marco regulador de referencia respecto a la protección de los derechos fundamentales del trabajador frente a las facultades empresariales de control. La perspectiva jurídica la fija el RGPD, estableciendo como mandato que las normas específicas estatales, a las que se remite, "incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales", con especial atención "a la transparencia del tratamiento, … y a los sistemas de supervisión en el lugar de trabajo" (art. 88.2).

Se puede decir que este marco regulador se apoya en la legitimación del poder de control empresarial en las relaciones laborales dentro de un marco normativo basado en los principios de legitimidad de fines, transparencia en la información y proporcionalidad en los métodos de control de medios digitales de trabajo. Estos parámetros delimitadores de la legitimidad de los poderes empresariales de control se consolidan expresamente en el Protocolo, aprobado en 2018, de revisión del Convenio nº 108 del Consejo de Europa, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*[29]. Este Convenio clarifica las bases legales bajo las cuales se considera legítimo el tratamiento de los datos personales y subraya, en la nueva versión de su art. 5º, determinados principios a respetar en el procesamiento de datos, en particular, el principio de trasparencia, el de proporcionalidad de acuerdo

[29] Protocolo de modificación del Convenio de 18 de mayo de 2018, adoptado en la 128.ª sesión del Comité de Ministros del Consejo de Europa.

con el fin legítimo perseguido y el de minimización del procedimiento.

El RGPD no establece una regulación específica de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, limitándose a remitirse a la regulación específica que puedan establecer los Estados a través de disposiciones legislativas o de convenios colectivos (art. 88). La LOPD da respuesta a este mandato mediante su Título X, referido a la "Garantía de los derechos digitales" (art. 79 y sigs.), donde se incluye el precepto de nuestro interés, el art. 87, referido al "Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral".

La configuración técnica de las garantías legales es deficiente, porque la protección se sitúa en el derecho a la intimidad (art. 87.1 LOPD y 20 bis ET), cuando también deben contemplarse los derechos al secreto de las comunicaciones y a la protección de datos. Por otro lado, en los preceptos de la LOPD referidos a la relación laboral la perspectiva fundamental no es tanto el reconocimiento de "derechos digitales", cuanto la protección de los derechos fundamentales del trabajador frente a las facultades empresariales de vigilancia y control de la actividad laboral[30].

El art. 87 LOPD se construye desde tres parámetros. En primer lugar, la norma se inicia en su apartado primero resaltando esta perspectiva, al establecer que "Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador". Esta perspectiva constitucionalista, implícita en el propio tratamiento formal de la norma[31], se va a traducir en concretas reglas y obligaciones en el ejercicio empresarial de aquellas facultades. La regulación aquí es relevante porque estaría fijando el marco de las injerencias legítimas en la privacidad del trabajador amparada por el art. 8.2 CEDH[32]. En segundo lugar, recoge una consolidada jurisprudencia en virtud de la cual, en el marco de las facultades de autoorganización, dirección y control correspondientes al empresario, es admisible la ordenación y regulación del uso de los medios informáticos de titularidad empresarial, así como su facultad de vigilancia y control del cumplimiento de las obligaciones relativas a la utilización del medio en cuestión, siempre con pleno respeto a los derechos fundamentales (SSTC 241/2012 y 170/2013). En tercer lugar, se apuesta por una perspectiva preventiva, exigiendo a la empresa el establecimiento de una política sobre el uso de dispositivos digitales y la garantía a este respecto de una información previa al trabajador.

En el apartado 2º la norma reconoce el derecho del empleador a acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores, pero circunscribiéndolo a dos finalidades legítimas, esto es, "a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos". Esta justificación del control viene amparada por el art. 8.2 CEDH (las injerencias en la privacidad del trabajador pueden ampararse en "la protección de los derechos y las libertades de los demás") que, conforme a la jurisprudencia del TEDH comentada, legitima el interés empresarial en controles de cara al buen funcionamiento de la empresa y el cumplimiento por el trabajador de sus compromisos contractuales. La concreción de los fines legítimos del ap. 2º del art. 87 LOPD se puede matizar a la luz de la delimitación de tales fines por la jurisprudencia[33] o documentos sobre la materia[34].

---

[30] Cfr. en este sentido, J. García Murcia y I.A. Rodríguez Cardo, "*La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo*", en *Revista Española de Derecho del Trabajo*, nº 216, enero, 2019, págs. 58-59.

[31] No en vano, el precepto tiene naturaleza orgánica frente al art. 20 bis ET, dotado de rango de ley ordinaria *ex* DF 1ª LOPD.

[32] Conforme al art. 8.2 CEDH, "(n)o podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley…".

[33] Véase más atrás, STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, y STS 26-9-2007, rec. 966/2006.

[34] Por ejemplo, GT29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo (WP 249).

Cabe indicar, por un lado, que, conforme al criterio expuesto en el *asunto Barbulescu*, los legítimos objetivos que justifican la injerencia empresarial no pueden serlo en abstracto; por otro lado, será útil esta exigencia para valorar la proporcionalidad del tipo de control que se efectúa, por ejemplo, en casos de una medida empresarial de monitorización de los medios digitales por sospechas fundadas de ilícitos laborales por el trabajador[35]. Será aquí relevante distinguir si se trata del control de dispositivos de comunicación (móviles o correo electrónico) o el control de los contenidos en los correspondientes ficheros informáticos en que quedan registrados.

Finalmente, conviene recordar que el RGPD recoge entre los principios básicos en la protección de datos que los mismos deben ser recogidos "con fines determinados, explícitos y legítimos", y que serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" (art. 5.1 b) y c) RGPD), lo que resulta contrario a prácticas de monitorización indiscriminadas o permanentes.

Para garantizar el derecho a la intimidad del trabajador, el art. 87 LOPD establece dos tipos de garantías en su apartado 3º, la obligación empresarial de fijar criterios de utilización de los dispositivos digitales y un deber de información previa al trabajador.

3.2. La obligación empresarial de fijar criterios de utilización de los dispositivos digitales

Los empleadores deberán establecer criterios de utilización de los dispositivos digitales. En este sentido, la norma fija como pauta que se establecerán "respetando en todo caso" los estándares mínimos de protección de su intimidad "de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente". El respeto de los estándares constitucionales y legales mínimos parece de recibo; la referencia a los usos sociales entronca con la observación en la doctrina del TS de la evidencia de "una utilización personalizada y no meramente laboral o profesional del medio facilitado por la empresa", y "la generalización de una cierta tolerancia con un uso moderado de los medios de la empresa" (STS 26-9-2007).

En su elaboración "deberán participar" los representantes de los trabajadores (ap. 3, pár. 1º)[36]. Nada indica la norma sobre los términos de esta participación, que habrá que situar en el contexto de los derechos de participación de los mismos (art. 61 ET), y su concreción en los de información y consulta (arts. 64 ET). La norma de referencia aquí debe ser el art. 64.5 pár. 3º letra f) ET, que prevé el derecho de los representantes a emitir informe, con carácter previo a la ejecución por parte del empresario de las decisiones adoptadas por este, sobre la implantación y revisión de sistemas de organización y control del trabajo. Este derecho de consulta se refuerza con el art. 64.6 ET, que prevé un derecho de información que, al objeto de garantizar el efecto útil de esta previsión, debe tener lugar "en un momento, de una manera y con un contenido apropiados, que permitan a los representantes de los trabajadores proceder a su examen adecuado y preparar, en su caso, la consulta y el informe".

Debe tenerse en cuenta también el posible papel regulador para la negociación colectiva en la materia, respaldado tanto por el RGPD[37], como por la LOPD. El artículo 91 LOPD dispone que los convenios colectivos podrán establecer "garantías adicionales" de los derechos y libertades relacionados con el tratamiento de los datos

[35] J. Baz Rodríguez, "*La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático*", en *Trabajo y Derecho*, nº 54, junio, 2019, p. 58.

[36] Como se subraya en diversos documentos internacionales relevantes en este terreno: Recomendación CM/Rec(2015)5 del Comité de Ministros de los Estados miembros del Consejo de Europa (apartado 21 c)), e Informe 2/2017 del Grupo de Trabajo 29 en interpretación de la derogada Directiva 95/46/CE.

[37] Arts. 9 y 88 RGPD.

personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

La norma prevé implícitamente en su pár. 2º que, en la fijación de criterios, el empleador pueda admitir o excluir el uso de los dispositivos digitales con fines privados[38]. En efecto, el art. 87.3 pár. 2º LOPD se refiere a las reglas que el empleador debe respetar en el acceso al contenido de dispositivos digitales "respecto de los que haya admitido su uso con fines privados". La norma está reconociendo el supuesto de la existencia de medios digitales de trabajo respecto de los que el empresario *no* admite su uso privado. Como ya vimos, tanto la jurisprudencia del TC como del TS recogen el criterio de que se trata de medios que son propiedad de la empresa y por ello puede prohibirse absolutamente su uso para fines propios.

Hay que tener en cuenta que el apartado 3º del art. 87 LOPD centra las garantías de protección del trabajador en el supuesto de "acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados", dejando fuera del marco legal el supuesto de prohibición. Pero debemos recordar que, incluso existiendo una prohibición empresarial absoluta, es necesario que el control empresarial del uso de los dispositivos digitales por el trabajador respete el test de legitimidad o el juicio de proporcionalidad. Por ejemplo, el empresario estaría legitimado para realizar monitorizaciones aleatorias y puntuales de cara a verificar el respeto de las reglas de prohibición de uso particular de los medios digitales, limitando la intromisión en la privacidad del trabajador y evitando si no es necesario entrar en contenidos de "navegación", de la mensajería electrónica, de los archivos de los ordenadores, y con la información previa y clara sobre tales posibles controles[39]. En este sentido creo que debe entenderse la doctrina de la STEDH (Gran Sala), *asunto Barbulescu*, de que la mera prohibición no justifica la eliminación absoluta de la privacidad del trabajador.

Cabe insistir en que, no obstante, la norma fija como pauta el establecimiento de una regulación que admita en alguna medida el uso privado y en este caso se genera una expectativa de privacidad. Aquí la norma impone al empresario la obligación de especificar "de modo preciso" los usos autorizados y las garantías para preservar la intimidad de los trabajadores, refiriendo a título ejemplificativo "la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados" (ap. 3, pár. 2º). La norma impone claramente a la empresa una obligación de trasparencia[40]. Estos criterios van a delimitar el ámbito de la expectativa razonable de privacidad del trabajador y condicionan la facultad empresarial de acceder al contenido de los dispositivos digitales respecto de los que haya admitido su uso con fines privados.

En definitiva, la norma recoge la recomendación de una política preventiva en la materia plasmada en documentos e informes de instituciones supranacionales[41],

[38] En el mismo sentido, F. Pérez de los Cobos Orihuel, "*Poderes del empresario y derechos digitales del trabajador*", en *Trabajo y Derecho*, nº 59, noviembre 2019, p. 19.

[39] La STS 8-2-2018, rec. 1121/2015, que hemos comentado en este estudio es un buen ejemplo.

[40] J. Baz Rodríguez, "*La Ley Orgánica 3/2018 como marco embrionario de garantía…*", *cit.* pp. 59-60.

[41] GT29, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, 17/ES, WP 249: "la prevención debería tener mucho más peso que la detección: prevenir el uso indebido de Internet mediante medios técnicos resulta más beneficioso para los intereses del empresario que invertir recursos en detectarlo" (p. 16). Recomienda el Dictamen que el empresario explore otros medios menos invasivos para proteger la confidencialidad de los datos del cliente y la seguridad de la red. Por ejemplo, configurar el sistema de control de forma que se evite el registro permanente de la actividad del trabajador, por ejemplo, bloqueando el tráfico entrante o saliente sospechoso y redireccionando al usuario a un portal de información en el que pueda solicitar la revisión de dicha decisión automatizada. También se observa, como buena práctica, que el empresario ofrezca a los trabajadores un acceso alternativo no controlado (ofreciendo WiFi gratis, o dispositivos o terminales independientes) al fin de que los trabajadores puedan ejercer su derecho legítimo a utilizar las instalaciones de trabajo para algún uso privado (pp. 14-15). Se aconseja también que cuando se espere que los trabajadores utilicen aplicaciones en línea que traten da-

así como lo recoge igualmente la jurisprudencia[42].

3.3. Deber de transparencia sobre los criterios de uso de los medios digitales laborales

Los trabajadores deberán ser informados de los criterios de utilización fijados por la empresa (ap. 3, pár. 3º del art. 87 LOPD). Esta escueta exigencia debe ser interpretada en su alcance conforme al deber de transparencia delimitado normativamente (art. 5 RGPD[43]) y también por la jurisprudencia, y aplicando analógicamente los criterios que el propio legislador fija en otros supuestos de control empresarial: los empleadores habrán de informar a los trabajadores "con carácter previo, y de forma expresa, clara y concisa" (art. 89.1), o "(c)on carácter previo" y "de forma expresa, clara e inequívoca" (art. 90.2).

Sobre la posibilidad de controles ocultos (un programa espía de monitorización, por ejemplo), que, por tanto, eluden el deber de trasparencia, hay que decir que desde las primeras recomendaciones en el ámbito internacional se admiten dicha posibilidad en materia de vigilancia[44]. En este asunto, es relevante la reciente STEDH (Gran Sala) 17-10-2019, *Asunto López Ribalda y otros*, que admite tal posibilidad, sometiéndola a un juicio de proporcionalidad. En un caso referido a una videovigilancia oculta, entiende el Tribunal que la medida se justifica al no existir otra medida adecuada a la finalidad pretendida, ya que "informar a cualquier integrante del personal podía comprometer efectivamente la finalidad de la videovigilancia" (ap. 128). El Tribunal recuerda que "la exigencia de trasparencia y el derecho a la información que se deriva del mismo reviste un carácter fundamental" (ap. 131), pero entiende el TEDH que es posible justificar la ausencia de información previa cuando exista "un imperativo preponderante relativo a la protección de intereses públicos o privados importantes" (ap. 133); en el caso, sospechas de graves irregularidades cometidas por la acción concertada de un grupo de trabajadores que afecta al buen funcionamiento de la empresa (ap. 134). Por tanto, el incumplimiento del deber de información previa sólo supondrá una vulneración del derecho fundamental a la protección de datos tras una ponderación de la proporcionalidad de la medida adoptada, en aplicación del test de legitimidad ya delimitado en la STEDH 5-9-2017 (Gran Sala), *asunto Barbulescu*.

4. EL ALCANCE PROCESAL DE LA PRUEBA MEDIANTE CONTROL EMPRESARIAL ILÍCITO

Un tema relevante en la práctica procesal es el referido a la consecuencia jurídica en procesos por despido cuando la prueba aportada en el proceso judicial mediante el control empresarial es considerado judicialmente ilícito

tos personales (como las aplicaciones de oficina en línea), los empresarios deben considerar la posibilidad de permitir que los trabajadores designen ciertos espacios privados a los que el empresario no puede tener acceso bajo ninguna circunstancia, como un correo privado o una carpeta de documentos (p. 26).

[42] Así se indicaba en la STS 26-9-2007 (rec. 966/06): "lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios –con aplicación de prohibiciones absolutas o parciales– e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones". La sentencia concluye indicando que "si el medio se utiliza para usos privados en contra de estas prohibiciones y con conocimiento de los controles y medidas aplicables, no podrá entenderse que, al realizarse el control, se ha vulnerado "una expectativa razonable de intimidad"".

[43] El art. 5.1 a) indica que los datos personales serán tratados "de manera lícita, leal y transparente en relación con el interesado".

[44] Así el documento de la OIT, *Protección de los datos personales de los trabajadores. Repertorio de recomendaciones prácticas de la OIT*, de 1997, admite esta posibilidad siempre que se realice de conformidad con la legislación nacional; o bien porque existan sospechas suficientes de actividad delictiva u otras infracciones graves (apartado 6.14).

por violación de los derechos fundamentales del trabajador.

Una primera cuestión es la referida a los efectos procesales de la sentencia de suplicación que revoca la valoración por el Juzgado de la prueba obtenida mediante el control empresarial. En determinados casos se estima la nulidad de la sentencia de instancia y la reposición de autos al momento previo al juicio (por lesión de garantías del procedimiento ex art. 24 CE y 90 LRJS)[45]. En otros casos, atendiendo al principio de celeridad propio del proceso laboral, no se declara la nulidad de la sentencia del Juzgado (dado que se entiende que la empresa ve tutelado su derecho ex art. 24 CE en vía de suplicación), sino que se revoca la sentencia del juzgado en la concreta valoración de la prueba y sus efectos, procediendo el Tribunal a una nueva calificación de la licitud o ilicitud de la prueba, amparándose en las facultades de examen del fondo del asunto del Tribunal de Suplicación, ex art. 202 LRJS, siempre que el relato de hechos probados sea suficiente para permitir dicho enjuiciamiento de fondo[46]. La primera de las soluciones está avalada por la STS 2-2-2017, Rec. 554/2016, que revoca la de suplicación (que ratificó la declaración de improcedencia del despido en la instancia por inadmisión de la prueba de videovigilancia), y obliga a un nuevo pronunciamiento en instancia con admisión de la prueba.

Una segunda cuestión procesal, se refiere a los efectos de la ilicitud de la prueba sobre la calificación del despido. En este caso, la doctrina de suplicación se posiciona sobre dos tesis. La primera tesis estima que la consecuencia de dicha conclusión será la proscripción de la obtención de prueba ilícita con arreglo a los arts. 11 LOPJ, 287 LEC y 90 LRJS. En este caso, de no existir otros medios de prueba que avalen la procedencia del despido, la consecuencia será la declaración de improcedencia del mismo. Los pronunciamientos en este sentido argumentan que "lo que no se ha admitido es el medio de prueba contaminado (…) pero no se ha concluido que la decisión extintiva, en sí mismo considerada, pretendiera la vulneración de un derecho fundamental o libertad pública del trabajador, que llevara aparejada la calificación de nulidad del mismo (art. 55 LET)"[47]. Desde esta óptica se estima que "la sanción de nulidad del despido tiene su fundamento en el móvil del empresario cuando el despido en sí mismo responde a una causa vulneradora de un derecho fundamental, de ahí la prescripción del artículo 55 ET, pero no cuando la finalidad que mueve al empresario es comprobar un comportamiento del trabajador para obtener la prueba de la existencia de la causa alegada para justificar el despido, en cuyo caso, procede la nulidad de dicha prueba obtenida con vulneración de derechos fundamentales o libertades públicas, sin que tal nulidad pueda extenderse a la calificación del despido"[48].

De manera que no puede confundirse el despido con violación de derechos fundamentales con la infracción de derechos fundamentales en la obtención de la prueba de los hechos en los que se basó la empresa para adoptar tal sanción. El tribunal directamente resuelve sobre las consecuencias de dicha ilegalidad de la prueba, eliminando del enjuiciamiento todos los hechos acreditados mediante el control empresarial irregular, calificando, en su caso, el despido como improcedente[49]. Esta tesis viene avalada indirectamente por el TS, que declara la invalidez de la prueba por la vulneración del derecho a la intimidad personal relacionada con el uso del ordenador para fines personales, prohibido por la empresa. En consecuencia, al no existir fundamento

[45] STSJ Andalucía 17-1-2018, rec. 1878/2017.

[46] STSJ Madrid 15-2-2017, rec. 890/2016; STSJ Canarias 17-1-2018, rec. 584/2017.

[47] STSJ Castilla-La Mancha 10-6-2014, rec. 1162/2013.

[48] STSJ Castilla-La Mancha 12-1-2018, rec. 1416/2017.

[49] SSTSJ Islas Canarias 27-3-2017, rec. 934/2016, y 3-4-2017, rec. 743/16; STSJ Madrid 23-4-2018, rec. 74/2018; STSJ Madrid 4-6-2018, rec. 217/2018; STSJ Madrid 13-9-2018, rec. 417/2018; STSJ Madrid 28-9-2018, rec. 275/2018; STSJ Com. Valenciana 19-11-2018, rec. 2490/2018; STSJ Asturias 22-1-2019, rec. 2361/2018; SJS nº 3 Bilbao 4-4-2019, nº 128/2019

probatorio para el despido, el mismo se declara improcedente[50].

La segunda tesis, en contraposición a la anterior, argumenta que la consecuencia de la consideración como ilícita de la prueba será la nulidad del despido, aplicando el art. 55 LET. Esta tesis se plantea en supuestos en que la única prueba que sustenta los hechos que motivan el despido es la deducible de la vigilancia declarada invalida.

Se argumenta que, como la única prueba que sirve de base al acto extintivo es obtenida violando el derecho fundamental a la intimidad del demandante y que, por lo tanto, el conocimiento de los hechos motivadores de la extinción se debe en exclusiva a una prueba ilícitamente obtenida, con vulneración de esa garantía constitucional, la consecuencia que de ello deriva es la nulidad del despido de conformidad con el art. 55.5 LET. Se razona desde esta tesis que, atendiendo a criterios gramaticales, finalistas y de interpretación conforme a la Constitución, en la citada previsión legal encuentran cobijo no sólo los supuestos en que el cese se produce como consecuencia del ejercicio legítimo de un derecho fundamental, sino también aquellos otros en que los hechos que lo sustentan han sido conocidos por el empresario mediante métodos que conculcan los derechos fundamentales del afectado.

Esta solución se apoya en la STC 196/2004 en la que se examina una decisión extintiva fundada en la ineptitud de la recurrente para el trabajo conforme a los resultados de un reconocimiento médico atentatorio a su intimidad; dicha prueba médica se consideró por el JS contraria al derecho a la intimidad ex art. 18.1 ET y, dado que sirvió para fundamentar la extinción del contrato, justifica la calificación de nulidad de la extinción. En el procedimiento de amparo ante el TC, ni las partes o el ministerio fiscal formulan alegación alguna sobre los efectos de la declaración de nulidad de la prueba, centrándose en las revisiones médicas y su impacto sobre el derecho a la intimidad. La STC confirma la violación del derecho fundamental en cuestión y entiende que "la reparación de la lesión de un derecho fundamental que hubiese sido causado por el despido laboral, debe determinar la eliminación absoluta de sus efectos, es decir, la nulidad del mismo". De forma que se anula la STSJ que revocó la del JS y confirma la firmeza de la sentencia del JS.

A la misma conclusión se llega aplicando lo dispuesto en el art. 9.2 de la Ley Orgánica 1/1982, con arreglo al cual la tutela judicial frente a las intromisiones ilegítimas en el derecho a la intimidad "comprenderá la adopción de todas las medidas necesarias para poner fin a la intromisión ilegítima de que se trate y, en particular, las necesarias para: a) el restablecimiento del perjudicado en el pleno disfrute de sus derechos, con la declaración de la intromisión sufrida, el cese inmediato de la misma y la reposición del estado anterior"[51].

En nuestra opinión debe prevalecer la primera tesis. La LRJS contiene una previsión específica de tutela de derechos fundamentales en el plano procesal de los medios de prueba. Dentro de la regulación de los medios de prueba, el art. 90 prevé la regulación incidental por ilicitud constitucional de la prueba, al objeto de evitar que la admisión de este tipo de pruebas contamine el proceso y la sentencia. Responde al mandato del art. 11.1 LOPJ, conforme al cual, "(n)o surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales". Concretamente, el apartado 2º del art. 90 LRJS dispone que "(n)o se admitirán pruebas que tuvieran su origen o que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas".

[50] STS 26-9-2007, rec. 966/2006.

[51] STSJ País Vasco 10-5-2011, rec. 644/2011; STSJ País Vasco 27-2-2018, rec. 226/2018; STSJ Asturias, 22-1-2016, rec. 2404/2015; STSJ Cataluña 9-3-2017, rec. 39/2017; STSJ Andalucía 5-4-2017, rec. 277/2017; STSJ Castilla y León 11-4-2018, rec. 407/2018; SJS Sevilla nº 9 de 3-9-2018, sent. 296/2018.

En definitiva, los efectos de la ilicitud de la prueba lo son sobre la admisibilidad de la prueba, no sobre la calificación del despido, y ello es independiente del momento de valoración de la prueba (en el acto de juicio o bien, como suele ocurrir en la práctica, en el momento de valorar la prueba al dictar la sentencia)[52]. De forma que el juez en su enjuiciamiento no puede tomar en consideración las pruebas obtenidas con violación de derechos fundamentales. Es decir, existirá enjuiciamiento al margen de la prueba ilícita. Lo cual quiere decir que la aportación de una prueba ilícita no conlleva por si misma un juicio de nulidad del despido. Si se han respetado las normas y garantías de procedimiento, y no corresponde decretar la nulidad de actuaciones, podrá calificarse el despido como nulo si "tiene como como móvil alguna de las causas de discriminación prevista en la Constitución y en la ley, o cuando se produzca con violación de derechos fundamentales y libertades públicas del trabajador" (art. 55.5 ET y 108.1 LRJS). En consecuencia, cuando han sido excluidas las únicas pruebas (obtenidas ilegalmente) que dan fundamento al despido, la decisión extintiva empresarial queda desprovista de fundamento, y la opción legal para todos los supuestos reconducibles a esta situación es la improcedencia del despido con los efectos legales correspondientes.

La admisión de una prueba que pueda calificarse contraria a derechos fundamentales afecta al derecho a la tutela judicial efectiva (art. 24.1 CE) y puede motivar la nulidad de la sentencia. Ahora bien, cuando en suplicación se acoge la pretensión de parte de la ilicitud de la prueba, la garantía de la tutela judicial se produce mediante una nueva calificación del despido excluyendo las pruebas obtenidas ilegalmente.

En esta lógica se mueve la doctrina constitucional cuando se aborda la cuestión de la prueba tachada de ilegítima, por atentatoria a los derechos fundamentales. Así, en la STC 114/1984 la cuestión se centra en las actuaciones del juzgador y, específicamente, la admisión por éste de una prueba tachada por la parte de ilegítima, por atentatoria a los derechos reconocidos en el art. 18.3 de la Constitución. Para el TC, "si la ilicitud en la obtención de la prueba fuese cierta y si fuese posible inferir de nuestro ordenamiento una regla que imponga su ineficacia procesal, habría que concluir que la decisión jurisdiccional basada en tal material probatorio pudo afectar a los derechos fundamentales del recurrente a un proceso con todas las garantías (art. 24.2 de la Constitución) y, en relación con ello, al derecho a la igualdad de las partes en el proceso (art. 14 de la Constitución)". Esta misma perspectiva es la adoptada por la STC 186/2000, cuyo supuesto de hecho es el despido de un trabajador basándose en pruebas obtenidas mediante videovigilancia, y cuestionadas por el mismo por violación de su derecho a la intimidad. Aquí el debate se centra en si se ha vulnerado el derecho a la tutela judicial efectiva del trabajador despedido (art. 24.1 CE), porque los órganos judiciales han fundado sus decisiones en pruebas que debieron calificarse como nulas por haberse obtenido con violación del derecho fundamental a la intimidad (art. 18.1 CE).

BIBLIOGRAFIA CITADA

J. Baz Rodríguez, "La Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", en Trabajo y Derecho, nº 54, junio, 2019,

M.E. Casas Bahamonde, "Informar antes que 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", en Derecho de las Relaciones Laborales, nº 2, 2018

Desdentado Bonete y E. Desdentado Daroca, "La segunda sentencia del TEDH en el caso Barbulescu y sus consecuencias sobre el control del uso laboral del ordenador", en Revista de Información Laboral, nº 1/2018 (Base Aranzadi, BIB 2018, 6059)

[52] Cfr. A. M. Orellana Cano, *El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores*, Th.R. Aranzadi, 2019, p. 177.

J. García Murcia y I.A. Rodríguez Cardo, "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", en Revista Española de Derecho del Trabajo, nº 216, enero, 2019

J.L. Goñi Sein, "Los derechos fundamentales inespecíficos en la relación laboral individual: ¿necesidad de una reformulación?", en AEDTSS, Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social, Ed. Cinca, 2014

J.L. Goñi Sein, "La protección de las comunicaciones electrónicas del trabajador: la doctrina del Tribunal de Estrasburgo y la jurisprudencia constitucional", en Trabajo y Derecho, nº 40, 2018

J.L. Goñi Sein, "Nuevas tecnologías digitales, poderes empresariales y derechos de los trabajadores: análisis desde la perspectiva del Reglamento Europeo de Protección de Datos de 2016", en Revista de Derecho Social, nº 78

M. Orellana Cano, El derecho a la protección de datos personales como garantía de la privacidad de los trabajadores, Th.R. Aranzadi, 2019

F. Pérez de los Cobos Orihuel, El derecho al respeto de la vida privada: los retos digitales, una perspectiva de Derecho comparado, Consejo de Europa. Estudio, octubre 2018

F. Pérez de los Cobos Orihuel, "Poderes del empresario y derechos digitales del trabajador", en Trabajo y Derecho, nº 59, noviembre 2019

F. Valdés Dal-Ré, "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", en Revista de Derecho Social, nº 79

F. Valdés Dal-Ré, "Nuevas tecnologías y derechos fundamentales de los trabajadores", en Derecho de las Relaciones Laborales, nº 2, febrero 2019

RESUMEN El control empresarial de la actividad laboral del trabajador, amparada genéricamente en el art. 20.3 ET, como concreción del derecho empresarial de organización del trabajo en la empresa y de la libertad de empresa (art. 38 CE), ha supuesto un sólido respaldo a las facultades empresariales de control de la actividad laboral mediante medios de videovigilancia en el lugar de trabajo e instrumentos de control de los medios digitales empresariales puestos a disposición del trabajador. Pero dicho control empresarial puede plantear situaciones que afectan al derecho a la intimidad, a la protección de datos y al secreto de las comunicaciones de los trabajadores. El estudio pretende poner de manifiesto que en los últimos años se avanza desde una cultura jurídica contractualista a otra constitucionalista en relación con la protección de la *privacy* del trabajador. El estudio, en primer lugar, describe el importante papel de la jurisprudencia en la materia. Conforme a la doctrina del TS, a partir de la delimitación de los usos autorizados y prohibidos (y por tanto de las expectativas de privacidad del trabajador), la legitimidad de los controles empresariales debe valorarse a partir de un juicio de proporcionalidad, dentro del cual se incluye el criterio de la trasparencia informativa. La doctrina de nuestro TC en su canon de razonamiento básicamente se alinea con la doctrina del TS descrita. El TC estima, en primer lugar, que el uso de los medios digitales por el trabajador, y en particular el control de sus comunicaciones vía correo electrónico, están protegidas por el derecho a la intimidad (art. 18.1 CE) y el secreto de las comunicaciones (art. 18.3 CE). En segundo lugar, el TC resuelve el conflicto de intereses realizando una ponderación de bienes constitucionalmente relevantes a partir de la configuración de las condiciones de disposición y uso de las herramientas informáticas y de las instrucciones que hayan podido ser impartidas por el empresario a tal fin. En tercer lugar, el canon de razonamiento parte de la premisa de la existencia o no de una expectativa de privacidad, pero ello no es excluyente de la valoración de las características de la injerencia empresarial a la luz del principio de proporcionalidad. La STEDH (Gran Sala) 5-9-2017, asunto Barbulescu, configura un canon de garantías sobre la aplicación del juicio de proporcionalidad en relación con el derecho a la privacidad del trabajador en su actividad laboral (art. 8 CEDH). Se puede decir que el test de legitimidad diseñado por el TEDH tiene un alcance general respecto de los medios de vigilancia empresarial, que incluye el uso por el trabajador de los dispositivos digitales. En la evolución reciente juega un papel de vanguardia el TEDH, que, al hacer efectiva las garantías del art. 8 CEDH, plantea en términos nuevos la dialéctica entre el poder de vigilancia del empresario y el respeto a la privacidad y el secreto de las comunicaciones del trabajador. La STEDH (Gran Sala) 5-9-2017, *asunto Barbulescu*, configura un canon de garantías sobre la aplicación del juicio de proporcionalidad en relación con el derecho a la privacidad del trabajador en su actividad laboral (art. 8 CEDH). El test de legitimidad diseñado por el TEDH en esta Sentencia tiene un alcance general respecto de los medios de vigilancia empresarial, que incluye el uso por el trabajador de los dispositivos digitales. Conforme al test de legitimidad, en primer lugar, se considera esencial respetar un criterio de trasparencia, de forma que el empleado ha debido ser informado de la posibilidad del empleador de adoptar medidas de control y su aplicación. En segundo lugar, conforme al test de legitimidad, debe existir una justificación para el control empresarial. En tercer lugar, el test exige el respeto del principio de proporcionalidad y de minimización. Este criterio debe tomar en consideración el tipo de medida adoptada y sus características, que deben regirse por el principio de minimización (limitada a lo necesario para el fin pretendido). El estudio permite concluir, en su estudio jurisprudencial, como la jurisprudencia del TEDH y de nuestros tribunales coinciden, no sin dudas y contradicciones, en una evolución hacia la clarificación de los parámetros que justifican el sacrificio de la privacidad del trabajador (existencia de un fin legítimo, tras-

parencia informativa y proporcionalidad y minimización del control). Una segunda parte del estudio se orienta al análisis de la regulación normativa en la materia. El Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, constituyen el marco normativo de referencia respecto a la protección de los derechos fundamentales del trabajador frente a las facultades empresariales de control. En los preceptos de la LOPD referidos a la relación laboral la perspectiva fundamental no es tanto el reconocimiento de "derechos digitales", cuanto la protección de los derechos fundamentales del trabajador frente a las facultades empresariales de vigilancia y control de la actividad laboral. Se puede decir que este marco regulador se apoya en la legitimación del poder de control empresarial en las relaciones laborales dentro de un marco jurídico basado en los principios de legitimidad de fines, transparencia en la información y proporcionalidad en los métodos de control de medios digitales de trabajo. Desde un plano normativo, el estudio se centra en el análisis de los distintos aspectos relevantes del art. 87 LOPD, concretamente, la delimitación de los fines que pueden justificar la vigilancia empresarial y de los dos tipos de garantías que recoge, la obligación empresarial de fijar criterios de utilización de los dispositivos digitales y el deber de información previa al trabajador. La escueta regulación de la norma en algunos extremos puede ser objeto de aclaración a la luz del bagaje jurisprudencial descrito en el estudio. Finalmente, se aborda en el estudio la problemática referida a las consecuencias jurídicas, sobre todo en procesos por despido, cuando la prueba aportada en el proceso judicial mediante el control empresarial es considerado judicialmente ilícito por violación de los derechos fundamentales del trabajador, donde los tribunales ofrecen soluciones contradictorias. Frente a la tesis que mantiene que la consecuencia de una prueba ilícita debe ser la nulidad del despido de conformidad con el art. 55.5 LET, se defiende en el estudio la tesis de que la consecuencia debe circunscribirse a la inadmisión de la prueba ilícita con arreglo a los arts. 11 LOPJ, 287 LEC y 90 LRJS.

Palabras clave: Poder de control empresarial; privacidad trabajador; protección de datos; jurisprudencia; Tribunal Europeo Derechos Humanos; Tribunal Constitucional; Tribunal Supremo; Ley Orgánica Protección Datos.

ABSTRACT The surveillance measures of the employer in the workplace, through the use of computers and digital media by employees, may be intrusive in their private life (their personal privacy, the secrecy of their communications and the right to respect the personal data). Employer control of the employee's work activity, generally protected by art. 20.3 ET, as a concretization of the employer right of work organization in the company and the freedom of enterprise (art. 38 CE), has provided solid support to the business faculties of control of the work activity by means of video surveillance in the workplace and instruments of control of the business digital means made available to the worker. The study aims to show that in recent years progress has been made from a contractualist legal culture to a constitutionalist one, in relation to the protection of employees' privacy. The study describes the important role of case law in this area, considering recent evolutions of the Case-law of the European Court of Human Rights and the Spanish Courts (Highs Courts and Constitutional Court). According to the doctrine of the SC, from the delimitation of the authorized and prohibited uses (and therefore of the employee's privacy expectations), the legitimacy of the employer controls must be assessed on the basis of a judgment of proportionality, which includes the criterion of information transparency. The doctrine of our TC in its reasoning canon basically aligns with the TS doctrine described. The Constitutional Court considers, first, that the use of digital media by the employee, and in particular the control of his communications via e-mail, are protected by the right to privacy (art. 18.1 CE) and the secrecy of communications (art. 18.3 CE). Second, the TC resolves the conflict of interests by weighing up constitutionally relevant assets based on the configuration of the conditions of disposition and use of computer tools and the instructions that may have been given by the employer for this purpose. Third, the reasoning fee is based on the premise of whether or not there is an expectation of privacy, but this does not preclude an assessment of the characteristics of employer's interference in the light of the principle of proportionality. The STEDH (Grand Chamber) 5-9-2017, Barbulescu case, establishes a canon of guarantees on the application of the judgment of proportionality in relation to the worker's right to privacy in his work activity (art. 8 CEDH). It can be said that the legitimacy test designed by the TEDH has a general scope with respect to employer surveillance means, which includes the use by the employee of digital devices. In recent developments, the TEDH plays an avant-garde role in giving effect to the guarantees of art. 8 CEDH, proposing in new terms the dialectic between the power of surveillance of the employer and respect for privacy and the secrecy of communications of the employee. The STEDH (Grand Chamber) 5-9-2017, Barbulescu case, establishes a canon of guarantees on the application of the judgment of proportionality in relation to the employee's right to privacy in his work activity (art. 8 ECHR). The legitimacy test designed by the European Court of Human Rights in this judgment has a general scope with regard to corporate surveillance means, which includes the use by the employee of digital devices. According to the test of legitimacy, firstly, it is considered essential to respect a criterion of transparency, so that the employee has to be informed of the possibility of the employer to adopt control measures and their implementation. Secondly, according to the legitimacy test, there must be a justification for employer control. Third, the test requires compliance with the principle of proportionality and minimisation. This criterion must consider the type of measure adopted and its characteristics, which must be governed by the principle of minimization (limited to what is necessary for the intended purpose). The study allows us to conclude, in its jurisprudential study, that the case law of the European Court of Human Rights and our Courts coincide, not without doubts and contradictions, in an evolution towards the clarification of the parameters that justify the sacrifice of the worker's privacy (existence of a legitimate purpose, transparency of information and proportionality and minimization of control). A second part of the study focuses on the analysis of regulation in this topic. The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and the Organic Law 3/2018, constitute the normative framework of reference with respect to the protection of the

fundamental rights of the worker against the employer powers of control. In the precepts of the LOPD referring to the labor relationship the fundamental perspective is not so much the recognition of "digital rights", but rather the protection of the fundamental rights of the employee from the employer's powers of supervision and control on the work activity. It can be said that this regulatory framework is based on the legitimization of employer's control power, within a legal framework based on the principles of legitimacy of purposes, transparency in information and proportionality in the control methods of digital working media. From a normative level, the study focuses on the analysis of the different relevant aspects of art. 87 LOPD, specifically, the delimitation of the finality that can justify business surveillance about the use of computers and digital media by employees, and the two types of guarantees that it includes, the business obligation to set criteria for the use of digital devices and the duty of prior information to the worker. The Courts' case-law may be relevant to understand and apply the Spanish law. Finally, the study regards the question of legal consequences, especially in dismissal proceedings, when the evidence provided in the judicial process through business control is considered judicially unlawful for violation of the fundamental rights of the worker, where the courts offer contradictory solutions. In contrast to the thesis that maintains that the consequence of an illegal test must be the nullity of the dismissal in accordance with art. 55.5 LET, the study defends the thesis that the consequence must be limited to the inadmissibility of the illicit evidence under arts. 11 LOPJ, 287 LEC and 90 LRJS.

Keywords: Power of employer control; privacy of workers; protection of personal data; Case-law; European Court of Human Rights. Spanish Constitutional Court; Spanish High Court; Spanish Organic Law Protection Personal Data.

Videovigilancia laboral y grabación de sonidos en el lugar de trabajo

Labor video surveillance and sound recording in the workplace

JESÚS LAHERA FORTEZA*

1. JURISPRUDENCIA SOBRE VIDEOVIGILANCIA LABORAL

La videovigilancia laboral y la grabación de sonido en el lugar de trabajo carecía, hasta el art.89 de la Ley de Protección de Datos Personales y Derechos Digitales 3/2018 (LOPD), de una regulación específica en el ordenamiento laboral, siendo por ello esencial su configuración por parte de la jurisprudencia del Tribunal Constitucional (TC), Tribunal Supremo (TS) y del Tribunal Europeo de Derechos Humanos (TEDH). No resulta posible comprender el art.89 LOPD sin conocer esta jurisprudencia previa, pues este precepto es deudor, en parte, de la misma. Igual que es imposible aplicar el art.89 LOPD sin tener en cuenta esta jurisprudencia, completamente viva y vigente en la solución de problemas prácticos tras la entrada en vigor de esta norma. Por ello, antes de analizar la regulación del art.89 LOPD con detalle, creo necesario repasar brevemente esta jurisprudencia del TC, TS y TEDH en videovigilancia laboral.

En primer lugar, la jurisprudencia constitucional tiene dos líneas referentes en la videovigilancia laboral[1].

De un lado, las SSTC 98/2000 y 186/2000 establecen los límites marcados por el derecho a la intimidad del trabajador del art.18.1 CE ante la utilización empresarial de estas vías de control tecnológico. De otro lado, las SSTC 29/2013 y 39/2016 efectúan una renovada lectura de estos límites a la luz del derecho a la protección de datos de carácter personal amparado por el art.18.4 CE. Ambos binomios de pronunciamientos del TC son complementarios, siendo necesario efectuar esta doble lectura, en torno a los arts.18.1 y 18.4 CE, para asegurar el respeto a la intimidad y de protección de datos personales del trabajador ante estos sistemas de control audiovisual.

De inicio, las SSTC 98/2000 y 186/2000 integran el derecho a la intimidad del trabajador del art.18.1 CE desde la técnica clásica de la modulación de derechos personales en el contrato de trabajo. El TC parte de la premisa del pleno reconocimiento de la intimidad personal de los trabajadores en los centros de trabajo, sin por ello descartar estos sistemas de control tecnológico. Ambas sentencias exigen, desde la ponderación jurídica entre la intimidad del trabajador y la libertad de empresa,

* Profesor Titular Derecho del Trabajo Universidad Complutense y consultor despacho AbdónPedrajas.

[1] Ver ARBONES LAPENA, H., "Grabación de imagen o sonido y control electrónico por el empresario", *Nueva Revista Española de Derecho del Trabajo*, nº 178, 2015, pp. 193-222; TASCÓN LÓPEZ, R., "Tecnovigilancia y derecho de los trabajadores", *Revista Centro Estudios Financieros*, 2017, nº 415, pp. 55 y ss; LAHERA FORTEZA, J., "Nueva jurisprudencia constitucional en la videovigilancia laboral: valoración crítica", *Derecho de Relaciones Laborales* 2016, nº 5, pp. 494 y ss.

que los sistemas de videovigilancia laboral sean una medida:

a) *"Adecuada o idónea"* para la consecución de una finalidad empresarial legítima como el control del cumplimiento del contrato de trabajo

b) *"Necesaria"*, no existiendo otra alternativa con menor riesgo de sacrificio de la intimidad personal del trabajador para la consecución de este fin legítimo

c) *"Proporcionada"* al fin perseguido, lo que exige contrastar la relevancia del beneficio obtenido por la empresa y el sacrificio de la intimidad personal del trabajo

Este juicio de *"idoneidad, necesidad y proporcionalidad"* debe ser razonado en cada caso concreto. Así, la STC 186/2000 avala la constitucionalidad de una instalación de cámaras ocultas, en una zona de cajas de una empresa, al existir razonables sospechas de comisión por el trabajador de irregularidades graves en su puesto de trabajo, existiendo proporcionalidad en la medida, al limitarse la grabación a la zona acotada y con una duración temporal limitada. Con el mismo canon interpretativo, la STC 98/2000 entiende ilegítima la captación de sonido, en un sistema de videovigilancia laboral, por no quedar acreditado que fuera imprescindible para el correcto desenvolvimiento de la actividad productiva ni ser una medida proporcionada al fin perseguido, sacrificando en exceso la intimidad de los trabajadores.

Por su parte, la STC 29/2013 completa esta jurisprudencia constitucional integrando en el contrato de trabajo también el derecho a la protección de datos personales, amparado por el art.18.4 CE. Según el TC, las imágenes grabadas con estos sistemas constituyen un *"dato de carácter personal"* bajo la cobertura del art.18.4 CE. El TC diferencia, así, el derecho a la intimidad personal del art.18.1 CE, que exige la ponderación jurídica antes desarrollada, y el derecho a la protección de datos personales del art.18.4 CE, que implica nuevos límites cuando se adopte la medida. La STC 29/2013 afirma, desde esta perspectiva, el derecho del trabajador a ser informado del tratamiento de los datos personales resultantes de la captación de imágenes a través de este sistema de control empresarial. Esta información ha de ser *"previa, expresa, precisa, clara e inequívoca en conexión con la finalidad pretendida por la empresa"*. En particular, la STC 29/2013 rechaza, por falta de esta información, que las imágenes captadas por una cámara en un recinto universitario sirva de prueba para la imposición de sanciones a un trabajador.

La STC 39/2016, finalmente, relaja sustancialmente este deber de información al admitir, en determinadas cámaras, su cumplimiento a través del distintivo general de videovigilancia de seguridad. La sentencia cambia, ante la presencia de indicios de irregularidad grave cometida por el trabajador, la doctrina respecto a las exigencias de información, porque estima suficientes estos distintivos informativos visibles en la empresa, conforme a la Instrucción 1/2006 de la Agencia de Protección de Datos Personales (APD). En el caso planteado, el trabajador no había sido informado expresamente de la instalación de videocámaras, pero existía este distintivo informativo visible. El TC admite como suficiente este modo de información; cumplido este requisito, el trabajador *"podía conocer la existencia de cámaras y la finalidad para la que habían sido instaladas"*. Opera, a juicio del TC, una especie de proporcionalidad en la información cuando existen indicios de irregularidades del trabajador.

La suma de ambas líneas jurisprudenciales concluye, en definitiva, en esta doble exigencia cuando se articula en una empresa un sistema de videocámaras. De un lado, motivar su articulación con un juicio de idoneidad, necesidad y proporcionalidad respecto al fin perseguido. De otro lado, informar al trabajador controlado de esta finalidad y, al ser datos personales, del tratamiento de las imágenes captadas, quedando aceptados, ante indicios

de irregularidad cometida por el trabajador, los distintivos visibles informativos de videovigilancia de seguridad.

La fundamentación jurídica de esta doctrina consolidada, elaborada antes del art.89 LOPD, también es apuntada en la STC 39/2016. El TC parte de la conexión constitucional entre la libertad de empresa del art.38 CE y el derecho a la propiedad del art.33 CE con el poder de dirección y control del art.20.3 ET, así definido: *"el poder de dirección empresarial, imprescindible para la buena marcha de la organización productiva que es reflejo de los derechos constitucionales reconocidos en los arts. 33 y 38 CE, que se concreta en el art.20.3 ET que expresamente faculta al empresario a adoptar medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales"*. Esta conexión permite efectuar, desde una dimensión constitucional, la ponderación jurídica entre la libertad de empresa del art.38 y la propiedad privada del art.33 CE con el derecho a la intimidad personal del trabajador del art.18.1 CE y con la protección de sus datos personales del art.18.4 CE.

La jurisprudencia ordinaria de la SALA IV del TS en videovigilancia laboral es deudora de la expuesta jurisprudencia constitucional porque ha seguido una idéntica evolución y ha terminado exigiendo los dos límites de la intimidad personal y la protección de datos personales, con las mismas técnicas utilizadas por el TC[2], incluida la expuesta relajación de la información ante indicios de irregularidades del trabajador.

Un buen ejemplo de esta confluencia es la STS 13 de Mayo de 2014 (Rec. 1685/2013) construida jurídicamente desde la doble referencia de las SSTC 98/2000 y 186/2000 y de la STC 29/2013. Tras aplicar las técnicas clásicas de necesidad, idoneidad y proporcionalidad de la cámara, en aras del respeto a la intimidad personal, la sentencia exige el requisito de la información al trabajador, porque "*no hay una habilitación legal expresa para esa omisión del derecho a la información sobre el tratamiento de datos personales en el ámbito de las relaciones laborales*". La STS 13 Mayo 2014 no avala, así, una prueba obtenida por cámara en una zona de cajas porque "*no se dio información previa a la trabajadora de la posibilidad de tal tipo de grabación ni de la finalidad de dichas cámaras*". Subraya también esta jurisprudencia la debida consulta a los representantes de los trabajadores exigida por el art.64.5.f ET.

Las SSTS 7 Julio 2016 (Rec.630/2016), 31 Enero 2017 (Rec.3331/2015), 1 Febrero 2017 (Rec. 3262/2015) y 2 Febrero 2017 (Rec. 554/2016) se sitúan en este plano técnico de doble exigencia, pero reciben la doctrina de la STC 39/2016, antes expuesta, que reconoce el papel de los distintivos visibles de información de la videovigilancia, ante sospechas fundadas de irregularidades del trabajador. Son, en este marco, admitidas como pruebas lícitas grabaciones de trabajadores, justificadas, que carecían de información individual bajo la cobertura del distintivo visible informativo de videovigilancia de seguridad.

Finalmente, la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) de 9 Enero 2018, asunto Lopez Ribalda 1, debe ser tenida muy en cuenta, en este análisis jurisprudencial previo a la LOPD[3], aunque su corrección, en SALA general, es posterior y más reciente, el 17 Octubre 2019, asunto López Ri-

[2] Ver TASCON LÓPEZ, R., "Tecnovigilancia empresarial y derechos de los trabajadores", *cit.*, pp. 85-86; PRECIADO DOMENECH, C.H., "La videovigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos personales", *Revista Derecho Social* 2017, nº 77, pp. 175 y ss.

[3] Ver GOÑI SEIN, J.L., "Videovigilancia empresarial mediante cámaras ocultas: su excepcional validez como control defensivo *ex post*", *Trabajo y Derecho* 2018, nº 47, pp. 74 y ss; CASAS BAAMONDE, M.E., "Informar antes que vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital?" y ROJO TORRECILLA, E., "Derecho del trabajador a la privacidad en la empresa y límites a su control por las cámaras de videovigilancia", ambas aportaciones en *Derecho Relaciones Laborales* 2018, nº 2, pp. 103 y ss y pp. 135 y ss.

balda 2[4]. El TEDH analiza el supuesto específico de una cámara oculta, ante la sospecha fundada de robos de empleados, donde no se había informado al trabajador. La doctrina de López Ribalda 1 y López Ribalda 2 es bastante similar, estando la diferencia en el enjuiciamiento y calificación de los hechos acontecidos. El TEDH parte de la regla general de la información al trabajador para generar una expectativa de intimidad ante la grabación y proteger el dato personal de la imagen, siguiendo en ello la senda de la STEDH 5 de Septiembre 2017, asunto Barbulescu 2 en control de correos electrónicos corporativos. El marco general de actuación empresarial es, por tanto, la información de la videovigilancia, y de sus fines, al trabajador grabado. Esta información debe ir unida a una justificación adecuada, necesaria y proporcionada de la utilización de este medio de control, en términos muy similares a los utilizados por el TS y TC. El TEDH, sin embargo, admite la ausencia de información en cámaras ocultas instaladas ante indicios y sospechas fundadas de irregularidades graves del trabajador grabado con exigentes requisitos. El indicio debe ser cierto y acreditado, la videovigilancia limitada al área y trabajador sobre el que pesan estas sospechas fundadas, la duración de la instalación puntual y de tiempo proporcionado al fin de control, las imágenes deben ser vistas exclusivamente por responsables de la empresa, nunca difundidas, y con un tratamiento sólo dirigido a la penalización de esta irregularidad grave, siendo luego sometidas a las mayores garantías y exigencias de la protección de datos personales. Esta suma de requisitos conlleva un grado razonable y proporcionado de intromisión en la privacidad, no contrario al art.8 de la CDH, y origina una prueba lícita en un proceso, sin vulnerar el art.6 de la CDH. La ausencia de información en esta cámara oculta fundamentada y proporcionada puede dar lugar a responsabilidades administrativas de protección de datos personales o civiles de daños, pero no anula la prueba laboral lícita y las reacciones empresariales ante la comisión de irregularidades graves, así acreditadas. La única diferencia entre Lopéz Ribalda 1 y 2, es que en la primera sentencia no quedan acreditados estos requisitos y se aprecia vulneración de los arts. 8 y 6 CDH, y en la reciente y segunda sentencia sí se constatan probados estos requisitos y se avala la prueba laboral así obtenida. A diferencia del TC, que aplica una especie de proporcionalidad en la información debida, el TEDH pone el foco en los requisitos de la cámara oculta, aceptando la ausencia de información.

Tampoco es ésta una doctrina internacional novedosa porque ya existía el precedente del asunto Köpke, 5 Octubre 2010, donde el TEDH admite, sin información previa, una cámara coyuntural oculta ante indicios claros de conducta ilícita del trabajador instalada con esta exclusiva finalidad de constatar las sospechas, durante un tiempo limitado y con estos exigentes requisitos. El TEDH abre así la puerta a cámaras ocultas, con estas garantías, como ya hiciera en su día las SSTC 186/2000 y 98/2000 y, de otro modo, utilizando el distintivo genérico visible de cámaras de seguridad, la STC 39/2016.

2. TÉCNICA Y FUNDAMENTACIÓN JURÍDICA DE LA PRIMERA REGULACIÓN LEGAL DE LA VIDEOVIGILANCIA LABORAL EN LA LEY ORGÁNICA 3/2018 DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍAS DIGITALES

Los derechos digitales en la empresa – videocámaras, uso de dispositivos digitales, control mails, grabaciones telefónicas, geolocalización, desconexión digital – no estaban hasta ahora regulados legalmente. Durante años, la

[4] Ver ROJO TORRECILLA, E., "Medias verdades y fake news en el mundo jurídico. No todo cabe en la videovigilancia de una persona trabajadora. A propósito de la sentencia TEDH López Ribalda II, 17 Octubre 2019", *blog Eduardo Rojo, entrada 23 Octubre 2019*, dando cuenta de algunas aportaciones disponibles en versión digital sobre esta sentencia (HUGO PRECIADO, C.; MOLINA NAVARRETE, C.; GONZÁLEZ ESPADA, J.A., etc.)

jurisprudencia constitucional y ordinaria, con apoyo colateral de TEDH, ha ido solucionando problemas de control tecnológico y uso digital en la empresa, creando criterios y reglas sobre la base del respeto a los derechos constitucionales de imagen e intimidad personal (art.18.1 CE), protección de datos personales (art.18.4 CE) y secreto de comunicaciones (art.18.3 CE). El poder empresarial de dirección (art.20 ET) ha sido modulado y limitado en función de estos tres derechos constitucionales. La analizada jurisprudencia de videovigilancia laboral es una manifestación clara de esta configuración jurídica.

La LOPD, tras el Reglamento Europeo 2016/679 de protección de datos personales (REPD), regula, por primera vez y tras esta intensa jurisprudencia, los derechos digitales en el ámbito laboral. Responde así, en parte, a la previsión del art.88 REPD para que los Estados regulen *"normas más específicas para garantizar la protección de derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral… en particular la ejecución del contrato laboral … con especial atención a los sistemas de supervisión en el lugar de trabajo"*. Pero lo que es más importante, es una respuesta a una carencia normativa laboral que era incomprensible en una sociedad ya digitalizada[5].

La técnica empleada, en la DF 13 LOPD, que añade un nuevo art.20.bis ET es la siguiente:

> – *«Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*
>
> *Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales».*

La opción legal, en la línea jurisprudencial, es modular y limitar el poder contractual de dirección y control empresarial del art.20 ET con estos derechos constitucionales. La técnica utilizada es la remisión a la legislación específica de protección de datos personales y garantía de derechos digitales, en concreto los arts.87-90 LOPD. De manera específica, la videovigilancia laboral, y sus limitaciones, es, en consecuencia, mencionada en la DF 13 LOPD e incorporada en este nuevo arts.20.bis ET. Y la remisión a la legislación vigente en la regulación es al art.89 LOPD, en diálogo con el art. 22 LOPD, que regula, de manera concreta, el derecho a la intimidad frente al uso de herramientas de videovigilancia laboral y grabación de sonido en los lugares de trabajo.

El art.22.1 LOPD declara que *"las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de personas y bienes, así como de sus instalaciones"*. Los arts. 22.7 y 8 LOPD establecen dos remisiones específicas: a la Ley 5/2014 de seguridad privada, en cámaras instaladas con estas finalidades, y al art.89 LOPD, en el tratamiento de datos obtenidos por imágenes por las empresas en el ámbito laboral. El art.89.1 LOPD declara, como norma específica laboral en diálogo con el art.22 LOPD, que *"los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo"*.

[5] CASAS BAAMONDE, M.E., "Informar antes de vigilar …", *cit.*, p.119; SALA, T.; TARABINI-CASTELLANI, M., "El derecho a la intimidad personal y el control del trabajador" en dir. SALA, T., *Propuestas para un debate sobre la reforma laboral*, Lefebvre, Madrid, 2018, pp. 256-257.

El art.22.1 LOPD entronca con el interés legítimo de la seguridad que sustenta el tratamiento del dato personal de la imagen grabada, sin consentimiento expreso, en línea de lo exigido con carácter general en el art. 6.1.f REPD. El art.89.1 LOPD es una proyección de este interés legítimo de seguridad en el ámbito laboral pero, a la vez, entronca de manera específica con un interés empresarial legítimo al control de los trabajadores y con la necesidad de garantizar el cumplimiento del contrato de trabajo, como excepción al consentimiento de los arts.6.1.f y b REPD[6]. En este marco de fundamentación jurídica, el diálogo entre el art.22.1 LOPD y 89.1 LOPD no desemboca en restringir la videovigilancia laboral a la función exclusiva de preservar la seguridad de personas, bienes e instalaciones dentro de la empresa, sino que supone, por la remisión del art.22.8 LOPD en conexión con los arts.6.1.f y b REPD, un reconocimiento de estos dispositivos como herramienta específica de control de los trabajadores, sin consentimiento expreso de éstos, siempre que se respete la intimidad personal y la protección de datos personales. En la función de control laboral cabe utilizar cámaras para preservar la *"seguridad de personas, bienes e instalaciones"*, como sucede ante sospechas de robos de los empleados, un supuesto que ofrece la práctica. Pero el término específico, *"control de los trabajadores"* del art.89 LOPD es más extensivo que la mera preservación de la *"seguridad"* del art. 22 LOPD y habilita, respetando los límites correspondientes, la instalación de cámaras con esta finalidad, sirviendo la imagen como prueba lícita de sanción o despido disciplinario. En cada caso, como ahora veremos, habrá que justificar la medida para no invadir de manera injustificada la privacidad del empleado y cumplir con la legislación vigente de datos personales, incluido el art.22 LOPD, lo que delimita, de suyo, esta capacidad de control laboral. Pero ello no conduce a restringir la cámara a supuestos de seguridad como robos de bienes o dinero a la empresa. Pueden existir otros supuestos, como acosos laborales o sexuales de empleados, mala conducta que derive en incumplimientos contractuales laborales, comisión de irregularidades laborales graves u otros, donde encaje una cámara con obtención de pruebas lícitas[7]. Lo que no resultará en ningún modo admisible, siguiendo la doctrina de la Agencia de Protección de Datos Personales (APD), es utilizar imágenes no relevantes en el ámbito laboral, ni instalar una cámara para verificar comportamientos o características personales ajenas al contrato de trabajo[8].

El sistema legal dual, además, diferencia las cámaras de seguridad y las laborales, no sólo en este diálogo entre los arts.22 y 89 LOPD, sino en el art. 42.4 de la Ley de Seguridad Privada 5/2014 (LSP), al declarar que las grabaciones obtenidas por la videovigilancia de *"seguridad no pueden destinarse a uso distinto de su finalidad"*. Esta base legal distingue, así, claramente, entre sistemas de videovigilancia, de seguridad privada en espacio público y de control empresarial del trabajador, sujetos a mecanismos de información y procedimientos distintos, también ante la APD. Los arts 22 y 89 LOPD deben ser leídos sobre esta distinción dual, presente ya antes de la LOPD de 2018, en nuestro ordenamiento.

El fundamento jurídico de esta primera regulación legal laboral específica de la videovigilancia laboral tiene una clara huella jurisprudencial constitucional. La integración del poder de dirección y control del art.20 ET en los derechos constitucionales de libertad de empresa del art.38 CE y de propiedad privada

[6] ALTES TARREGA, J.A., "La videovigilancia de la actividad laboral", en prensa, ejemplar original, próxima publicación.

[7] No comparto por todas estas razones jurídicas la tesis restrictiva de videovigilancia laboral exclusiva de funciones de seguridad de personas, bienes e instalaciones de BAZ RODRÍGUEZ, J., "La Ley orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales", *Trabajo y Derecho* 2019, nº 54, pp. 62-65. Sí comparto la tesis extensiva de videovigilancia laboral asociada el control del contrato de trabajo, en similares términos a los aquí expresados, de ALTES TARREGA, J.A., "La videovigilancia en la actividad laboral", *cit.*

[8] MERCADER UGUINA, J., *Protección de datos y garantías de los derechos digitales en las relaciones laborales*, Lefebvre, Madrid, 2019, p.139.

del art. 33 CE ofrece cobertura legal a la instalación empresarial de herramientas de videovigilancia y grabación de sonido para controlar el cumplimiento de los contratos de trabajo, con los límites correspondientes. Queda reconocida de manera expresa esta herramienta de control audiovisual de los trabajadores, con una mención ya literal en el art.20 ET. Pero, a la vez, la necesaria ponderación entre los arts.38 y 33 CE y los derechos personales del trabajador exige la limitación de estos dispositivos para respetar la intimidad y protección de datos personales de los arts.18.1 y 4 CE, lo que explica la expresa mención legal en el art.20 ET a la intimidad del trabajador, también reconocida en el art.4.2.e ET. La regulación legal en el art.89 LOPD de la videovigilancia laboral está marcada, desde su rótulo, por estas coordenadas, el reconocimiento del uso de estas herramientas de control por las empresas y su limitación para proteger la intimidad personal y los datos personales del trabajador. El art.89 LOPD, norma específica frente al art.22 LOPD, es, en consecuencia, resultado de una ponderación jurídica, ya mostrada por el TC y TS, entre los arts.38 y 33 CE, y su manifestación legal en el art.20 ET – poder contractual de control de la empresa – y los arts.18.1 y 4 CE, y su manifestación legal en el art.4.2.e ET – derechos de intimidad personal y protección de datos personales del trabajador controlado –[9].

Estas raíces constitucionales no dejan, sin embargo, de ser controvertidas. El voto particular de D.Fernando Valdés a la STC 39/2016, que descarta una conexión automática entre los arts.33 y 38 CE con los poderes contractuales laborales del art.20 ET, muestra esta controversia[10]. Frente a la tesis amplia, que asocia la libertad de empresa sin matices con la buena marcha de la organización productiva, aparece la tesis más restrictiva, que niega la vinculación directa y automática de este derecho con los poderes empresariales en el contrato de trabajo. A mi juicio, como vía intermedia, es necesario otorgar un mínimo de contenido esencial a la libertad de empresa del art.38 CE que, desde su conexión con la propiedad privada del art.33 CE, fundamente el poder empresarial de control de sus medios de producción y la gestión de la ajenidad y dependencia que implica la relación contractual laboral. No tanto en clave de productividad como apunta el TC (en aras de una buena marcha de la organización productiva), como de disposición de la propiedad de los medios de producción y del propio patrimonio, lo que puede conllevar facultades de control a los trabajadores. Sin esta fundamentación constitucional del art.38 CE es muy difícil este tipo de ponderación jurídica – triple test de necesidad, idoneidad y proporcionalidad – que viene efectuando el TC en los derechos fundamentales de los trabajadores. Porque sin anclaje constitucional, resulta difícil admitir que un poder de exclusiva naturaleza legal (art.20.3 ET) pueda restringir un derecho fundamental del trabajador (art.18 CE) sobre la justificación de ser una medida necesaria, idónea y proporcional. El único que puede limitar a un derecho constitucional es otro derecho constitucional, como sucede en el diálogo ponderado entre la libertad de empresa y la intimidad/protección de datos personales del trabajador. La opción legal del art.89 LOPD se sitúa en este espacio de ponderación jurídica constitucional.

3. TIPOLOGÍA DE VIDEOVIGILANCIA LABORAL

La lectura del art.89 LOPD, a la luz de la expuesta jurisprudencia, deduce tres tipos de

[9] Esta ponderación jurídica entre control audiovisual de la empresa e intimidad personal y protección de datos personales del trabajador ha dominado el tratamiento doctrinal de la cuestión, con posiciones más restrictivas del control –incluso negando su legitimidad– y más proclives a asumir este tipo de herramientas con respeto a estos límites. Un repaso doctrinal con interesantes reflexiones sobre estos debates y un riguroso análisis sobre el alcance de la intimidad personal en el lugar de trabajo en DESDENTADO BONETE, A.; MUÑOZ RUIZ, A.B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012, pp. 40-71.

[10] ROJO TORRECILLA, E., "Derecho del trabajador a la privacidad en la empresa y límites a su control por las cámaras de videovigilancia", *cit.*, pp. 135 y ss.

videovigilancia laboral[11], dos expresamente regulados y uno dejado a la interpretación de la ponderación jurídica entre el poder de control empresarial y los derechos personales del trabajador de intimidad y protección de datos personales.

El primer tipo de videovigilancia laboral es la **cámara estructural** que tiene como finalidad el control de los trabajadores con los límites pertinentes. La instalación de esta herramienta de videovigilancia es continua y estable. El art.89 LOPD regula, como ahora expondré, sustancialmente este tipo de cámara estructural, con esta finalidad laboral, imponiendo límites que deben ser valorados, así como garantías y reglas que deben ser cumplidas. El art.89 LODP recoge, en este sentido, la jurisprudencia antes expuesta, que, a la vez que avala este medio de control, es garantista en el respeto de los derechos personales de intimidad y protección de datos personales del trabajador.

El segundo tipo de videovigilancia laboral previsto en el art.89 LOPD es el **hallazgo casual**, la comisión flagrante de acto ilícito del trabajador, a través de una cámara de seguridad, donde resulta suficiente el distintivo informativo genérico y visible exigido por la Agencia de Protección de Datos en este tipo de cámaras. El art.89 LOPD también está inspirado, pero con muchos matices, en la antes mencionada jurisprudencia constitucional que había admitido este distintivo genérico en determinadas captaciones de imágenes del trabajador.

La carencia del art.89 LOPD es el tercer tipo de videovigilancia laboral, las **cámaras ocultas** instaladas *ad hoc* ante indicios de irregularidades del trabajador. Pese a existir jurisprudencia, constitucional y del TEDH, que pondera control empresarial y derechos personales del trabajadores en este tipo de cámaras, la LOPD no establece reglas claras de su admisión y uso. Esta tipología de videovigilancia es, por ello, la más controvertida y abierta a interpretaciones de ponderación jurídica, sobre los límites mencionados con carácter general en el art.89 LOPD. Siendo la formulación donde, ante el vacío normativo, cabe más acudir a la expuesta jurisprudencia constitucional e internacional.

Creo fundamental diferenciar, como punto de partida, estos tres tipos de videovigilancia laboral – estructural, hallazgo casual y oculta *ad hoc* – pues los límites, reglas y garantías son, como ahora expondré, diferentes.

4. CÁMARA ESTRUCTURAL PARA EL CONTROL LABORAL

El art.89 LOPD regula sustancialmente las cámaras estructurales con finalidad de control laboral, diferenciadas, como ya he expuesto, de las cámaras de seguridad del art. 22 LOPD, que se remite en su apartado 8, como norma específica, a este precepto. El art. 89 LOPD admite la cámara estructural laboral pero es muy garantista en el respeto a la intimidad personal y protección de datos personales del trabajador, en línea con los límites impuestos ya por la jurisprudencia constitucional, ordinaria e internacional.

De un lado, el respeto a la intimidad personal del trabajador aparece expresamente en el nuevo art.20 bis ET e, implícitamente, en el art.89 LOPD. Los mencionados *"límites inherentes al marco legal"*, de manera autorreferencial, vienen determinados, sin duda, por la intimidad personal del trabajador de los arts.20 bis y 4.e ET, expresamente mencionada en la apertura del art.89 LOPD, "*derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo*". La videocámara debe respetar, en consecuencia, la intimidad personal del trabajador, y, por tanto, conforme a la jurisprudencia examinada, ser adecuada, necesaria y proporcionada al fin perseguido. La empresa debe justificar, en cada caso, la instalación

[11] LAHERA FORTEZA, J., "Seguridad jurídica en la videovigilancia laboral de las empresas", *Cinco Días/El País*, 29 Octubre 2019.

necesaria y proporcionada de videocámaras laborales estructurales. La remisión al marco legal es, a su vez, un reenvío a la jurisprudencia consolidada, que limita el uso de estos dispositivos, exigiendo, en cada supuesto de hecho, la superación de los test de adecuación, necesidad y proporcionalidad para contrastar el debido respeto a la intimidad personal del trabajador. Cobran pleno vigor, desde esta cobertura legal, las técnicas clásicas jurisprudenciales de examen de la videovigilancia laboral utilizadas por el TC, el TS y también, en otro plano, por el TEDH, con las sentencias de referencia antes expuestas. De manera más específica, el art.89.2 LOPD concreta el debido respeto a la intimidad personal declarando lo siguiente: *"En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos"*. Esta prohibición es claramente deudora de la jurisprudencia constitucional antes analizada (SSTC 98/2000 y 186/2000) que, expresamente, impide el uso de estos dispositivos de control en estos lugares de descanso o esparcimiento como vestuario, aseos, comedores y análogos, donde siempre prevalece la intimidad personal del trabajador. La influencia jurisprudencial es evidente en esta prohibición expresa, que ya tiene plena habilitación legal. Queda descartado cualquier juicio de necesidad y proporcionalidad en estas cámaras porque debe ser respetado siempre, por encima de todo, el derecho a la intimidad, determinado, en este caso, por el espacio de privacidad del trabajador dentro del centro de trabajo. Algo que ha recordado también la STEDH 17 Octubre 2019, asunto López Ribalda 2, al referirse a estos especiales y protegidos espacios de privacidad de los empleados en las empresas.

De otro lado, la debida protección de los datos personales, considerando la imagen grabada como un dato personal, recibe consolidación legal, en este tipo de cámaras, con una clara huella jurisprudencial en el art.89.1.2º párrafo LOPD: "*Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida"*. La jurisprudencia constitucional antes expuesta (SSTC 29/2013 y 39/2016) y su recepción por el TS (STS 13 Mayo 2014) obligan a esta información, desde la óptica de la protección del dato personal de la imagen, en los términos ahora ya expresados legalmente. La empresa debe informar al trabajador, individualmente, con carácter previo, y de manera clara e inequívoca de la instalación de la videocámara y de sus finalidades de control y sancionadoras, así como del tratamiento de este dato personal. Las SSTEDH 9 Enero 2018 y 17 Octubre 2019, asunto Lopez Ribada 1 y 2, subrayan también de manera concreta este deber de información, ahora fortalecido legalmente. El tratamiento de dato personal de la imagen exige un protocolo de información individualizada, pero también la exigencia de una expectativa de intimidad del trabajador grabado, que debe ser consciente de ser objeto de este control tecnológico.

Está ya fuera de toda duda, en fin, la exigencia de información individual, clara y explícita, al trabajador, de la instalación de un sistema estructural de videovigilancia, en términos similares a los exigidos en el art.12 REPD con carácter general. La información clara y transparente debe consistir en la identidad del responsable del tratamiento, la localización exacta de la cámara, la finalidad, exclusivamente sancionadora, del tratamiento del dato personal de la imagen grabada y la posibilidad del trabajador de ejercer los derechos de los arts.15-22 REPD, que permiten al interesado acceder y controlar los datos personales, así como la posibilidad de limitar su tratamiento u oponerse al mismo en determinadas circunstancias[12]. Ello desmiente la jurisprudencia constitucional menos exigente

[12] ALTES TARREGA, J.A., "La videovigilancia de la actividad laboral", *cit.*, subrayando la presencia de infracciones muy graves y leves en caso de incumplimiento, en los arts.72.1.h, 72.1.d y 74.b LOPD.

con este deber (STC 39/2016) y su recepción por la SALA IV del TS, que admiten, en ocasiones, un dispositivo visible y genérico de cámaras como procedimiento informativo. Como ahora veremos, este tipo de dispositivo, aplicable en cámaras de seguridad, puede tener trascendencia en hallazgos causales de actos ilícitos del trabajador – art.89.1.3º LOPD– o en cámaras ocultas –art.22 LOPD –, pero no sirve nunca para dar cumplimiento al deber de información del tratamiento del dato personal de la imagen, que debe ser, en los términos antes descritos, individual, claro y expreso. La decisión legal del art.89.1.2º LOPD es razonable, porque la información del uso del dato personal existe o no existe: o el trabajador es legalmente informado del uso laboral de la videocámara o no. Resultaba desconcertante la aplicación por parte de la STC 39/2016 de la técnica de la proporcionalidad en el reconocimiento de la información, como si pudieran existir grados intermedios en ser informado o ésta pudiera llegar a ser desproporcionada[13]. Técnica de la proporcionalidad que puede ser útil en la ponderación entre derechos constitucionales, pero no en reconocer si ha existido o no una información exigida legalmente al empresario, como bien sostuvo en su día el voto particular de D. Fernando Valdés a dicha sentencia. La deficiencia de información no puede ser ponderada porque no hay derecho de la empresa en juego que sirva de espejo frente a la protección de datos personales del art.18.4 CE que, en su contenido esencial, tiene esta garantía jurídica. La libertad de empresa del art.38 CE ampara los márgenes proporcionados del poder contractual de control pero no justifica de ninguna manera incumplir la exigencia de informar al trabajador del instrumento controlador cuando, como ya sucedía con la anterior LOPD, lo exige expresamente la Ley.

La Instrucción 1/2006 de la APD, que exige colocar estos *"distintivos informativos en un lugar suficientemente visible, tanto en espacios abiertos como cerrados",* se refiere a cámaras estructurales de seguridad y no a las estrictamente laborales. Como ha sido anticipado, el art.42.4 de la Ley de Seguridad Privada 5/2014 declara que las grabaciones obtenidas por la videovigilancia de *"seguridad no pueden destinarse a uso distinto de su finalidad",* de igual modo que el art. 22 LOPD, vinculado a la seguridad, queda diferenciado del art.89 LOPD, conexo con el control laboral. Estas bases legales distinguen, así, entre sistemas de videovigilancia, de seguridad privada en espacio público y de control empresarial del trabajador en su lugar de trabajo, sujetos a mecanismos de información y procedimientos distintos, también ante la APD. Por eso es tan importante la información al trabajador del uso de la cámara y de su finalidad disciplinaria, confirmada por el art.89 LOPD. Técnicamente una cámara de seguridad privada puede ser aprovechada para el control laboral pero siempre que el trabajador reciba la información de este uso específico con claridad. Grabar a un trabajador sin informar, a través de la cámara de seguridad privada, vulnera el art.42.4 de la LSP. Y es en este contexto donde hay que situar la manida Instrucción 1/2006 de la APD, pensada para el dominio de la seguridad en espacio público, donde resulta suficiente la pegatina en un cristal de una empresa, pero no para el ámbito laboral, donde la información debe ser más específica y clara. El art.89.1.2º LOPD, al establecer un deber individual claro de información, excepciona en el ámbito laboral lo dispuesto en el art.22.4 LOPD, que la colocación del distintivo informativo visible es suficiente para el tratamiento del dato personal de la imagen. Quedan reconciliados, así, los arts.42.4 LSP con el art.89.1 LOPD y 22.4 LOPD, corrigiendo la confusión creada por la errática STC 39/2016. Las cámaras de seguridad tienen el régimen jurídico de información y tratamiento de datos personales del art.22 LOPD, y, en coherencia con el art.42.4 LSP, las cámaras laborales se sujetan al régimen específico del art. 89.1 LOPD, con una información individualizada, clara y explícita del fin y tratamiento del dato personal.

[13] LAHERA FORTEZA, J., "Nueva jurisprudencia constitucional en la videovigilancia laboral: valoración crítica", *Derecho de Relaciones Laborales* 2016, nº 5, pp. 494 y ss.

Por otra parte, el art.89.1.2º párrafo LOPD subraya la necesaria, en su caso, *"información a los representantes de los trabajadores"* de la instalación del sistema de videovigilancia laboral estructural. La previsión debe ser completada con el art.64.5.f ET, que exige a la empresa informar y consultar a los representantes de los trabajadores de la instalación de la videocámara y de sus finalidades de control y sancionadoras. Se debe respetar este derecho colectivo, como por otra parte, venía recordando la jurisprudencia constitucional (STC 29/2013) y ordinaria (STS 13 Mayo 2014). Ello implica no sólo informar, como menciona el art.89 LOPD, sino también consultar a los representantes de los trabajadores, como exige el art.64.5.f ET, elaborando éstos un informe no vinculante sobre la instalación de la cámara estructural laboral, en el plazo general máximo de quince días desde la información recibida conforme a lo previsto en el art.64.6 ET.

La remisión del art.22.8 LOPD al art. 89 LOPD plantea, finalmente, si resultan aplicables otras reglas de tratamiento del dato personal de la imagen del art.22 LOPD a la videovigilancia laboral, en especial la destrucción de imágenes del apartado 3 en el plazo de un mes desde su captación, salvo que acrediten la comisión de actos que atentan contra la integridad de personas, instalaciones o bienes. El art.89 LOPD, por el contrario, no regula la destrucción de imágenes en ningún plazo, a diferencia de la grabación de sonidos, como veremos a continuación. A mi juicio, la remisión del art.22.8 LOPD al art.89 LOPD en el tratamiento de imágenes laborales y la ausencia de remisión al art.22.3 LOPD en la supresión de imágenes, a diferencia de la grabación de sonidos, concluye en la inaplicación de este plazo mensual de destrucción desde la captación[14]. Tiene lógica esta conclusión porque permite la utilización de la imagen grabada como prueba lícita en juicio posterior al mes o recoger imágenes de reiteración de irregularidades del empleado en tramos superiores al mes. La prueba será destruida cuando ya no sea útil y en el tiempo de conservación no podrá ser difundida la imagen, ni dentro ni fuera de la empresa, en respeto a la intimidad personal de los grabados y del tratamiento de sus datos personales. Con esta salvedad, el tratamiento del dato personal de la imagen del trabajador se sujeta a las reglas generales de protección de datos personales del art.22 LOPD y a los principios del art.5 REPD. En especial resulta aplicable la limitación de la finalidad de los datos personales, que *"serán recogidos con fines determinados, explícitos y legítimos y no serán tratados ulteriormente de manera incompatible con dichos fines"*, del art.5.1.b REPD[15]. La imagen grabada se sujeta, en fin, a los más estrictos requisitos de confidencialidad, de no difusión a terceros y de tratamiento exclusivo, por los responsables de tratamiento de datos personales en cada caso, con esta finalidad.

5. HALLAZGO CASUAL DE ACTO ILÍCITO DEL TRABAJADOR

El art.89.1. 3º párrafo de la LOPD establece un tratamiento específico, del segundo tipo de videovigilancia laboral, el hallazgo casual de acto ilícito: "*en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica".*

El art.22.4 LOPD contempla el distintivo visible y general de videocámaras con fines de seguridad de personas, bienes e instalaciones, al que hace referencia la citada instrucción 1/2006 de la APD. La regla general es, como ha sido razonado, que este distintivo informativo no es suficiente en la videovigilancia laboral estructural porque el art.22.8 LOPD se remite al art.89

[14] Defiende, en cambio, la aplicación del plazo mensual de destrucción BAZ RODRÍGUEZ, J., "La Ley Orgánica 3/2018 como marco embrionario de la garantía de derechos digitales laborales", *cit.*, p.62.

[15] ALTES TARREGA, J.A., "La videovigilancia de la actividad laboral", *cit.*

LOPD, que establece un deber de información individual, mucho más exigente, en los términos antes descritos. La excepción a esta regla general es el supuesto de hecho de *"captación de comisión flagrante de actos ilícitos"*, donde resulta suficiente el distintivo visible y general del art.22.4 LOPD de las cámaras de seguridad.

Puede parecer que este criterio legal confirma la STC 39/2016, que admite distintivos visibles de cámaras de seguridad como información para el tratamiento de dato personal de la imagen en el ámbito laboral. Como ha sido antes razonado, el art.89.1.2º LOPD es más bien una corrección de esta confusa sentencia, que no diferencia entre tipos de cámaras. Sí se acerca la excepción del art.89.1.3º LOPD al preciso contenido del voto particular a la STC 39/2016 de D. Juan Antonio Xiol Rius. La prueba lícita penal del hallazgo casual, en una imagen grabada en espacio abierto o cerrado, es aplicable en cámaras de seguridad privada, donde un distintivo visible es suficiente en la protección de datos personales. Sólo así es posible instalar, por eficiencia, controles de seguridad en espacios donde pueden entrar miles de clientes, siendo útil el hallazgo causal como prueba en un procedimiento sancionador o judicial. Sería absurdo informar individualmente y ello explica que la APD admita distintivos visibles que están expuestos en tantas empresas abiertas a consumidores y clientes de nuestra realidad social. Hasta el art.89.1.3º LOPD esta doctrina no tenía proyección legal explícita en el ámbito laboral, generando algunas contradicciones. Si el trabajador cometía un delito en el centro de trabajo, y ello era grabado por la cámara de seguridad, la prueba era lícita por hallazgo causal en el ámbito penal, pero podía ser ilícita en el plano laboral disciplinario. El art.89.1.3º LOPD supera esta contradicción y aplica el hallazgo casual también al ámbito laboral, sin por ello relajar la información debida con carácter general al trabajador en la videovigilancia estructural laboral. Es una excepción, en fin, que confirma la regla general.

Por actos ilícitos en el hallazgo causal hay que entender, por supuesto, delitos, que era el término utilizado en la versión original del proyecto de la LOPD. La grabación de delitos por hallazgo causal del trabajador mediante una cámara de seguridad es una prueba lícita también en el plano disciplinario laboral, superando la contradicción antes expresada. Queda la duda de si ampliar la validez de estas pruebas por hallazgo casual a conductas no delictivas del trabajador, pero sí ilícitas en el plano laboral. La sustitución del término *"delictivo"* por *"ilícito"* en la tramitación de la LOPD es una base para sostener la admisión de estas pruebas estrictamente laborales, que puedan sustentar una sanción o despido disciplinario. Al fin y al cabo el incumplimiento contractual es un acto ilícito, como lo es cualquier irregularidad laboral. No es necesario que se abra un procedimiento penal al trabajador, por tanto, para admitir grabaciones por hallazgo casual de cámaras de seguridad que motiven una sanción o despido disciplinario. Es una cuestión, en todo caso, que la jurisprudencia irá configurando. Una alternativa intermedia es delimitar las pruebas de hallazgos casuales a irregularidades laborales especialmente relevantes, que pueden sustentar un despido disciplinario procedente, descartando su uso en sanciones disciplinarias menores.

6. CÁMARA OCULTA *AD HOC* ANTE INDICIOS DE IRREGULARIDAD GRAVE DEL TRABAJADOR

En los términos expuestos, el art.89. 1 y 2 LOPD establecen, por tanto, el régimen jurídico de dos tipos de videovigilancia, la estructural laboral para controlar a trabajadores cuando sea necesario, adecuado y proporcionado, y el hallazgo casual de actos ilícitos flagrantes captados por imágenes de cámaras de seguridad. Las reglas son en, ambos casos, identificables, claras, aún con algún margen interpretativo, y ofrecen seguridad jurídica a las empresas. El casuismo resulta inevitable en cada supuesto de hecho, a examen de las técnicas empleadas, pero el régimen jurídico está identificado con claridad.

El art.89 LOPD no aborda, por el contrario, un tercer tipo de cámaras laborales, de gran incidencia práctica, las coyunturales ante indicios de irregularidad del trabajador. Las videocámaras ocultas instaladas *ad hoc* ante la existencia de indicios de acto ilícito del trabajador para obtener pruebas de cara a una sanción o despido disciplinario no están reguladas en el art.89 LOPD.

Resulta, de un lado, absurdo aplicar a este tipo de cámara coyuntural, las reglas de información al trabajador del art.89.1 LOPD, como si fuera estructural, porque se rompería la finalidad probatoria ante los indicios detectados; una vez informado, el trabajador dejaría de cometer estos actos ilícitos que van a ser grabados y la cámara no sería ya oculta. Lo secreto nunca se preavisa.

De otro lado, tampoco es aplicable el expuesto régimen del hallazgo casual, con distintivo informativo visible, del art.89.1.3º LOPD, que se refiere a cámaras con fines de seguridad que graban la comisión flagrante de actos ilícitos, porque este supuesto de hecho responde a poner directamente una cámara laboral oculta que grabe irregularidades del trabajador a efectos de control y sanción. Es una contradicción en sus propios términos intentar derivar las cámaras ocultas *ad hoc* al hallazgo causal de acto ilícito del art.89.1 LOPD; si el hallazgo es casual, ya no lo es porque se instala *ad hoc* una cámara oculta, si la comisión es flagrante es que no había indicios previos de dicha acción grabada, y si lo capta una cámara de seguridad, ya no está instalada *ad hoc* en el escenario de la irregularidad. La captación flagrante de ilícito del trabajador no se corresponde con la captación premeditada ante sospechas de ilícito con una cámara oculta instalada *ad hoc*[16]. Existe, en definitiva, una laguna normativa en este tipo de cámaras.

Ante la ausencia legal, vuelve a ser la jurisprudencia protagonista en este tercer tipo de cámara laboral. La primera jurisprudencia constitucional (STC 186/2000), antes analizada, ya avaló este tipo de cámara coyuntural ante indicios de graves irregularidades del trabajador al ser una medida idónea, necesaria y proporcionada. La cámara era puntual, limitada en el tiempo, afectaba sólo a los trabajadores sospechosos, en zonas delimitadas, y estaba destinada a constatar las irregularidades sospechadas. La evolución jurisprudencia posterior, que subraya la información al trabajador al ser la imagen un dato personal, desviaron el foco de este tipo de medida, extendiendo este deber a cualquier cámara tratada siempre como estructural (STC 29/2013 y STS 13 Mayo 2014). La STC 39/2016 eludió afrontar, de nuevo, el problema de las cámaras coyunturales en un supuesto de hecho de sospecha de irregularidades, al relajar este deber informativo con el distintivo visible, pero de nuevo con un tratamiento similar de cámara estructural y mezclado con las cámaras de seguridad. Se produce, en esta evolución, una confusión jurisprudencial entre cámaras estructurales, hallazgos casuales de cámaras de seguridad y esta videovigilancia laboral coyuntural, que impide ofrecer una solución específica al problema. En medio de esta confusión, no resulta nada claro que la jurisprudencia admita este tipo de medidas de control coyuntural con cámaras ocultas, más bien parece prohibir esta opción al generalizar la información al trabajador incompatible con esta herramienta de vigilancia[17]. La laguna normativa del art.89 LOPD, sin embargo, no puede ser contemplada como una prohibición.

La jurisprudencia que ofrece ahora más luz en este tipo de cámara oculta es la antes expuesta del TEDH, 5 Octubre 2010, asunto Köpke, 9 Enero 2018, asunto Lopez Ribalda

[16] No comparto, por estas razones, la tesis de encajar la cámara oculta en el supuesto de hallazgo causal del art.89.1 LOPD de Baz Rodríguez, J., "La ley orgánica 3/2018 como marco embrionario de garantía de derechos digitales laborales", *cit.*, pp. 68-69.

[17] Goñi Sein, J.L., "Videovigilancia empresarial mediante cámaras ocultas ...", *cit.*, p. 79.

1 y, sobre todo, la reciente 17 Octubre 2019, asunto López Ribalda 2. El TEDH admite la ausencia de información en cámaras ocultas instaladas ante indicios y sospechas fundadas de irregularidades graves del trabajador grabado con exigentes requisitos. El indicio debe ser cierto y acreditado, la videovigilancia limitada al área y trabajador/es sobre el que pesan estas sospechas fundadas, la duración de la instalación puntual y de tiempo proporcionado al fin de control, las imágenes deben ser vistas exclusivamente por responsables de la empresa, nunca difundidas, y con un tratamiento sólo dirigido a la penalización de esta irregularidad grave, siendo luego sometidas a las mayores garantías y exigencias de la protección de datos personales. Esta suma de requisitos conlleva un grado razonable y proporcionado de intromisión en la privacidad, no contrario al art.8 de la CDH, y origina una prueba lícita en un proceso, sin vulnerar el art.6 de la CDH. La ausencia de información en esta cámara oculta fundamentada y proporcionada puede dar lugar, apunta el TEDH, a responsabilidades administrativas de protección de datos personales o civiles de daños, pero no invalida la prueba laboral lícita y las reacciones empresariales ante la comisión de irregularidades graves así acreditadas. En estas condiciones, se solventa la proporcionalidad y se exime de la información previa, contraria a la propia naturaleza de este tipo de cámara oculta. El respeto a la intimidad personal del art. 89 LOPD también es aplicable a estas cámaras, lo que exige una justificación proporcionada muy exigente de su uso, exclusivo ante indicios de irregularidades graves del trabajador, y sin, en ningún caso, traspasar la privacidad en los ámbitos mencionados de aseos, vestuarios y lugares de esparcimiento del trabajador. Hay dos argumentos añadidos que, en el marco del art.89 LOPD, fortalecen la admisión de estas cámaras ocultas en línea con lo establecido por el TEDH.

De un lado, la aplicación de transparencia del art.89.1.2º LOPD se puede hacer, en este tipo de cámara, con una información preventiva y previa de posible instalación de estos dispositivos ante hipotéticas y futuras sospechas de irregularidades del trabajador en el centro de trabajo. Puede ser una vía formal para las empresas comunicar estas informaciones preventivas para ofrecer cobertura a una futura videovigilancia laboral coyuntural, si quedan acreditados indicios previos de irregularidades del trabajador y se cumplen los criterios del TEHD. No es posible informar ante el hecho puntual pero sí de manera preventiva y de este modo genérico. Es la única manera de solventar el problema desde una exigencia de transparencia porque es evidente que la información puntual desmonta este mecanismo de control secreto.

De otro lado, cabe mantener la opción interpretativa, por analogía, de argumentar la presencia de distintivo visible de videovigilancia, contemplado para los hallazgos casuales del art.89.1.3º LOPD, pero también con carácter general informativo en el art.22.4 LOPD. El dispositivo visible ampararía la cámara oculta justificada, confirmando, de alguna manera, el criterio de la STC 39/2016 por el camino interpretativo de la analogía ante el actual vacío legal. Se trataría de aplicar, por otra parte, la regla general del art.22.4 LOPD. Si cabe el hallazgo casual o azaroso sin que existan indicios de irregularidad grave, también cabrá la cámara oculta, con los requisitos del TEDH, si están acreditados estos indicios previamente. Quien puede lo más puede lo menos.

Ambas vías legales, en conjunción con la doctrina del TC y TEDH, pueden amparar cámaras ocultas justificadas y respetuosas con la intimidad personal del trabajador, en el marco de los arts. 22 y 89 LOPD. Pero, incluso, sin este mecanismo preventivo informativo o sin distintivo visible, creo se puede defender, con los argumentos iniciales del TC y el refuerzo del TEDH, este tipo de cámara coyuntural, si se acreditan indicios de irregularidades graves y se procede a instalar, con cautelas y de manera proporcionada, este dispositivo que confirme las sospechas de irregularidades laborales con imágenes que sirvan de prueba lícita. El principio de transparencia

informativa cedería en este tipo de situaciones que pueden ser denominadas como un control empresarial defensivo *ex post*[18].

La finalidad de esta cámara es, esta vez sí, exclusivamente de protección de seguridad de bienes, personas y daños, aplicando la regla general del art. 22.1 LOPD, y el control es defensivo, porque ya están acreditados indicios de actos ilícitos del trabajador contra esta seguridad. El supuesto más claro es el de los robos por parte del empleado o el de cualquier otra comisión de delitos en el lugar de trabajo. La prudencia jurídica creo debe limitar estas cámaras secretas a la comisión de actos delictivos. El interés público a la seguridad y cumplimiento de la ley penal debe prevalecer sobre el principio de transparencia de protección de datos personales. En este marco, y con los límites apuntados por el TDEH, la cámara oculta es legítima y la imagen obtenida del ilícito una prueba legal.

La doctrina judicial y jurisprudencia futura tendrá, en todo caso, que despejar de manera clara la viabilidad de este tipo de cámaras ocultas y no informadas, las más abiertas, tras el art. 89 LOPD, a la controversia jurídica. He razonado, con apoyo legal y jurisprudencial, argumentos favorables a su admisión con garantías y requisitos. Pero no habría que descartar interpretaciones formales sustentadas en el vacío de regulación en el art.89 LOPD y en la exigencia de información que pudieran concluir en una prohibición legal en España de este tipo de cámaras, pese a la doctrina del TC y TEDH que sí las admite. El TC y TS tendrán que aclarar en un futuro esta controversia jurídica con claridad.

7. TRATAMIENTO ESPECÍFICO DE LA GRABACIÓN DE SONIDO EN EL LUGAR DE TRABAJO

La grabación de sonidos tiene especiales restricciones, con una exigente protección de la intimidad de los trabajadores, prevista en el art.89.3 LOPD en los siguientes términos: *"la utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley".*El tratamiento específico de la grabación de sonido en el lugar de trabajo muestra una mayor conexión con el art.22 LOPD que el de la estricta videovigilancia laboral. A diferencia de las cámaras, la captación de sonido no es una posible herramienta de control del trabajador, en el cumplimiento del contrato de trabajo, si resulta justificado. El art.89.3 LOPD, a diferencia del art.89.1 LOPD, delimita la grabación de sonidos cuando *"resulte relevante para la seguridad de bienes, personas e instalaciones"* en el centro de trabajo, en los mismos términos que expresa el art.22 LOPD respecto a la videovigilancia no estrictamente laboral. Sólo será trascendente, y relevante jurídicamente, el sonido grabado en el lugar de trabajo, cuando preserve la seguridad de bienes, personas e instalaciones, operando entonces como prueba lícita. La norma específica retorna así a la norma general del art. 22 LOPD.

Este criterio restrictivo tiene huella jurisprudencial porque la iniciática STC 98/2000 ya entendió, en su día, ilegítima la captación de sonido por la empresa de los trabajadores al ser un sistema en exceso intrusivo con la privacidad, desproporcionado y falto de fundamento; también la APD se ha pronunciado en esta misma dirección delimitadora[19]. La opción del art.89.3 LOPD viene a confirmar

[18] Utilizando la terminología de Goñi Sein, J.L., "Videovigilancia empresarial mediante cámaras ocultas ...", *cit.*, pp. 74 y ss

[19] Mercader Uguina, J., *Protección de datos ..., cit.*, p.148.

esta jurisprudencia y criterio garantista, diferenciando la mera videovigilancia de las grabaciones de sonidos. De igual modo, la normativa más garantista se explica por la protección añadida del secreto de comunicaciones, que aparece directamente como bien jurídico en los sistemas de control de las grabaciones telefónicas y de cualquier sonido. La STC 85/1994 declaró, ya en su día, que *"la observación de telecomunicaciones supone una grave injerencia en la esfera de la intimidad personal"*, de tal modo que debe *"estar sometida al principio de legalidad y de proporcionalidad"*. El art.18.4 CE avala la libertad de comunicaciones y comprende *"su secreto con la interdicción del conocimiento antijurídico de comunicaciones ajenas"*, en la línea de la STC 114/1984. El régimen singular del art.89.3 LOPD tiene raíces en esta conexión y jurisprudencia consolidada.

La instalación de cámaras con grabación de sonidos está sujeta, así, a una mayor restricción que la mera videovigilancia laboral sin audio. Es común la prohibición de grabar sonidos en lugares destinados a descanso o esparcimiento, como aseos, vestuarios o comedores del art.89.2 LOPD. Pero la captación de imagen del art.89.1 LOPD tiene un espacio mucho más amplio, como posible herramienta de control de los trabajadores, que la grabación de sonido del art.89.3 LOPD, necesariamente ligada a la seguridad de personas, bienes e instalaciones en la empresa.

A partir de esta conexión, el art.89.3 LOPD apela a una intervención mínima y proporcional, que respete al máximo la intimidad personal, expuesta en conversaciones, de o entre, los empleados. Parece lógico aplicar las expuestas garantías legales de la videovigilancia laboral – medida justificada y proporcionada, información individual al trabajador, consulta a los representantes de los trabajadores – con una mayor exigencia en las técnicas de limitación porque el art.89.3 LOPD exige una intervención mínima. Se debe optar por la fórmula menos intrusiva de la privacidad de los empleados.

Es interesante subrayar, finalmente, que las grabaciones de sonidos sí están sujetas al plazo de destrucción de un mes desde la grabación del art.22.3 LOPD, como otra manifestación de mayor garantismo respecto a la mera videovigilancia sin audio.

Esta regulación garantista pone en cierta tensión la jurisprudencia que admite sistemas de grabaciones telefónicas con finalidad de control laboral. Hay que recordar, en este sentido, que la STS 5 de Diciembre de 2003 (Rec. 52/2003) admitió la grabación de conversaciones telefónicas de trabajadores, siempre que el personal esté correctamente preavisado, generando una expectativa de intimidad; las conversaciones pueden ser escuchadas y grabadas exclusivamente a efectos de vigilar y controlar la prestación laboral, existiendo teléfonos, no intervenidos, para el uso privado. La medida se entendió *"adecuada y proporcionada al objetivo laboral pretendido"* sin que se plantearan especiales problemas con el secreto de comunicaciones del art.18.4 CE[20]. Desde entonces, en el sector de telemarketing o call center es habitual utilizar estos sistemas de grabación telefónica con finalidad de control laboral.

Si aplicamos ahora, estrictamente, el art.89.3 LOPD, estos sistemas deberían estar conectados a una finalidad exclusiva de seguridad de personas, bienes e instalaciones, con una intervención mínima. Sin embargo, al ser la herramienta de trabajo el teléfono, y no existir ninguna medida alternativa de control laboral menos intrusiva en la privacidad, cabría admitir su procedencia. Además, este tipo de cláusulas van acompañadas del consentimiento del trabajador, en su contrato o en documento adjunto, escapando de las restricciones del art.89.3 LOPD. Podría plantearse, incluso, que

[20] DESDENTADO BONETE, A.; MUÑOZ RUIZ, A. B., *Control informático, videovigilancia y protección de datos en el trabajo*, *cit.*, pp. 28-29.

el mero preaviso informativo es suficiente, porque el tratamiento de dato personal responde a la finalidad de ejecución de contrato de trabajo del art.6.1.b REPD, pero las empresas del sector refuerzan la viabilidad de la medida con consentimientos individuales acreditados, en el marco del art.6.1.a REPD.

Recientemente, la STS 10 Abril 2019 (Rec.227/2017) ha avalado una cláusula contractual firmada, incluso, de cesión de imagen, mediante videollamada, en el sector del telemarketing. No parece que sea previsible una línea jurisprudencial estricta con estos sistemas consentidos de grabaciones telefónicas, en estos sectores, donde la principal herramienta de trabajo es el teléfono y la función laboral la atención o propaganda telefónica a ciudadanos. El art.6.1.a REPD parece avalar estos tratamientos específicos de datos personales en el marco de grabaciones de sonidos con finalidad exclusivamente laboral. Pero el nuevo art.89.3 LOPD abre ciertas grietas jurídicas en este tipo de sistemas, sobre todo si no existe consentimiento expreso del trabajador, que la futura doctrina judicial y jurisprudencia tendrá que ir valorando.

BIBLIOGRAFÍA

ALTES TARREGA, J.A., "La videovigilancia de la actividad laboral", ejemplar original, próxima publicación.

ARBONES LAPENA, H., "Grabación de imagen o sonido y control electrónico por el empresario", *Nueva Revista Española de Derecho del Trabajo*, nº 178, 2015.

BAZ RODRÍGUEZ, J., "La Ley orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales", *Trabajo y Derecho* 2019, nº 54.

CASAS BAAMONDE, M.E., "Informar antes que vigilar. ¿Tiene el Estado la obligación positiva de garantizar un mínimo de vida privada a los trabajadores en la empresa en la era digital?", *Derecho Relaciones Laborales* 2018, nº 2.

DESDENTADO BONETE, A.; MUÑOZ RUIZ, A.B., *Control informático, videovigilancia y protección de datos en el trabajo*, Lex Nova, Valladolid, 2012.

GOÑI SEIN, J.L., "Videovigilancia empresarial mediante cámaras ocultas: su excepcional validez como control defensivo *ex post*", *Trabajo y Derecho* 2018, nº 47.

LAHERA FORTEZA, J., "Nueva jurisprudencia constitucional en la videovigilancia laboral: valoración crítica", *Derecho de Relaciones Laborales* 2016, nº 5.

– "Seguridad jurídica en la videovigilancia laboral", *Cinco Días-El País,* 29 Octubre 2019.

MERCADER UGUINA, J., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Lefebvre, Madrid, 2019.

Preciado Domenech, C.H., "La videovigilancia en el lugar de trabajo y el derecho fundamental a la protección de datos personales", *Revista Derecho Social* 2017, nº 77.

ROJO TORRECILLA, E., "Derecho del trabajador a la privacidad en la empresa y límites a su control por las cámaras de videovigilancia", *Derecho Relaciones Laborales* 2018, nº 2.

– "Medias verdades y fake news en el mundo jurídico. No cabe toda la videovigilancia de una persona trabajadora. A propósito de la sentencia TEDH 17 Octubre 2019, López Ribalda", *blog Eduardo Rojo*, entrada 23 Octubre 2019.

SALA Franco, T.; TARABINI-CASTELLANI AZNAR, M., "El derecho a la intimidad personal y el control del trabajador" en dir. SALA, T., *Propuestas para un debate sobre la reforma laboral*, Lefebvre, Madrid, 2018.

TASCÓN LÓPEZ, R., "Tecnovigilancia y derecho de los trabajadores", *Revista Centro Estudios Financieros*, 2017, nº 415.

RESUMEN Tras décadas de incertidumbre en el tratamiento de la videovigilancia laboral en las empresas, por fin aparece la luz de la seguridad jurídica, tras la Ley Orgánica de Protección de Datos Personales 3/2018 (LOPD) y la jurisprudencia reciente del Tribunal Europeo de Derechos Humanos, asunto López Ribalda II 17 Octubre 2019. La regulación específica de las cámaras con finalidad de control del trabajador en el art.89 LOPD, y la jurisprudencia, en sus distintos niveles legal, constitucional e internacional, abre un escenario donde hay que distinguir tres tipos distintos de videovigilancia, con reglas y garantías diferenciadas. El conflicto entre, de un lado, la libertad de empresa que fundamenta el posible poder contractual de control laboral con estas herramientas, y, de otro, los derechos de intimidad y protección de datos personales del trabajador, está presente en estos tres tipos, pero la solución jurídica es diferenciada.

El primer tipo es la cámara estructural laboral, que tiene como finalidad el control estable y continuo de determinados trabajadores. El art.89 LOPD regula estas cámaras, recogiendo la jurisprudencia más garantista con los derechos personales del trabajador, sin descartar la admisión de este medio de control. La instalación de esta herramienta debe estar plenamente justificada, ser razonable, y proporcionada al fin perseguido, sin vulnerar en ningún caso la intimidad del trabajador. Se descarta su uso en zonas de descanso y aseo en los espacios de la empresa y tan sólo se admite, en determinados puestos de trabajo, cuando exista un motivo objetivo claro para este control, bajo el prisma siempre de la proporcionalidad. En la práctica queda prácticamente reducido a un control asociado con la seguridad en la empresa, si el trabajador maneja dinero o sus funciones justifican esta excepcional vigilancia. Con estas condiciones, el trabajador debe ser informado, con carácter previo y de manera expresa y clara, de la presencia de la cámara para proteger sus datos personales y generar una expectativa de intimidad. También debe ser informada y consultada la representación legal de los trabajadores. Las imágenes grabadas se someten a importantes exigencias de protección de datos personales.

El segundo tipo, también previsto en el art.89 LOPD, es el hallazgo casual de imagen, que capta la comisión flagrante de acto ilícito del trabajador, a través de una cámara de seguridad en la empresa. Las empresas pueden instalar, con las condiciones del art. 22 LOPD, y cumpliendo las instrucciones de la Agencia de Protección de Datos Personales (APD), cámaras de seguridad, que pueden grabar, no sólo a trabajadores, sino a clientes y ciudadanos. Son cámaras conocidas por todos al entrar en establecimientos comerciales y públicos. Si una cámara de seguridad capta un acto ilícito del trabajador, el art.89 LOPD avala la grabación, como prueba laboral, siempre que la empresa tenga expuesto de manera visible el distintivo informativo genérico exigido por la APD. El hallazgo casual de conducta ilícita del trabajador, a través de cámara de seguridad, puede servir, así, de prueba, no sólo penal, sino también laboral. La protección de datos personales queda así asegurada y cede, en parte, la intimidad personal, en favor de la acreditación de un acto ilícito del trabajador, tanto en la vía penal como en la estrictamente laboral.

El tercer tipo y más controvertido es la instalación, excepcional, coyuntural y puntual, de una cámara oculta y secreta ante indicios de irregularidades del trabajador en la empresa. Este tipo de cámara no está regulada expresamente en el art.89 LOPD y resultaría absurdo proyectar sobre la misma la exigencia legal de información previa y clara al trabajador, que desvirtúa la reacción empresarial frente a acreditados indicios de irregularidad del trabajador. Lo secreto nunca es preavisado. Tampoco es un hallazgo casual porque la instalación de la cámara es *ad hoc*. La solución a la admisión de este tipo de control fue apuntada en su día por el Tribunal Constitucional y ahora por el Tribunal Europeo de Derechos Humanos. La prueba de la imagen grabada será válida

si existen acreditados indicios de irregularidad del trabajador, la instalación es puntual, proporcionada y delimitada a quien comete los actos ilícitos, temporal y con la duración menor posible, en zona laboral, y nunca de privacidad dentro de la empresa, siendo sometida luego la imagen a las mayores exigencias de protección de datos personales, que evitan cualquier difusión o conocimiento de terceros fuera de un juicio penal o laboral. Con estas condiciones, sería una cámara laboral aceptada. Además, su posible conexión con el art.22 LOPD permite interpretar que, si existe dispositivo genérico de información, este control con la finalidad mixta de seguridad y laboral está avalado, siempre que se den estos exigentes requisitos. La prudencia debe delimitar, en este marco jurídico, el uso de estas cámaras secretas a la captación exclusiva de actos delictivos del trabajador, por ejemplo robos de dinero o bienes, de doble dimensión penal y laboral.

Merece especial atención, finalmente, la grabación de sonidos en el lugar de trabajo que, conforme al art. 89.3 ET está sujeta a un principio de intervención mínima muy garantista. Las razones de estas especiales restricciones están asociadas a posibles vulneraciones del secreto de comunicaciones.

En conclusión, esta distinción entre cámaras laborales estructurales, de seguridad con hallazgos causales y ocultas puntuales, con reglas y límites diferenciados, y, de por su parte, grabaciones de sonidos, otorga ya un gran margen de seguridad jurídica a la videovigilancia en las empresas. Este estudio, desde estos planteamientos, analiza, con detalle, estas cuatro vertientes de la videovigilancia en los lugares de trabajo.

Palabras clave: Cámara laboral; intimidad personal; protección datos; secreto comunicaciones.

ABSTRACT I After decades of uncertainty in the treatment of labor video surveillance in companies, the light of legal security finally appears, after the Organic Law on Protection of Personal Data 3/2018 (LOPD) and the recent jurisprudence of the European Court of Human Rights , López Ribalda II matter 17 October 2019. The specific regulation of the chambers with the purpose of controlling the worker in article 89 LOPD, and the jurisprudence, at its different legal, constitutional and international levels, opens a scenario where it is necessary to distinguish three different types of video surveillance, with different rules and guarantees. The conflict between, on the one hand, the freedom of company that bases the possible contractual power of labor control with these tools, and, on the other, the rights of privacy and protection of personal data of the worker, is present in these three types, but the legal solution is differentiated.

The first type is the structural labor chamber, whose purpose is the stable and continuous control of certain workers. Article 89 LOPD regulates these chambers, collecting the most guaranteeing jurisprudence with the personal rights of the worker, without ruling out the admission of this means of control. The installation of this tool must be fully justified, reasonable, and proportionate to the end pursued, without in any way infringing the privacy of the worker. Its use in rest and toilet areas in company spaces is discarded and it is only allowed, in certain jobs, when there is a clear objective reason for this control, always under the prism of proportionality. In practice, it is practically reduced to a control associated with security in the company, if the worker handles money or their functions justify this exceptional vigilance. With these conditions, the worker must be informed, in advance and expressly and clearly, of the presence of the camera to protect their personal data and generate an expectation of privacy. The legal representation of the workers must also be informed and consulted. Recorded images are subject to significant personal data protection requirements.

The second type, also provided for in article 89 of the LOPD, is the accidental discovery of an image, which captures the flagrant commission of an illicit act by the worker, through a security camera in the company. Companies can install, with the conditions of art. 22 LOPD, and complying with the instructions of the Personal Data Protection Agency (APD), security cameras, which can record, not only workers, but customers and citizens. They are cameras known to all when entering commercial and public establishments. If a security camera captures an illicit act by the worker, article 89 of the LOPD endorses the recording, as proof of work, provided that the company has the generic informational badge required by the APD visibly displayed. The accidental finding of illicit behavior by the worker, through a security camera, can thus serve as evidence, not only criminal, but also labor. The protection of personal data is thus ensured and cedes, in part, personal privacy, in favor of the accreditation of an illicit act of the worker, both in criminal and strictly labor proceedings.

The third and most controversial type is the installation, exceptional, temporary and punctual, of a hidden and secret camera in the face of indications of irregularities by the worker in the company. This type of chamber is not expressly regulated in article 89 of the LOPD and it would be absurd to project on it the legal requirement of prior and clear information to the worker, which undermines the business reaction to proven signs of worker irregularity. The secret is never forewarned. It is also not a chance find because the installation of the camera is ad hoc. The solution to the admission of this type of control was pointed out in its day by the Constitutional Court and now by the European Court of Human Rights. The proof of the recorded image will be valid if there are accredited indications of irregularity of the worker, the installation is punctual, proportionate and limited to whoever commits the illegal acts, temporary and with the shortest possible duration, in a work area, and never privacy within the company, the image being then subjected to the highest personal data protection requirements, which prevent any dissemination or knowledge of third parties outside of a criminal or labor

trial. With these conditions, it would be an accepted labor chamber. Furthermore, its possible connection with article 22 of the LOPD makes it possible to interpret that, if there is a generic information device, this control with the mixed purpose of safety and labor is endorsed, provided that these demanding requirements are met. Prudence must limit, in this legal framework, the use of these secret cameras to the exclusive capture of criminal acts of the worker, for example theft of money or property, with a double criminal and labor dimension.

Finally, the recording of sounds in the workplace deserves special attention which, according to art. 89.3 ET is subject to a very guaranteeing minimum intervention principle. The reasons for these special restrictions are associated with possible breaches of communications secrecy.

In conclusion, this distinction between structural labor cameras, security cameras with specific causal and hidden findings, with differentiated rules and limits, and, for its part, sound recordings, already provides a great margin of legal security to video surveillance in companies. . This study, from these approaches, analyzes, in detail, these four aspects of video surveillance in the workplace.

Keywords: Chamber of work; personal privacy; data protection; secret communications.

Utilización de sistemas de geolocalización en el ámbito laboral*

Worker surveillance through geolocation devices

IVÁN ANTONIO RODRÍGUEZ CARDO**

1. INTRODUCCIÓN

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

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

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

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

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

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

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

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

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

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

2. GEOLOCALIZACIÓN Y RELACIÓN LABORAL

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3. LA PREOCUPACIÓN POR LA GEOLOCALIZACIÓN EN EL CONTEXTO INTERNACIONAL

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

El legislador, así pues, muestra ciertas dudas sobre cuál es el derecho principalmente concernido, aunque en último término parece decantarse por la protección de datos, como se desprende del apartado 1 de ese art. 90 LOPD, que faculta a los empleadores para «tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados

públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo». Ese art. 20.3 ET, por cierto, permite al empresario «adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad», sin aludir ni al derecho a la intimidad ni a la protección de datos personales.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

El análisis no estaría completo sin una referencia al apartado 2 del art. 90 LOPD, a cuyo tenor la implementación de este tipo de dispositivos como medidas de control del trabajador requiere que «con carácter previo», el empleador informe «de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos». Asimismo, también deberá «informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión».

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[79] Recurso 6188/1996.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

RESUMEN

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Derecho a la desconexión digital en el ámbito laboral

Right to digital disconnection in the workplace

CAROLINA SAN MARTÍN MAZZUCCONI*

1. CONTEXTO

Las tecnologías disruptivas y la digitalización de nuestras relaciones avanzan con prisa y sin pausa. Dado que la globalización económica deriva en un proceso de acusada acentuación de la competitividad empresarial, es lógico que las organizaciones productivas se afanen por incorporar a sus estructuras todo aquello que facilita y mejora su producción, lo que desde luego pasa en buena medida por la implementación permanente de adelantos tecnológicos que están en continuo desarrollo.

El mercado de trabajo permeable a los avances tecnológicos plantea importantes desafíos jurídicos que han de ser afrontados por toda la comunidad laboral: empresas, trabajadores, agentes sociales, legislador, órganos judiciales, etc. En esta línea, no hay duda de que un ámbito en el que los conflictos jurídicos se hacen especialmente presentes es el de la confrontación entre las posibilidades que ofrece la progresión tecnológica, por un lado, y los derechos fundamentales de los trabajadores, por otro.

Hasta hace poco, las principales pautas disponibles para resolver estos conflictos derivados del uso de las tecnologías disruptivas en las empresas han venido de la mano de los Tribunales, nacionales y supranacionales. Entre los primeros pronunciamientos referenciales en la materia, cabe citar la conocida Sentencia del Tribunal Constitucional sobre el caso del Casino de La Toja[1], que hubo de analizar si resultaba lícito que el empleador colocara dispositivos de captación de sonido, junto a las videocámaras que ya existían, para vigilar el trabajo de sus empleados. También se ha planteado si era lícito colocar cámaras que enfocaran a las cajas en un economato[2]; más adelante surgió el tema de los controles de correo electrónico[3], de la navegación por internet[4] y de los chats[5]; de la videovigilancia[6]; de los dis-

* Catedrática de Derecho del Trabajo y de la Seguridad Social. Universidad Rey Juan Carlos.

[1] STC 98/2000, de 10 de abril.

[2] STC 186/2000, de 10 de julio.

[3] SSTS de 26 de septiembre de 2007 (Rec. 966/2006), de 8 de marzo de 2011 (Rec. 1826/2010), de 6 de octubre de 2011 (Rec. 4053/2010); SSTC 241/2012, 170/2013; SSTEDH de 12 de enero de 2016 (caso "Barbulescu I") y de 4 de septiembre de 2017 (Caso "Barbulescu II"). Véase SEMPERE NAVARRO, A.V., SAN MARTÍN MAZZUCCONI, C.: "¿Puede la empresa controlar el ordenador usado por su trabajador? Comentario a la STS 26 de septiembre de 2007, Recurso 966/2006 (JUR 2007, 306130)", *Repertorio de Jurisprudencia* núm. 21, 2007; SAN MARTÍN MAZZUCCONI, C.: "El control empresarial de los ordenadores: estado de la cuestión en España", *Para Jorge Leite. Escritos jurídico-laborais* (vol. I), (J. Reis, L. Amado, L. Fernandes, R. Redinha, Coords.), Coimbra Editora, 2014.

[4] Por todas, STS 119/2018, de 8 de febrero de 2018.

[5] SAN MARTÍN MAZZUCCONI, C.: "¿Cómo se mide el "uso moderado" de Internet para fines personales?: ¿transgrede la buena fe contractual tener abierto un programa para "chatear"? Comentario a la STSJ Cataluña de 11 de marzo 2004 (AS 2004, 1231)", *Aranzadi Social* núm. 2, 2004.

[6] STC 29/2013, de 7 de octubre; SSTS de 13 de mayo de 2014 (Rec. 1685/2013), de 7 de julio de 2016 (Rec. 3233/2014), de 31 de enero de 2017 (Rec. 3331/2016); SSTEDH de 9 de enero de 2018 (caso "López Ribalda I") y de 17 de octubre de

positivos de geolocalización de empleados[7]; del uso de redes sociales[8]; de sistemas de fichaje electrónico[9], de recibos de salario en formato digital[10]; del compromiso contractual del trabajador de suministrar su número de móvil o dirección de correo electrónico para comunicaciones laborales[11], etc.

La evolución de los problemas ha sido también la evolución de los derechos fundamentales en juego. Comenzamos preguntándonos si un trabajador tenía derecho al uso personal de los medios tecnológicos de la empresa, para pasar a reflexionar sobre si el control de ese uso respetaba o no el derecho a la intimidad. Más adelante entró en escena el derecho al secreto de las comunicaciones, que aportaba mayores dosis de seguridad jurídica, y por último adquirió protagonismo el derecho a la protección de datos personales.

En definitiva, pues, la intimidad del trabajador, el secreto de las comunicaciones, la protección de datos personales, incluso la libertad sindical, llevan años midiendo fuerzas con el uso y control laboral de ordenadores, cámaras de videovigilancia, dispositivos de geolocalización, teléfonos móviles, fichajes informáticos, emisores de radiofrecuencia, etc. Y veremos, más pronto que tarde, posibilidades que aún no somos capaces siquiera de imaginar y a las que habrá que dar respuesta también desde el Derecho del Trabajo. Así, apenas atisbamos lo que se avecina cuando leemos acerca del *smart-working*[12], o de empresas que ofrecen a sus empleados implantarles un microchip subcutáneo de identificación por radiofrecuencia, que les permite abrir puertas o acceder al ordenador[13].

Más allá de la problemática respecto de los derechos fundamentales de los trabajadores, las innovaciones tecnológicas trazan un modelo de trabajo en el que los límites son cada vez más difusos, con posibilidades de conectividad permanente e incontrolada. Ello pone en cuestión, una vez más, los esquemas clásicos de tiempo de trabajo versus tiempo de descanso[14], rigidez *versus* flexibilidad, en un escenario en el que las confrontaciones binarias tradicionales se ven superadas por la complejidad de la realidad productiva actual.

En este contexto, tras décadas de silencio el legislador decidió acometer una regulación de todas estas materias, y lo hizo aprovechando la promulgación de la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPD). Durante la tramitación parlamentaria de la norma, se incorporó su Título X, rubricado como "Garantía de los derechos digitales", en cuyos arts. 87 a 91 regula su alcance en el ámbito laboral[15].

2019 (caso "López Ribalda II"). Puede verse un análisis de la STC 29/2003 en San Martín Mazzucconi, C., Sempere Navarro, A.V.: *Las TICs en el ámbito laboral*, Francis Lefebvre, 2015. Sobre el tema, más ampliamente, véase San Martín Mazzucconi, C.: "El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos", en *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico* (San Martín Mazzucconi, C., Dir.), EOLAS, 2014.

[7] ATS de 19 de julio de 2018 (Rec. 3945/2017); SAN 13/2019, de 6 de febrero de 2019.

[8] Por ejemplo STSJ Cataluña 609/2017, de 30 de enero de 2017; STSJ Canarias 257/2019, de 19 de marzo de 2019.

[9] SSTSJ Murcia de 3 de febrero de 2003 (3) (Recs. 55/2003, 56/2003 y 57/2003); Cataluña de 10 de diciembre de 2003 (Rec. 4919/2002); SSTS de 3 de octubre de 2006 (Rec. 146/2005) y de 25 de abril de 2006 (Rec. 147/2005); Cantabria de 10 de enero de 2003 (2) (RJCA 2003/5 y Rec. 517/2002), de 14 de marzo de 2003 (Rec. 893/2002) y de 28 de marzo de 2003 (Rec. 759/2002).

[10] STS de 1 de diciembre de 2016 (Rec. 3690/2014).

[11] STS de 21 de septiembre de 2015 (Rec. 259/2014).

[12] Se habla del "smart-working" como una evolución del teletrabajo basada en la movilidad y flexibilidad horaria, el trabajo por objetivos y el uso masivo de las nuevas tecnologías ("'Smart worker', el profesional que revoluciona el trabajo", *Expansión*, 24 de febrero de 2017).

[13] EFE 18 de febrero de 2017, ABC 12 de julio de 2019.

[14] "El paulatino avance de la tecnología digital ha terminado decididamente por difuminar y desdibujar los contornos existentes con anterioridad entre los tiempos dedicados al trabajo y al descanso" [Taléns Visconti, E.E.: "La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva", *Revista de Información Laboral* núm. 4, 2018 (BIB 2018/8599), p. 1].

[15] Pérez Campos, A.I., presume que la inclusión del derecho a la desconexión digital en la LOPD se ha podido deber, quizá, a

En lo que aquí interesa, la LOPD reconoce y regula el "derecho a la desconexión digital en el ámbito laboral" en su art. 88, que tiene carácter de ley ordinaria y cuya relación con la protección de datos es meramente remota e indirecta[16].

Esta categorización como norma de rango ordinario ha sido criticada por algunos autores, que consideran que constituye desarrollo del derecho fundamental a la intimidad, o incluso a la integridad física y psíquica[17]. También se ha rebatido implícitamente en una reciente sentencia del Juzgado de lo Social núm. 23 de Madrid, de 31 de octubre de 2019 (Autos núm. 880/2019), que anula la sanción impuesta a un trabajador –controlador aéreo– por "desobediencia abierta a las órdenes o instrucciones de un superior", al haberse negado a realizar cursos on line de formación obligatoria para el mantenimiento de la habilitación en períodos programados como descanso. El Magistrado razona que "el derecho a la desconexión informática forma parte del derecho fundamental reconocido en el art. 18.4 de nuestra C.E. aun cuando se haya desarrollado y concretado por una reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6/12/2018), Ley de fecha posterior a la conducta de resistencia del trabajador a obedecer una orden de la empresa, que claramente se muestra desconocedora de ese derecho fundamental, en tanto y cuando obligaba al actor y a otros compañeros, a realizar unos cursos vía online, usando herramientas informáticas, durante su tiempo de descanso."

En mi opinión, siendo sumamente sugerentes estas reflexiones, la relación del art. 88 LOPD con los derechos fundamentales mencionados podría considerarse indirecta, porque la protección de datos no tiene por qué estar presente necesariamente en su ejercicio, y porque, como se razonará más adelante, la intimidad ha de protegerse tanto en momentos de desconexión como de conexión[18]. Por tanto, comparto la configuración de la norma como ordinaria.

Señalado lo anterior, veamos por fin el texto del precepto concernido:

> *"Artículo 88. Derecho a la desconexión digital en el ámbito laboral.*
> *1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso,*

"motivos o razones de conveniencia legislativa, por el consenso que siempre ha tenido esta norma en tiempo de minorías parlamentarias" ("La desconexión digital en España: ¿un nuevo derecho laboral?", *Anuario Jurídico y Económico Escurialense*, LII, 2019, p. 21).

[16] Mercader Uguina, J., realiza una sugerente interpretación integradora de la LOPD para concluir que, aunque la desconexión digital no versa sobre una cuestión relativa a la protección de datos personales, la Agencia Española de Protección de Datos podría llegar a intervenir, de manera refleja, en el control de la definición y diseño de los criterios y protocolos en esta materia, "por lo que bien pudiera convertirse, desde esta particular perspectiva, en referente a la hora de concretar el alcance y los límites de este nuevo derecho" ("Aspectos laborales de la Ley Orgánica 3/2018 de 5 de diciembre: una aproximación desde la protección de datos", *La Ley* 4433/2019, p. 10).

[17] Serrano Olivares, R., critica que el legislador lo haya configurado como ley ordinaria porque, a su juicio, se trata de "una expresión concreta de los derechos a la intimidad y a la integridad física y psíquica en el trabajo (en su dimensión de seguridad y salud en el trabajo)" ("Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *IUSLabor* núm. 3, 2018, p. 226). En el mismo sentido, Preciado Domenech, C.H., mantiene que el derecho a la desconexión constituye "una garantía del derecho a la intimidad, es decir una regulación del ejercicio de la intimidad que por vía de ley ordinaria disciplina la forma y el tiempo de ejercitar el derecho fundamental en el seno de la relación laboral fuera del tiempo de trabajo. Ello nos decanta a concluir que su vulneración supone una vulneración de la intimidad, por lo que el despido como represalia por no 'conectarse' y responder a requerimientos de la empresa fuera del horario laboral habría de considerarse un despido con vulneración de derechos fundamentales" (*Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales*, Aranzadi, 2019).

[18] Según Baz Rodríguez, J., la relación con el art. 18.4 CE es menor, si bien sí aprecia el vínculo con la protección de la intimidad personal y familiar ("Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *La Ley* 6823/2019, p. 3).

permisos y vacaciones, así como de su intimidad personal y familiar.
2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.
3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas."

Sin perjuicio del análisis detenido que se acomete en los epígrafes sucesivos, la lectura de la norma permite apreciar que el derecho a la desconexión digital se reconoce a trabajadores y empleados públicos de todo tipo de empresas para garantizar el respeto a su tiempo de no trabajo así como su intimidad. Las modalidades del ejercicio del derecho deben sujetarse a lo establecido en acuerdos colectivos, y el empleador ha de elaborar una política interna definiéndolas.

Las Disposiciones Finales Decimotercera y Decimocuarta de la norma orgánica ordenan, respectivamente, la inclusión del derecho en el Estatuto de los Trabajadores (ET) y en el Estatuto Básico del Empleado Público (EBEP). Sin embargo, probablemente de modo inconsciente, no lo hacen con la misma intensidad, pues, mientras se adiciona una nueva letra j bis en el art. 14 del EBEP[19] para reconocerlo como un derecho individual de los empleados públicos, en el Estatuto de los Trabajadores se añade un nuevo art. 20 bis[20], configurándose como un límite al poder de dirección sin reflejo en el catálogo de derechos básicos.

2. ANTECEDENTES

Es la primera vez que se reconoce el derecho laboral a la desconexión digital en España[21], aunque contábamos con algunas circunstancias previas que, seguramente, alentaron al legislador a abordar la figura:

a) La inclusión del derecho en el Código de Trabajo francés[22].

El contenido del art. 88 LOPD es una importación adaptada de lo dispuesto en el apar-

[19] "Artículo 14. Derechos individuales.
Los empleados públicos tienen los siguientes derechos de carácter individual en correspondencia con la naturaleza jurídica de su relación de servicio: (...)
j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales."

[20] "Artículo 20 bis. Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.
Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales."

[21] Y además como derecho autónomo [BEL ANTAKI, J.: "Nuevos derechos digitales de los trabajadores: claves en cinco preguntas y respuestas", *Actualidad Jurídica Aranzadi* núm. 948, 2019, p. 2 (BIB 2019/604)].

[22] TALÉNS VISCONTI, E.E., señala la regulación francesa como punto a partir del cual se abre en España el debate sobre la conveniencia o no de legislar sobre la desconexión digital, sin que hasta el momento existiera una conflictividad reseñable ["La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva", *Revista de Información Laboral* núm. 4, 2018, p. 2 (BIB 2018/8599)].

tado 7º del art. 2242-17 del actual Código de Trabajo francés, introducido por la Ley 2016-1088, de 8 de agosto de 2016, relativa al trabajo, a la modernización del diálogo social y al aseguramiento de trayectorias profesionales.

Su contenido[23] podría traducirse así:

La negociación anual sobre igualdad profesional entre las mujeres y los hombres y la calidad de vida en el trabajo incluirá las modalidades del pleno ejercicio por el trabajador de su derecho a la desconexión y la puesta en marcha por las empresas de dispositivos reguladores del uso de herramientas digitales, a fin de asegurar el respeto del tiempo de descanso y permisos, así como la vida personal y familiar. A falta de acuerdo, el empleador elaborará una política, previa audiencia del comité de empresa o, en su defecto, de los delegados de personal. Esta política definirá las modalidades de ejercicio del derecho a la desconexión y preverá, además, la implementación de acciones de formación y de sensibilización sobre un uso razonable de los dispositivos digitales, dirigida a los trabajadores, mandos intermedios y dirección.

Los puntos de encuentro entre la norma francesa y la española son evidentes[24], pudiendo destacarse lo siguiente:

- Lo primero que llama la atención es que la norma francesa no define el derecho a la desconexión, lo que probablemente sea la causa de que la disposición española tampoco lo haga.

- Nótese que la desconexión se contempla en el marco de la negociación de planes de igualdad –para empresas de 50 o más trabajadores–, con el objetivo de respetar el descanso y la conciliación de vida familiar y personal. En nuestro caso la desconexión posee un reconocimiento independiente y desvinculado formalmente de la negociación de planes de igualdad y de las dimensiones de la empresa, pero también está presidido por la finalidad de fomentar la conciliación de vida laboral, personal y familiar de los trabajadores.

- La disposición francesa establece que las modalidades de ejercicio del derecho deben negociarse colectivamente, y en su defecto el empleador elabora una política de actuación, previa audiencia a los representantes de los trabajadores. No es descartable que el legislador español pretendiera lo mismo, pero lo cierto es que la literalidad del art. 88 LOPD conduce a otra solución, sobre la que volveremos más adelante: el empresario tiene encomendada la elaboración de una política, previa audiencia de los representantes de los trabajadores, que, obviamente, deberá respetar lo que se acuerde colectivamente, en su caso.

- Tanto en el Código francés como en la LOPD se establece que la citada política empresarial debe fijar las modalidades de ejercicio del derecho, así como acciones de formación y sensibilización, para trabajadores y directivos. La norma francesa añade expresamente a los mandos intermedios. Por su parte, la disposición española introduce dos innovaciones: dedica una mención es-

[23] *"La négociation annuelle sur l'égalité professionnelle entre les femmes et les hommes et la qualité de vie au travail porte sur: (...) 7º Les modalités du plein exercice par le salarié de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale. A défaut d'accord, l'employeur élabore une charte, après avis du comité d'entreprise ou, à défaut, des délégués du personnel. Cette charte définit ces modalités de l'exercice du droit à la déconnexion et prévoit en outre la mise en œuvre, à destination des salariés et du personnel d'encadrement et de direction, d'actions de formation et de sensibilisation à un usage raisonnable des outils numériques".*

[24] Un análisis del derecho a la desconexión a partir de las pautas francesas puede verse en ALEMÁN PÁEZ, F.: "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la «Loi Travail No 2016-1088", *Revista Trabajo y Derecho* núm. 30, 2017.

pecífica a los trabajadores que prestan servicios a distancia o en sus domicilios y alude a la necesidad de evitar el riesgo de fatiga informática.

- Ambas legislaciones omiten referir ninguna clase de sanción por el incumplimiento de sus previsiones.

En la misma línea, el 26 de marzo de 2018 el derecho a la desconexión digital irrumpió en la legislación belga, a través de la Ley de fortalecimiento del crecimiento económico y la cohesión social. Su art. 16[25] se traduciría como sigue:

> *Con el fin de garantizar el respeto por los tiempos de descanso de los trabajadores, las vacaciones anuales y otros permisos y preservar el equilibrio entre el trabajo y la vida privada, el empleador negociará en el Comité para la Prevención y Protección en el trabajo, periódicamente y cada vez que los representantes de los trabajadores lo soliciten, sobre desconexión del trabajo y uso de medios digitales de comunicación. El Comité podrá formular propuestas y emitir informes.*

La previsión belga es bastante más escueta que la francesa, pudiendo señalarse que, al igual que su homóloga, esquiva definir el derecho y remite su contenido a la negociación colectiva. No obstante, repárese en que esta última conecta directamente con la prevención de riesgos laborales, al llevarse a cabo en el seno del comité paritario con competencias en dicha materia.

Se señala igualmente un precedente italiano, aunque algo más difuso pues, aunque alude a la desconexión digital, no lo refiere como un derecho[26].

b) La regulación expresa del derecho en el Convenio Colectivo del Grupo AXA.

El Convenio Colectivo del Grupo Axa (2017-2020)[27] dedicó un Capítulo a la "Organización del trabajo y nuevas tecnologías", en el que aborda, entre otras figuras, la desconexión digital, sintetizada básicamente en el reconocimiento del derecho de los trabajadores a no responder a los mensajes profesionales fuera de su horario de trabajo, salvo causa de fuerza mayor o circunstancias excepcionales[28].

---

[25] *"En vue d'assurer le respect des temps de repos, des vacances annuelles et des autres congés des travailleurs et de préserver l'équilibre entre le travail et la vie privée, l'employeur organise une concertation au sein du Comité pour la Prévention et la Protection au Travail tel que visée à l'article I.1-3, 14° du code du bien-être au travail, à des intervalles réguliers et à chaque fois que les représentants des travailleurs au sein du Comité le demandent, au sujet de la déconnexion du travail, et de l'utilisation des moyens de communication digitaux. Le Comité peut formuler des propositions et émettre des avis à l'employeur sur la base de cette concertation."*

[26] Lo indica TALÉNS VISCONTI, E.E.: "La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva", *Revista de Información Laboral* núm. 4, 2018, p. 6 (BIB 2018/8599). La Legge 22 maggio 2017, núm. 81, Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato, establece en su art. 19.1: *"L'accordo individua altresi'i tempi di riposo del lavoratore nonche' le misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro."*

[27] BOE de 10 de octubre de 2017.

[28] "Artículo 14. Derecho a la desconexión digital.

Los cambios tecnológicos producidos en las últimas décadas han provocado modificaciones estructurales en el ámbito de las relaciones laborales. Es innegable que hoy en día el fenómeno de la «interconectividad digital» está incidiendo en las formas de ejecución del trabajo mudando los escenarios de desenvolvimiento de las ocupaciones laborales hacia entornos externos a las clásicas unidades productivas: empresas, centros y puestos de trabajo.

En este contexto, el lugar de la prestación laboral y el tiempo de trabajo, como típicos elementos configuradores del marco en el que se desempeña la actividad laboral, están diluyéndose en favor de una realidad más compleja en la que impera la conectividad permanente afectando, sin duda, al ámbito personal y familiar de los trabajadores y trabajadoras.

Es por ello que las partes firmantes de este Convenio coinciden en la necesidad de impulsar el derecho a la desconexión digital una vez finalizada la jornada laboral. Consecuentemente, salvo causa de fuerza mayor o circunstancias excepcionales, AXA reconoce el derecho de los trabajadores a no responder a los mails o mensajes profesionales fuera de su horario de trabajo."

Publicaciones especializadas en divulgación y actualidad jurídica[29], así como varias generalistas, dieron cuenta de la novedad de esta inclusión convencional, que por primera vez reconocía expresamente el derecho.

Posteriormente tuvieron lugar otros acuerdos colectivos del mismo signo, como fue el caso de Ikea[30], pero sin duda el del Grupo Axa fue el de mayor repercusión pública.

c) La existencia de políticas de desconexión en algunas empresas.

Al margen de acuerdos colectivos, varias empresas contaban con prácticas de desconexión[31]: desviar correos durante vacaciones[32], interrumpir la comunicación entre servidores y teléfonos móviles de los empleados desde el fin de la jornada hasta el inicio de la siguiente[33], alertas para disuadir de conexiones fuera de horario[34], etc.

En este sentido, son habituales las referencias doctrinales a los acuerdos firmados en Alemania por Volkswagen (2011), seguida por otras empresas del sector, como Daimler-Benz y BMW.

d) Ciertos pronunciamientos judiciales señalados como antecedentes.

Los estudios sobre desconexión digital coinciden en apuntar, como primer antecedente del tratamiento judicial del derecho, a la SAN de 17 de julio de 1997 (proc. 120/1997), que aborda la cuestión desde la óptica de los límites del poder de dirección. El pronunciamiento conoce del caso de una empresa que comunicó a todos los empleados que tuvieran a su disposición el teléfono móvil de la compañía, y que su uso sería exclusivamente para temas profesionales. Además, ordenó a los comerciales que siempre tenían que tener conectado el teléfono. La Sala consideró que se sobrepasan los derechos regulares del poder de dirección "si se obliga a los empleados a desarrollar su actividad profesional o a estar pendientes de recibir comunicaciones en todo momento, incluso en horas no coincidentes con la jornada de trabajo asignada a cada uno de ellos".

También se cita recurrentemente la STS de 21 septiembre 2015 (Rec. 259/2014, caso Unisono), que abordó un supuesto en el que la empresa había incluido en los contratos una cláusula por la que acordaban que cualquier tipo de comunicación relativa al contrato, a la relación laboral o al puesto de trabajo, podría ser enviada al trabajador vía mensaje de texto o correo electrónico, según los datos facilitados por el trabajador a efectos de contacto. El Tribunal concluye que los datos pueden cederse voluntariamente a estos efectos, pero cuestiona que esa voluntad exista en el momento germinal del contrato. Nótese que, en realidad, el abordaje del problema no se realiza desde una óptica reconducible a la desconexión digital sino desde el estricto prisma de la protección de datos.

3. IDENTIFICACIÓN DEL DERECHO LABORAL A LA DESCONEXIÓN DIGITAL

El derecho a la desconexión digital de los trabajadores se reconoce por la Ley, pero no se

[29] Entre otras: "Axa, primera empresa en aprobar la desconexión digital en España" (*Noticias Jurídicas* 25-7-17 http://noticias.juridicas.com/actualidad/noticias/12193-axa-primera-empresa-en-aprobar-la-desconexion-digital-en-espana/); "El derecho del empleado a la desconexión no tardará en reconocerse en España" (Legal Today 15-11-17 http://www.legaltoday.com/actualidad/noticias/el-derecho-del-empleado-a-la-desconexion-no-tardara-en-reconocerse-en-espana), "El derecho a la desconexión digital y su aplicación práctica" (El Derecho 11-1-18 https://elderecho.com/el-derecho-a-la-desconexion-digital-y-su-aplicacion-practica)

[30] Acuerdo sobre distribución de jornada, de 27 de junio de 2018. "Artículo 13. Desconexión digital: Ambas partes coinciden en la necesidad de impulsar este derecho, por esta razón se establece que los trabajadores/as tienen derecho a no responder cualquier tipo de comunicación por cualquier canal (correo electrónico, teléfono, Whatsapp, redes sociales, etc.) fuera de su horario de trabajo, salvo causa de fuerza mayor. La comisión de seguimiento realizará una vigilancia de la implantación de esta medida."

[31] *Expansión,* 4 de noviembre de 2018. (https://www.expansion.com/juridico/actualidad-tendencias/2018/11/04/5bdc3c3f46163ff9638b45e4.html)

[32] Mercedes Benz, 2016.

[33] Volkswagen, 2011.

[34] Michelin, 2016.

define. A la hora de intentar perfilar sus contornos cabe acudir al Diccionario de la Real Academia Española, en el que sí figura la palabra "desconectar". Su cuarta acepción se relaciona con las tecnologías y define el término como "interrumpir el enlace entre aparatos, o entre aparatos y personas, para que cese el flujo existente entre ellos". Y la quinta acepción alude a "dejar de tener relación, comunicación, enlace, etc.". Respecto del adjetivo "digital", la tercera acepción del citado Diccionario lo recoge así: "dicho de un dispositivo o sistema: que crea, presenta, transporta o almacena información mediante la combinación de bits".

Por tanto, podríamos decir que el derecho a la desconexión digital supone garantizar la interrupción del enlace o relación entre el trabajador y los dispositivos o sistemas digitales, de modo que cese el flujo de información de contenido laboral[35].

Desde luego, parece evidente que el derecho así configurado ya existía en su formulación básica, antes de que fuera recogido por el art. 88 LOPD. En efecto, cuando el art. 34 ET limita la jornada de trabajo, confiere al trabajador el derecho a desconectarse más allá de la misma[36]. La novedad, entonces, no sería el límite al tiempo de trabajo, que ya existía, sino la intención de evitar su transgresión mediante el uso de herramientas tecnológicas. Tiene sentido si se observa la extraordinaria capacidad de comunicación permanente que permiten algunos dispositivos, lo que hace mucho más incisivo el riesgo de penetración en el ámbito del tiempo de descanso o de no trabajo.

En definitiva, el derecho a la desconexión digital viene a ser una subespecie del derecho a la limitación de la jornada, que ya teníamos recogido en la regulación del tiempo de trabajo. Por eso puede decirse que, en realidad, ya existía el derecho a desconectar, sólo que ahora se reconoce de modo específico y expreso, anudando una serie de medidas conexas que son las realmente novedosas: la obligación de contar con una política empresarial de desconexión y la programación de acciones de formación y sensibilización. Por tanto, la regulación específica del derecho a la desconexión digital ha supuesto la oportunidad para introducir nuevas obligaciones que no existen fuera del art. 88 LOPD.

4. CONTENIDO DEL DERECHO

Del mismo modo en que la Ley no define el derecho, tampoco identifica su contenido. Su alcance real se ha de integrar conforme a lo que se establezca en la política de empresa al fijar las modalidades de ejercicio y, en su caso, con lo que pueda preverse en la negociación colectiva.

Ahora bien, lo que sí define la LOPD es la finalidad perseguida con el derecho a la desconexión digital, cual es "garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar". Y, aunque es evidente que el contenido y la finalidad de un derecho son dos elementos muy distintos que no deberían confundirse, sin embargo, en ausencia de un contenido preestablecido, parece que los objetivos a perseguir con el ejercicio del derecho podrían ayudar a perfilarlo.

Lo anterior no obsta a que pueda apreciarse alguna inconsistencia: no hay dificultad en comprender que la desconexión se

[35] SERRANO ARGÜESO, M., propone una definición muy sencilla e intuitiva: "El derecho a la desconexión digital no es más que reconocer a los trabajadores el derecho a no conectarse a cualquier herramienta digital durante sus periodos de descanso o vacaciones y que las nuevas tecnologías no diluyan lo que fue una conquista social: la limitación de la jornada y el derecho al descanso." ("Always on. Propuestas para la efectividad del derecho a la desconexión digital en el marco de la economía 4.0", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo* núm. 2, 2019, p. 175).

[36] Por eso, entre otros motivos, VALLECILLO GÁMEZ, M.R. alude a un esnobismo del derecho al descanso ("El derecho a la desconexión ¿novedad digital o esnobismo del viejo derecho al descanso?", *Revista de Trabajo y Seguridad Social CEF* núm. 408, 2017, p. 177.

vincule a garantizar el derecho al descanso, pero lo que no parece tener sentido es relacionarla con la garantía de la intimidad personal y familiar del trabajador, porque el derecho a la intimidad puede ejercerse tanto en tiempo de descanso como en tiempo de trabajo. Sólo se entiende si se vincula a la protección de la intimidad durante el tiempo de descanso, en términos de hacer efectiva la conciliación de la vida familiar y laboral, que es probablemente a lo que pretendería apuntar el legislador.

Por otra parte, como se adelantó, el art. 88 LOPD regula una serie de obligaciones conexas para el empresario, que se concretan en la obligación de contar con una política en materia de desconexión digital y poner en marcha acciones de sensibilización sobre la materia.

5. LÍMITES DEL DERECHO: LA POLÍTICA INTERNA

La regulación de la desconexión gira en torno a un eje muy claro: la política o protocolo que regule su ejercicio. Esta centralidad se observa en dos circunstancias:

Por un lado, respecto del sujeto obligado a garantizar el derecho a la desconexión. En principio sería el empresario, como responsable de que se respete el derecho al descanso de los trabajadores y vigilante de su salud laboral. Sin embargo, el art. 88 LOPD quita fuerza a la obligación al diluirla en función de lo que se acuerde o protocolice. En otras palabras, el precepto no contiene la obligación directa del empleador de garantizar la desconexión, sino la indirecta de elaborar una política que defina las modalidades de su ejercicio.

Por otra parte, al no precisarse legalmente el derecho ni fijarse su contenido, para identificar los límites es necesario integrarlo con la política empresarial que desarrolle sus modalidades de ejercicio, estando esta última vinculada a una serie de finalidades y a los acuerdos colectivos que existan. Sólo en tal instrumento se dará contenido al derecho y, por tanto, se establecerá su alcance real.

Cabría decir, pues, que el derecho a la desconexión no es absoluto, dado que, aunque se reconoce absolutamente, se condiciona su ejercicio[37].

Esta conclusión lleva a hacerse dos preguntas: ¿qué características ha de guardar la citada política empresarial? Y, en relación con ello, ¿hasta qué punto la misma puede limitar el derecho a la desconexión digital? Una vez despejadas estas incógnitas, debe analizarse el procedimiento para su elaboración y su contenido obligatorio.

5.1. Márgenes

El apartado segundo del art. 88 LOPD establece que las modalidades de ejercicio del derecho a) atenderán a la naturaleza y objeto de la relación laboral; b) potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar; c) y se sujetarán a lo establecido en la negociación colectiva.

De aquí cabe colegir las siguientes pautas que han de presidir la elaboración de la política interna:

1º) Desde luego, la política interna ha de sujetarse a lo que, en su caso, se haya pactado colectivamente. A este respecto la redacción es algo oscura, lo que obliga a realizar dos precisiones:

- Aunque el art. 88 LOPD alude a "lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores", esto resulta redundante

[37] TODOLÍ SIGNES, A., considera que "el derecho a la desconexión digital existe de manera absoluta, pero que la negociación colectiva puede matizar ese ejercicio conforme a la naturaleza y objeto de la relación laboral y sector concreto" ("El Derecho a la Desconexión Digital aprobada por la LOPDGDD y la Prevención de riesgos laborales", Blog del autor, 17 de enero de 2019).

y hace pensar que quizá se confunde negociación colectiva con uno de sus específicos productos: el convenio colectivo de naturaleza normativa, de modo que el art. 88, en realidad, se refiere al convenio colectivo o, en su defecto, al acuerdo informal de empresa[38].

La equívoca fórmula no es novedosa: nuestro legislador ya la había utilizado en el art. 22 ET. Tampoco es una fórmula aislada: en el apartado 9 del art. 34 ET –incorporado por Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo– se refrenda esta concepción de la negociación colectiva y el acuerdo de empresa como categorías alternativas.

- Tal como se ha redactado el precepto y la distribución de sus apartados, no parece que la política deba ser, en todo caso, el resultado de un acuerdo colectivo, sin perjuicio de tener que respetarlo si existe, obviamente. Ni siquiera es exigible la negociación colectiva[39]. Así se deduce de la referencia a la política en el apartado tercero, en el que obliga al empleador a elaborarla previa audiencia a los representantes de los trabajadores. Esto permite concluir que es el empresario el unilateralmente obligado a diseñar una política[40], que habrá de sujetarse a los acuerdos alcanzados al respecto pero que podrían no existir, ya que de otro modo no tendría sentido exigir que se diera audiencia previa a los representantes de los trabajadores.

  Una interpretación distinta –que requiriera negociación y/o acuerdo colectivo en todo caso– podría resultar contradictoria con el amplio ámbito de aplicación del precepto, pues dejaría al margen a todas aquellas organizaciones productivas que no contaran con representación de los trabajadores.

  No obstante, como se verá más adelante, es importante tener en cuenta que el art. 88 LOPD anuda la política de desconexión a la potenciación de la conciliación de la vida laboral, familiar y personal, y que el comité de empresa es competente para "colaborar con la dirección de la empresa en el establecimiento y puesta en marcha de medidas de conciliación" (art. 64.7.d ET). Aunque la colaboración no tiene por qué identificarse con negociación y acuerdo, no hay duda de que una política concertada con los representantes de los trabajadores garantizaría el cumplimiento de esta previsión.

2º) Por otra parte, la política interna ha de potenciar el derecho a la conciliación de la actividad laboral y la vida personal y familiar.

La referencia a la "vida personal" recuerda a la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, que aludía reiteradamente a la vida personal como

[38] Así lo interpreta con naturalidad BAYLOS GRAU, A.: "Los derechos digitales y la negociación colectiva", *La Ley* 15588/2018, p. 2.

[39] En contra, BAYLOS GRAU, A., quien opina que la realización del derecho a la desconexión digital "está plenamente condicionada a su desarrollo en convenio colectivo o acuerdo informal de empresa" ("Los derechos digitales y la negociación colectiva", *La Ley* 15588/2018, p. 2).

[40] Lo entiende del mismo modo QUÍLEZ MORENO, J.M.: "La garantía de derechos digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores", *Revista Española de Derecho del Trabajo* núm. 217, 2019, BIB 2019/1558, p. 16. En este sentido, SERRANO OLIVARES, R., tacha a la regulación de "descafeinada" desde la perspectiva de la defensa colectiva de los intereses de los trabajadores. Reconoce que "el convenio colectivo o el acuerdo de empresa podrá o no regular la materia –sin que haya obligación alguna de negociarla–, recayendo en el empresario la obligación de elaborar una política interna, que podrá tener carácter unilateral desde el principio, en la medida en que la ley solamente exige la previa audiencia de la representación del personal. Eso sí, si existe convenio o acuerdo de empresa que regule las modalidades de ejercicio del derecho, la política interna empresarial deberá respetar sus directrices" ("Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *IUSLabor* núm. 3, 2018, p. 228).

un espacio a compatibilizar con el tiempo de trabajo. Como es sabido, aquella mención quedó en una mera declaración de intenciones al no instrumentarse ninguna figura específica para hacerla realmente efectiva y centrarse todos los esfuerzos en las responsabilidades vinculadas a la familia. Pero el legislador actual reflota el concepto, tanto en el art. 88 LOPD como en el Real Decreto-ley 6/2019, de 1 de marzo, de medidas urgentes para garantía de la igualdad de trato y de oportunidades entre mujeres y hombres en el empleo y la ocupación. Sin perjuicio de que no vaya más allá, en cuanto al derecho a la desconexión digital podría identificarse con el respeto a los descansos y al ocio, es decir al tiempo de no trabajo, se tengan o no responsabilidades familiares.

Por otra parte, conviene no confundir desconexión digital con jornada rígida o uniforme. Estamos ante un derecho vinculado al descanso, un instrumento para garantizar la efectiva posibilidad de disponer de nuestro tiempo de no trabajo para desarrollar actividades personales y familiares. Consecuentemente, nada impide contar con una jornada flexible gracias al uso de medios tecnológicos, en la que el trabajador configure su tiempo conforme a sus necesidades si así lo ha acordado con la empresa, sin perjuicio de que, una vez alcanzados los límites de su jornada, por muy flexibles que sean, tenga derecho a dejar de trabajar.

3º) El derecho a la desconexión digital ha de atender a la naturaleza y objeto de la relación laboral. Esta mención refuerza nuestra idea inicial, conforme a la cual el derecho no es absoluto puesto que su ejercicio puede condicionarse[41].

Evidentemente, los límites y restricciones no podrán ser de tal entidad que conviertan al derecho en impracticable. Deberán aplicarse pautas de razonabilidad y proporcionalidad, adaptando los contornos y alcance del derecho a la desconexión a las concretas circunstancias de una legítima prestación de servicios. En definitiva, han de aplicarse los mismos criterios que ya rigen sobre el tiempo de trabajo, garantizando los descansos de los trabajadores.

Por ello, es perfectamente posible que determinadas situaciones puedan devolver al trabajador a su tiempo de trabajo, con las consecuencias jurídicas inherentes, y así debería contemplarse en la correspondiente política interna. Es el caso de necesidades urgentes y extraordinarias, o incluso de un régimen de guardias, con las puntualizaciones que sobre estas últimas ha vertido el Tribunal de Justicia de la Unión Europea.

Ahora bien, sentada la teoría, reconozcamos que la práctica es mucho más compleja, pues la obligación del registro de jornada impuesta por el Real Decreto-ley 8/2019 ha ocasionado una revolución conceptual en materia de tiempo de trabajo. Ya sabíamos que la dimensión binaria de la Directiva 2003/88/CE resultaba a todas luces insuficiente e insatisfactoria para contener nuestra realidad productiva, pero la ausencia de controles internos y externos permitía revestir de flexibilidad las imprecisiones. Así, por ejemplo, no sólo podíamos pasar sin tener del todo claro si ciertos desplazamientos a cargo de la empresa computaban o no como tiempo de trabajo más allá del caso Tyco[42], sino que admitíamos con naturalidad el criterio del Tribunal de Justicia de la Unión Europea conforme al cual podría ser tiempo de descanso aquel en el que el trabajador está obligado a permanecer en contacto, computándose como tiempo de trabajo exclusivamente cuando comienza a "proporcionar servicios después de una llamada"[43]. Hoy más que nunca esa afirmación ha de venir precedida de una reflexión sobre las

[41] De "modular" el ejercicio del derecho hablan GARCÍA MURCIA, J., RODRÍGUEZ CARDO, I.A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo* núm. 216, 2019, BIB 2019/1432, p. 35.

[42] STJUE de 10 de septiembre de 2015, Asunto C-266/14, Tyco.

[43] STJUE de 3 de octubre de 2000, Asunto C-303/98, Simap.

circunstancias específicas de cada caso, pues estar en contacto puede suponer estar conectado, y la disponibilidad tecnológica se situará a un lado u otro de los límites de la jornada según los perfiles del supuesto concreto[44].

Las imprecisiones ya no son una opción, por lo que el debate científico y judicial es tan urgente como inaplazable. Solo avanzando en él podremos hacerlo también en los contornos del derecho a la desconexión digital[45].

5.2. Procedimiento y contenido

Para su elaboración el empresario ha de dar audiencia previa a los representantes de los trabajadores. Esta obligación, reflejada de modo incondicionado en la norma, debería matizarse en función de las circunstancias, pues en el caso de que la política sea el resultado de un acuerdo colectivo no tiene sentido dar audiencia a aquéllos con quienes se alcanzó el mismo. Pero sí si se trata de representantes que no participaron en la negociación, o si la política es más amplia o se separa en algo respecto de lo acordado.

También parece razonable dar trámite de audiencia cuando ha pasado tiempo desde el acuerdo, de modo que los representantes podrían actualizar sus propuestas u opiniones. En esta línea, aquellas empresas que ya disponen de una política de desconexión acordada con los representantes de los trabajadores antes de la entrada en vigor de la LOPD, deberían revisar que cumplen todas las premisas del art. 88 LOPD y, desde luego, dar siquiera trámite de audiencia para su actualización.

Por descontado, la obligación de dar audiencia previa a los representantes de los trabajadores no ha de operar en aquellas empresas en las que no existe dicha representación, sin que exista habilitación legal para entender exigible la conformación de comisiones *ad hoc*.

En cuanto al contenido de la política, además de definir las modalidades de ejercicio del derecho a la desconexión conforme a los márgenes ya señalados, ha de identificar las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. Esto se relaciona directamente con la salud laboral, aunque llama la atención que el foco se ponga de modo específico y exclusivo en la denominada "fatiga informática".

Según el Instituto Nacional de Seguridad y Salud en el Trabajo[46], la fatiga informática es uno de los tipos de fatiga mental, definiéndose esta última como la progresiva disminución de la capacidad de respuesta humana ante un esfuerzo intenso o prolongado de tipo cognitivo (atencional, de memoria, etc.). Por tanto, podríamos decir, quizá, que la fatiga informática sería la fatiga mental ocasionada por el uso de herramientas informáticas, de modo que la política empresarial ha de sensibilizar a los trabajadores sobre la importancia de un uso mesurado de las mismas para evitar el problema.

Pero, ¿por qué la formación ha de ir dirigida a evitar este riesgo y no cualesquiera otros de los muchos asociados al uso intensivo de dispositivos digitales?

No hay duda de que la generalización tecnológica y la hiperconectividad que conlleva

[44] Aluden a la "disponibilidad tecnológica" MORENO GONZÁLEZ-ALLER, I.: "El derecho de los trabajadores a la desconexión tecnológica", *www.elderecho.com*, 17 de agosto de 2018; PURCALLA BONILLA, J.J.: "Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: notas a propósito de la Ley 3/2018 de 5 de diciembre", *Revista Española de Derecho del Trabajo* núm. 218, 2019, BIB 2019/2891, p. 19.

[45] Como afirma PÉREZ CAMPOS, A.I., la regulación legal del derecho a la desconexión es propicia solo "como garantía adicional a los márgenes de distinción entre tiempo de trabajo y tiempo de descanso" ("La desconexión digital en España: ¿un nuevo derecho laboral?", *Anuario Jurídico y Económico Escurialense*, LII, 2019, p. 9).

[46] NTP 445: Carga mental de trabajo: fatiga.

puede generar, además de riesgos físicos[47], situaciones de estrés, agotamiento por sobrecarga informativa, ansiedad ocasionada por las dificultades para conciliar la vida personal y familiar con el trabajo, adicción tecnológica y sus consecuencias, etc. Estamos ante un factor de riesgo psicosocial importante[48], y, siendo cierto que el art. 88 LOPD no exige ir más allá de la fatiga informática, la necesaria integración con la Ley de Prevención de Riesgos Laborales abre la puerta a avanzar en un sentido más amplio, altamente recomendable.

La política ha de ir dirigida a los trabajadores, incluidos los que ocupen puestos directivos. La mención es más amplia que la de altos directivos, por lo que deberían quedar integrados todos los trabajadores de la empresa, con independencia de la naturaleza ordinaria o especial de su relación laboral. Ello es coherente con la concepción extensa de la desconexión digital que plasma el art. 88 LOPD, como un derecho a proteger para todos los trabajadores en todo tipo de empresa. Además, es sumamente relevante dar formación a quienes tienen empleados a su cargo, pues de ellos depende, en la práctica, que estos últimos vean respetado su derecho a la desconexión digital.

También, expresamente se indica que se preservará el derecho en los supuestos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas. Por tanto, la política debería contener previsiones específicas para estos casos.

6. PAPEL DE LOS REPRESENTANTES DE LOS TRABAJADORES

Los representantes de los trabajadores tienen un triple papel, que en parte ya se ha analizado pero que no se agota ahí. Ha de tenerse presente su espacio en la conformación y seguimiento de una política de desconexión digital, en la medida en que así lo contemplan las distintas normas en presencia.

En primer lugar, pueden acordar medidas en torno a la desconexión en los convenios o acuerdos colectivos, generales o específicos, y nada impide que la política de desconexión se pacte colectivamente. Es más, el art. 91 LOPD establece que los convenios colectivos "podrán establecer (…) la salvaguarda de los derechos digitales", lo que, al margen de la críptica redacción, alberga una invitación a la negociación colectiva para que se decida a hacer suyo un espacio a estos efectos.

En segundo lugar, los representantes de los trabajadores deben ser oídos por el empresario antes de elaborarse la política.

Pero además y en tercer lugar, ha de atenderse a los derechos reconocidos en el art. 64 ET. En su virtud, el comité de empresa ejerce una labor de vigilancia en el cumplimiento de las normas, pactos y condiciones vigentes (art. 64.7.a.1º ET), lo que sin duda incluye la política de desconexión. También vigila y controla las condiciones de seguridad y salud en el desarrollo del trabajo en la empresa (art. 64.7.a.2º ET), y la desconexión está anudada a la salud laboral. Finalmente, colabora con la dirección de la empresa en el establecimiento y puesta en marcha de medidas de conciliación (art. 64.7.d ET), entre las que se cuenta la política de desconexión digital.

---

[47] AGUILERA IZQUIERDO, R., y CRISTOBAL RONCERO, R.: "Nuevas tecnologías y tiempo de trabajo: el derecho a la desconexión tecnológica", *Conferencia Nacional Tripartita: El futuro del trabajo que queremos*, OIT, 2017, p. 3. MELLA MÉNDEZ, L., llama la atención sobre los riesgos físicos derivados de malas posturas corporales, deformaciones de las extremidades u otras enfermedades relacionadas con el sedentarismo. Incluso sugiere el posible impacto de las radiaciones de las ondas electromagnéticas ("Nuevas tecnologías y nuevos retos para la conciliación y la salud de los trabajadores (1)", *La Ley* 1902/2016, p. 5).

[48] ARAGÜEZ VALENZUELA, L., "El impacto de las nuevas tecnologías de la información y de la comunicación en el tiempo de trabajo: una especial referencia a la desconexión digital", en AA.VV.: *El Derecho del Trabajo español ante el Tribunal de Justicia: problemas y soluciones* (MIRANDA BOTO, J.M., Dir.), Cinca 2018, p. 393.

Recuérdese que, conforme al art. 7.7 de la Ley sobre Infracciones y Sanciones en el Orden Social, constituye infracción grave la transgresión de los derechos de información, audiencia y consulta de los representantes de los trabajadores y de los delegados sindicales, en los términos que legal o convencionalmente estuvieren establecidos.

7. CONSECUENCIAS DE LOS INCUMPLIMIENTOS

El legislador ha contemplado el derecho a la desconexión digital de los trabajadores, pero, según ya advertimos, no ha reflejado el correlativo deber empresarial de garantizarlo más que indirectamente a través de la obligación de elaborar una política empresarial al respecto. Y, ni la vulneración del derecho a la desconexión, ni la ausencia de la citada política, parecen tener consecuencias laborales, dado que ninguna de las dos conductas se ha tipificado específicamente en la Ley sobre Infracciones y Sanciones en el Orden Social[49]. En otras palabras, el legislador omite uno de los elementos que integran la estructura de las normas jurídicas conforme a la teoría kelseniana.

Cuestión distinta es que la ausencia de una política de desconexión pudiera tener otro tipo de implicaciones. Nótese, a este respecto, que la implantación de esta política forma parte de la información no financiera a suministrar por las sociedades que formulen cuentas consolidadas, según dispone el art. 49.6 del Código de Comercio, tras su reforma por la Ley 11/2018.

Pero, volviendo al ámbito específicamente laboral, frente a quienes pudieran propugnar que, sobre la base del principio de tipicidad, la norma no es exigible dado que no se sanciona su incumplimiento, cabe proponer una visión más ajustada a la voluntad del legislador, al margen de su técnica jurídica: el incumplimiento debería quedaría diluido en los tipos más amplios desde los que se aborda la materia. Ya hemos dicho que el derecho a la desconexión es un subtipo de derecho al descanso y a la limitación de la jornada, lo que tiene un vínculo con la salud laboral, y además está prevista la participación de los representantes de los trabajadores. Veamos, pues, los tipos concernidos:

Obviamente, la tipificación más clara es la relativa al tiempo de trabajo. Es infracción grave la transgresión de las normas y los límites legales o pactados en materia de jornada, descansos y, en general, el tiempo de trabajo a que se refieren los arts. 12, 23 y 34 a 38 del ET (art. 7.5 LISOS)[50].

Por el vínculo con la salud laboral, debe mencionarse la infracción leve consistente en el incumplimiento de la normativa de prevención de riesgos laborales que carezca de trascendencia grave para la integridad física o la salud de los trabajadores (art. 11.4 LISOS), así como la infracción grave derivada de los incumplimientos de las obligaciones en materia de formación e información suficiente y adecuada a los trabajadores acerca de los riesgos del puesto de trabajo susceptibles de provocar daños para la seguridad y salud y sobre las medidas preventivas aplicables (art. 12.8 LISOS).

Dado que el art. 88 LOPD anuda la desconexión digital al derecho a la intimidad, aunque no compartimos ese vínculo directo, conviene tener presente que constituyen infracción muy grave los actos del empresario contrarios al respeto de la intimidad de los trabajadores (art. 8.11 LISOS).

Si atendemos a la desconexión como vía para la conciliación de la vida laboral, familiar y personal y lo relacionamos con los planes de igualdad, adquiere relevancia la infracción grave consistente en no cumplir las obligacio-

[49] Una crítica a la óptica del derecho del trabajador y no de las responsabilidades empresariales puede verse en LAHERA FORTEZA, J.: "Es solo marketing el derecho a desconectar?", *Cinco Dias*, 30 de enero de 2019.

[50] Téngase en cuenta que el derecho a la desconexión no reside en ninguno de estos preceptos, sino en el art. 20 bis ET.

nes que en materia de medidas de igualdad establecen la Ley Orgánica 3/2007, el Estatuto de los Trabajadores o el convenio colectivo (7.13 LISOS).

Por último, ya vimos que es infracción grave la transgresión de los derechos de información, audiencia y consulta de los representantes de los trabajadores (art. 7.7 LISOS).

8. PERFILES DE LA DESCONEXIÓN COMO UN DERECHO-DEBER DEL TRABAJADOR

De lo expuesto hasta aquí cabe extraer ciertas ideas conclusivas:

- La generalización de un modelo de trabajo flexible gracias a las tecnologías ha hecho que el péndulo oscile en el sentido contrario: surgen figuras jurídicas "contracorriente", que pretenden poner límite a eventuales abusos. Frente a los microchips[51], el smartworking y aplicaciones cada vez más sofisticadas para garantizar la conexión[52], se subraya el esquema clásico de descanso versus trabajo y la obligación del registro horario. El reconocimiento del derecho a la desconexión digital se adscribe a esta última tendencia.

- Tal como se configura en el art. 88 LOPD, la desconexión es un derecho del trabajador. En principio, eso significa que, al no tratarse de un deber, el empleado podría conectarse si lo deseara, aunque no le sería exigible ni cabría que se le sancionara por no hacerlo. Obviamente, no son descartables supuestos excepcionales en los que el empresario podría exigir la conexión por razones justificadas conforme se prevea en la política correspondiente.

- La configuración de la desconexión como un derecho del trabajador supone que el superior jerárquico podrá remitirle comunicaciones fuera de jornada y horario, advirtiendo que el empleado no está obligado a atenderlas en tiempo de descanso. No obstante, ha de quedar perfectamente clara la libertad de opción del trabajador, pues en la medida en que se vea compelido a conectarse para evitar represalias, estaría viendo vulnerado su derecho. Por eso es tan importante la formación del personal con funciones directivas, para que procuren no condicionar la voluntad de trabajadores.
  Como es lógico, abundan críticas doctrinales a la opción del legislador por un derecho del trabajador sin la contrapartida de un claro deber de abstención por parte del empresario, señalándose que este enfoque propicia un altísimo riesgo de que el derecho resulte ineficaz[53].

- Dado que, con carácter general, no cabe exigir al trabajador que se conecte fuera de su jornada y horario, lo que se le comunique extemporáneamente no deberá suponerle un perjuicio en caso de no ser atendido de modo inmediato. Por ejemplo, vulneraría el derecho a la desconexión digital la comunicación de

[51] ABC, 12 de julio de 2019, https://www.abc.es/tecnologia/electronica/abci-microchips-subcutaneos-no-necesitaras-tarjetas-llaves-201907121051_noticia.html

[52] Es el caso de aplicaciones especializadas en grupos de chat de trabajo (RRHH Digital, 31 de julio de 2019, http://www.rrhhdigital.com/secciones/tecnologia-e-innovacion/137814/Asi-es-la-nueva-alternativa-a-WhatsApp-para-los-empleados-que-no-trabajan-frente-al-ordenador-).

[53] Entre otros, Beltrán de Heredia Ruiz, I., propugna un deber de abstención empresarial, pues de lo contrario "es probable que, en la práctica, la efectividad del derecho acabe siendo especialmente tenue. En particular porque, si no fuera así, reparen que la desconexión recaería exclusivamente sobre la voluntariedad del propio trabajador y, en tal caso, se corre el riesgo que (por los motivos que sea), no sea «capaz» de abstenerse de responder." ("El derecho a la desconexión digital", Blog del autor, 20 de noviembre de 2019). También denuncia el error de enfoque Talens Visconti, E.E.: "El derecho a la desconexión digital en el ámbito laboral", *Revista Vasca de Gestión de Personas y Organizaciones Públicas* núm. 17, 2019, p. 159.

cambios de turno para el día siguiente, pues el trabajador tendría que estar pendiente de este tipo de decisiones durante su tiempo de descanso en orden a organizarse adecuadamente y cumplir con la próxima jornada.

- Lo que se reconoce es el derecho a la desconexión; por el contrario, no existe el derecho a la conexión. Consecuentemente, nada impide a la empresa imponer la desconexión de sus empleados si las circunstancias de la organización productiva lo permiten, lo cual constituye la opción más segura para evitar eventuales responsabilidades empresariales.

- Una vez prohibida la conexión, el incumplimiento de esta directriz podrá ser sancionado por desobediencia.

- Desde la óptica de la prevención de riesgos laborales, el derecho adquiere perfiles de deber, en la misma medida en que lo hace el derecho al descanso de los trabajadores.
  Recuérdese que el Tribunal de Justicia de la Unión Europea ha declarado que el reconocimiento del derecho al descanso sólo es efectivo si el empresario tiene encomendado velar por el efectivo disfrute por parte del trabajador. Ello no llega hasta el punto de exigirle que obligue a sus trabajadores a utilizar efectivamente los períodos de descanso que les corresponden, pero sí ha de hacer lo necesario para que los empleados se encuentren efectivamente en condiciones de ejercer tal derecho[54].
  Desde luego, las políticas internas que prohíben la conexión fuera de la jornada y el horario laboral se amalgaman perfectamente con esta perspectiva y neutralizan el riesgo de responsabilidades empresariales en materia de seguridad y salud en el trabajo.

9. PRIMERAS POLÍTICAS EMPRESARIALES DE DESCONEXIÓN

El legislador de los últimos tiempos ha optado por protocolos internos para dar forma a ciertos derechos laborales.

Así, se ha visto que el art. art. 88 LOPD insta a elaborar una política sobre desconexión digital, pero también el art. 87 LOPD conmina a los empresarios, con participación de los representantes de los trabajadores, a fijar criterios de utilización de los dispositivos digitales en el ámbito laboral. Por su parte, el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, obliga a la empresa a garantizar el registro diario de jornada, so pena de incurrir en infracción grave, y ha de organizarlo y documentarlo conforme a lo que pacte colectivamente o, en su defecto, lo que establezca por sí mismo previa consulta con los representantes de los trabajadores.

En pocos meses, las empresas se han visto conminadas a contar con protocolos de actuación en diversas materias. Pero la ausencia de consecuencias sancionatorias claras por carecer de políticas de desconexión ha propiciado que estas últimas no se acometieran inmediatamente[55].

El verdadero punto de inflexión ha sido el citado Real Decreto-ley 8/2019, o, más proba-

[54] STJUE de 7 de septiembre de 2006, Asunto C484/04, Comisión de las Comunidades Europeas contra Reino Unido de Gran Bretaña e Irlanda del Norte.

[55] Según datos volcados en la difusión del IV Congreso Nacional de AdiReLab, en noviembre de 2019 el 20% de las empresas no tenía aún un plan de acción ante la digitalización (https://confilegal.com/20191114-un-ano-despues-de-su-regulacion-el-derecho-a-la-desconexion-digital-sigue-siendo-la-asignatura-pendiente-en-muchas-de-las-empresas/). Según Comisiones Obreras, poco más de un 11% de los convenios laborales firmados en 2019 mencionan el derecho a la desconexión laboral de los empleados (eldiario.es, 12 de diciembre de 2019).

blemente, la espada de Damocles de la Inspección de Trabajo advirtiendo del comienzo de una campaña específica en 2020 para verificar y controlar los sistemas de registro de jornada requeridos por la norma de urgencia[56]. En consecuencia, comienzan a suscribirse protocolos sobre registro de jornada y en algunas organizaciones productivas se aprovecha para acometer simultáneamente una política de desconexión digital, lo que es lógico teniendo en cuenta que ambos instrumentos giran en torno a un eje común: la delimitación de lo que forma parte de la jornada de trabajo y aquello que queda extramuros de la misma.

De este modo, la desconexión se sube al carro del registro de jornada y, por fin, recibe tratamiento una política que la LOPD venía exigiendo desde su entrada en vigor el 7 de diciembre de 2018.

El análisis de diversos acuerdos de desconexión implementados en grandes empresas permite concluir que en un primer paso se ha optado por pautas bastante genéricas, no albergándose ánimo de regular con precisión las circunstancias particulares, lo que es natural teniendo en cuenta lo novedoso de la norma y lo difuso de sus contornos.

Sin duda, un dato altamente positivo es que los protocolos se han acordado con los representantes de los trabajadores. Esto no sólo minimiza conflictos sino que ayuda a que, entre todos, se identifiquen las circunstancias dignas de plasmación y la mejor vía para su enfoque. Además, se da cumplimiento a las exigencias de participación de los representantes de los trabajadores contenidas en el art. 88 LOPD y en el art. 64 ET.

Algunos de los textos que han trascendido son los siguientes: Acuerdo colectivo BBVA sobre Registro de Jornada y Desconexión Digital, de 25 de septiembre de 2019 (en adelante Acuerdo BBVA), suscrito por la empresa y la representación de las secciones sindicales presentes en los Comités de Empresa y Delegados de Personal (CCOO, ACB, CGT, UGT, SEC, CIG, ELA, LAB, SCAT); Política Interna Reguladora del Derecho a la Desconexión Digital de las Personas Trabajadoras de Telefónica, de 17 de julio de 2019 (en adelante Acuerdo Telefónica), suscrita por la empresa con los Secretarios Generales de las Federaciones de Comunicaciones de UGT y de CCOO. Protocolo del derecho a la desconexión digital del Grupo Repsol, de 28 de noviembre de 2019 (en adelante Acuerdo Repsol), suscrito por la empresa y los sindicatos que forman la mesa del Acuerdo Marco: CCOO, UGT y STR.

Las políticas citadas reúnen las siguientes consideraciones básicas y pautas comunes:

- Se indica expresamente que resultan de aplicación a todos los empleados de la empresa[57]. De este modo, se cumple con la previsión legal de que la política se dirija a también a los directivos, si bien resultaría más clara una mención expresa a los mismos, siquiera sea por motivos pedagógicos.

- Se contempla, con carácter general el "derecho" a no responder comunicaciones tras el fin de la jornada laboral, sin que ello conlleve represalias[58]. Sin embargo, se introducen excepciones razonables:

  a) por "fuerza mayor o grave e inminente perjuicio empresarial o del negocio, cuya urgencia temporal necesita indubitadamente de una respuesta inmediata"[59]. La pléyade de conceptos jurídicos indeterminados podría generar conflictos, pero es comprensible que se desee dejar las ideas lo más abiertas posible en esta fase de implantación inicial.

[56] Nota de prensa de la Inspección de Trabajo y Seguridad Social, 11 de noviembre de 2019 (http://prensa.mitramiss.gob.es/WebPrensa/downloadFile.do?tipo=documento&id=3.647&idContenido=3.483).

[57] Acuerdo BBVA y Acuerdo Telefónica.

[58] Acuerdo BBVA y Acuerdo Telefónica.

[59] Acuerdo Telefónica.

b) por "excepciones justificadas que supongan un grave o evidente perjuicio empresarial, cuya urgencia temporal necesite de una respuesta inmediata"[60]. La fórmula es similar a la anterior, mereciendo idéntica valoración.

c) por percibir un complemento de disponibilidad[61]. Seguramente se alude a los trabajadores sometidos a un régimen de guardias, que, obviamente, tendrán sus especialidades en materia de desconexión. Así se plasma expresamente en algún caso, indicando que el derecho a la desconexión se adaptará a la naturaleza y características de cada puesto y funciones, y en especial a las guardias[62]. Pero esto no debería interpretarse como que los trabajadores con régimen de guardias no tienen derecho a descansar y, por consiguiente, a desconectar, bien que con unas peculiaridades que, más tarde o más temprano, deberían integrarse en esta política.

- Si concurre alguna de las excepciones, la empresa ha de comunicar al trabajador la situación y su conexión se computará como tiempo de trabajo[63]. En algunos casos se fijan los cauces por los que se transmitirá esta comunicación.

- Se contempla expresamente el deber de la empresa de evitar el uso de medios informáticos y tecnológicos fuera de la jornada estipulada[64].

Esta previsión convive con otras complementarias: se reconoce el derecho a enviar comunicaciones libremente, aunque sin esperar respuesta[65]. Y se plasma el deber de los superiores jerárquicos de no requerir contestación y asumir que han de esperar por ella, así como el correlativo derecho del trabajador de no contestar hasta el comienzo de la jornada siguiente[66].
Se aprecia cierto nivel de contradicción entre el deber de evitar la conexión fuera de la jornada y el derecho a conectarse sin esperar respuesta. Pero esta aparente contradicción es coherente con la naturaleza de derecho-deber que reviste el derecho a la desconexión digital.

- Cuando se envíen correos electrónicos a deshora, se utilizará preferentemente la configuración del envío retardado para hacer llegar los mensajes dentro del horario laboral del destinatario[67].

- En caso de distintos husos horarios, se tratarán de mantener las comunicaciones en los horarios de solape entre las distintas personas o en el momento más próximo posible a dicho solape[68]. En otras palabras, se admite una nueva excepción a la desconexión por motivos justificados.

- No se convocarán reuniones, presenciales o telemáticas, fuera del horario de trabajo salvo excepciones justificadas que deriven de fuerza mayor[69] o supongan un grave o evidente perjuicio empresarial, y en este último caso deberán preavisarse con una antelación mínima y la asistencia será voluntaria[70].

[60] Acuerdo BBVA.
[61] Acuerdo Telefónica.
[62] Acuerdo BBVA.
[63] Acuerdo BBVA y Acuerdo Telefónica.
[64] Acuerdo Telefónica, Acuerdo BBVA y Acuerdo Repsol. En el Acuerdo de Telefónica y en el de Repsol se matiza que este deber es exigible "en la medida de lo posible", e incluso en el de Repsol se indica que se evitarán las comunicaciones fuera del horario de trabajo "salvo que concurran circunstancias que lo justifiquen".
[65] Acuerdo Telefónica, Acuerdo BBVA.
[66] Acuerdo Telefónica.
[67] Acuerdo Repsol.
[68] Acuerdo Repsol.
[69] Acuerdo Telefónica.
[70] Acuerdo BBVA, que contempla una antelación de 72 horas.

- Durante sus ausencias, los trabajadores dejarán un aviso en el correo electrónico indicando la persona de contacto. Esta práctica se configura como algo obligatorio[71] o meramente recomendable[72].

- La formación obligatoria tendrá lugar, preferentemente, en horario de trabajo[73].

- Se anuncia la puesta en marcha de acciones de sensibilización[74]. En algún caso se atribuye a los superiores jerárquicos la responsabilidad de formar "mediante la práctica responsable"[75]. No parece que de este modo se esté cumpliendo con la obligación legal de "definir" las acciones de formación y sensibilización del personal sobre un uso razonable de las herramientas tecnológicas. Quizá las prisas han impedido hacer un diseño acorde con este objetivo, pero debería tenerse en cuenta que lo que se pide es algo más que anunciar un futurible genérico.

- Respecto de los teletrabajadores, simplemente se alude a la garantía de su derecho a la desconexión, sin añadir ninguna precisión adicional[76]. Cuesta pensar que con esta previsión se esté dando efectivo cumplimiento a la exigencia legal de "preservar" el derecho a la desconexión digital de quienes realizan su trabajo total o parcialmente a distancia o desde su domicilio, pero al menos los teletrabajadores aparecen reflejados. Confiemos en que poco a poco irán perfilándose sus especialidades.

- Por último, se constituye una comisión paritaria para el seguimiento del acuerdo colectivo[77], a la que incluso podrá hacérsele llegar noticia de prácticas o comportamientos contrarios al protocolo para que, en su caso, se adopten las medidas oportunas[78].
  Esto es muy positivo, en la línea de que las políticas de desconexión se adscriban a las vigentes en materia de *compliance*, de modo que se establezca un canal para reclamar en caso de que el derecho no se esté respetando. Y es óptimo contar con representantes de los trabajadores en estos cauces.

En conclusión, las políticas analizadas cumplen el objetivo de definir modalidades de ejercicio del derecho a la desconexión, aunque seguramente se perfilarán mejor más adelante, una vez que se compruebe su aplicación simbiótica con el sistema de registro de jornada. También aparece alguna previsión que podría relacionarse con la naturaleza y objeto de la relación laboral. Por ahora, los términos son tímidos y cautelosos, incluso ambiguos en algunos de los puntos, lo que permitirá un ajuste menos traumático a lo que puedan establecer los Tribunales cuando se diriman los inevitables conflictos sobre la naturaleza de determinados tiempos como de trabajo o de descanso.

Los trabajadores a distancia son los eternos postergados. Era el momento de afrontar su situación, sin miedo a que ello suponga restar flexibilidad a su prestación de servicios. Una vez más, parece que se esquivará la adopción de acuerdos a este respecto.

Se echa en falta una mayor implicación en cuanto a las acciones de formación y sensibilización sobre la utilización razonable de herramientas tecnológicas, lo que podría haberse hecho sin problemas, pues no se trata de materia expuesta a eventuales vaivenes judiciales sobre tiempo de trabajo. Además, se ha desaprovechado la oportunidad de conectar con la política de uso de dispositivos digitales y así cumplir con las exigencias del art. 87 LOPD.

[71] Acuerdo Telefónica.
[72] Acuerdo Repsol.
[73] Acuerdo BBVA.
[74] Acuerdo Telefónica, Acuerdo BBVA, Acuerdo Repsol.
[75] Acuerdo Telefónica. También el Acuerdo Repsol hace alusión a la importancia de dar ejemplo.
[76] Acuerdo Telefónica y Acuerdo BBVA.
[77] Acuerdo Telefónica y Acuerdo BBVA.
[78] Acuerdo Repsol.

10. REFLEXIÓN FINAL

La OIT alerta: hay que ampliar la soberanía sobre el tiempo de trabajo. *"Las tecnologías de la información y de la comunicación que permiten que se trabaje en cualquier lugar, en cualquier momento, difuminan la línea entre las horas de trabajo y la vida personal, y pueden contribuir a ampliar las horas de trabajo. En la era digital, los gobiernos y las organizaciones de empleadores y de trabajadores tendrán que encontrar nuevos medios para aplicar de forma eficaz a nivel nacional determinados límites máximos de las horas de trabajo, por ejemplo, estableciendo el derecho a la desconexión digital."*[79]

Sin duda, la deriva tecnológica y sus consecuencias sobre las relaciones de trabajo pueden analizarse desde un prisma apocalíptico, negativo y crítico, o bien desde una visión positiva. Siendo esto cierto, también lo es que la posición positiva pasa en buena medida por cierta dosis de realismo, de asumir que estamos ante procesos imparables que no tienen vuelta atrás, y en los que el reto es saber adaptarse no sólo para sobrellevar sus efectos sino para sacarles el mayor partido posible en términos de empleo y condiciones laborales.

Hay que aceptar que el desarrollo tecnológico ha cambiado radicalmente la concepción de la prestación laboral[80]. El empleo y el trabajo son conceptos ahora más volátiles y requieren competencias distintas, así como una mayor flexibilidad. Es preciso ofrecer un marco jurídico adecuado para que los avances digitales no se constituyan ni se conciban como una afrenta a los derechos laborales. Desde luego, son necesarios los límites para evitar abusos amparados en las posibilidades técnicas[81], pero esos límites no han de ser de tal calado que, en realidad, supongan impedir el avance mismo.

En definitiva, han de redefinirse y reajustarse las conquistas sociales en función de unas coordenadas bastante más dinámicas y complejas que las que tradicionalmente han acompañado al ordenamiento laboral. Y en este escenario deben tomar la iniciativa, sobre todo, la acción sindical y la negociación colectiva[82], y en cualquier caso también las empresas como protagonistas en la oferta de un trabajo que responda a un modelo tan digno como eficiente.

Para estas últimas, la obligación de elaborar una política de desconexión digital debería observarse como una oportunidad de asumir el control del cambio tecnológico y convertirse en una empresa tecnológicamente responsable[83]. Ha de asumirse la imposibilidad de frenar los avances digitales y dar un paso al frente para situarse en la vanguardia. La política de des-

[79] Comisión Mundial sobre el Futuro del Trabajo: *Trabajar para un futuro más prometedor*, OIT, 2019, p. 41.

[80] San Martín Mazzucconi, C.: "Generalización tecnológica: efectos sobre las condiciones de trabajo y empleo", en AA.VV. *Conferencia Nacional Tripartita: El futuro del trabajo que queremos*, 2017.

[81] Por ejemplo, desde luego parece excesiva la situación que describe el *MIT Technology Review* de 21 de febrero de 2017 ("Las oficinas 2.0 espían a los trabajadores para aumentar su rendimiento"), según el cual en Estados Unidos "varias compañías han instalado sensores para medir cuánto, cuándo y con quién hablan sus empleados y qué programas usan". Estos sensores, instalados en sistemas de iluminación, en paredes y debajo de mesas, "miden el movimiento, el sonido y la ubicación, entre otras cosas, lo que permite que la empresa sepa lo que realmente hace su plantilla". Al parecer, "los dispositivos incluso son capaces de medir lo que se conoce como latencia. Se trata del tiempo pasa un individuo sin intercambiar una palabra con nadie y cuando sí se pronuncia esa palabra, dónde y a quién se dirige. Eso podría indicar, por ejemplo, que los empleados generan sus mejores ideas en una zona común concreta, o que pasan demasiado tiempo charlando en la cocina."

[82] En este sentido, son bienvenidas las reflexiones sobre la necesaria reconversión de la acción sindical en orden a gestionar el cambio de la organización del trabajo; impulsar la adquisición de mayores competencias; controlar el uso de datos para evaluar el comportamiento y el rendimiento; analizar los efectos sobre la jornada laboral y el lugar del trabajo, teniendo en cuenta sus consecuencias sobre la vida privada (Comisiones Obreras: *Industria 4.0. Una apuesta colectiva*, 2016).

[83] Propone esta línea de actuación Mercader Uguina, J.R.: "El mercado de trabajo y el empleo en un mundo digital", *Revista de Información Laboral* núm. 11, 2018, p. 9 (BIB 2018/13994).

conexión debería aprovecharse para incluir todo lo relacionado con el uso de herramientas tecnológicas en la empresa (utilización por trabajadores, control por el empresario).

La responsabilidad social empresarial es, igualmente, una herramienta a considerar en materia de desconexión digital como vía para la conciliación de la vida laboral y personal, en la inteligencia de que si se exige desconexión laboral fuera de la jornada es posible que la contrapartida sea la desconexión personal durante la misma[84]: nuevamente, la virtud estará en el equilibrio, en el uso razonable y moderado de todo aquello que nos ayuda a comunicarnos más eficazmente en todos los ámbitos, también en el laboral[85].

Limitarse a parcelar la jornada en compartimentos estancos de trabajo y descanso forma parte de una visión binaria de la prestación de servicios, que, se quiera o no –o mejor dicho, lo quiera la Directiva 2003/88/CE o no–, ha resultado claramente superada por las tecnologías y por la flexibilidad asociada a los nuevos estilos de vida[86]. Pretender encorsetar la realidad para que siga ajustándose a una norma de hace casi dos décadas no solo es ineficiente; es, valga la paradoja, muy poco realista y del todo inútil.

Estamos ante un reto, de los muchos a los que se enfrenta el ordenamiento laboral en este siglo. Y la sociedad debe estar a la altura, dejando de lado el catastrofismo para centrase en la reconversión y el cambio de paradigma.

El desafío es enorme y en absoluto fácil: hemos de perder el miedo a cambiar las normas, a transformar el Derecho del Trabajo, pues solo así será posible continuar aplicando los principios básicos de nuestro ordenamiento, tan necesarios hoy como siempre.

BIBLIOGRAFÍA

Aguilera Izquierdo, R., y Cristobal Roncero, R.: "Nuevas tecnologías y tiempo de trabajo: el derecho a la desconexión tecnológica", en AA.VV. *Conferencia Nacional Tripartita: El futuro del trabajo que queremos*, 2017.

Alemán Páez, F.: "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la «Loi Travail No 2016-1088", *Revista Trabajo y Derecho* núm. 30, 2017.

Aragüez Valenzuela, L., "El impacto de las nuevas tecnologías de la información y de la comunicación en el tiempo de trabajo: una especial referencia a la desconexión digital", en *El Derecho del Trabajo español ante el Tribunal de Justicia: problemas y soluciones* (Miranda Boto, J.M., Dir.), Cinca, 2018.

Baylos Grau, A.: "Los derechos digitales y la negociación colectiva", *La Ley* 15588/2018.

Baz Rodríguez, J.: "Ley Orgánica 3/2018 como marco embrionario de garantía de los derechos digitales laborales. Claves para un análisis sistemático", *La Ley* 6823/2019.

Bel Antaki, J.: "Nuevos derechos digitales de los trabajadores: claves en cinco preguntas y respuestas", *Actualidad Jurídica Aranzadi* núm. 948, 2019.

Beltrán de Heredia Ruiz, I.: "El derecho a la desconexión digital", Blog del autor, 20 de noviembre de 2019.

Comisiones Obreras: *Industria 4.0. Una apuesta colectiva*, 2016.

García Murcia, J., Rodríguez Cardo, I.A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Revista Española de Derecho del Trabajo* núm. 216, 2019.

[84] Lantarón Barquin, D.: "La seducción de los horizontes: reflexiones sobre el derecho a la desconexión digital del trabajador", *Noticias Cielo* núm. 5, 2019, p. 1: "Conexión laboral al margen del tiempo de trabajo y, su reverso, 'conexión personal' dentro del tiempo de trabajo son fenómenos que, aunque no siempre digitales, han acompañado a las relaciones de trabajo *sino ab origine* sí claramente tiempo ha. La ordenación del tiempo de trabajo siempre se ha interesado por establecer fronteras sólidas si bien razonablemente permeables entre ambos espacios vitales del ser humano."

[85] Como advierte Ushakova, T., "no debe obviarse la realidad que dicta un nuevo modelo de bienestar. El avance tecnológico impone un nuevo paradigma, que no supone una separación espacial y temporal entre el trabajo y la vida privada" ("De la conciliación a la desconexión tecnológica. Apuntes para el debate", *Revista Española de Derecho del Trabajo* núm. 192, 2016, BIB 2016/85593, pp. 16 y 17).

[86] En este sentido, Tascón López, R.: "El derecho de desconexión del trabajador (potencialidades en el ordenamiento español) (1)", *La Ley* 3170/2018, p. 7.

LAHERA FORTEZA, J.: "Es solo marketing el derecho a desconectar?", *Cinco Días*, 30 de enero de 2019.

LANTARÓN Barquin, D.: "La seducción de los horizontes: reflexiones sobre el derecho a la desconexión digital del trabajador", *Noticias Cielo* núm. 5, 2019.

MELLA MÉNDEZ, L.: "Nuevas tecnologías y nuevos retos para la conciliación y la salud de los trabajadores (1)", *La Ley* 1902/2016.

MERCADER UGUINA, J.: "Aspectos laborales de la Ley Orgánica 3/2018 de 5 de diciembre: una aproximación desde la protección de datos", *La Ley* 4433/2019, p. 10.

MERCADER UGUINA, J.R.: "El mercado de trabajo y el empleo en un mundo digital", *Revista de Información Laboral* núm. 11, 2018.

MORENO GONZÁLEZ-ALLER, I.: "El derecho de los trabajadores a la desconexión tecnológica", *www.elderecho.com*, 17 de agosto de 2018.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO: *Informe de la Comisión Mundial Sobre el Futuro del Trabajo: Trabajar para un futuro más prometedor*, 2019.

PÉREZ CAMPOS, A.I.: "La desconexión digital en España: ¿un nuevo derecho laboral?", *Anuario Jurídico y Económico Escurialense*, LII, 2019.

PRECIADO DOMENECH, C.H.: *Los derechos digitales de las personas trabajadoras. Aspectos laborales de la LO 3/2018, de 5 de diciembre de Protección de Datos y Garantía de los Derechos digitales*, Aranzadi, 2019.

PURCALLA BONILLA, J.J.: "Control tecnológico de la prestación laboral y derecho a la desconexión de los empleados: notas a propósito de la Ley 3/2018 de 5 de diciembre", *Revista Española de Derecho del Trabajo* núm. 218, 2019.

QUÍLEZ MORENO, J.M.: "La garantía de derechos digitales en el ámbito laboral: el nuevo artículo 20 bis del Estatuto de los Trabajadores", *Revista Española de Derecho del Trabajo* núm. 217, 2019.

SAN MARTÍN MAZZUCCONI, C.: "Generalización tecnológica: efectos sobre las condiciones de trabajo y empleo", en AA.VV. *Conferencia Nacional Tripartita: El futuro del trabajo que queremos*, OIT, 2017.

SAN MARTÍN MAZZUCCONI, C.: "¿Cómo se mide el "uso moderado" de Internet para fines personales?: ¿transgrede la buena fe contractual tener abierto un programa para "chatear"? Comentario a la STSJ Cataluña de 11 de marzo 2004 (AS 2004, 1231)", *Aranzadi Social* núm. 2, 2004.

SAN MARTÍN MAZZUCCONI, C.: "El control empresarial de los ordenadores: estado de la cuestión en España", *Para Jorge Leite. Escritos jurídico-laborais* (vol. I), (Reis, J., Amado, L., Fernandes, L., Redinha, R., Coords.), Coimbra Editora, 2014.

SAN MARTÍN MAZZUCCONI, C.: "El derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos", en *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico* (San Martín Mazzucconi, C., Dir.), EOLAS, 2014.

SAN MARTÍN MAZZUCCONI, C., SEMPERE NAVARRO, A.V.: *Las TICs en el ámbito laboral*, Francis Lefebvre, 2015.

SEMPERE NAVARRO, A.V., SAN MARTÍN MAZZUCCONI, C.: "¿Puede la empresa controlar el ordenador usado por su trabajador? Comentario a la STS 26 de septiembre de 2007, Recurso 966/2006 (JUR 2007, 306130)", *Repertorio de Jurisprudencia* núm. 21, 2007.

SERRANO ARGÜESO, M.: "Always on. Propuestas para la efectividad del derecho a la desconexión digital en el marco de la economía 4.0", *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo* núm. 2, 2019.

SERRANO OLIVARES, R., "Los derechos digitales en el ámbito laboral: comentario de urgencia a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales", *IUSLabor* núm. 3, 2018.

TALÉNS VISCONTI, E.E.: "El derecho a la desconexión digital en el ámbito laboral", *Revista Vasca de Gestión de Personas y Organizaciones Públicas* núm. 17, 2019.

TALÉNS VISCONTI, E.E.: "La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva", *Revista de Información Laboral* núm. 4, 2018.

TASCÓN LÓPEZ, R.: "El derecho de desconexión del trabajador (potencialidades en el ordenamiento español) (1)", *La Ley* 3170/2018.

TODOLÍ SIGNES, A.: "El Derecho a la Desconexión Digital aprobada por la LOPDGDD y la Prevención de riesgos laborales", Blog del autor, 17 de enero de 2019.

USHAKOVA, T.: "De la conciliación a la desconexión tecnológica. Apuntes para el debate", *Revista Española de Derecho del Trabajo* núm. 192, 2016.

VALLECILLO GÁMEZ, M.R.: "El derecho a la desconexión ¿novedad digital o esnobismo del viejo derecho al descanso?", *Revista de Trabajo y Seguridad Social CEF* núm. 408, 2017.

RESUMEN

Las innovaciones tecnológicas trazan un modelo de trabajo en el que los límites son cada vez más difusos, con posibilidades de conectividad permanente e incontrolada. En este contexto, tras décadas de silencio el legislador decidió acometer la regulación específica del derecho a la desconexión digital de los trabajadores, aprovechando la promulgación de la vigente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. El art. 88 permite apreciar que el derecho a la desconexión digital se reconoce a trabajadores y empleados públicos de todo tipo de empresas para garantizar el respeto a su tiempo de no trabajo así como su intimidad. Las modalidades del ejercicio del derecho deben sujetarse a lo establecido en acuerdos colectivos, y el empleador ha de elaborar una política interna definiéndolas.

No se trataba de una figura improvisada y de surgimiento espontáneo, sino que respondía a un contexto en el que diversos antecedentes determinaron que el legislador considerara la oportunidad de regularlo. Además de algunos pronunciamientos judiciales y ciertas prácticas a nivel empresarial, unilaterales o acordadas colectivamente y de gran difusión mediática, destaca la regulación francesa como inspiradora directa de la norma española. Por tanto, el estudio del derecho a la desconexión digital comienza por desgranar esos antecedentes, con especial mención al Código de Trabajo francés, pasando revista crítica a sus puntos de similitud y diferencia respecto de la norma española.

Seguidamente el análisis se centra en el contenido del art. 88 de la Ley Orgánica 3/2018, identificando las pautas que suministra para identificar el derecho. En esta línea, se llama la atención sobre la ausencia de un concepto legal de desconexión digital, lo que obliga a buscar elementos para suplir este silencio de un modo que no resulte tautológico. Se concluye que el derecho a la desconexión digital viene a ser una subespecie del derecho a la limitación de la jornada, que ya teníamos recogido en la regulación del tiempo de trabajo, pero que ahora se reconoce de modo específico y expreso, anudando una serie de medidas conexas que son las realmente novedosas: la obligación de contar con una política empresarial de desconexión y la programación de acciones de formación y sensibilización.

Del mismo modo en que la Ley no define el derecho, tampoco identifica su contenido. Su alcance real se ha de integrar conforme a lo que se establezca en la política de empresa al fijar las modalidades de ejercicio y, en su caso, con lo que pueda preverse en la negociación colectiva, conforme a una serie de finalidades señaladas en la norma. Por tanto, la regulación de la desconexión gira en torno a un eje muy claro: la política o protocolo que regule su ejercicio, lo que permite concluir que el derecho no es absoluto, dado que, aunque se reconoce absolutamente, se condiciona su ejercicio.

Esta conclusión lleva a hacerse dos preguntas: ¿qué características ha de guardar la citada política empresarial? Y, en relación con ello, ¿hasta qué punto la misma puede limitar el derecho a la desconexión digital? Para despejar estos interrogantes se analizan los márgenes que el legislador proporciona, en cuya virtud han de tenerse en cuenta la naturaleza y objeto de la relación laboral, el derecho a la conciliación de la actividad laboral y la vida personal y familiar, así como, por supuesto, lo establecido en la negociación colectiva.

En este punto se concluye que la política no tiene por qué ser, en todo caso, el resultado de un acuerdo colectivo, y ni siquiera es exigible su negociación. Además, es perfectamente posible que determinadas situaciones puedan devolver al trabajador a su tiempo de trabajo, con las consecuencias jurídicas inherentes, y así debería contemplarse en la correspondiente política interna. Es el caso de necesidades urgentes y extraordinarias, o incluso de un régimen de guardias, con las puntualizaciones que sobre estas últimas ha vertido el Tribunal de Justicia de la Unión Europea.

Se examina el procedimiento para la elaboración de la política empresarial, y la obligación de que la misma defina no sólo las modalidades de ejercicio del derecho a la desconexión sino también las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas, así como menciones específicas para quienes trabajan a distancia.

Un apartado específico se dedica al papel de los representantes de los trabajadores, que posee una triple dimensión: como negociadores, como consultores y como vigilantes.

Respecto de las consecuencias de los incumplimientos empresariales, ni la vulneración del derecho a la desconexión, ni la ausencia de una política interna parecen tener consecuencias laborales, dado que ninguna de las dos conductas se ha tipificado específicamente en la Ley sobre Infracciones y Sanciones en el Orden Social. Pero, frente a quienes pudieran propugnar que, sobre la base del principio de tipicidad, la norma no es exigible dado que no se sanciona su incumplimiento, cabe proponer una visión más ajustada a la voluntad del legislador, al margen de su técnica jurídica: el incumplimiento debería quedaría diluido en los tipos más amplios desde los que se aborda la materia, que tienen que ver con el derecho al descanso y a la limitación de la jornada, la salud laboral y la participación de los representantes de los trabajadores.

Todo lo anterior confluye en perfilar la desconexión como un derecho-deber del trabajador, idea que se pormenoriza en un apartado específico.

Seguidamente se analizan algunas de las primeras políticas empresariales de desconexión acordadas en grandes empresas, en orden a identificar su contenido básico y ciertas pautas comunes. Se concluye que las políticas analizadas cumplen el objetivo principal de definir modalidades de ejercicio del derecho a la desconexión, si bien los términos son tímidos y cautelosos, incluso ambiguos en algunos de los puntos.

Por último, se propone una reflexión final sobre la oportunidad de asumir el control del cambio tecnológico con valentía, aceptando el reto de transformar el Derecho del Trabajo en lo necesario, pues solo así será posible continuar aplicando los principios básicos de nuestro ordenamiento, tan necesarios hoy como siempre.

Palabras clave: Tecnologías; desconexión; negociación; protocolo.

ABSTRACT Technological innovations are a model of work in which the limits are increasingly diffuse, with possibilities of permanent and uncontrolled connectivity. In this context, after decades of silence the legislator decided to undertake the specific regulation of the workers' right to digital disconnection, taking advantage of the promulgation of the current Organic Law 3/2018, December 5th, on the Protection of Personal Data and Guarantee of Digital Rights. Article 88 grants the right to digital disconnection for workers of all types of companies to ensure respect for their non-working time as well as their privacy. The right's modalities of exercise should attend to the provisions of collective agreements, and the employer must develop an internal policy defining them.

It was not an improvised figure and spontaneous emergence, but responded to a context in which various backgrounds determined that the legislator considered the opportunity to regulate it. In addition to some judicial pronouncements and certain practices at the corporate level, unilateral or collectively agreed and analyzed by the media, the French regulation stands out as a direct inspiration of the Spanish norm. Therefore, the study of the right to digital disconnection begins by disselling this background, with particular reference to the French Labour Code, reviewing its points of similarity and difference with respect to the Spanish rule.

The analysis then focuses on the content of Article 88 of Organic Law 3/2018, identifying the guidelines it provides to identify the right. In this line, we notice the absence of a legal concept of digital disconnection, which forces us to look for elements to supplement this silence in a way that is not tautological. It is concluded that the right to digital disconnection becomes a subspecies of the right to limit of the day, which we already had in the regulation of working time, but which is now recognized in a specific and express way, by nudating a series of related measures that are the really novel: the obligation to have a business policy of disconnection and the programming of training and awareness-raising actions.

Just as the Law does not define the right, it does not identify its content either. Its actual scope must be integrated in accordance with the provisions of the company policy when setting the exercise arrangements and, where appropriate, with what can be foreseen in collective bargaining, in accordance with a number of purposes set out in the rule. Therefore, the regulation of disconnection revolves around a very clear axis: the policy or protocol regulating its exercise, which makes it possible to conclude that the right is not absolute, since, although it is absolutely recognized, its exercise is conditioned.

This conclusion leads to two questions: what characteristics should the above-mentioned business policy keep? And, to what extent can it limit the right to digital disconnection? In order to clear these questions, we analyze the margins provided by the legislator, taking into account the nature and object of the employment relationship, the right to the reconciliation of work and personal and family life, and, of course, the provisions of collective bargaining.

This point concludes that the policy does not have to be, in any event, the result of a collective agreement, and its negotiation is not even enforceable. Moreover, it is perfectly possible that certain situations may return the worker to his working time, with the inherent legal consequences, and this should be considered in the policy. This is the case of urgent and extraordinary needs, or even of a system of guards, with the points which the Court of Justice of the European Union has poured on the latter.

We examine the procedure for the elaboration of business policy, and the obligation for it to define not only the modalities for the exercise of the right to disconnection but also the training and awareness-raising actions of staff on a use of technological tools, as well as specific mentions for those working remotely.

A specific section is devoted to the role of workers' representatives, which has a threefold dimension: as negotiators, as consultants and as watchdogs.

With regard to the consequences of business defaults, neither the breach of the right to disconnection nor the absence of an internal policy appear to have labour consequences, since neither has been specifically typified by the Law on Offences and Sanctions in the Social Order. However, on the contrary of those who might argue that, on the basis of the principle of typicality, the rule is not enforceable since non-compliance is not sanctioned, a view more close to the will of the legislator can be proposed, apart from its legal technique: the non-compliance should be diluted in the broader rates from which the matter is addressed, which relate to the right to rest and the limitation of working time, occupational health and the participation of workers' representatives.

All of the above converges on shaping the disconnection as a worker's right-duty, an idea that is detailed in a specific section.

Some of the first business disconnection policies agreed in large enterprises are discussed, in order to identify their core content and certain common guidelines. It is concluded that the policies analyzed fulfil the main objective of defining modalities for the exercise of the right to disconnection, although the terms are timid and cautious, even ambiguous in some of the points.

Finally, a last reflection is proposed on the opportunity to courageously take control of technological change, accepting the challenge of transforming Labour Law, as it is only in this way that it will be possible to continue applying the basic principles of our ordering, as necessary today as ever.

Keywords: Technologies; disconnection; negotiation; protocol.

Protección de datos personales y garantía de derechos digitales en el empleo público

Protection of personal data and guarantee of digital rights in public employment

FERRAN CAMAS RODA*

DELIMITACIÓN INTRODUCTORIA DEL OBJETO DE ESTE ESTUDIO

La realización de este trabajo se ancla en dos pilares, el estudio del Derecho de protección de datos personales por un lado (incluyendo la intersección de este derecho con el relativo a la intimidad respecto del uso de dispositivos digitales o tecnologías de control), y su reconocimiento al colectivo de empleados públicos por otro.

Por lo que hace al primero de los factores mencionados, se ha de recordar que el Derecho a la protección de datos es un derecho fundamental autónomo al que se le ha atribuido su anclaje jurídico en el art. 18.4 de la Constitución Española (en adelante, CE), cuyo objeto es otorgar un poder de control a todo sujeto sobre sus datos personales. Como tiene proclamado el Tribunal Constitucional, dicho derecho es autónomo respecto del Derecho fundamental a la intimidad personal y familiar reconocido en el art. 18.1 CE. Así, en su sentencia núm. 292/2000, de 30 de noviembre de 2000, consolidó la diferenciación entre ambos derechos fundamentales al decir que mientras el de intimidad busca proteger frente a cualquier invasión que pueda realizarse en dicho ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, el de protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Añadía el TC que, de forma adicional, mientras el contenido del derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión a su esfera íntima, el de protección de datos concede a su titular un haz de facultades que trasladan a los demás unos deberes "de hacer", principalmente, el derecho a que se requiera previo consentimiento para la recogida y uso de datos personales, el derecho a saber y a ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar esos datos, en definitiva, el poder de disposición sobre los datos personales (que van más allá de los estrictamente íntimos).

El desarrollo del Derecho fundamental a la protección de datos se encuentra recogido en la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Esta nueva normativa ha venido a derogar expresamente (pero de forma parcial) a su antecesora, la *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*. Al amparo de esta última norma, se adoptó el *Real Decreto 1720/2007, de 21 de diciembre*, que no ha sido eliminado expresamente por la LO 3/2008, la cual sólo prevé en su disposición derogatoria

* Catedrático de Derecho del Trabajo y de la Seguridad Social y Director de la Cátedra de Inmigración, Derechos y Ciudadanía de la Universidad de Girona.

que queden derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

La posible aplicación de aquel Real Decreto 1720/2007 debe resultar en todo caso marginal teniendo en cuenta lo que se va decir a continuación sobre la LO 3/2018, en función de la labor selección que pueda hacer el operador jurídico. En este sentido, el art. 1 de dicha Ley se ha encargado de acotar la canalización legal del Derecho fundamental de las personas físicas a la protección de datos personales al establecer que éste solo podrá ejercerse a través de lo previsto en la propia legislación orgánica y en la norma europea que se encarga de adaptar en España, que es el *Reglamento (UE) 2016/2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos.*

Del conjunto de esta normativa, y simplemente a modo de enmarque de este estudio, cabe decir en primer lugar que los datos personales que regula a efectos de su protección tienen un alcance ciertamente amplio, no solo por la propia definición que sobre ellos se hace en el art. 4.1 del Reglamento europeo, sino por la propia evolución jurisprudencial sobre su alcance, como por ejemplo lo prueba, en nuestro ámbito laboral, la Sentencia del Tribunal de Justicia de la Unión Europea (en adelante, TJUE), de 19 de junio de 2014 (C-683/13), que consideró que el registro del tiempo de trabajo, que incluye una indicación para cada trabajador del inicio y del final del trabajo y las interrupciones o descansos correspondientes, coincide con la definición de datos personales de la normativa europea.

En segundo lugar, en relación al modelo de tratamiento de los datos personales, su objeto centra en abarcar cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, "ya sea por procedimientos automatizados o no" (art. 4.2). En consecuencia, la protección dispensada lo es tanto con respecto a mecanismos basados en sistemas informáticos como los que no operen de esa forma. También el Tribunal de Justicia de la Unión Europea ha incluido como tratamiento de datos la recogida, organización, conservación, consulta y utilización de datos de tiempo de trabajo y descansos por el empleador por un lado, o la conducta consistente en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, por otro (véase la Sentencia del TJUE de 30 de mayo de 2013, Asunto C-342/12, o de 6 de noviembre de 2003, Asunto C-101/01).

En tercer lugar, y relacionado justamente con la cuestión anterior del tratamiento de datos, este solo pasa a ser lícito si está fundamentado en alguna de las condiciones que fija el art. 6 del Reglamento 2016/2016/679, entre las que se encuentra el consentimiento del interesado (letra a) del precepto), pero también otras bases jurídicas como que el tratamiento deba ejercerse en función de la ejecución de un contrato (b); por el cumplimiento de una obligación legal (c); para proteger intereses vitales del interesado u otra persona física (d); por interés público o ejercicio de poderes públicos (e); o para la satisfacción de intereses legítimos del responsable del tratamiento (f). Una primera conclusión de la lectura de este artículo es que el consentimiento del interesado es el principio para el tratamiento de datos que en primer lugar es el mencionado por el precepto, lo que está justificado por la fortaleza garantista al que se le envuelve en el Reglamento 2016/679 (como la necesidad de que tenga carácter activo o que deba ser unidireccional respecto de una finalidad determinada, como se recoge en el art. 6 de la LO 3/2018); ahora bien, pese a esa primera mención en la norma reglamentaria europea y la incrustación en el régimen propio del consentimiento de importantes garantías para su ejercicio, lo cierto es que no deja de ser una base legiti-

madora más del tratamiento de datos, compartiendo el mismo nivel de amparo para esta utilización que el resto de bases que establece el art. 6 del Reglamento 2016/679.

Dicho todo lo anterior relativo a la normativa de protección de datos, este estudio va a tratar con que alcance es aplicable al régimen de empleados públicos, partiendo del modo como están calificados en el *Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público* (RDL 5/2015). Como establece esta normativa, su ámbito de aplicación se focaliza en el personal funcionario por un lado, y en lo que proceda en la propia norma al personal laboral al servicio de las Administraciones Públicas por otro (es decir, respecto del personal laboral se le aplica lo establecido en el RDL 5/2015, y lo que proceda en el *Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores* –LET–, o en su normativa de desarrollo).

Para empezar, se ha de señalar que la normativa de protección de datos española prevista en la LO 3/2018 ha residenciado en su seno la regulación de determinados derechos a la intimidad derivados del uso de dispositivos digitales, es decir, no los ha emplazado en la LET o en el RDL 5/2015, más allá del propio reconocimiento genérico de aquellos. Cuestión no baladí ya que la visión protectora no solo de la intimidad, sino también de la protección estricta del régimen de protección de datos respecto de los dispositivos digitales, queda más visible y garantizada al regularse prioritariamente en la LO 3/2018, que de haberlo hecho en la legislación laboral.

Tanto en la LET como en el RDL 5/2015 se ha incluido un redactado parecido, donde focalizando nuestra atención en los empleados públicos, se ha incluido en el art. 14.j bis) del RDL 5/2015 el reconocimiento al derecho individual "a la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales". Se trata de una misma garantía que la prevista para los trabajadores sometidos a la legislación laboral en el ámbito privado, con el pequeño matiz en el redactado de que mientras a aquellos la norma les reconoce el derecho a la intimidad frente a los equipamientos de control o geolocalización instalados por su empleador, en el RDL 5/2015 no se habla de este último sujeto activo, sino que a tenor del precepto la privacidad del trabajador lo seria ante cualquier mecanismo de control instalado fuera quien fuese el responsable de su instalación; en todo caso, de la lectura de los preceptos correspondientes que concretan esos derechos en la LO 3/2018, la cobertura de la protección de la intimidad y protección de datos personales es similar a ambos colectivos.

En segundo lugar, como se acaba de mencionar, el régimen de uso de dispositivos digitales, utilización de aparatos de vigilancia o geolocalización, o el derecho a la desconexión digital se residencia en la normativa específica de protección de datos español integrando de forma expresa en una misma regulación común el ejercicio de esos derechos por trabajadores del sector privado y empleados (en régimen laboral o de función pública) que prestan sus servicios para la Administración pública). En cambio, eso no sucede respecto a la regulación del Derecho a la protección de datos personales, en la que no hay una mención directa a su ejercicio por ambos colectivos en el ámbito laboral.

Naturalmente, se ha de confirmar que la normativa de protección de datos personales prevista en el Reglamento 2016/679 y en la LO 3/2018 reconoce y ampara el correspondiente derecho respecto de las personas físicas, también naturalmente en tanto éstas ejerzan una prestación de servicios tanto en el ámbito privado como en el público. Ahora bien, reconocido ese principio su aplicación deviene más compleja en contextos laborales,

ya que, como se va a comprobar, no se ha realizado una diferenciación general y expresa entre trabajadores del sector privado y personal del sector público en materia específica de tratamiento de datos personales y el modo de ejercer los derechos que puede derivar de dicha pertenencia. De hecho, centrándonos en el empleo público, ni la normativa europea ni la española de protección de datos han delimitado su regulación entre personal laboral al servicio de la Administración pública y funcionarios públicos, cuando el régimen jurídico de trabajo de ambos es diverso. Sólo en situaciones específicas va a adoptarse una regulación aplicable al sector público que lo va a diferenciar del sector privado, lo cual, por tanto, añadirá singularidades en el régimen de protección de datos del personal laboral en la Administración Pública respecto del mismo tipo de empleado asalariado en las empresas privadas.

En este sentido, el análisis de bajo que fundamentos pueden las Administraciones Publicas tratar los datos personales de sus empleados públicos, y con que alcance se dispone su protección en función del colectivo en concreto al que se dirija dicho tratamiento, es a lo que se van a dedicar los dos siguientes apartados.

1. LAS BASES LEGITIMADORAS DEL TRATAMIENTO DE DATOS EN EL EMPLEO PÚBLICO

Como ha sido anteriormente objeto de comentario, el tratamiento lícito de datos personales exige su justificación en uno de los fundamentos previstos en el art. 6 del Reglamento 2016/679. Por tanto, una de las primeras cuestiones de interés respecto al tratamiento por la Administración publica en tanto que empleadora de los datos del personal a su servicio, lleva a hacer un ejercicio sobre qué tipo de base legitimadora de entre las listadas en el precepto reglamentario da cobertura a dicha actuación.

En primer lugar, se encuentra la condición o justificación del tratamiento basada en el consentimiento del interesado para uno o varios fines específicos. Este, no obstante, no debe ser por regla general el fundamento para tratar los datos personales del empleado público en cuanto tal, ni de los trabajadores que prestan su servicio en el sector privado. Como ha sido objeto de análisis respecto del consentimiento, partiendo del hecho de que en el contexto del empleo se produce un desequilibrio de poder[1], dada la dependencia que resulta de la relación entre el empleador y el empleado, no es probable que el interesado pueda negar a su empleador el consentimiento para el tratamiento de datos sin experimentar temor o riesgo real de que su negativa produzca efectos perjudiciales. En este sentido, debido a que es probable que ante la petición de la parte empresarial de un tratamiento de datos a petición sobre la base del consentimiento, este no se otorgue libremente por su personal, se concluye que en el ámbito del trabajo, la base jurídica no puede y no debe ser el consentimiento de los trabajadores [artículo 6, apartado 1, letra a)] debido a la naturaleza de la relación entre empleador y empleado[2].

De hecho, el propio Considerando 43 del Reglamento 2016/679 alerta de que el consentimiento no debe constituir un fundamento jurídico válido del tratamiento de datos de carácter personal en aquel caso concreto en los que exista un desequilibro claro entre el interesado y el responsable del tratamiento, ello en particular, añade el considerando, cuando "dicho responsable sea una autoridad pública". En mi opinión, el Considerando no se

[1] Grupo de trabajo del artículo 29 sobre Protección de Datos. 17/ES WP259 y rev.01: Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/2016/679. Adoptadas el 28 de noviembre de 2017 revisadas por última vez y adoptadas el 10 de abril de 2018.

[2] Grupo de trabajo del artículo 29 sobre Protección de Datos. 17/ES WP259 y rev.01: Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/2016/679. Adoptadas el 28 de noviembre de 2017 revisadas por última vez y adoptadas el 10 de abril de 2018. Así se expresaba también, pero con referencia a la Directiva 95/46/CE, sobre protección de datos, el mismo Grupo de Trabajo en su Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017.

está refiriendo específicamente a la actuación de dicha autoridad en tanto que empleadora, pero en todo caso puede valer la referencia orientativa del considerando para descartar que, en el contexto de prestación de servicios de un empleado público respecto de la Administración para la que presta sus servicios el consentimiento sea el fundamento básico y general del tratamiento de datos.

En segundo lugar, se ha de expresar que el art. 6.1b) del Reglamento 2016/679 establece como base legitimadora del tratamiento de datos, el que éste sea necesario para "la ejecución de un contrato" en el que el interesado es parte o para la aplicación a petición de este de "medidas precontractuales".

Respecto de los trabajadores que prestan sus servicios para el sector privado y también, por lo que hace referencia a nuestro ámbito de estudio, el personal laboral de las Administraciones públicas, el cual como dice el RDL 5/2015, presta sus servicios para éstas en virtud de un "contrato de trabajo" (art.11), queda claro que la condición prevista en el art. 6.1b) del Reglamento 2016/679 puede ser una de las que da cobertura al tratamiento de datos personales de dicho personal laboral en tanto que empleado público.

Cuestión más compleja es lo que sucede con otro tipo de empleados públicos, en concreto los funcionarios de carrera u aquellos otros sometidos a su mismo régimen. Se ha de recordar que según el art. 9 del RDL 5/2015, funcionarios públicos son aquellos quienes, en virtud de nombramiento legal, están vinculados a una Administración Pública por una relación estatutaria regulada por el Derecho Administrativo para el desempeño de servicios profesionales retribuidos de carácter permanente. Por tanto, el régimen estatutario de los funcionarios públicos no se basa en la realización de una relación contractual, eje sobre el que se sustenta el fundamento para la protección de datos del art. 6.1b) del Reglamento 2016/679. Ello podría significar que esta base legitimadora resultara inválida para el tratamiento de datos personales por la Administración de los funcionarios públicos o aquellos otros empleados cubiertos por su mismo régimen, para la cual prestan sus servicios.

En todo caso, a los efectos de quebrar esa interpretación restrictiva deben tenerse en cuenta varios argumentos que apoyarían que la "ejecución de un contrato" como uno de los fundamentos a utilizar para el tratamiento de los datos personales de los funcionarios públicos. Para empezar, tradicionalmente ese anclaje contractual ha sido el utilizado también por nuestra normativa en relación a los datos personales de los empleados públicos, incluyendo a los funcionarios públicos: téngase en cuenta que así se venía haciendo al amparo del art. 6.2 de la Ley 15/99 ya derogada, así como también por el art. 10.3b) del Real Decreto 1720/1999, según el cual, los datos de carácter personal pueden tratarse sin necesidad del consentimiento del interesado cuando se recaben por el responsable del tratamiento "con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento". Considero que este precepto reglamentario integraría la aplicación de la base legitimadora prevista en el art. 6.1b) del Reglamento europeo para validar su aplicación en el caso de los funcionarios públicos.

A mi modo de ver, el objetivo del art. 6.1b) del Reglamento 2016/679 es englobar de forma general los supuestos de tratamiento de datos en contextos profesionales o de empleo. La norma no habría llegado al punto de delimitar estatutos específicos (laborales o de función pública) dentro de ellos, ya que asume una óptica aplicativa global, en el sentido de legitimar el tratamiento de datos por una parte empleadora en relación al personal que le preste servicios laborales, cualquiera que sea el régimen jurídico bajo el que lo haga.

La validez que predico de la ejecución contractual como fundamento del tratamiento de datos en el marco de una relación de prestación

de servicios entre empleados públicos-funcionarios y Administración pública-empleadora no debe esconder el hecho de que, con la normativa adoptada en el ámbito europeo y española, la base regulada en el art. 6.1b) del Reglamento 2016/679 ha reducido su margen de actuación en el tratamiento de datos en el sector público (aquí también incluyendo a su personal laboral), como va a comprobarse a continuación.

El tratamiento de datos personales de los empleados públicos puede basarse en esa base legitimadora relativa a la ejecución de contrato, entendido como una relación negocial o de empleo (art. 6.1b) del Reglamento 2016/679), pero no es la única que lo puede amparar. En particular, hay un ámbito en el que aquella base ha cedido paso a otra para tratar determinados datos: según la Disposición adicional duodécima de la LO 3/2018, los tratamientos de los registros de personal del sector público se entenderán realizados "en el ejercicio de poderes públicos" conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento 2016/679 [esta letra ampara el tratamiento de datos cuando sea necesario por "interés público" o en el "ejercicio de poderes públicos" conferidos al responsable del tratamiento]. La Disposición citada de la LO 3/2008 añade en su segundo apartado que los registros de personal del sector público podrán tratar datos personales relativos a "infracciones y condenas penales e infracciones y sanciones administrativas", limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines. No sólo respecto de los "registros del personal" puede la Administración tratar datos personales correspondiente a sus empleados, sino que también se ha impuesto la obligación a las autoridades públicas a que respecto del "registro de actividades" de tratamiento de datos personales que realizan, identifiquen quién trata los datos, con qué finalidad y qué base jurídica legitima ese tratamiento (véase la modificación de la LO 3/2018 de la Ley 19/2013**,** de 9 de diciembre, *de transparencia, acceso a la información pública y buen gobierno,* que será objeto de estudio con posterioridad).

La Disposición Adicional Duodécima de la LO 3/2018 justifica que la Autoridad pública trate los datos (en especial, infracciones y sanciones imputadas a aquellos) incluidos en los registros del personal del sector público, tanto laboral como funcionario, bajo la base del interés público o el ejercicio del poder público. Dicho precepto cumple así el propio requerimiento previsto en la LO 3/2018 de que un tratamiento de datos solo pueda considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable "cuando derive de una competencia atribuida por una norma con rango de ley" (art. 8.2). De hecho, el requerimiento inscrito en el art. 8.2, la LO 3/2018 da cumplimiento a lo exigido por el art. 6.2 del Reglamento 2016/679, que regula una serie de requisitos adicionales a la justificación del tratamiento de datos cuando su referencia es el interés público o el ejercicio del poder público, o también el cumplimiento de una obligación legal, entre otras, la necesidad de que la base de dicho tratamiento venga establecida por el Derecho de la Unión o de un Estado miembro, o que la finalidad del tratamiento quede determinada en la propia norma de cobertura.

El objetivo de este marco limitador de la utilización del interés público o el ejercicio de poderes públicos seria restringir su campo de actuación como base legitimadora para el tratamiento de datos, ya que no dejan de ser nociones de carácter determinado reconocidos a la Administración Pública en contextos sensibles como pueden ser los de carácter laboral, que reclaman que las circunstancias en las cuales se reconozca la pertinencia de dichas bases legitimadoras sean muy limitadas[3].

Esa limitación al uso del interés público o el ejercicio de poderes públicos como fundamentos del tratamiento de datos no sólo es de

[3] Groupe de travail «Article 29» sur la protection des données (5062/01 FR/Final WP 48): Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel. Adopté le 13 septembre 2001.

carácter formal, en el sentido de que ello deba ser autorizado por una ley, sino también en un sentido sustantivo: el tratamiento datos del Registro debe realizarse cuando sea necesario, o como dice la ley, respecto de los datos estrictamente necesarios para el cumplimiento de sus fines. Por ello, si un determinado tratamiento no es "necesario" para el cumplimiento de la misión realizada en interés público o en el ejercicio de los poderes públicos conferidos por el ordenamiento, dicho tratamiento no sólo carecería de base jurídica suficiente legitimadora prevista en el art. 6.1e) del Reglamento 2016/679, sino que, además, infringiría el principio de minimización de datos contenido en el artículo 5.1.c) de la propia norma, aplicable igualmente a los tratamientos de datos llevados a cabo por la Administración pública[4].

En todo caso, el tratamiento de datos bajo la cobertura del interés público o el ejercicio de poderes públicos no solo se ha regulado en relación a los registros de personal, sino también respecto del denominado Derecho a la limitación del tratamiento del art. 18 del Reglamento 2016/679, en el marco de procedimientos de personal. En virtud del art. 18.1 del Reglamento 2016/679 se prevé que los interesados (incluidos por tanto quienes prestan sus servicios como empleados públicos) tengan derecho a la limitación del tratamiento de datos por el responsable (la Administración Pública) en una serie de supuestos, como cuando se impugne la exactitud de aquellos; o el tratamiento sea ilícito y el interesado se haya opuesto a su supresión; o el responsable ya no los necesite pero el interesado sí, o el interesado se haya opuesto al tratamiento. Pese a esa limitación, el propio reglamento europeo permite que se traten esos datos, entre otras bases, por razones de un interés público importante de la Unión o de un determinado Estado miembro.

Esa permisión ha sido recogida por la LO 3/2018, la cual ha establecido en el apartado 3 de su Disposición Adicional duodécima autoriza que los datos cuyo tratamiento haya sido limitado, puedan ser no obstante tratados cuando sea necesario para el desarrollo de los procedimientos de personal en razón del interés público.

En conclusión, la base legitimadora para el tratamiento de datos en interés público o en el ejercicio de poderes públicos, pese a la restricción que su naturaleza impone en la justificación de dicho tratamiento y en los datos a tratar, se está erigiendo en un fundamento importante respecto del personal, ya sea laboral, ya sea funcionario, que presta servicios para las Administraciones públicas, de forma que progresivamente va ampliando su campo de aplicación en este ámbito. Como se ha visto, facetas importantes como son los registros de personal, los procedimientos en el marco de expedientes de tratamientos limitados de datos, e incluso, como se verá posteriormente, las informaciones públicas sobre determinados datos conectados al puesto de trabajo de los empleados públicos están recayendo bajo su amparo.

En tercer lugar y último lugar, otros fundamentos que el Reglamento 2016/679/2018 prevé para el tratamiento de los datos personales son aquel que es que aquel sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (art. 6.1c), base que tiene su importancia en el ámbito laboral, donde a la Administración pública en tanto que empleadora puede estar obligada a tratar y comunicar datos con otras autoridades como las que tienen competencias de fiscalidad o de Seguridad Social[5].

También se ha de analizar la hipotética concurrencia en materia de empleo público de la base legitimadora del tratamiento de datos consistente en la satisfacción de "inte-

[4] Agencia Española de Protección de Datos. Gabinete Jurídico. N/REF 010601/2019.

[5] Véanse las explicaciones sobre esta base legitimadora en: Groupe de travail «Article 29» sur la protection des données (5062/01 FR/Final WP 48): Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel. Adopté le 13 septiembre 2001.

reses legítimos" perseguidos por el responsable del tratamiento (art. 6.1f) del Reglamento 2016/679). Dicho precepto, añade, en todo caso, que este fundamento "no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones". Esta coletilla cerraría la puerta a la utilización de la condición del interés legítimo como fundamento del tratamiento de datos por la Administración Publica. En todo caso, hay opiniones que no dejan cerrada la puerta a que ello sea así, en particular derivadas de la Agencia Española de Protección de Datos (AEPD), en cuyo ámbito se ha sostenido que la Administración no puede utilizar como base jurídica del tratamiento el interés legítimo, pero con una condición: siempre que se entienda que otro de los fundamentos del Reglamento europeo, en particular el relativo al "interés público", se interprete de forma que permita a las Administraciones los tratamientos de datos personales necesarios para las finalidades legítimas que el ordenamiento les concede o permite incluso en el ámbito del Derecho Privado[6]. En este sentido, tras la entrada en vigor del Reglamento europeo y de la LO 3/2018 considero de interés señalar la amplitud que estaría adquiriendo el fundamento del interés público o el ejercicio de poderes públicos, ya que, por ejemplo, el *Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones*, utilizaría aquellas bases legitimadoras en relación al tratamiento de datos derivados de todas las fases de contratación, licitación y ejecución del contrato de la Administración con contratistas y subcontratistas (véase el art. 5 de dicho Real Decreto-ley).

Por mi parte, considero que en el ámbito del empleo público, la utilización del "interés legítimo" de la Administración público para tratar datos de sus empleados está vetado por el propio Reglamento europeo, al margen de que se conceda más o menos amplitud a otra base, la del "interés público", que en materia de prestaciones laborales no puede ser concebido como una base legitimadora general sino ceñida a situaciones de tratamiento específicas.

2. LA APLICACIÓN A LOS EMPLEADOS PÚBLICOS DEL RÉGIMEN DE TRATAMIENTO DE DATOS EN EL ÁMBITO LABORAL

El Reglamento 2016/2016/679 dispone de una serie de reglas de interés en materia de tratamiento de datos personales en el contexto profesional o derivada de relaciones de trabajo. Con ello se confirma la relevancia de la aplicación de la normativa de protección de datos personales en dicho ámbito[7].

De forma específica, el art. 88 del Reglamento europeo, que lleva por epígrafe, "Tratamiento en el ámbito laboral", otorga a los Estados miembros la posibilidad (aunque la doctrina iuslaboralista ve en ella una exigencia[8]), de que a través de disposiciones normativas o de convenios colectivos pactados entre los empleadores y la representación de los trabajadores, se establezcan 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 sobre una serie de ámbitos que se acogen en el propio precepto.

La primera cuestión que interesa a este estudio es si este precepto, que centra su objeto en el ámbito laboral, y su sujeto en los trabajadores, es aplicable, más allá de los empleados

[6] Informe del Gabinete Jurídico de la Agencia Española de Protección de Datos sobre la base jurídica para el tratamiento de datos. Ampliación del Informe emitido en los expedientes 108/2018 (ref. 181577/2018) y 155/2018 (ref. 200012/2018).

[7] JESÚS BAZ RODRÍGUEZ: *Privacidad y protección de datos de los trabajadores en el entorno digital*. Wolters Kluwer España, S.A., Madrid, 2019.

[8] *Idem*.

públicos de carácter laboral, también a los funcionarios públicos. Ese precepto, el art. 88 del Reglamento 2016/679, tendría su fuente de explicación en el Considerando 155 de la propia norma, en el que se explica como el Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador u otros fines. En este sentido, considero que la respuesta a la pregunta planteada debe ser afirmativa por cuanto el espíritu que subyace al precepto es general, es decir, se busca referenciar determinados aspectos en el marco de u "contexto laboral" en el que se producen desequilibrios entre las partes por la relación de trabajo establecida, y por tanto, el precepto es aplicable a cualquier relación de prestación de servicios entre empleado y administración. De hecho, así lo entiende también la legislación española concretada en la LO 3/2018, ya que, como al efecto se verá posteriormente, cuando regula determinados derechos digitales también bajo el paraguas del "ámbito laboral", lo hace incluyendo de forma expresa a trabajadores y empleados públicos (y, por tanto, también a empleados con una relación administrativa). Por otra parte, el art. 91 de dicha legislación orgánica, relativo a los derechos digitales en la negociación colectiva, establece que los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral. Esa referencia al tratamiento de datos y a los derechos digitales de análisis posterior como objeto de regulación de la negociación colectiva, lo son tanto para los empleados como para los funcionarios públicos que también tienen reconocido ese derecho colectivo (de hecho, los derechos digitales que regula la LO 3/2018 son aplicables tanto a los trabajadores sometidos a la legislación laboral como a los funcionarios amparados por la legislación de función pública).

Siguiendo con el alcance del art. 88 del Reglamento 2016/679, la posibilidad de que los Estados miembros o los pactos colectivos (incluidos, por tanto, los aplicables a los funcionarios públicos) especifican mayores garantías para el tratamiento de datos personales respecto de determinas materias que aparentemente pertenecen más al Derecho del Trabajo en su vertiente privatista que al Derecho de la función pública, como son la contratación de personal, o la ejecución del contrato laboral, o la extinción de la relación laboral. A mi modo de ver, estas materias son citadas en el art. 88 de forma ejemplificativa, y por tanto podría sostenerse que la aplicación de las garantías previstas por el precepto iluminarían otros ámbitos más allá de los que estrictamente expresa, donde podrían incluirse materias propias del régimen administrativo de los funcionarios públicos; en todo caso, debería considerarse también el significado extenso de nociones como contratación de personal, ejecución del contrato laboral, aplicables de forma análoga a situaciones propias de la función pública, como el nombramiento de un funcionario o la ejecución de su relación de servicios u otras condiciones de trabajo.

Finalmente, la posibilidad de mayor especificación por parte del Derecho de los Estados miembros o la negociación colectiva se hace con el objeto de garantizar la protección de los derechos del empleado, no para disminuir el alcance de las reglas que estén incluidas en el Reglamento. Por tanto, la normativa aprobada por el Estado español o los pactos colectivos (también reconocidos a los funcionarios públicos que puedan alcanzar las partes sociales podrán regular aspectos no previstos en el Reglamento, o concretar aquellos que resulten incluidos, pero bajo la óptica de salvaguardar el derecho a la protección de datos del trabajador.

2.1. Especificaciones de la normativa de protección de datos sobre las relaciones de empleo en el sector público

De lo analizado hasta ahora, el Reglamento 2016/679 y la LO 3/2018 son aplicables a las relaciones de los empleados públicos, en el ámbito del tratamiento de datos conforme a los criterios que se han estudiado. La idea que subyace a dicha regulación es que tiene un alcance general, ya que, de hecho, debe aplicarse a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 2.1 de la Ley 3/2018).

Lo anterior viene a cuento, de forma singular, por el hecho de que en el antiguo RD 1720/2017 se preveía que la normativa de protección de datos personales entonces vigente no era aplicable a "los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales", y por tanto el empleador podía utilizarlos sin limitaciones; en cambio, con la actual regulación de protección de datos esa cuestión si ha pasado a formar parte del ámbito normativo garantista en su tratamiento. Así, el art. 19 de la LO 3/2018 prevé que, salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento 2016/679 ["intereses legítimos" del responsable], el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica, siempre que dicho tratamiento se refiera únicamente a los datos necesarios para su localización profesional, o que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

En todo caso, como se ha dicho anteriormente, dicho tratamiento por la Autoridad Pública de los datos de contacto o de función laboral de los empleados, en concreto de los que prestan servicios a la Administración pública, no puede estar cubierto por la base legitimadora de los "intereses legítimos" (art. 6.1f) del Reglamento 2016/679). El fundamento que podría encajar ese tratamiento seria el que avanza el artículo 86 de la propia norma europea que, en función del interés público, permite la comunicación por las autoridades de los datos personales que dispongan con el acceso público a los documentos oficiales donde se contengan, por tanto, al amparo del art. 6.1e) del Reglamento 2016/679.

Al amparo de esa regulación, la cuestión de la información pública de los datos de los empleados públicos está recogida en la LO 3/2018, cuya Disposición Adicional Segunda dispone que "la publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica". Por lo tanto, el acceso público a la información que contenga datos personales de personal empleado para la Administración pública, que venga regulada por el Estado o la Comunidad Autónoma en función de sus competencias, se reenvía a su sometimiento a los efectos del tratamiento de datos, desde la LO 3/2018, entre otras normas (incluyendo ella misma), a lo dispuesto a la *Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

El objeto del art. 15 de la Ley 19/2013 es amparar, como regla general, la información pública de los datos referidos directamente a la realización de puestos de trabajo que ocupa cada empleado, sin perjuicio de las reservas

que el propio precepto establece[9]. Enlazando con dicha normativa de información pública, debe mantenerse la opción legal por la publicación de las relaciones de los puestos de trabajo de las Administraciones públicas (con las precauciones del art. 15 de la Ley 19/2013). De hecho, el art. 74 del RDL 5/2015 prevé, de forma general, que sean públicas las relaciones de puestos de trabajo u otros instrumentos organizativos[10]. Otras cuestiones específicas como pueden ser las retribuciones de un determinado puesto de trabajo han sido objeto de análisis en 2015 por la AEPD y el Consejo de Transparencia y Buen Gobierno, del Gobierno de España[11], quienes han abogado por la posibilidad de ser sujetas a información pública, si las partidas correspondientes no estén ligadas a una persona en concreto (por ejemplo, trienios o complementos de productividad[12]), y de forma prioritaria, a modo de gradación en el tratamiento de dichos datos, respecto de los puestos de trabajo de mayor nivel de responsabilidad y mayor autonomía en la toma de decisiones, ya que en estos casos prevalece el interés público.

A reseñar también por su importancia la modificación que la LO 3/2018 ha realizado en la Ley 19/2013, respecto al derecho al acceso a la información pública sobre datos que contengan aspectos de interés en los empleados públicos como la afiliación sindical, en cuyo caso el acceso únicamente se podrá autorizar si se cuenta con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. Por tanto, en el específico ámbito del acceso a información relativa a la afiliación sindical de un empleado público la normativa otorga al consentimiento del trabajador la clave de dicho conocimiento, a diferencia del régimen general de la LO 3/2018 sobre tratamiento de datos como el de la afiliación sindical en el ámbito laboral, donde a efectos de evitar situaciones discriminatorias, no permite que con el sólo consentimiento del interesado se levante la prohibición de que sean tratado.

Otro aspecto a reseñar con interés respecto del empleo público lo constituye la Disposición adicional séptima de la LO 3/2018,

[9] De interés es la Resolución 263/2019, de 9 de mayo, de la *Comissió de Garantia del Dret d'Accés a la Informació Pública* (GAIP-Generalitat de Catalunya), en la cual se afirma que respecto de los datos del personal al servicio de las administraciones públicas (que incluyen tanto los datos identificativos de la persona, con nombre y apellidos, como los datos identificativos del cargo o puesto que ocupa dentro de la organización administrativa), la legislación catalana establece una regla general de acceso, que admite excepciones en determinados casos en atención a la concurrencia de circunstancias personales que justifiquen que el acceso resultaría extraordinariamente lesivo en cuanto a los derechos de la persona afectada. Por esa razón, admite que la administración pública (en el caso, un Ayuntamiento), deba permitir el acceso público al nombre y apellidos de las personas que ocupan puestos de trabajo. En este sentido, se remite a un informe de la Agencia Catalana de Protección de Datos en la que se dice que "desde el punto de vista de los trabajadores/as municipales es obvio que la vinculación de cada persona al puesto de trabajo que ocupa (con el detalle del grupo o categoría profesional), facilita información ocupacional de esta persona de la que se puede inferir información sobre su titulación, la retribución bruta aproximada, la localidad donde trabaja, etc.) y su divulgación puede afectar la privacidad de estas personas. En cualquier caso, se trata de personas que ocupan puestos de trabajo públicos, y, por lo tanto, dentro de sus expectativas de privacidad deben contar con la posibilidad de que cualquier ciudadano pueda identificarlos como tales".

[10] Véase el comentario sobre este extremo que se realiza en el blog *Nosoloaytos. Web oficial de Víctor Almonacid Lamelas* 2019: ¿Los datos de los empleados públicos son públicos?. 20 de mayo de 2019: https://nosoloaytos.wordpress.com/2019/05/20/los-datos-de-los-empleados-publicos-son-publicos/

[11] CTBG-AEDP: "Ley 19/2013, de 9 de diciembre (Art. 15) –Criterios de aplicación. Solicitud 1/2015 –Oficina para la Ejecución dela Reforma de la Administración (OPERA)". 23 de marzo de 2015.

[12] En todo caso, según dice el Gabinete Jurídico de la AEPD en su informe de referencia 010601/2019 sobre la cuestión de si las partidas retributivas consistentes en las cantidades abonadas en concepto de complemento de productividad pueden ser informadas a los demás funcionarios del Departamento u Organismo interesado, la respuesta es afirmativa en función de que así lo establece expresamente el artículo 23.3.c) de la Ley 30/1984, de 2 de agosto, de medidas para la reforma de la Función Pública. Añade además que, como recuerda el informe de la Agencia 13/2019, no procederá su comunicación a los representantes sindicales, al haber sido derogado tácitamente el último inciso del citado precepto por el artículo 40 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público.

sobre el régimen de identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos, lo que por ejemplo resulta de interés en procedimientos de selección de personal. En este sentido, dicha norma establece, entre otras cuestiones, que cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente[13]; mientras que cuando se trata de notificación por medio de anuncios (particularmente en casos de notificaciones infructuosas reguladas por el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas), se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

La norma considera excesivo identificar a una persona con nombre y DNI en publicaciones de carácter administrativo u oficial; esto estaría en sintonía con las directrices que el propio Reglamento 2016/679 establece sobre los datos personales sean tratados bajo el principio de la minimización, o que se en relación al diseño del tratamiento se apliquen técnicas de la seudonimización (tratar datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, ex art. 4 del Reglamento).

Estos principios llevarían al que en documentos administrativos o oficiales de los que se dé conocimiento público fueran anonimizadas, excluyendo los datos de personas físicas así como que las publicaciones de resoluciones no deben contener la firma manuscrita de quién adoptó el acuerdo[14].

2.2. Protección de datos en materia de prevención de riesgos laborales

Las cuestiones de seguridad y salud en el trabajo resultarían, al tratarse de un asunto relativo a la base legitimadora de ejecución de un contrato previsto en el Reglamento 2016/679, en la forma que anteriormente se ha visto, un campo en el que el tratamiento por la parte empleadora no requeriría el consentimiento del empleado público.

La Administración pública debe cumplir su obligación de protección de la salud del empleado público conforme a los deberes específicos regulados en la *Ley 31/1995, de 8 de noviembre*, *de prevención de riesgos laborales*, que como es sabido se aplica tanto a los trabajadores reguladas por la LET como a las relaciones de carácter administrativo o estatutario del personal civil al servicio de las Administraciones públicas (art. 3)

De aquellos deberes específicos, el que mayor conflictividad plantea es el de la vigilancia de la salud del trabajador, que la normativa de prevención establece de forma general como obligatoria para el empleador para dotarla, pero voluntaria para el trabajador en aceptarla, a no ser que de forma excepcional venga exigido en aquellas situaciones que prevé la propia LPRL. En uno u otro caso, la ejecución de la medida de vigilancia de la salud es llevada a cabo por personal especialmente capacitado para ello de los servicios de prevención que disponga la parte empleadora, la cual no podrá recibir información sobre las condiciones sanitarias del trabajador más

[13] La forma de llevar a cabo esta publicación ha sido objeto de recomendación por la AEPD en el documento "Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD": https://www.aepd.es/media/docs/orientaciones-da7.pdf

[14] A. Acín Ferrer: "Protección de datos. Aplicación de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, en las entidades locales. Entidades locales-Actuaciones y responsabilidades". *La Administración Práctica* núm. 2/2019. Base de Datos Thomson Reuters Aranzadi-Instituciones: BIB 2019/654.

allá de la aptitud o ineptitud del trabajador en materia de salud a los exclusivos efectos de trabajo para los cuales se haya realizado la vigilancia[15].

En todo caso, y centrándonos en el uso de los datos personales de salud por los servicios de prevención acogidos por la parte empleadora, que si son de carácter ajeno a esta tienen la consideración de responsables del tratamiento de datos personales de los empleados, deben tener en consideración la normativa que regula este específico dato sensible: se ha de traer a colación que el art. 9.1 del Reglamento 2016/679 establece una prohibición general sobre el tratamiento de datos personales que revelen datos relativos a la salud.

En todo caso, esa prohibición queda desarbolada ante dos circunstancias, una de ellas que ampararía la vigilancia de la salud como deber específico de la parte empleadora y del servicio de prevención ajeno si ese es la organización designada por aquel, ya que la norma europea permite el tratamiento 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 o de los Estados miembros o un convenio colectivo; y en segundo lugar, como norma más pensada para los servicios sanitarios que realizan la vigilancia, cuando el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario. En este último caso, el art. 9 de la LO 3/2018 le anuda la garantía que el tratamiento de datos deberá estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

2.3. Protección de datos en el ámbito de las relaciones colectivas de trabajo

En el ejercicio de esas funciones, los representantes de los trabajadores pueden gestionar los datos de trabajadores en los Tablones de anuncios a los que tienen derecho. Al realizarlo, los responsables del tratamiento de datos en el tablón de anuncios y por tanto de las informaciones publicadas en el mismo, serán aquellos órganos que decidan sobre su uso y finalidad y sitúe materialmente la información en él. Dicha información en los tablones solo debe estar visible para aquellos a los que se dirige, los empleados públicos correspondientes, por esa razón, en caso que el tablón sea digital u on-line es fundamental que se instalen en la intranet de la empresa, nunca en Internet (véase la Sentencia de lo Contencioso-Administrativo de la Audiencia Nacional de 8 de julio de 2009).

Relacionado con lo anterior, hay que referirse al envío de información sindical a través del correo electrónico. Esta actividad requiere el tratamiento de datos personales puesto que se considera la dirección electrónica como un dato personal. De entrada, ha de recordarse que la AEPD ha elaborado unas recomendaciones sobre al tratamiento de datos personales de los trabajadores a cargo de la representación sindical en la empresa. En este sentido, la AEPD admite que en función del art. 28.1 de la CE, que reconoce como derecho fundamental la libertad sindical, y por lo tanto la acción sindical en la empresa, es adecuado a Derecho que la empresa comunique las direcciones de correo electrónico de los trabajadores a las secciones sindicales más representativas que están presentes en aquella.

[15] Según la AEPD la superación de esta estricta información se admite de forma muy limitada, estrictamente para el cumplimiento de aquellas de sus obligaciones que desborden el contenido apto/no apto, por ejemplo, si debe adaptarse una pantalla de ordenador si se constatan problemas visuales (Guía de la AEPD sobre protección de datos en las relaciones laborales de 2009 ya citada).

Ahora bien, sobre la posibilidad de que los trabajadores que reciben información digital de los sindicatos o representación social, aunque es cuestión debatida, se debería admitir la posibilidad de que aquellos soliciten su baja en la recepción de información excepto cuando se esté llevando a cabo un proceso electoral donde los trabajadores no pueden oponerse al tratamiento de sus datos personales, justamente por la preponderancia que en este asunto puede tener también el art. 28.1 de la CE, siempre que el uso que realice el sindicato se ajuste a la finalidad para la que se envían dichos correos que es la propia campaña electoral de carácter sindical.

La AEPD manifiesta en este ámbito que debe reconocerse el derecho de los trabajadores a mostrar su oposición a la recepción de mensajes con contenido sindical y, consiguiente, la obligación de los Sindicatos de cesar en el tratamiento de los datos de los solicitantes. No obstante, en lo referente a la información sindical remitida a los trabajadores en período electoral, debería considerarse la preponderancia del derecho a la actividad sindical sobre el derecho a la protección de datos. En consecuencia, los trabajadores durante el proceso electoral sindical, no pueden oponerse al tratamiento de sus datos personales, siempre que el uso que realice el Sindicato sea adecuado para los fines del propio proceso electoral[16].

En todo caso, la AEPD recuerda que existen procedimientos automatizados que pueden permitir la satisfacción del derecho a la libertad sindical sin necesidad de realizar una cesión de datos y, por tanto, minimizando los riesgos y las obligaciones de cumplimiento normativo para el empresario y el sindicato (la utilización de listas de distribución permite que el sindicato remita la información a una dirección corporativa de la empresa, sin acceso a los datos). También prevé la AEPD que la comunicación se limite a los estrictamente necesarios y que los datos se usen para la finalidad por la que son cedidos. Una vez recibidos, el Sindicato es el organismo que debe cumplir con las obligaciones de la legislación de protección de datos.

Una de las cesiones de datos más comunes es la relativa al cobro de la cuota sindical en el pago de la nómina por la empresa. La *Ley Orgánica 11/1985, de 2 de agosto, de Libertad Sindical* impone la necesidad de la conformidad del trabajador para realizarla. Puesto que se trata de una iniciativa que tiene su origen en la voluntad del trabajador, el consentimiento que da a dicha gestión puede resultar acreditado en el propio documento de afiliación sindical, en el que puede constar el tratamiento de las cesiones de datos que hubieran de realizarse entre el empresario y el sindicato para garantizar la efectividad de la forma de pago que el propio trabajador ha elegido. Por ello es válida la cesión por el sindicato al empresario de los datos identificativos del trabajador que solicita el descuento de su nómina de la cuota sindical y la cesión por el empresario al sindicato de la efectiva deducción producida en la nómina de cada uno de sus afiliados, no siendo necesaria la solicitud de un consentimiento adicional al trabajador.

Por lo que hace a la cesión o transmisión de informaciones o datos relativos a los empleados públicos, la regulación aplicable estaría configurada por la normativa reglamentaria europea (básicamente art. 6, ya analizado), la legislación laboral y sindical y el RDL 5/2015 en lo que hace referencia a las competencias de los representantes de los trabajadores sobre la obtención de información por parte de la parte empleadora y, *last but not least*, las funciones que legalmente poseen de vigilar el cumplimiento de las normas vigentes en materia de condiciones de trabajo, prevención de riesgos laborales, seguridad social y empleo.

La primera cuestión es que si la legislación atribuye a los órganos de representación de personal de competencias informativas o

[16] Agencia Española de Protección de Datos: https://www.agpd.es [En dicha página web pueden encontrarse como documentos de interés utilizados relacionados con lo que se acaba de exponer en el texto la publicación: Guía 'La protección de datos en las relaciones laborales' – 2009.

de conocimientos, ello constituirá una base, la de obligación legal, para transferirla. En todo caso, se ha alegado que partiendo únicamente de aquellas competencias legales no puede haber cesión de nóminas de los trabajadores al Comité de Empresa o a los Delegados de personal; únicamente existiría obligación de entregar los TC-1, boletín de cotización para la Seguridad Social en el que se reflejan los datos relativos a la identificación de la empresa y a la determinación de la deuda y el TC-2 en el que aparece reflejada la relación nominal de trabajadores y los datos relativos a la identificación de los trabajadores, a sus bases de cotización y a las prestaciones que les hayan sido satisfechas en régimen de pago delegado[17].

No obstante, respecto del posible amparo de cesiones masivas de datos a la representación de los trabajadores, desde la AEPD viene manteniendo una postura restrictiva en función de los parámetros normativos sobre competencias de información y vigilancia de la actividad. Se considera que la función de vigilancia y protección de las condiciones de trabajo puede llevarse a adecuado desarrollo sin necesidad de proceder a una cesión masiva de los datos referentes al personal que presta sus servicios en el Órgano o Dependencia correspondiente, y únicamente en el supuesto en que la vigilancia o control se refieran a un sujeto concreto, que haya planteado la correspondiente queja ante el órgano representativo correspondiente, será posible la cesión del dato específico de dicha persona[18]. En conclusión, según el informe de la AEPD que se reseña, de forma general no es posible una comunicación masiva a los órganos de representación de los empleados públicos, sean estos funcionarios o laborales, sino que únicamente será posible, en caso de que resulte necesario para el ejercicio de su función de control (respecto del seguimiento de una situación individualizada relativa a un caso concreto), siempre que se acreditase la correspondiente legitimación vinculada a que el sindicato en cuestión ostentara la representación de los trabajadores sobre los que solicita la información[19].

Desde la doctrina *iuslaboralista* se sostiene también la importancia del principio de proporcionalidad en los tratamientos de datos gestionados por los representantes de los trabajadores o de los funcionarios públicos, de forma que la información publicitada sea la estrictamente necesaria para ejercer con eficacia sus funciones. Así, por ejemplo, en caso de publicarse una determinada resolución administrativa o una sentencia judicial de interés para los trabajadores debería procederse a la anonimización de los datos cuando se pueda afectar a los derechos de las partes u otras personas que pudieran aparecer en ellos y la publicación de los datos carezca de relevancia desde el punto de vista de la libertad sindical[20].

3. NUEVOS DERECHOS DE CARÁCTER DIGITAL DE LOS EMPLEADOS PÚBLICOS

La LO 3/2018 ha supuesto la inclusión en la LET y en el RDL 5/2015 del reconocimiento de unos nuevos derechos para los trabajadores y los empleados públicos relacionados con el uso de dispositivos digitales, de videovigilancia, grabación de sonidos, geolocalización, así como sobre desconexión digital. En concreto, la LE 3/2008, bajo la égida su Título X de tratarse de "Garantías de los derechos digitales", ha buscado proteger la intimidad "en el ámbito laboral", incluyendo en ese campo una misma regulación tanto para trabajadores (del sector privado) como para empleados públicos.

[17] Véase la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: https://www.agpd.es [En dicha página web pueden encontrarse como documentos de interés utilizados relacionados con lo que se acaba de exponer en el texto la publicación: Guía ‹La protección de datos en las relaciones laborales› – 2009.

[18] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Gabinete Jurídico. N/REF 010601/2019.

[19] *Idem.*

[20] HUGO PRECIADO, C.: *El Derecho a la Protección de Datos en el Contrato de Trabajo.* Thomson Reuters, Cizur Menor, 2017.

En primer lugar, el art. 87 regula un derecho a la intimidad en el uso de dispositivos digitales que hayan sido puestos a disposición de los empleados públicos (por tanto, personal laboral y funcionarios públicos) por su empleador. El precepto obliga a la parte empleadora a que establezca criterios de utilización de dichos equipos con la participación de los representantes de los trabajadores, respetando en todo caso "los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente". Por tanto, en relación a la elección de la propia tecnología y el impacto que puede tener sobre los datos que recopile de los trabajadores se incorpora un único criterio, aunque no menos importante, que es el establecimiento de un estándar mínimo de protección de la intimidad del trabajador seguido a través del dispositivo. En este asunto, considero que tanto en relación a la elección de dispositivos como en su utilización debe prevalecer que tengan un impacto mínimo en el seguimiento de la persona a tenor de lo que establece el art. 25 del Reglamento 2016/679 que establece determinados criterios sobre la protección de datos desde el "diseño" del tratamiento de datos. Dicho precepto incorpora el principio de minimización de datos, así como al realizar el tratamiento de datos que solo se conozcan aquellos que sean necesarios para cada uno de los fines específicos del tratamiento. En este sentido, comparto las tesis que abogan que en función del principio de protección de datos desde el diseño se impone a que cuando los empleadores deban decidir que dispositivos tecnológicos de seguimiento del trabajo asignan a los empleados, seleccionen las soluciones más *privacy-friendly,* es decir, las más respetuosas y con simpatía por la privacidad de las personas[21].

En segundo lugar, se ha previsto un Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo en el art. 89 de la LO 3/2018. En este ámbito, se atribuye a la parte empleadora a que trate las imágenes obtenidas a través de cámaras o videocámaras para el ejercicio de sus funciones de control de los trabajadores o los empleados públicos que estén previstas en la LET o en la legislación de función pública, siempre que dichas funciones se ejerzan dentro de ese marco, y se utilicen informando previamente a los empleados públicos y, en su caso, a sus representantes.

No obstante, no podrán instalarse en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos (apartado 2 del precepto), y en el caso de equipos de grabación de sonidos, solo se admitirán cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas en función de la actividad desempeñada en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima (apartado 3 del precepto).

El análisis de este campo de la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos no puede permanecer al margen de la doctrina judicial que la ha ido encauzando. Así, la normativa ha venido a validar la permisión judicial a la instalación de tecnologías audiovisuales de vigilancia, respetando el margen que corresponda los derechos fundamentales que al trabajador también le corresponden, como el de intimidad personal o el de protección de datos.

Esa admisión de la instalación permanente de cámaras de vigilancia se condicionaba, en materia de intimidad del trabajador, al hecho de que no se implanten en espacios íntimos o de privacidad del trabajador en la empresa y que aquellos hayan sido previamente informados de ello. Por tanto, las cámaras de vigilancia podían implantarse tanto en el lugar en el que trabaja el empleado, como en aquellos espacios restringidos a terceros de la empresa, pero a las que acudiesen los trabajadores del establecimiento, aunque solo sea para tomar un refrigerio. La vigilancia en es-

[21] The working party [article 29 Data Protection Working Party]: *Opinion 2/2017 on data processing at work*, Adopted on 8 June 2017.

tos casos se admitía si la empresa puede argüir argumentos para ello, como la protección del patrimonio empresarial, y siempre que los trabajadores lo supiesen, por ejemplo, por existir carteles indicadores de ello (véase, por ejemplo, la STS de 17 de Julio de 2016. Nº de Recurso: 3233/2014).

Por lo que hace referencia al tratamiento de los datos personales derivados de la instalación de aparatos receptores de imágenes a en el lugar de trabajo, el Tribunal Constitucional había dictaminado en su sentencia 39/2016, de 3 de marzo de 2016, dos cuestiones que son de interés, si es necesaria la búsqueda de un consentimiento "expreso" del trabajador para realizarlo y la información a suministrarle. En lo que se refiere al consentimiento, el Tribunal manifestó que no se requiere de ningún consentimiento "expreso" o específico del trabajador para el tratamiento de las imágenes que han sido obtenidas a través de las cámaras instaladas en la empresa con la finalidad de seguridad o control laboral, ya que se trata de una medida dirigida a controlar el cumplimiento de la relación laboral y es conforme con el art. 20.3 del texto refundido de la Ley del estatuto de los trabajadores, que establece que «el empresario podrá 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 humana». Para el TC, el consentimiento se entiende implícito en la propia aceptación del contrato que implica reconocimiento del poder de dirección del empresario. Por lo demás, el hecho de que no se exija consentimiento expreso o específico para tratar los datos necesarios para el cumplimiento de la relación laboral abarca también los datos personales obtenidos por el empresario al controlar el cumplimiento de las obligaciones laborales del trabajador.

De hecho, en su Sentencia de 3 de marzo de 2016 el TC avala que puede ser suficiente para respetar el derecho fundamental a la protección de datos previsto en el art. 18.4 de la Constitución española el cumplimiento de la obligación informativa a través de la colocación de distintivos en lugares visibles para el trabajador, que puedan mostrar que estos sabían de la existencia de las cámaras y la finalidad para la que habían sido instaladas. Esta doctrina la ha acabado asumiendo, aunque considero que de forma más reforzada, la LO 3/2018, según lo cual los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la adopción de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Ese deber informativo solo dispone de una atenuación, atinente a un caso particular[22], que es que como consecuencia de la comprobación por las videocámaras, se capte la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos, en cuyo caso dice el art. 89 que se entenderá cumplido aquel deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de la propia LO 3/2018 (que regula el contenido de un dispositivo informativo en lugar suficientemente visible). En consecuencia, para implantar estos mecanismos no es obligado que el empleador deba contar con el consentimiento de los trabajadores, ya que la finalidad de su instalación y tratamiento estarían enfocados al control estricto de la actividad laboral de los trabajadores, pero en cambio si es necesario que éstos resulten previamente informados de su puesta en práctica[23]. El enfoque garantis-

[22] Dice FERNÁNDEZ ORRICO que otra cosa diferente al régimen general de información prevista en el precepto, como consecuencia de la comprobación por las videocámaras de vigilancia general y no específica del control de los trabajadores, se capte la comisión flagrante de un acto ilícito, en cuyo caso es cuando el deber de informar se entiende cumplido con la imagen distintiva que regula la normativa (véase "Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre". En *Revista Española de Derecho del Trabajo* núm. 222/2019, BIB 2019/7744 de Base de Datos Thomson Reuters Aranzadi).

[23] También derivado de la evolución judicial debe confirmarse que la información a los trabajadores ha de ser clara en lo que respecta la política de la empresa en cuanto a utilización del correo electrónico e Internet, describiendo de forma pormenorizada en qué medida los trabajadores pueden utilizar

ta sobre la necesidad de que los trabajadores vean reconocidos su derecho a la vida privada en el trabajo con el requerimiento al empresario de informar debidamente a los trabajadores cuando son objeto de videovigilancia, ha sido mantenido por las sentencias de la Corte Europea de Derechos Humanos en el asunto Barbulescu, especialmente de la de 5 de septiembre de 2017, así como también de su sentencia de 17 de octubre de 2019, en el asunto Lopez Ribalda[24].

En tercer lugar, se reconoce un Derecho a la intimidad del trabajador cuando el empresario utilice sistemas de geolocalización para controlar la actividad del trabajador (art. 90). Para hacerlo, deberá informar previamente a aquél de las características del dispositivo. De la misma forma que en materia de videovigilancia, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos, así como acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Respecto de los sistemas de geolocalización, pueden aparecer conflictos derivados tanto de la intimidad del trabajador como del tratamiento de sus datos particularmente en el caso de los empleados móviles que puedan ejecutar sus servicios fuera de los locales o sedes centrales de trabajo con dispositivos digitales de geolocalización, da en el bajío el conocimiento constante por el empleador del lugar en el que se localiza el trabajador. También el hecho de que en la ejecución de su trabajo se hagan depender los objetivos que tengan asignados de la ubicación en que se encuentran en cada momento, es decir que deban ir modificando sus cometidos laborales en función de las ordenes empresariales basadas en su localización territorial y horaria. Sin lugar a dudas, la geolocalización en función de sistemas GPS son un factor más en la trazabilidad del trabajo[25], es decir, de los movimientos, pausas, rendimiento, resultados de los encargos del trabajador, que tienen indudables efectos laborales.

Varias han sido las sentencias que han resuelto cuestiones en las que se encontraban involucrados dispositivos de GPS, en primer lugar la del *Tribunal Superior de Justicia de Asturias de 3 de octubre de 2017* (Rec. 1908/2017)[26], que resuelve el despido de un comercial por falta muy grave consistente en la comisión de faltas repetidas e injustificadas de asistencia o puntualidad al trabajo, al imputársele que a partir de una hora determinada del mediodía no realice visita alguna y apenas desempeñe actividad laboral de ningún tipo, complementado por el hecho de haberse detectado no haber iniciado nunca su trabajo antes de las 8,40 h/am. La sentencia considera acreditado el despido con la base del informe elaborado por la empresa en función de la geolocalización del actor. En todo caso, el trabajador no cuestionó ni en la instancia ni en sede

los sistemas de comunicación de la empresa con fines privados o personales– Véase sobre este particular CAMAS RODA, F.: «La intimidad y la esfera privada del trabajador ante las nuevas modalidades de control y vigilancia de la actividad laboral». en AA.VV.: *Nuevas tecnologías de la Información y la comunicación y Derecho del Trabajo* (Coordinado por M.R. ALARCÓN CARACUEL y R. ESTEBAN LEGARRETA), Editorial Bomarzo, Alicante, 2004, pp. 161-186.

[24] Como dice el Pr. EDUARDO ROJO al comentar esta sentencia, se refuerza la importancia del derecho a la información de la persona trabajadora, ya que como afirma la Gran Sala, "solo un imperativo preponderante relativo a la protección de los intereses públicos o privados podría justificar la ausencia de la información anterior" (véase su entrada de blog: "Medias verdades y fake news en el mundo jurídico. No cabe todo en la videovigilancia de una persona trabajadora. A propósito de la sentencia "López Ribalda" de la Gran Sala del TEDH de 17 de octubre de 2019 (y recordatorio de la sentencia de Sala de 9 de enero de 2018 y del caso Barbulescu II, sentencia de Gran Sala de 5 de septiembre de 2017": https://www.rojotorrecilla.es (23 de octubre de 2019).

[25] MURO, Ignacio: "Trazabilidad del trabajo: el futuro ya está aquí",en: https://economistasfrentealacrisis.com/trazabilidad-del-trabajo-el-futuro-ya-esta-aqui/

[26] Véase en la página web del Poder Judicial (aparado Jurisprudencia): http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8173816&links=%221908%2F2017%22&optimize=20171023&publicinterface=true

de recurso de suplicación la licitud de la prueba de geolocalización utilizada por la empresa para llevar a cabo el registro y seguimiento de su actividad laboral, lo que deja sin respuesta que hubiera sucedido en sentido contrario, es decir, si se hubiera impugnado en función de la utilización del GPS como sistema de control o fin de la jornada, como mecanismo de seguimiento de las actividades del trabajador, o en cuánto dispositivo que puede tenerlo controlado incluso fuera de su horario laboral.

Hay que recordar que el art. 20.3 de la LET puede fundamentar la adopción de un sistema tecnológico como el de la geolocalización como medida de vigilancia y control del trabajador en el cumplimiento de sus obligaciones laborales. Ahora bien, este precepto únicamente ampararía la utilización del GPS en atención a dichas finalidades. Además, la adopción de este dispositivo debería ir acompañado de la disposición de otras medidas complementarias como la atribución al trabajador de la información necesaria para su utilización. También se debería garantizar la imposibilidad de recoger datos relativos a la localización de un empleado fuera del horario de trabajo, por lo que deberá existir algún método para que el trabajador pueda desactivar dicho dispositivo, o en caso de disponer de un equipo propio de *Internet of Things* después de su tiempo efectivo de trabajo[27].

Caso aparte fue lo resuelto por la *STSJ de Andalucía (Granada) Sala de lo Social, 18/09/2017 (rec. 770/2017)*, en el que no se pronuncia en un caso de no desactivación del GPS, sino todo lo contrario, por la falta de activación de un Gestor GPS por una trabajadora móvil conforme a las órdenes que en dicho sentido le había trasladado la empresa. De hecho, el TSJ valida la decisión extintiva empresarial por incumplimiento continuado y reiterado de la obligación de la trabajadora de activar el dispositivo GPS de seguimiento y control de rutas e inicio y fin de jornada, así como por la omisión del deber de atender las peticiones de explicaciones de la empresa de porque no activaba dicho dispositivo. Tampoco en este caso es cuestionada la utilización de este sistema de geolocalización, que indica la posición del dispositivo en cada momento durante la jornada laboral, así como el tratarse de un mecanismo que calcula el rendimiento del trabajador y establece los objetivos que debe cumplir. La sentencia valida, en todo caso, que la empresa pueda despedir en función de la falta de colaboración del trabajador en la activación del dispositivo electrónico.

Finalmente cabe destacare que la nueva normativa de protección de datos ha regulado el Derecho a la desconexión digital, es decir, el derecho de los trabajadores y los empleados públicos a no utilizar sistemas de comunicación tecnológica vinculados a su trabajo (e-mail, móviles, etc) fuera del tiempo de trabajo legal o convencionalmente establecido, a fin de garantizar el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

La LO 3/2018 impone a la parte empleadora el deber de elaborar una política interna dirigida a su personal, incluidos los que ocupen puestos directivos. El debate se está produciendo sobre si esa referencia a los "puestos directivos" incluye a los Altos directivos (sometidos al correspondiente régimen laboral especial en el sector privado), o al personal directivo profesional, funcionarial o laboral (en este último caso también subordinado al régimen laboral especial de Altos directivos), según está previsto en el RDL 5/2015. Al hilo del precepto orgánico, los argumentos que defienden que el derecho a la desconexión digital no se aplica al personal directivo se trae a colación que respecto al régimen laboral no se ha producido una modificación de la normativa reglamentaria que lo regula de forma que acoja ese nuevo derecho, junto al hecho de que no se apliquen limitaciones a la jornada

[27] *Proyecto Technos. Internet of Things y su impacto en los Recursos Humanos y en el Marco Regulatorio de las Relaciones Laborales* (Dir. SALVADOR DEL REY GUANTER. Coord. GUILLERMO TENA PLANAS), Wolters Klwuer, Octubre 2017, p. 246.

derivadas de la normativa europea[28]. Si se sigue este argumento, respecto al régimen del personal directivo profesional de carácter funcionarial, se podría defender también que en cuanto funcionarios son empleados públicos, pero el RDL 5/2015 tienen una regulación al margen de su calificación como tales empleados, del que se les atribuye un régimen específico. En todo caso, lo que si considero es que a tenor del art. 88 de la LO 3/2018 la realización por la parte empleadora de una "política interna" sobre desconexión dirigida a su personal, incluidos los directivos, hace que estos deban verse obligados a seguir algunas de esas medidas o sean beneficiarios de algunas de las acciones de esa política. El precepto dice que esa política debe definir las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En este sentido, esas acciones de formación o de sensibilización deben incluir al personal directivo, principalmente como sujetos beneficiarios de esas medidas formativas o de concienciación del valor de la desconexión en el momento de organizar o dirigir el trabajo del resto de empleados.

CONCLUSIONES

Este trabajo ha pretendido poner de manifiesto la complejidad que está adquiriendo el derecho de protección de datos en el ámbito del empleo público, ya que, más allá de que la normativa no haya realizado una diferenciación general y expresa entre trabajadores del sector privado y personal del sector público, tampoco se ha delimitado regulación en un campo tan básico como es el tratamiento de datos personales entre personal laboral al servicio de la Administración pública y funcionarios públicos. Este trabajo ha pretendido aportar soluciones a esta situación diversa, empezando por la afirmación de unificar en una misma base legitimadora el tratamiento de datos entre ambos colectivos, cual es la prevista en el art. 6.1b) del Reglamento 2016/679 (es decir, la ejecución de un contrato como fundamento del tratamiento). En todo caso, la validez de esa condición en el marco de una relación de prestación de servicios entre empleado-funcionario y Administración pública-empleadora no debe esconder el hecho de que, con la normativa adoptada en el ámbito europeo y española, la base regulada en el art. 6.1b) del Reglamento 2016/679 ha reducido su margen de actuación en el tratamiento de datos en el sector público. De hecho, es otra base legitimadora, en concreto la del interés público o el ejercicio de los poderes públicos se está erigiendo en un fundamento importante respecto del personal, ya sea laboral, ya sea funcionario, que presta servicios para las Administraciones públicas, cuando el uso de este fundamento debiera ser especialmente restrictivo, tanto respecto al reconocimiento sobre las situaciones en las que debe proceder, como respecto a los datos que se deben tratar bajo su paraguas.

En todo caso, este estudio ha aportado argumentos para salvaguardar también la aplicación a todo el personal público, incluidos los funcionarios, las disposiciones del Reglamento europeo sobre tratamientos de datos en el ámbito laboral, especialmente su art. 88. A juicio de quién esto escribe, el espíritu que subyace al precepto es general, es decir, se busca referenciar determinados aspectos en el marco de u "contexto laboral" en el que se producen desequilibrios entre las partes por la relación de trabajo establecida, y por tanto, el precepto es aplicable a cualquier relación de prestación de servicios entre empleado y administración. De hecho, así lo entiende también la legislación española concretada en la LO 3/2018, ya que, como al efecto se verá posteriormente, cuando regula determinados derechos digitales también bajo el paraguas del "ámbito laboral", lo hace incluyendo de forma expresa a trabajadores y empleados públicos (y, por tanto, también a empleados con una relación

[28] Véase SERRANO OLIVARES, R.; SABATÉ CANELLES, M.: "Los Derechos a la desconexión digital y al registro de la jornada". En *Revista Jurídica de Catalunya*, núm. 3, de 2019, p. 59.

administrativa). La aplicación del ar.t 88 del Reglamento 679/2016 es básico para poder delegar en el Derecho de los Estados miembros o en la negociación colectiva las especificaciones en materia de protección de datos que mejoren lo dispuesto en esa norma europea.

Entre esas especificaciones se ha tratado la importante temática de la información pública de los datos referidos directamente a la realización de puestos de trabajo que ocupa cada empleado. Enlazando con dicha normativa de información pública, se ha mantenido la opción legal por la publicación de las relaciones de los puestos de trabajo de las Administraciones públicas (con las precauciones del art. 15 de la Ley 19/2013). También se han destacado las obligaciones sobre notificaciones y publicaciones de actos administrativos, donde se ha hecho presente la necesidad de realizarlos bajo el principio de seudonimización y minimización de datos. También deben ser especialmente protegidos por resultar una categoría especial de datos los relativos a la seguridad y salud de los trabajadores así como el régimen de derechos colectivos en el trabajo, en particular sobre derechos de información pasiva, donde se predica la importancia de velar por la función del cumplimiento de las competencias de vigilancia de los representantes de los trabajadores en ponderación con el Derecho fundamental de protección de datos personales, de forma que la información publicitada sea la estrictamente necesaria para ejercer con eficacia sus funciones.

La última parte de este trabajo, dedicada al régimen común de Derechos digitales de trabajadores del sector privado y personal al servicio de las administraciones públicas, así como sobre el régimen de control que la administración puede imponer en tanto que empleadora, en el que se pone de manifiesto las garantías de respeto al espacio íntimo del trabajador y de sus datos personales que pueden ser recogidos por los sistemas de vigilancia, bajo la condición básica pero reforzada por normativa española de protección de datos de que los trabajadores hayan sido previamente informados de ello.

BIBLIOGRAFÍA

Acín Ferrer, A.: "Protección de datos. Aplicación de la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, en las entidades locales. Entidades locales-Actuaciones y responsabilidades". *La Administración Práctica* núm. 2/2019. Base de Datos Thomson Reuters Aranzadi-Instituciones: BIB 2019/654.

Agencia Española de Protección de Datos. Gabinete Jurídico. N/REF 010601/2019.

Agencia Española de Protección de Datos: Informe del Gabinete Jurídico de la Agencia Española de Protección de Datos sobre la base jurídica para el tratamiento de datos. Ampliación del Informe emitido en los expedientes 108/2018 (ref. 181577/2018) y 155/2018 (ref. 200012/2018).

Agencia Española de Protección de Datos: https://www.agpd.es [En dicha página web pueden encontrarse como documentos de interés utilizados relacionados con lo que se acaba de exponer en el texto la publicación: Guía 'La protección de datos en las relaciones laborales' – 2009.

Agencia Española de Protección de Datos: Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD": https://www.aepd.es/media/docs/orientaciones-da7.pdf

Víctor Almonacid Lamelas 2019: Blog Nosoloaytos. Web oficial de Víctor Almonacid: ¿Los datos de los empleados públicos son públicos?. 20 de mayo de 2019: https://nosoloaytos.wordpress.com/2019/05/20/los-datos-de-los-empleados-publicos-son-publicos

Baz Rodríguez, Jesús: *Privacidad y protección de datos de los trabajadores en el entorno digital*. Wolters Kluwer España, S.A., Madrid, 2019.

Camas Roda, F.: «La intimidad y la esfera privada del trabajador ante las nuevas modalidades de control y vigilancia de la actividad laboral». en AA.VV.: *Nuevas tecnologías de la Información y la comunicación y Derecho del Trabajo* (Coordinado por M.R. Alarcón Caracuel y R. Esteban Legarreta), Editorial Bomarzo, Alicante, 2004, pp. 161-186.

CTBG-AEDP: "Ley 19/2013, de 9 de diciembre (Art. 15) –Criterios de aplicación. Solicitud 1/2015 –Oficina para la Ejecución dela Reforma de la Administración (OPERA)". 23 de marzo de 2015.

Fernández Orrico, F.J.: "Protección de la intimidad del trabajador frente a dispositivos digitales: análisis de la Ley Orgánica 3/2018, de 5 de diciembre". En *Revista Española de Derecho del Trabajo* núm. 222/2019, BIB 2019/7744 de Base de Datos Thomson Reuters Aranzadi).

GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. 17/ES WP259 y rev.01: *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/2016/679*. Adoptadas el 28 de noviembre de 2017 revisadas por última vez y adoptadas el 10 de abril de 2018.

GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS: Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, adoptado el 8 de junio de 2017.

GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS. Groupe de travail «Article 29» sur la protection des données (5062/01 FR/ Final WP 48) : Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel. Adopté le 13 septembre 2001.

HUGO PRECIADO, C.: *El Derecho a la Protección de Datos en el Contrato de Trabajo*. Thomson Reuters, Cizur Menor, 2017

MURO, IGNACIO: "Trazabilidad del trabajo: el futuro ya está aquí",en: https://economistasfrentealacrisis.com/trazabilidad-del-trabajo-el-futuro-ya-esta-aqui/

PROYECTO TECHNOS. *Internet of Things y su impacto en los Recursos Humanos y en el Marco Regulatorio de las Relaciones Laborales* (Dir. SALVADOR DEL REY GUANTER. Coord. GUILLERMO TENA PLANAS), Wolters Klwuer, Octubre 2017.

ROJO TORRECILLA, E.: "Medias verdades y fake news en el mundo jurídico. No cabe todo en la videovigilancia de una persona trabajadora. A propósito de la sentencia "López Ribalada" de la Gran Sala del TEDH de 17 de octubre de 2019 (y recordatorio de la sentencia de Sala de 9 de enero de 2018 y del caso Barbulescu II, sentencia de Gran Sala de 5 de septiembre de 2017": https://www.rojotorrecilla.es (23 de octubre de 2019)

RESOLUCIÓN 263/2019, de 9 de mayo, de la *Comissió de Garantia del Dret d'Accés a la Informació Pública* (GAIP-Generalitat de Catalunya).

SERRANO OLIVARES, R.; SABATÉ CANELLES, M.: "Los Derechos a la desconexión digital y al registro de la jornada". En *Revista Jurídica de Catalunya*, núm. 3, de 2019.

THE WORKING PARTY [ARTICLE 29 DATA PROTECTION WORKING PARTY]: *Opinion 2/2017 on data processing at work*, Adopted on 8 June 2017

RESUMEN

El estudio realizado por el Pr. Ferran Camas Roda, con el título "Protección de datos personales y garantía de derechos digitales en el empleo público", tiene por objeto analizar la aplicación del Reglamento (UE) 2016/679 *del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos,* y la Ley Orgánica 3/2018 *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,* respecto del personal que presta sus servicios para la Administración Pública. Es decir, el objeto de este estudio es analizar la aplicación de aquella normativa a la diferente tipología de empleados públicos que trabajan para el sector público, por una parte, el personal que está sometido a la legislación laboral, y por otra los funcionarios públicos cuyo régimen jurídico está regulado por la normativa de función pública, de carácter administrativo.

El artículo se divide en tres grandes apartados: en primer lugar el análisis de las bases jurídicas que legitiman el tratamiento de datos personales en el ámbito del empleo público; en segundo lugar, el estudio de la aplicación del tratamiento de datos personales respecto de los empleados públicos (personal laboral y funcionarios públicos), prestando una especial atención a las particularidades reguladas en la normativa, así como a la temática de la prevención de riesgos laborales, los derechos de los representantes de los trabajadores y el régimen de información pública de los datos de los empleados públicos; finalmente, el tercer y último apartado se centra en profundizar el régimen de los derechos digitales de los empleados públicos y, por tanto, el uso de dispositivos digitales de control en la Administración pública.

Para la realización de este estudio se ha partido del análisis de la legislación europea y española; también las sentencias judiciales del ámbito europeo y español en materia de protección de datos; naturalmente la principal doctrina científica que se ha derivado en estos temas hasta la actualidad, y especialmente los informes emitidos por grupos de trabajo o de expertos en el ámbito europeo en materia de protección de datos, o las resoluciones de las agencias públicas sobre esta materia, en particular la Agencia Española de Protección de Datos.

Para empezar, y en la propia parte introductoria del trabajo del Pr. Ferran Camas, ya se pone de manifiesto como la normativa que ha regulado el derecho de protección de datos en el contexto laboral, no ha delimitado su aplicación en función del tipo de empleado público que trabaja para la Administración, es decir si se trata de personal laboral, sometido básicamente a la Ley del Estatuto de los Trabajadores, o del personal funcionario, de régimen estatutario o administrativo.

Esa deficiencia en la delimitación de ambos colectivos tiene su plasmación más evidente respecto de la cuestión del tratamiento de datos personales. En este sentido, el Pr. Camas Roda detecta en su artículo que, si bien el Reglamento Europeo de protección de datos regula unas bases de legitimación para que dicho tratamiento de datos sea posible, la forma de regularlas dispone de algunas lagunas en su aplicación a los empleados públicos, en especial a los funcionarios públicos. El elemento más evidente de dichos déficits es la cuestión de la "ejecución de un contrato" como fundamento para poder realizar un tratamiento de datos, el cual está pensado para contratos laborales, pero no tanto para relaciones de funcionarios públicos. En todo caso, el artículo ofrece propuestas basadas en la potencialidad de aquel fundamento para canalizar el tratamiento de datos en el empleo público con el objeto de no causar distorsiones entre funcionarios y empleados sometidos al régimen laboral. En todo caso, la validez de la "ejecución de un contrato" en el marco de una relación de prestación de servicios entre empleado-funcionario

y Administración pública-empleadora ha reducido su margen de actuación en el tratamiento de datos en el sector público. De hecho, es otra base legitimadora, en concreto la del interés público o el ejercicio de los poderes públicos, la que se está erigiendo en un fundamento importante respecto del personal, ya sea laboral, ya sea funcionario, que presta servicios para las Administraciones públicas, sobre todo en materia de registros de personal, de procedimientos en el marco de expedientes de tratamientos limitados de datos, o sobre el acceso a las informaciones públicas sobre determinados datos conectados al puesto de trabajo de los empleados públicos. El Pr. Camas recuerda en su trabajo que el uso del fundamento del interés público o el ejercicio de poderes públicos debiera ser especialmente restrictivo, tanto respecto al reconocimiento sobre las situaciones en las que debe proceder, como respecto a los datos que se deben tratar bajo su paraguas. También se ha de destacar del estudio del Pr. Camas Roda, las propuestas que hace para adaptar al ámbito de las relaciones entre las Administraciones públicas y sus empleados el régimen del tratamiento de datos en materia de prevención de riesgos laborales, donde se apuesta por aplicar la cláusula del reglamento europeo que la permite en función de obligaciones derivadas del Derecho laboral, así como respecto de las informaciones que pueden ser facilitadas a los representantes legales de los trabajadores, siempre que no tengan carácter masivo.

Además de lo anterior, el estudio del Pr. Camas analiza las llamadas como garantías de los derechos digitales que se han regulado en la legislación española de protección de datos, principalmente respeto del uso de dispositivos digitales de los empleados públicos, la instalación de cámaras de control de la imagen y el sonido, la adopción por el empresario de sistemas de geolocalización y el llamado como Derechos digitales.

El estudio también aborda la configuración de dichos derechos tanto para personal del sector público como del sector privado, y aborda cuestiones como la selección de la tecnología o equipos por el empleador, los deberes específicos que debe cumplir si quiere instalarlos (con atención especial al deber de información a los trabajadores), así como los problemas que pueden tener algunos de ellos, en especial el derecho a la desconexión digital respecto de determinado tipo de personal público, como es el personal directivo en las Administraciones públicas.

Palabras clave: Tratamiento de Datos; derechos digitales; empleo público; funcionarios públicos; Derecho laboral; Derecho de la función pública; dispositivos de control; altos directivos.

ABSTRACT The study carried out by Pr. Ferran Camas Roda, entitled "Protection of personal data and guarantee of digital rights in public employment", aims to analyse the enforcement of *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, and Spanish Organic Law 3/2018, *of December 5, on the Protection of Personal Data and Guarantee of Digital Rights*, in relation to Public Administration staff. That is, the purpose of this study is to analyse the application of these laws to the different typology of public employees who work for the public sector; on the one hand, personnel who are subject to labour legislation, and on the other, civil servants whose legal regime is regulated by public law, a law of an administrative nature.

The article is divided into three main sections: first, the analysis of the legal bases that legitimize the processing of personal data in the field of public employment; secondly, the study of the application of the processing of personal data with respect to public employees (labour staff and civil servants), paying special attention to the particularities regulated in the regulations, as well as to the issues of occupational risk prevention, the rights of workers' representatives and the public information regime of public workforce data. Finally, the third section is focused on analysing in greater depth the regime pertaining to the digital rights of public employees and, therefore, the use of digital control devices in the Public Administration.

The analysis of European and Spanish legislation has been used to carry out this study as well as court judgments of European and Spanish scope regarding data protection, the main scientific doctrine that has been derived in these subjects until the present time. Special attention has been given to reports issued by working groups or experts in the European field regarding data protection, or the resolutions of public agencies on this matter, in particular the Spanish Agency for Data Protection.

To begin, the introductory part of this paper shows that the new laws have already clearly assumed the regulation of the right to data protection in the labour context, although their application has not been delimited depending on the type of public employees that work for the Administration. That is, a distinction has not been made between labour employees, basically submitted to the Statute of Workers' Rights, and civil servants, governed by public law.

This deficiency in the delimitation of both groups has its most obvious expression regarding the issue of personal data processing. In this regard, Pr. Camas Roda points out in his article that, although Regulation *(EU) 2016/679* regulates a basis of legitimation so that such data processing is possible, the way it is regulated has some gaps in its application to public employees, especially civil servants. The most obvious element of these deficits is the "execution of a contract" as the basis for data processing, which is intended for labour contracts, but not so much for the legal relations of civil servants. Nonetheless, the article offers proposals based on the potential of this legal basis to channel data processing in public employment in order not to cause distortions between civil servants and employees subject to the labour regime. However, the validity of the "execution of a contract" within the framework of work relationships between employees-civil servants and public employers/Administration has reduced its scope for data processing in the public sector. In fact, another legitimizing basis, specifically that of "public interest or the exercise of public powers", is being built on an important foundation regarding personnel, whether labour, or public civil servants, that provides services for public administrations especially with regard to personnel records, procedures within the framework of limited data processing files, or access to public information on certain data connected to the job of public employees. Pr. Camas recalls in his work that the use of the basis of public interest or the exercise of public powers should be especially restrictive, both with regard to the recognition of situations in which it should proceed, and with respect to the data to be treated under its umbrella. Proposals made by Pr. Camas Roda, to adapt the regime of

data processing in the field of prevention of occupational hazard to the field of relations between public administrations and their employees should also be noted. In this case, the clause of the European regulation, based on obligations derived from labour law, is committed to its application, as well as regarding the information that can be provided to the legal representatives of the workers, provided that it is not massive.

In addition to the above, this study analyses the guarantee of digital rights that has been regulated in the Spanish data protection legislation, mainly in relation to the use of digital devices by public employees, the use of surveillance cameras and sound control, the adoption by the entrepreneur of geolocation systems and the so-called Digital Rights.

The study also analyses the configuration of these rights for both public and private sector staff. It also addresses issues such as the selection of technology or equipment by the employer, the specific duties that must be met to install them (with special attention to the duty of information to workers), as well as the problems that some of them may have, especially the right to digital disconnection with respect to certain types of public employees, such as senior management in public administrations.

Keywords: Data processing, digital rights, public employment, civil servants, Labor law, Public service law, control devices, senior managers.

Registro de jornada de trabajo y protección de datos personales

The record of the dayly working hours and the right to personal data

ANA BELÉN MUÑOZ RUÍZ*

I. LA NUEVA OBLIGACIÓN DE REGISTRO DE JORNADA DEL EMPRESARIO Y SU VÍNCULO CON EL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Mucho se ha escrito sobre los aspectos estrictamente laborales de la nueva obligación de registro de jornada y los antecedentes judiciales que la precedieron[1]. Como se sabe, la obligación del empresario de registro de jornada fue establecida por el RD-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo. La reforma incorpora un nuevo apartado 9 en el artículo 34 del ET indicando que la empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo. Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada[2]. En consecuencia, se establece la obligación de garantizar el registro de la jornada respecto de la totalidad de los trabajadores, tanto a tiempo completo como a tiempo parcial, realicen o no horas extraordinarias[3].

* Profesora Titular Visitante de Derecho del Trabajo y de la Seguridad Social. Universidad Carlos III de Madrid

[1] Entre otros, cabe mencionar los trabajos de ARAGÓN GÓMEZ, C., A partir de este domingo (12 de mayo de 2019) todas las empresas deben proceder al registro diario de la jornada de trabajo, Blog "Foro de Labos", 2019, https://forodelabos.blogspot.com/2019/05/a-partir-de-este-domingo-12-de-mayo-de.html; BELTRÁN DE HEREDIA RUIZ, I., El TJUE exige la obligatoriedad del registro de jornada (y confirma la oportunidad de la reforma del RDLey 8/2019), Blog "Una mirada crítica a las relaciones laborales", 2019, https://ignasibeltran.com/2019/05/15/el-tjue-exige-la-obligatoriedad-del-registro-de-jornada-y-confirma-la-oportunidad-de-la-reforma-del-rdley-8-2019/MORENO SOLANA, A., El Registro de Jornada. Es el turno del Criterio Técnico 101/2019 de la Inspección de Trabajo y Seguridad Social, "Blog Foro de Labos", 2019, https://forodelabos.blogspot.com/2019/06/el-registro-de-jornada-es-el-turno-del.html; MORÓN PRIETO, R., "El registro de jornada en los tiempos líquidos: limitaciones en la regulación y de la regulación del registro de jornada", en AA.VV. (Dir. A. DE LA PUEBLA PINILLA y J.R. MERCADER UGUINA), *Tiempo de reformas: en busca de la competitividad empresarial y de la cohesión social* Tirant Lo Blanch, 2019, pp. 177-198; ROJO TORRECILLA, E., Registro obligatorio de la jornada diaria de trabajo a tiempo completo. 12, 13 y 14 de mayo de 2019: Tres días que cambiarán la vida laboral de muchas empresas en España. Atención especial a la sentencia del TJUE de 14 de mayo (asunto C-55/18), 2019, Blog del Prof. Eduardo Rojo Torrecilla, http://www.eduardorojotorrecilla.es/2019/05/registro-obligatorio-de-la-jornada.html

[2] La reforma se justifica debido al elevado número de denuncias recibidas por la Inspección de Trabajo por incumplimientos laborales relacionados con el tiempo de trabajo, así como los datos publicados por la EPA del último trimestre de 2018 que señalaban que "un 48 por ciento de las personas trabajadoras que declaran realizar horas extraordinarias también manifiestan que no les son abonadas, ni por tanto, se cotiza por ellas a la Seguridad Social", lo que "supone un perjuicio grave para esas personas y para el sistema de Seguridad Social.

[3] Junto a esta nueva obligación de registro de la jornada ordinaria se mantiene la necesidad de registrar la jornada

Precisamente, la entrada en vigor del deber de registro de jornada desde el 12 de mayo de 2019 suscita algunos interrogantes en materia de protección de datos de carácter personal de los empleados que también deben ser objeto de análisis. De ahí la necesidad de integrar la obligación laboral de registro de jornada con el sistema normativo de protección de datos de carácter personal aplicando así el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y el artículo 18.4 de la CE así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y también los informes y resoluciones de la Agencia Española en materia de Protección de Datos (AEPD).

2. LOS DATOS DE CARÁCTER PERSONAL DE LOS EMPLEADOS COMO CONTENIDO DEL REGISTRO HORARIO

Aplicando el Reglamento (UE) 2016/679 de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD)**,** los datos extraíbles del registro horario hacen identificable al trabajador y, por ello, tienen la consideración de dato personal. Conviene recordar que son «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" y, cabe entender por tratamiento de datos "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (art. 4 RGPD).

Esta ha sido también la interpretación formulada por los Tribunales tanto comunitario como nacional. En el plano comunitario, se debe recordar la Sentencia del TJUE de 30 de mayo de 2013[4] que se refiere a los datos relativos a periodos de trabajo diario y a los periodos de descanso como datos personales[5]. En nuestro país, la STS de 23 de marzo de 2017[6] y la STSJ C. Valenciana de 3 de mayo de 2018[7] afirmaron antes de la reforma que la creación de este registro implica un aumento del control empresarial de la prestación de servicios y un tratamiento de los datos obtenidos, máxime en los supuestos de jornada flexible, de trabajo en la calle o en casa, que pueden suponer una injerencia indebida de la empresa en la intimidad y libertad del trabajador, así como en otros derechos fundamentales que tutela nuestra Constitución, especialmente en su artículo 18-4, máxime cuando la pretensión ejercitada y, el fallo que la estima van más allá del

extraordinaria de trabajo en el art. 35 ET y la jornada de los trabajadores a tiempo parcial (art. 12 ET).

[4] C-343/2012, caso Worten.

[5] De la Morena Corrales, P., "El Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo (en especial, la obligación de registro de jornada)", *Trabajo y Derecho*, núm. 54, 2019, p. 9.

[6] Recurso de Casación núm. 81/2016. Referencia jurisprudencial tomada del trabajo de Mercader Uguina, J.R., *Protección de datos en las relaciones laborales*, Francis Lefebvre, 2ª Ed, 2018, pp. 98-99.

[7] Recurso 910/2018. Sentencia citada en el artículo de Marin Alonso, I., "La obligación empresarial de registro de la jornada ordinaria ante el Derecho de la Unión Europea y el Derecho Interno*", Revista General de Derecho del Trabajo y de la Seguridad Social (IUSTEL),* número 53, 2019.

simple control de entrada y salida, por cuánto requiere almacenar datos que permitan comprobar el adecuado cumplimiento de los horarios pactados, objetivo cuyo logro requiere, incluso, un tratamiento anual de los datos recogidos para determinar el cumplimiento de la jornada anual.

Respecto al contenido del registro horario, el apartado 9 del artículo 34 del ET tan solo indica que la empresa debe garantizar el registro diario de jornada, que tiene que incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada trabajador remitiendo su organización y documentación a los convenios colectivos o acuerdos de empresa y, en su defecto, la decisión del empresario previa consulta con los representantes legales. Al respecto, algunos sindicatos han ofrecido pautas para concretar el contenido del registro horario y que sea respetuoso con el derecho fundamental de protección de datos del trabajador. Así se dice que: "En todo caso, si por parte de los delegados de personal, se negociase este sistema de registro (sistema de registro en soporte papel) debe exigirse que en el documento o plantilla que registre la jornada diaria se contengan, como mínimo, los siguientes datos: los datos del trabajador y de la empresa, el día y la hora de entrada y salida concreta, los descansos entre jornadas en caso de existir, la jornada ordinaria a realizar por el trabajador/a, el detalle de las horas ordinarias, complementarias y extraordinarias desglosadas por cada día de trabajo y la firma del trabajador y del representante legal; debiendo prohibirse que los trabajadores firmen a la vez, la entrada y salida, o que se acumulen los registros para su relleno y firma en fechas posteriores"[8]. En esta misma línea, se han detectado regulaciones convencionales que han detallado el contenido del registro de jornada estableciendo un régimen más garantista para el trabajador al utilizar códigos de empleados en lugar de los nombres y apellidos de éstos como, por ejemplo, el Convenio Colectivo del Comercio de Actividades Diversas para la Comunitat Valenciana 2019-2020 que indica: "Artículo 10. Jornada de trabajo. El registro de jornada, como recoge el articulado, debe de recoger, el nombre de la empresa, la dirección del centro de trabajo, el día de la prestación de servicios, un código de empleado (nunca nombre y apellidos u otro dato que pueda incurrir en vulneración de la ley de protección de datos), la hora de entrada, que quedará confirmada con la firma o cualquier otro método autorizado, del empleado/a, hora de salida, con la misma confirmación que a la entrada, y debe de estar firmada y cuñada por el responsable de RR.HH. de la citada empresa. (…)"[9]. No obstante, conviene advertir que ambas opciones (identificar nombre y apellidos del trabajador o utilizar códigos de identificación) son igualmente válidas a los efectos de dar cumplimiento a la legislación de protección de datos de carácter personal.

En todo caso, los datos de registro horario deben ser exactos, estar actualizados y, el empresario solo recabar aquellos datos de carácter personal de los empleados que sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades de registro de jornada (art. 5 RGPD y art. 4 LOPDGDD). En este sentido, no estarían permitidas fórmulas de registro basadas en la agregación de datos y la inclusión de datos personales debería ser la mínima necesaria, siendo solo recomendable una mayor concreción para casos específicos (inclusión de referencias a trabajadores

[8] CCOO, El Registro de la jornada de trabajo. Especial consideración de los sistemas de registro y su impacto en materia de protección de datos, junio 2019.

[9] DO. Generalitat Valenciana 3 octubre 2019, núm. 8648. En este mismo Convenio Colectivo se establece un distinto plazo para implantar el registro informático de jornada en función del número de trabajadores de la empresa: "(…) A tenor del texto del art. 34.9 del ET, las empresas implantarán a partir del 12 de mayo de 2019 un sistema de registro diario de control de la jornada individual de cada trabajador/a. En las empresas de más de 25 trabajadores se les da un plazo hasta diciembre de 2020 para implantar un sistema informático para llevar a cabo dicho control, para el resto de empresas esta medida se prolongará hasta diciembre de 2021". Cabe entender que hasta la fecha indicada las empresas utilizarán sistemas manuales de registro de jornada.

con jornadas especiales por circunstancias personales)[10].

3. LA REGLA DE LA NO EXIGIBILIDAD DEL CONSENTIMIENTO DEL TRABAJADOR Y EL CUMPLIMIENTO DEL DEBER DE TRANSPARENCIA DEL EMPRESARIO

Con carácter general y para la implementación del registro de jornada no se precisa del consentimiento del trabajador, siendo base suficiente de legitimación la propia norma laboral, que en el artículo 34.9 ET[11] establece la obligación de las empresas de realizar dicho registro de la jornada con carácter individual de cada trabajador y que, de acuerdo con lo previsto en el artículo 6.1.c del RGPD, el tratamiento de datos personales de los trabajadores derivado de la implantación del registro de jornada es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. En este punto, conviene recordar que no es preciso el consentimiento cuando los datos de carácter personal se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento (art. 6-7 y 9 RGPD y arts. 6 y 9 LOPDGDD). No obstante lo anterior, la existencia de una lícita condición para el tratamiento de los datos de los empleados sin necesidad del consentimiento de los trabajadores no excluye el deber de las empresas de informar a los trabajadores de la existencia del registro y de la finalidad del tratamiento de los datos personales individuales que se obtienen con dicho registro.

En este sentido, la lectura del artículo 13 del RGPD es ilustrativa a estos efectos. De este modo, el Reglamento configura la transparencia como un principio básico de la protección de datos, junto con otros principios como el de calidad de los datos. Cabe destacar que los principios generales de protección de datos constituyen el contenido esencial del derecho a la generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos. Gráficamente, se percibe el cambio cuando se computan las veces que aparece mencionado en la Directiva (1 vez) y en el Reglamento (hasta en 24 ocasiones)[12]. El contenido del deber de información en materia de protección de datos viene recogido en los artículos 13 RGPD y 11 LOPDGDD. Conforme a estos preceptos, cuando se obtengan del trabajador datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará: i) la identidad y los datos de contacto del responsable y, en su caso, de su representante; ii) los datos de contacto del delegado de protección de datos, en su caso[13]; iii) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; iv) cuando el tratamiento se base en el artículo 6, apartado 1, letra f) RGPD, los intereses legítimos del responsable o de un tercero; v) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; vi) en su caso, la intención del responsable de transferir datos

[10] De la Morena Corrales, P., "El Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo (en especial, la obligación de registro de jornada)", *Trabajo y Derecho*, núm. 54, 2019, pp. 7-8.

[11] Sirve de refuerzo también las facultades de control laboral reconocidas al empresario en el art. 20.3 del ET.

[12] Gil González, E., "Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías Big data y de aprendizaje computacional", *Revista Española de la Transparencia*, núm. 5, 2017, p. 167.

[13] Su designación es obligatoria siempre que: i) El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; ii) Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o; iii) Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales (art. 37 RGPD). Así como también es obligatoria en los supuestos enumerados en el art. 34 LOPDGDD.

personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo RGPD, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

Además, el responsable del tratamiento debe facilitar al trabajador, en el momento en que se obtengan los datos personales: i) el plazo durante el cual se conservarán los datos personales (en este caso, cuatro años); ii) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; iii) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a) RGPD, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; iv) el derecho a presentar una reclamación ante una autoridad de control (en España, la Agencia Española de Protección de Datos); v) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; y, vi) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4 RGPD, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Además, cuando el responsable del tratamiento (el empresario) proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, debe proporcionar al empleado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente. Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el trabajador deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 RGPD.

4. LOS SISTEMAS DE CONTROL HORARIO Y SU PROBLEMÁTICA ESPECÍFICA EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El artículo 34.9 del ET no establece una modalidad específica o predeterminada para el registro diario de la jornada, limitándose a señalar que se debe llevar a cabo día a día e incluir el momento de inicio y finalización de la jornada. Para ello, y sobre el resto de elementos configuradores, llama a la autorregulación, mediante la negociación colectiva o el acuerdo de empresa. Así, será válido cualquier sistema o medio, en soporte papel o telemático, apto para cumplir el objetivo legal, esto es, proporcionar información fiable, inmodificable y no manipulable a posteriori, ya sea por el empresario o por el propio trabajador. Para ello, la información de la jornada debe documentarse en algún tipo de instrumento escrito o digital, o sistemas mixtos, en su caso, que garanticen la trazabilidad y rastreo fidedigno e invariable de la jornada diaria una vez de registrada. Ahora bien, en el supuesto de que el sistema de registro establecido requiera el acceso a dispositivos digitales o el uso de sistemas de videovigilancia o geolocalización, deben respetarse en todo caso los derechos de los trabajadores a la intimidad previstos en el

artículo 20 bis del ET, que remite a la LOPDGDD[14].

Teniendo en cuenta todo lo anterior, se analizan a continuación los posibles sistemas de control horario empleando tres categorías: en primer lugar, los sistemas de registro horario no controvertidos porque en principio cumplen los parámetros del principio de proporcionalidad; en segundo término, se describen los sistemas de registro proscritos ya que se basan en las herramientas de propiedad del trabajador; y, por último, los sistemas de registro basados en los datos biométricos del trabajador (principalmente, huella dactilar y tecnología de reconocimiento facial) que precisan de garantías adicionales.

4.1. Los sistemas de registro horario no controvertidos

Dentro de la categoría de sistemas de registro de horario no controvertidos cabe englobar las anotaciones en papel con firma del trabajador, aplicaciones informáticas, tarjetas de identificación electrónica o cualquier otro medio o soporte que acredite la conformidad del trabajador con el registro efectuado. Dichos medios deberán tener en consideración las distintas modalidades posibles que tienen las empresas en relación al establecimiento de las distintas fórmulas de prestación del trabajo, entre otras, horario fijo, jornada flexible, teletrabajo, jornada parcial, jornada reducida, jornada partida, jornada continuada, jornada intensiva, etc[15].

En ocasiones, se articulan en la negociación colectiva sistemas mixtos (máquinas de control horario situadas en los centros de trabajo y registro horario manual) atendiendo a ciertas características como, por ejemplo, tipo de horario o centro de trabajo. Así, se dice en el artículo 7º de la Modificación del VII Convenio Colectivo de Iberdrola Grupo que: "el colectivo 1 sería el personal que tuviera acceso a controles de fichaje mediante las máquinas de control situadas en nuestros edificios corporativos: deberá realizar el fichaje según el procedimiento establecido, reflejándose la hora de entrada y de salida. Teniendo en cuenta la flexibilidad que ya hemos comentado que existe durante la jornada, en cuanto a la posibilidad de hacer ciertos descansos o dedicar tiempos a temas no estrictamente laborales, ambas partes entienden que solo deben ser tenidas en cuenta como horas de exceso de jornada aquellas que vienen motivadas por una orden expresa de la jefatura. El exceso de horas que hubiera podido tener este personal con motivo de la orden de la jefatura de ampliar su jornada, lo reflejará como hasta ahora en el e-Go, considerando, por tanto, que las horas no reflejadas y aprobadas mediante la utilización de dicho sistema no se consideran horas de trabajo sino simplemente son tiempos de presencia en las instalaciones que no tienen consideración de trabajo efectivo". Y para el colectivo 2 que no tuviera acceso a controles de fichaje mediante las máquinas de control situadas en los edificios corporativos (p.e. determinados horarios como los de compacta, turnos, personal de brigadas, o por estar adscritos a centros de trabajo sin lectoras de fichajes…) se acuerda que: "estos trabajadores, y sus jefaturas

[14] Guía sobre el registro de jornada del Ministerio de Trabajo, Migraciones y Seguridad Social que puede consultarse en: http://www.mitramiss.gob.es/ficheros/ministerio/GuiaRegistroJornada.pdf. Así no ha sido validado por la AEPD el control de presencia de empleados utilizando la voz ya que, con carácter general, las grabaciones indiscriminadas de voz y conversaciones de los empleados y público en general que acceden a los edificios no cumple el principio de proporcionalidad, considerándose una medida intrusiva para la intimidad de los empleados y para su derecho a la protección de datos de carácter personal (Informe de la AEPD). Otros medios requerirán además del consentimiento del trabajador afectado. Por ejemplo, algunas empresas en Suecia han logrado que sus trabajadores acepten la implantación de microchips debajo de la piel debido a sus variadas aplicaciones. Desde nuestro punto de vista, los trabajadores tienen el derecho legítimo a rechazar su uso ya que existen otros medios menos intrusivos y que cumplen igual función.

[15] Estos son los medios previstos en algunos convenios colectivos como, por ejemplo, el artículo 1º relativo a la modificación del VI Convenio Colectivo General del Sector de la Construcción, BOE 5 noviembre 2019, núm. 266.

directas en caso necesario, rellenen y firmen manualmente, su registro horario diario con la indicación de la hora de entrada y de salida, no teniendo que especificar en dicho parte los motivos y los tiempos dedicados a aspectos propios de la flexibilidad dentro de la jornada que no tiene consideración de tiempo de trabajo (tiempo de presencia)"[16].

4.2. Sistemas de registro horario proscritos cuando se utilizan las herramientas de propiedad del trabajador

Pero, ¿qué ocurre cuando es el trabajador quien utiliza sus propios dispositivos electrónicos (teléfono móvil, ordenador, Tablet, etc.) para llevar a cabo el registro de jornada? Esta práctica se denomina "Bring your own device" (BYOD) y se refiere a que el trabajador accede con sus medios electrónicos a las aplicaciones corporativas como el email o bases de datos y almacena y trata datos de la empresa así como de los clientes de ésta[17]. Conviene aclarar que se trata de una práctica proscrita en materia de registro de jornada cuando resulta impuesta por parte del empresario. Es decir, dicho tratamiento excedería de lo permitido por la normativa de protección de datos, y en concreto, de la legitimación empresarial en base a la ejecución de un contrato de trabajo (arts. 6-7 y 9 del RGPD y arts. 6 y 9 LOPDGDD). Luego, se precisa del consentimiento del trabajador que podrá oponerse posteriormente a su tratamiento ejerciendo los derechos de oposición o supresión. Así lo ha confirmado la Sentene cia del Tribunal Supremo de 21 septiembre de 2015[18] y, también, la Sentencia de la Audiene cia Nacional de 6 de febrero de 2019[19]. Esta última Sentencia resolvió el conflicto colectivo del grupo de repartidores de Telepizza que mostraron su oposición a la cláusula en el contrato de las nuevas contrataciones conforme a la cual los repartidores serían geolocalizados cuando realizasen tareas de reparto mediante una app descargada en sus teléfonos móviles personales[20]. Concluyó la Audiencia Nacional que la aportación de un teléfono móvil con conexión de datos para desarrollar el trabajo en los términos descritos supone un manifiesto abuso de derecho empresarial, ya que quiebra con la ajenidad en los medios que caracteriza el contrato de trabajo (art. 1.1 ET). El fallo judicial declara la nulidad de la medida empresarial así como la nulidad de las cláusulas introducidas en los contratos/tipo o novaciones por estos argumentos:

En primer lugar, se considera que la empresa al imponer de forma unilateral dicho

[16] BOE 18 octubre 2019, núm. 251.

[17] Las ventajas para la empresa (ahorre de costes) y para los empleados (flexibilidad, satisfacción) son las razones principales de esta tendencia especialmente en las pequeñas empresas. Pero, ¿realmente no tiene coste para el empresario? El hecho que los trabajadores se conecten desde sus dispositivos a la red corporativa puede conllevar brechas de seguridad. Primero, la integración de dispositivos privados en la red corporativa facilita intrusiones de software maliciosos (virus, troyanos, etc.). Segundo, esta práctica también incrementa la posibilidad de pérdida y robo de datos. En este sentido, el CERT Gubernamental español, que forma parte del Centro Nacional de Inteligencia (CNI), realizó una encuesta a empleados BYOD. Según el CERT, "el dato más preocupante es que cerca de la mitad de los encuestados no manejan la información corporativa de forma cifrada en su dispositivo personal, incluso el 15,6% dice no saber cómo se debe manejar dicha información" (Riesgos y amenazas del Bring Your Own Device (BYOD)). Este tipo de trabajadores podría llegar a conectarse a redes desconocidas inseguras haciendo posible, sin quererlo, que se produzcan sobre sus dispositivos "ciberataques de tipo man-in-the-middle, que podrían interceptar e incluso modificar los datos en tránsito". Para evitar esta consecuencia, la primera medida de seguridad que recomienda el CERT es "usar mecanismos de cifrado fuerte", tales como el uso de redes privadas virtuales o VPN y sistemas de cifrado de datos.

[18] Rº 259/2014.

[19] Procedimiento nº 0000318/2018.

[20] El empleado es el responsable de activar y desactivar la APP al iniciar y concluir su turno de trabajo. La empresa abonará a los empleados un importe mensual por jornada de trabajo fija contratada, para compensar el desgaste de la herramienta que aporta el empleado, así como el consumo de datos móviles por tener activa la APP en el momento del reparto. La negativa reiterada o imposibilidad sobrevenida de aportación de esta herramienta por parte del trabajador, o de la aplicación informática antes mencionada, será causa suficiente para la extinción del contrato de trabajo al amparo de lo previsto en el artículo 49.1.b) del ET. Todo ello, se estipula, claro está, al margen del convenio colectivo de aplicación a estos trabajadores.

sistema ha incumplido con los deberes de información y consulta respecto de los representantes de los trabajadores según lo dispuesto en el art. 64.5 ET. En concreto, se concluye por la Audiencia Nacional que la información resultó insuficiente, por cuanto que se omiten datos esenciales (explicación del concreto funcionamiento de la app, esto es, cómo se instala en el teléfono móvil, a qué datos del terminal la misma debe acceder, qué concretos datos propios ha de aportar el trabajador para acceder a la aplicación, qué datos, en su caso, ha de archivar la misma y cómo van a ser tratados los mismos) para que los representantes de los trabajadores pudieran emitir un informe con el necesario conocimiento, máxime, cuando la geolocalización es una medida que afecta a datos personales de carácter del trabajador protegidos por el art. 18.4 CE.

En segundo término, no respeta el derecho a la privacidad de los trabajadores por cuanto que no supera el juicio de proporcionalidad. Si bien la medida implantada obedece a fines constitucionalmente legítimos en el desarrollo del derecho a la libre empresa (control el empleado en el desempeño de su puesto de trabajo y la oferta de un mejor servicio al cliente– de forma que éste pueda conocer en todo momento la ubicación de su pedido, dotando a la empresa de capacidad para proporcionar servicios que se afirma ya ofrecen otras empresas del sector), la misma finalidad se podría haber obtenido con medidas que suponen una menor injerencia en los derechos fundamentales de los empleados (implantación de sistemas de geolocalización en las motocicletas en las que se transportan los pedidos o las pulseras con tales dispositivos) y que no implican para el empleado la necesidad de aportar medios propios y lo que es más importante, ni datos de carácter personal como son el número de teléfono o la dirección de correo electrónico en la que han de recibir el código de descarga de la aplicación informática que activa el sistema. Además, para la implantación del sistema de geolocalización por parte del empleador se ha prescindido de proporcionar a los trabajadores de la información a que se refieren los arts. 12 y 13 del Reglamento 679/2016, 5 de la anterior Ley de protección de datos y 11 y 90 de la vigente LO 3/2018.

En tercer lugar, entraña abuso de derecho por el empresario, y finalmente, supone la creación de un régimen disciplinario al margen del convenio. Se califica de manifiesto abuso de derecho empresarial, ya que además de quebrar con la necesaria ajenidad en los medios que caracteriza la nota de ajenidad del contrato de trabajo (art. 1.1 ET) y desplazando el deber empresarial de proporcionar ocupación efectiva del trabajador (arts. 4.2 a) y 30 E.T) a éste al que se responsabiliza de los medios, de forma que cualquier impedimento en la activación del sistema de geolocalización implica cuando menos la suspensión del contrato de trabajo y la consiguiente pérdida del salario– ex art. 45.2 ET-; y, por otro lado, la compensación que se oferta por tal aportación resulta de todo punto insuficiente, ya que se calcula el valor de un terminal móvil de baja gama (se ha calculado un precio de 110 €, y sobre una vida útil de 3 años) y la contratación de unos datos por internet que únicamente se compensan en función de su utilización en el trabajo, prescindiendo de si tal contratación era o no deseada por el empleado para el desarrollo de su vida personal.

En definitiva, en ningún caso resulta admisible que los trabajadores tengan que poner a disposición de la empresa sus propios dispositivos para incorporar el sistema de registro de jornada, por tanto, el trabajador no tiene la obligación de utilizar su móvil o dispositivo digital para descargarse la app o aplicación para registrar su hora de entrada o salida. En este sentido, resultan muy loables las experiencias convencionales que enfatizan la idea de voluntariedad del uso por parte de los trabajadores de los dispositivos electrónicos de su propiedad. Así, por ejemplo, se indica en el Acuerdo Parcial del Convenio Colectivo del Sector de Cajas y Entidades Financieras de Ahorro que: "II Modelo de registro. Primero. Con el fin de garantizar el registro diario de jornada, las empresas pondrán a disposición

de las personas trabajadoras una aplicación, que podrá descargarse en todas o algunas de las herramientas tecnológicas propiedad de la entidad puestas a disposición de la persona trabajadora –Ordenador fijo o portátil, Tablet, Smartphone o cualquier otro dispositivo susceptible de ser utilizado como herramienta de trabajo y que admita la descarga de dicha aplicación–, con el fin de que la propia persona trabajadora pueda registrar su jornada diaria de trabajo (…)". Y, en el apartado tercero de este Convenio Colectivo se aclara que: "No se podrá descargar la aplicación para el registro de jornada en ningún dispositivo que no sea propiedad de la empresa, salvo autorización de la empresa y aceptación de la persona trabajadora (…)"[21].

Cuestión distinta es cuando se trata de una práctica consentida por los propios trabajadores. No resulta aplicable a estas situaciones novedosas la doctrina judicial sobre la legitimidad del control del ordenador y correo electrónico profesional por parte de la empresa que se apoya en que se trata de medios que son de su propiedad y que la empresa facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral[22]. Ahora bien, parece claro que el empresario conserva su condición de responsable de aquellos datos que forman parte de su actividad empresarial. En este sentido, tal y como apunta el Comité Europeo de Protección de Datos (antes denominado Grupo Europeo de Trabajo del artículo 29), el control de la localización y tráfico de tales dispositivos podría ser considerado interés legítimo para proteger los datos de carácter personal de los que es responsable el empresario. Sin embargo, este control podría ser ilegal si trata datos relativos a la vida personal y familiar del empleado. Con el propósito de prevenir el control de información privada, se aconseja adoptar medidas dirigidas a delimitar entre el uso privado y profesional de los dispositivos[23]. En este sentido, las empresas deberían recoger medidas para proteger los datos corporativos y los personales de los empleados, entre ellas, formación a los trabajadores sobre esta materia.

4.3. Sistemas de registro basados en los datos biométricos del trabajador con garantías adicionales

Cabe apuntar que los avances tecnológicos permiten el registro horario utilizando, por ejemplo, los datos biométricos de los empleados que son datos especialmente protegidos. La reforma proporciona una mínima información ciñéndose a los aspectos estrictamente laborales, pero no prohíbe el recurso a la tecnología para realizar el registro de jornada y tampoco dice nada respecto del sistema elegido y los derechos fundamentales de intimidad y protección de datos de los empleados. Se limita, por tanto, a señalar que se debe llevar a cabo día a día e incluir el momento de inicio y finalización de la jornada.

El punto de partida es lo dispuesto en el RGPD, donde se indica en su art. 4 que los datos biométricos pertenecen a la categoría de datos especiales que se obtienen partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o

[21] BOE 30 octubre 2019, núm. 261. Añade el apartado cuarto de este Convenio Colectivo que: "Si excepcionalmente la persona trabajadora no dispusiera de ninguna herramienta puesta a su disposición por la empresa susceptible de alojar la aplicación para el registro diario de jornada se pondrá a su disposición una hoja en papel en la que deberá constar cada día la hora de inicio de la jornada de trabajo, la hora de finalización de la misma y el número de horas de trabajo efectivo realizadas por la persona trabajadora, una vez descontados los tiempos de descanso u otras interrupciones del trabajo que no puedan considerarse tiempo de trabajo efectivo. Las empresas deberán informar previamente a la representación legal de los trabajadores de estos supuestos excepcionales de aplicación del registro de jornada en formato papel".

[22] *Vid.* STS de 26 de septiembre de 2007, Recurso 966/2006.

[23] Opinion 2/2017 on data processing at work-wp 249.

datos dactiloscópicos. Ahora bien, conviene advertir que hay datos biométricos de primera y segunda generación. La segunda generación de datos incluye tecnología biométrica que permite la autentificación a través de la captura de datos (forma de caminar, voz, olor corporal, ondas cerebrales, actividad eléctrica del corazón, temperatura corporal, dilatación de las pupilas) pero, a diferencia de la primera, desde una distancia y en movimiento. Estas características biométricas pueden en ocasiones ser tratadas mientras el titular de los datos no lo percibe. Lo que hace difícil verificar si los responsables del tratamiento cumplen con la legislación de protección de datos. La llamada segunda generación de datos podría ser usada para la elaboración de perfiles implicando que los individuos sean categorizados e incluso ser objeto de discriminación y estigma social. Como regla general, queda prohibido el tratamiento de datos personales que revelen datos biométricos dirigidos a identificar de manera unívoca a una persona física. No obstante, esta regla se excepciona 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 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 (art. 9 RGPD). En el caso del registro de jornada basado en la huella dactilar, el dato que se recoge de los trabajadores está constituido por varios puntos de la huella de uno de sus dedos índice que se tratan por un algoritmo matemático mediante el que se asocia a dicho conjunto de puntos un número que identifica al trabajador en cuestión. Contamos con algunas respuestas ofrecidas por la Agencia Española de Protección de Datos respecto a la posibilidad de implantar un sistema para el control horario de los trabajadores basado en la lectura de la huella digital, tanto antes del RGPD[24] como tras su aprobación[25].

A juicio de la AEPD, el tratamiento de la huella digital para el control de acceso por los trabajadores podría considerarse una medida de control amparada en el artículo 20 del ET (y ahora también en el artículo 34.9 ET), por lo que no exigiría consentimiento del empleado. No obstante, para implantar esta medida debe aplicarse el principio de minimización; es decir, debe limitarse a los supuestos en que se considere realmente necesaria para que el control sea eficaz. La AEPD ha señalado en diversos informes que existen buenas prácticas que permiten el control a través de la huella digital sin que el sistema tenga que almacenar el dato biométrico (por ejemplo, por su incorporación a una tarjeta inteligente que se contrastase con la huella y se mantuviera siempre en poder del trabajador)[26]. La misma doctrina ha sostenido también la Sala 3ª del Tribunal Supremo en la STS 2.7.2007[27], y la STSJ de Murcia de 25.1.2010[28]. En la STSJ de Islas Canarias de 21.7.2007[29], sobre idéntico asunto, se rechaza el argumento sindical de que este control horario reduzca las personas a un algoritmo ya que el alcance del sistema no llega a tanto.

Aunque no es necesario el consentimiento del trabajador para el tratamiento de los mencionados datos biométricos, la AEPD ha indicado que debe informarse al trabajador de lo dispuesto en el artículo 13 del RGPD, especialmente de las consecuencias disciplinarias que podría acarrear la negativa del trabajador al tratamiento de su huella digital[30]. Hay que advertir que el incumplimiento del principio de transparencia constituye infracción muy grave.

[24] Informe 0324/2009 de la AEPD.
[25] Documento de trabajo de la AEPD de 2018.
[26] Documento de trabajo de la AEPD de 2018.
[27] Recurso 5017/2003.
[28] Recurso 1071/2009.
[29] Recurso 93/2007.
[30] Expediente Nº : E/02116/2016.

Hace unos meses se investigaba en Bélgica la fuga de datos de los empleados de una conocidísima empresa de trabajo temporal (aproximadamente 2.000 empleados). La Agencia belga de protección de datos denunciaba la gravedad de los hechos teniendo en cuenta que la brecha de seguridad se refería al reconocimiento facial de los trabajadores. Al hilo de esta noticia surgen algunas cuestiones: ¿debemos tratar por igual al conjunto de los datos biométricos? ¿está legitimado el empresario para usar tecnología de reconocimiento facial en algunos casos? ¿cuáles serían las garantías requeridas para su correcta implantación? El Tribunal Europeo de Derechos Humanos ya advirtió en el Caso Marper de 4 de diciembre 2008 que no todos los datos biométricos deben ser tratados por igual porque no todos ellos conllevan la misma intrusión en los derechos de la persona[31]. En particular, el Consejo Europeo de Protección de Datos ha indicado en julio de 2019 que el reconocimiento facial implica riesgos más elevados para los derechos de los titulares de los datos y, que debido a ello, precisa de una mayor protección. Nada es más personal que el rostro de un individuo. El uso de esta tecnología se debe realizar preservando los principios de legalidad, necesidad, proporcionalidad y minimización de datos conforme a lo dispuesto en el RGPD. Pese a las ventajas asociadas a esta tecnología para la empresa, los responsables deben ante todo evaluar su impacto sobre los derechos y libertades y considerar medios menos intrusivos para alcanzar los propósitos legítimos de estos procesamientos[32].

En nuestro país, las resoluciones judiciales que existen sobre el control empresarial basado en datos biométricos de los trabajadores se han centrado en la lectura de la huella dactilar y todavía no se ha abordado la cuestión referida al tratamiento del rostro con software de reconocimiento facial. Por su parte, la AEPD ha realizado una distinción entre la tecnología de reconocimiento facial y los sistemas de fichaje por huella dactilar implantados en algunas empresas, mostrándose más permisiva respecto de los controles de huella dactilar que en los casos del reconocimiento facial. En relación con el reconocimiento facial, la AEPD ha indicado que habrán de tenerse especialmente en cuenta los principios de minimización y de licitud del tratamiento. Según criterio de la Agencia, en el ámbito laboral el uso de software de reconocimiento facial podría considerarse una medida de control por el empresario, admitida por el artículo 20 ET siempre y cuando sea proporcional, lo que exigiría tener en cuenta la naturaleza de la actividad y de las instalaciones para cuyo acceso se requiriese el reconocimiento facial. En los restantes supuestos, no existiría una habilitación similar, si bien podría ser posible el tratamiento cuando se tratase de preservar la seguridad de determinadas instalaciones como las estratégicas, así como determinados supuestos amparados por la Directiva 2016/680. Especial interés tiene el desarrollo francés sobre esta cuestión. En enero de 2019 la Autoridad francesa de Protección de Datos (CNIL) aprobó unas reglas sobre el uso empresarial de la información biométrica de sus empleados tales como el reconocimiento facial. Para su empleo, se requiere el cumplimiento de los siguientes requisitos: i) Justificar al CNIL por qué necesitan usar estos sistemas y no otros menos intrusivos; ii) Disponer de medidas de seguridad para proteger los datos biométricos; iii) Llevar a cabo una evaluación de impacto. Con respecto a la primera de las exigencias (justificar la necesidad del uso de los datos biométricos), las empresas deben indicar un contexto específico o razón que precise del uso de los datos biométricos como identificadores. Algunos ejemplos podrían ser que los empleados hayan sido autorizados para usar una máquina peligrosa o acceder a objetos de valor o grandes sumas de dinero. Además, la empresa deberá demostrar por qué un método menos intrusivo (por ejemplo, una credencial o clave) no resulta suficiente.

[31] Applications nos. 30562/04 and 30566/04.

[32] Guidelines 3/2019 on processing of personal data through video devices.

Finalmente, la empresa necesitará documentar su decisión[33].

5. DEBER DE SECRETO Y MEDIDAS DE SEGURIDAD

La empresa (responsable de los ficheros de registro de jornada) y aquellos otros (empleados, representantes legales de los trabajadores, terceros) que intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsisten aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo (art. 5 RGPD y art. 5 LOPDGDD).

Es preciso, a estos efectos, que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con la norma. Este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo. Al respecto, las medidas de responsabilidad proactiva son principalmente: i) Evaluación del impacto sobre la protección de datos; ii) Registro de actividades del tratamiento; iii) Protección de datos desde el diseño y por defecto; iv) Notificaciones de violaciones de seguridad de los datos antes de 72h; y, v) Medidas de seguridad y análisis de riesgos.

Además, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento deben aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: i) la seudonimización y el cifrado de datos personales; ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; iii) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y, iv) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad, el empresario debe tener particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Por último, la adhesión a un código de conducta o a un mecanismo de certificación puede servir de elemento para demostrar el cumplimiento de los requisitos descritos.

6. DERECHOS DE LOS TRABAJADORES (ACCESO, RECTIFICACIÓN, OPOSICIÓN Y SUPRESIÓN)

La empresa debe conservar los registros de jornada durante cuatro años y permanecerán a disposición de los trabajadores, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social. Nada refiere el artículo 34.9 del ET respecto al modo de conservación de los registros, por lo que debe entenderse válido cualquier medio de conservación siempre que se garantice su preservación y la fiabilidad e invariabilidad a posteriori de su contenido, ya se trate de soporte físico o cualquier otro que asegure idénticas garantías. Por otro

[33] Puede consultarse el caso francés en el link: https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf También resultan interesantes los elementos técnicos jurídicos y éticos publicados por la CNIL: https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux

lado, y a diferencia del registro de los contratos a tiempo parcial, el deber de conservación se extiende a los registros diarios y no se prevé la totalización de los mismos en periodos más extensos, sin perjuicio de las obligaciones previstas en el caso de horas extraordinarias[34].

El almacenamiento de datos de registro horario de los empleados debe permitir el derecho de acceso de éstos, como paso previo para, en su caso, poder solicitar su rectificación o cancelación así como la oposición a determinados tratamientos (por ejemplo, elaboración de perfiles) (arts. 15-22 RGPD y arts. 12-18 LOPDGDD). El trabajador tiene derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

La exigencia de que permanezcan a disposición debe interpretarse en el sentido de que sea posible acceder a los mismos en cualquier momento en que se soliciten por los trabajadores, sus representantes o la Inspección de Trabajo y Seguridad Social, garantizando el empresario su cumplimiento, que será coherente con el sistema de registro utilizado. Esta obligación está establecida directa y expresamente en la Ley por lo que no puede ser condicionada en ningún caso. En este sentido, que los registros "permanecerán a disposición" debe interpretarse en el sentido de estar y permanecer físicamente en el centro de trabajo, o ser accesibles desde el mismo de forma inmediata. Dicho con otras palabras, que sea posible acceder a dichos registros en cualquier momento, cuando así sea solicitado por los trabajadores, sus representantes y por la Inspección de Trabajo y Seguridad Social. Con ello, se evita, además, la posibilidad de la creación posterior, manipulación o alteración de los registros. En cuanto a la obligación de entrega o forma concreta de puesta a disposición, se ha aclarado que nada señala la norma que implique hacerla equivalente a los registros de jornada de los contratos a tiempo parcial, horas extraordinarias o de trabajadores móviles. Por tanto, debe entenderse, por razones de seguridad jurídica, que la permanencia a disposición no implica la obligación de entrega de copias, salvo pacto expreso en contrario, ni debe entregarse al trabajador individual copia de su registro diario, sin perjuicio de facilitar su consulta personal, ni a los representantes legales de los trabajadores, lo que no obsta, de nuevo, la posibilidad de estos últimos de tomar conocimiento de los registros de los trabajadores[35].

En la negociación más reciente se ha abordado el registro de jornada prestando una especial atención a los derechos de acceso de trabajadores y representantes de los trabajadores. Sirva de muestra el Acuerdo Parcial del Convenio Colectivo del Sector de Cajas y Entidades Financieras de Ahorro, cuyo apartado VI titulado "Accesibilidad, información y seguimiento del registro de jornada" establece que: "Primero. Los trabajadores y las trabajadoras podrán acceder a su registro diario de jornada a través de la aplicación puesta a su disposición para consultar los datos a que se ha hecho referencia en los apartados anteriores. En este mismo acuerdo, se pacta la entrega en soporte informático de los contenidos del registro de jornada a los representantes legales de los trabajadores: "Segundo. Con carácter mensual la empresa facilitará a la representación legal de los trabajadores, mediante soporte informático (formato hoja de cálculo) el contenido del registro de jornada de las personas trabajadoras del centro de trabajo en el que ejerzan su representación. La misma información, y en los mismos términos,

[34] Guía sobre el registro de jornada del Ministerio de Trabajo, Migraciones y Seguridad Social y Criterio Técnico 101/2019 sobre Actuación de la Inspección de Trabajo y Seguridad Social en materia de registro de jornada. Este último puede consultarse en: https://www.laboral-social.com/sites/laboral-social.com/files/CRITERIO_TECNICO_101_2019_REGISTRO_JORNADA.pdf

[35] Guía sobre el registro de jornada del Ministerio de Trabajo, Migraciones y Seguridad Social y Criterio Técnico 101/2019 sobre Actuación de la Inspección de Trabajo y Seguridad Social en materia de registro de jornada.

se facilitará a los Delegados Sindicales, en el ámbito de su representación, de conformidad con lo establecido en el artículo 10.2 y 3 de la Ley Orgánica de Libertad Sindical"[36].

Especiales previsiones se realizan cuando existan controversias o diferencias concretas en relación con los registros de algún trabajador. Es el caso de la modificación del VI Convenio Colectivo General del Sector de la Construcción, en concreto, el artículo 67 cuyo contenido dice lo siguiente: "De acuerdo con lo previsto en el artículo 34.9 del Estatuto de los Trabajadores los registros permanecerán a disposición de las personas trabajadoras y de sus representantes legales para su consulta. Para ello se facilitará la consulta a las personas trabajadoras respecto de su propio registro cuando éstas lo consideren necesario, así como a la representación legal de los trabajadores (evitando los datos de identificación personal) dentro de su respectivo ámbito de competencia (empresa o centro de trabajo) cuando existan controversias o diferencias concretas en relación con los registros de alguna persona trabajadora, pudiéndose fijar entre la empresa y la citada representación, a los efectos de racionalizar la consulta, en el ámbito de la empresa o centro de trabajo, plazos periódicos para el ejercicio de este derecho. Los representantes legales de los trabajadores deberán guardar la oportuna reserva y proteger los datos consultados de acuerdo con la normativa vigente de protección de datos personales, así como con lo establecido en el artículo 64 y 65.2 del Estatuto de los Trabajadores"[37].

Se remarca en la negociación colectiva el fácil acceso a los datos almacenados por parte de los trabajadores. Un ejemplo de ello es el Convenio Colectivo del Sector de Comercio Vario: "Artículo 40. Jornada laboral. El sistema de registro de jornada siempre garantizará la intimidad del trabajador/a y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Garantizará la objetividad, fiabilidad e invariabilidad de los datos, imposibilitará la manipulación, alteración o creación posterior del registro. Será un sistema que permita el fácil acceso y consulta de los datos por parte de los trabajadores/as y sus representantes"[38].

Los derechos de rectificación de los trabajadores también son objeto de tratamiento por parte de los negociadores: "Artículo 16 Bis (…). 16.3 El sistema debe permitir que los trabajadores puedan acceder en cualquier momento a los datos registrados de su jornada indicados en el apartado anterior. En caso de no ser posible, la información se le facilitará con carácter mensual, en la que constarán los datos indicados anteriormente. Independientemente de lo anterior, el trabajador podrá cotejar la información de su jornada mediante el acceso del propio trabajador a sus datos, por petición expresa al departamento correspondiente en cada Organismo. En el supuesto de que no se hallare conforme con el mismo, podrá efectuar la reclamación oportuna ante dicho departamento. Con carácter mensual, la Sección Sindical Regional correspondiente recibirá la misma información que la recibida por las personas trabajadoras de forma individual, así como la totalización de las horas de trabajo efectuadas mensualmente por cada uno de ellos (jornada laboral ordinaria, complementaria y extraordinaria). La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras y de sus Secciones Sindicales Regionales"[39].

[36] BOE 30 octubre 2019, núm. 261.

[37] BOE 5 noviembre 2019, núm. 266.

[38] BO. Comunidad de Madrid 26 octubre 2019, núm. 255.

[39] Convenio Colectivo Marco de la Unión General de Trabajadores 2019-2020, BOE 2 octubre 2019, núm. 237. En parecidos términos, cabe mencionar el Convenio Colectivo del Comercio de Actividades Diversas para la Comunitat Valenciana 2019-2020. DO. Generalitat Valenciana 3 octubre 2019, núm. 8648 que indica: "Una vez implantado el sistema informático de registro de jornada, a los/as trabajadores/as se les proveerá de una clave de acceso para poder acceder a dicho fichero. El sistema utilizado en momento alguno atentará contra el derecho de las trabajadoras y trabajadores, a su intimidad, a la protección de datos de carácter personal y los derechos digitales reconocidos en la normativa vigente. Con carácter semanal, el trabajador recibirá notificación con todo

Cuando el trabajador cesa en su relación laboral, este cese define el momento en que se inicia el bloqueo de sus datos y luego, cumplidos los correspondientes plazos, los datos serán eliminados ("Derecho al olvido"). Los datos deben permanecer "congelados" e inaccesibles a los usuarios mismos. En el caso de grabación de imágenes de los trabajadores con finalidad de control horario, se deben cancelar las imágenes en el plazo máximo de un mes y que únicamente se conservan aquellas que registren una infracción o incumplimiento de los deberes laborales (arts. 22.3 y 89.3 LOPDGDD).

7. EL TRATAMIENTO DE DATOS DEL REGISTRO DE JORNADA EN LAS ESTRUCTURAS EMPRESARIALES COMPLEJAS

El fenómeno de las estructuras empresariales complejas, plenamente extendido en la realidad española, comprende las contratas (y subcontratas), las empresas de trabajo temporal, así como los grupos de empresas. Todos ellos tienen en común la existencia de una pluralidad de empresarios en sentido económico-productivo: empresario principal y contratista; empresa de trabajo temporal y empresa usuaria; y las empresas pertenecientes al grupo. Sin embargo, desde el punto de vista legal, el poder de dirección así como el deber de seguridad del empresario no siempre es compartido por todas las empresas implicadas. Se debe plantear entonces quién es el responsable de realizar el tratamiento de los datos de registro de jornada en las mencionadas situaciones.

La respuesta no la encontramos en el RD-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, sino en la Guía sobre el registro de jornada del Ministerio de Trabajo, Migraciones y Seguridad Social que ofrece una solución interpretativa al respecto. En el caso de las empresas de trabajo temporal, el artículo 15.1 de la Ley 14/1994, de 1 de junio, por la que se regulan las empresas de trabajo temporal, referido a la dirección y control de la actividad laboral, establece que "cuando los trabajadores desarrollen tareas en el ámbito de la empresa usuaria, de acuerdo con lo previsto en esta norma, las facultades de dirección y control de la actividad laboral serán ejercidas por aquélla durante el tiempo de prestación de servicios en su ámbito". De modo que, correspondiendo a la empresa usuaria las facultades de dirección y control de la actividad laboral de los trabajadores puestos a disposición durante el tiempo en que estos presten servicios en su ámbito, habrá de ser la empresa usuaria la obligada al cumplimiento del deber de registro diario de la jornada establecida en el artículo 34.9 ET y, por tanto, la responsable del tratamiento de los datos de carácter personal de los empleados vinculados con el deber de registro. Y deberá cumplir con la obligación de conservar los registros a que se refiere este precepto durante cuatro años, manteniéndolos a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social. Ahora bien, toda vez que, conforme al artículo 12.1 de la Ley 14/1994 "corresponde a la empresa de trabajo temporal el cumplimiento de las obligaciones salariales y de Seguridad Social en relación con los trabajadores contratados para ser puestos a disposición de la empresa usuaria", la ETT y la empresa usuaria deben establecer los procedimientos de aportación de los registros para el cumplimiento de sus obligaciones[40].

el detalle necesario para su comprensión del control horario efectuado. En el supuesto de que no se hallare conforme con el mismo, podrá efectuar la reclamación oportuna ante el departamento correspondiente de la empresa. Con carácter mensual, la representación legal de los trabajadores recibirá la misma información que la recibida por las personas trabajadoras de forma individual, así como la totalización de las horas de trabajo efectuadas mensualmente por cada uno de ellos (...)".

[40] Guía sobre el registro de jornada del Ministerio de Trabajo, Migraciones y Seguridad Social.

En cuanto a la subcontratación del artículo 42 ET, dado que el control de la actividad permanece en la empresa contratista o subcontratista, verdadera empleadora, esta será la responsable del cumplimiento de todas las obligaciones laborales, incluidas las relativas a registro diario de jornada. No obstante, cuando los trabajadores de la contratista prestan actividad en la empresa principal, ambas empresas podrán acordar servirse de los sistemas de registro diario de jornada empleados en la principal para sus trabajadores. De esta manera, se dice en la mencionada Guía que se asegura la mayor fiabilidad de la jornada efectivamente realizada por los trabajadores de la contratista, así como su control por esta última de defectos o excesos de la jornada que puedan contradecir los términos acordados en la relación interempresarial y ser objeto de responsabilidad. En todo caso y a diferencia del caso de las ETT's sigue siendo obligación de la contratista conservar y mantener la documentación de los registros diarios realizados[41]. Pese a la posibilidad que se ofrece de uso de los medios de registro de la empresa principal, no resulta modificada la condición de responsable de la empresa contratista en materia de protección de datos. En este sentido, resulta conveniente que el sistema de registro de jornada de la empresa principal permita la identificación del trabajador y su respectiva empresa a los efectos de poder deducir posibles responsabilidades en caso de incumplimiento de la obligación de registro diario de jornada.

8. LAS SANCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y DE LA INSPECCIÓN DE TRABAJO Y SEGURIDAD SOCIAL: ¿SON COMPATIBLES?

Finalmente, en cuanto el régimen sancionador, las novedades incluidas en el Real Decreto-Ley 8/2019 suponen también la modificación del apartado 5 del artículo 7 del texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por el Real Decreto Legislativo 5/2000, de 4 de agosto, que queda redactado en los siguientes términos: "5. La transgresión de las normas y los límites legales o pactados en materia de jornada, trabajo nocturno, horas extraordinarias, horas complementarias, descansos, vacaciones, permisos, registro de jornada y, en general, el tiempo de trabajo a que se refieren los artículos 12, 23 y 34 a 38 del ET"[42]. La modificación introducida es clara, ya que tipifica como infracción grave la transgresión de las obligaciones en materia de registro de jornada, incluyendo su previsión específica en el artículo 7.5 transcrito. Sin embargo, se debe advertir que el régimen sancionador previsto en los artículos 83-84 RGPD y artículos 72-74 LOPDGDD resulta compatible con el previsto en la LISOS. Lo que significa que, además de las sanciones tipificadas en la LISOS, la empresa responsable del cumplimiento del deber de registro puede incurrir en sanciones específicas en materia de protección de datos impuestas por la Agencia Española de Protección de Datos cuando el trabajador y/o los representantes legales de los trabajadores denuncien vulneraciones del régimen de protección de datos explicado en los epígrafes anteriores.

[41] Guía sobre el registro de jornada del Ministerio de Trabajo, Migraciones y Seguridad Social. Algunas experiencias convencionales se han hecho eco de esta solución. Es el caso del Acuerdo sobre el registro de la jornada de trabajo derivado del VIII Convenio Colectivo de Enseñanza y Formación No Reglada, BOE 18 de octubre de 2019 que señala: "14. En el supuesto de subcontratación de la actividad, la empresa contratista, como empresa empleadora, será la obligada a llevar el control horario de sus trabajadores, sin que el centro formativo tenga ninguna responsabilidad al respecto. No obstante, el centro formativo como empresa principal, podrá acordar con la empresa contratista llevar a cabo el control horario de este personal en lugar de la empresa contratista. En todo caso, es obligación de la contratista conservar y mantener la documentación de los registros diarios realizados".

[42] Criterio Técnico 101/2019 sobre Actuación de la Inspección de Trabajo y Seguridad Social en materia de registro de jornada.

BIBLIOGRAFÍA

BLÁZQUEZ AGUDO, E., Aplicación práctica de la protección de datos en las relaciones laborales, Wolters Kluwer, 2018.

DE LA MORENA CORRALES, P., "El Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo (en especial, la obligación de registro de jornada)", Trabajo y Derecho, núm. 54, 2019, pp. 129-138.

GIL GONZÁLEZ, E., "Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional", Revista Española de la Transparencia, núm. 5, 2017, pp. 165-179.

GOÑI SEIN, J.L., La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018), Bomarzo, 2018.

MARIN ALONSO, I., "La obligación empresarial de registro de la jornada ordinaria ante el Derecho de la Unión Europea y el Derecho Interno", Revista General de Derecho del Trabajo y de la Seguridad Social (IUSTEL), núm. 53, 2019.

MERCADER UGUINA, J.R., Protección de datos en las relaciones laborales, Francis Lefebvre, 2ª Ed, 2018.

MORÓN PRIETO, R., "El registro de jornada en los tiempos líquidos: limitaciones en la regulación y de la regulación del registro de jornada", en AA.VV. (Dir. A. DE LA PUEBLA PINILLA y J.R. MERCADER UGUINA), Tiempo de reformas: en busca de la competitividad empresarial y de la cohesión social, Tirant Lo Blanch, 2019, pp. 177-198.

MUÑOZ RUIZ, A.B., Registro de jornada y modernidad tecnológica: ¿cómo afecta al derecho fundamental de protección de datos de carácter personal de los empleados?, Blog Foro de Labos, 2019. https://forodelabos.blogspot.com/2019/05/registro-de-jornada-y-modernidad.html

El uso de la tecnología de reconocimiento facial de los empleados en la empresa: una medida de control excepcional, Blog Foro de Labos, 2019, https://forodelabos.blogspot.com/2019/10/el-uso-de-la-tecnologia-de.html

La Audiencia Nacional declara nulo el sistema de geolocalización impuesto por Telepizza a sus repartidores, Blog Foro de Labos, 2019, https://forodelabos.blogspot.com/2019/02/la-audiencia-nacional-declara-nulo-el.html

La práctica "Bring your own device" y su incidencia en la relación de trabajo: ¿tecnología a coste cero para la empresa?, Foro de Labos, 2019, https://forodelabos.blogspot.com/2019/09/la-practica-bring-your-own-device-y-su.html

RESUMEN El nuevo deber del empresario de registro de la jornada de los trabajadores presenta algunos interrogantes en materia de protección de datos de carácter personal que deben ser objeto de análisis. Precisamente, en este trabajo se clarifican y estudian con detalle las obligaciones de protección de datos que el empresario debe cumplir cuando organiza y documenta el control horario. Para ello, se pone en conexión lo dispuesto en el artículo 34.9 del ET con el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y el artículo 18.4 de la CE así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y también los informes y resoluciones de la Agencia Española en materia de Protección de Datos (AEPD).

Se advierte en el estudio que, si bien es cierto que no se requiere el consentimiento del trabajador para el tratamiento de sus datos vinculado con el registro de jornada ya que son datos necesarios para la gestión de las obligaciones del empresario y no pertenecen a la categoría de datos sensibles, se debe informar al trabajador de forma exhaustiva de la existencia del registro y de la finalidad del tratamiento de los datos personales individuales que se obtienen con dicho registro.

Una especial atención se dedica a los posibles sistemas de registro de jornada que el empresario podría implantar, algunos de ellos de especial novedad debido al empleo de la tecnología emergente como el reconocimiento facial. Se recuerda en el trabajo que el artículo 34.9 del ET no establece una modalidad específica o predeterminada para el registro diario de la jornada, limitándose a señalar que se debe llevar a cabo día a día e incluir el momento de inicio y finalización de la jornada. Para ello, y sobre el resto de elementos configuradores, llama a la autorregulación, mediante la negociación colectiva o el acuerdo de empresa. A partir de estos datos, en la investigación se establecen tres categorías posibles de registro de jornada: en primer lugar, los sistemas de registro de jornada no controvertidos porque cumplen los parámetros del principio de proporcionalidad y pueden ser utilizados por el empresario para dar cumplimiento a la obligación de registro. Dentro de la categoría de sistemas de registro de horario no controvertidos cabe englobar las anotaciones en papel con firma del trabajador, aplicaciones informáticas, tarjetas de identificación electrónica o cualquier otro medio o soporte que acredite la conformidad del trabajador con el registro efectuado. En segundo lugar, los sistemas de registro prohibidos en la medida que se obliga al trabajador a utilizar los dispositivos electrónicos de su propiedad. Esta práctica se denomina "Bring your own device" (BYOD) y se refiere a que el trabajador accede con sus medios electrónicos a las aplicaciones corporativas como el email o bases de datos y almacena y trata datos de la empresa así como de los clientes de ésta. En el estudio se explica que se trata de una práctica proscrita en materia de registro de jornada cuando resulta impuesta por parte del empresario. Es decir, dicho tratamiento excedería de lo permitido por la normativa de protección de datos, y en concreto, de la legitimación empresarial en base a la ejecución de un contrato de trabajo. Luego, se precisa del consentimiento del trabajador que podrá oponerse posteriormente a su tratamiento ejerciendo los derechos de oposición o supresión. En último término, los sistemas de registro vinculados con los datos biométricos de los trabajadores (huella dactilar y reconocimiento facial). La investigación realizada advierte que, en nuestro país, las resoluciones judiciales que existen sobre el control empresarial basado en datos biométricos de los trabajadores se han centrado en la lectura de la huella dactilar y todavía no se ha abordado la cuestión referida al tratamiento del rostro con software de reconocimiento facial. Por su parte, la AEPD ha realizado una distinción entre la tecnología de reconocimiento facial y los sistemas de fichaje por huella dactilar

implantados en algunas empresas, mostrándose más permisiva respecto de los controles de huella dactilar que en los casos del reconocimiento facial.

Especial interés tiene el desarrollo francés sobre esta cuestión. En enero de 2019 la Autoridad francesa de Protección de Datos (CNIL) aprobó unas reglas sobre el uso empresarial de la información biométrica de sus empleados tales como el reconocimiento facial. Para su empleo, se requiere el cumplimiento de los siguientes requisitos: i) Justificar al CNIL por qué necesitan usar estos sistemas y no otros menos intrusivos; ii) Disponer de medidas de seguridad para proteger los datos biométricos; iii) Llevar a cabo una evaluación de impacto. Con respecto a la primera de las exigencias (justificar la necesidad del uso de los datos biométricos), las empresas deben indicar un contexto específico o razón que precise del uso de los datos biométricos como identificadores. Algunos ejemplos podrían ser que los empleados hayan sido autorizados para usar una máquina peligrosa o acceder a objetos de valor o grandes sumas de dinero. Además, la empresa deberá demostrar por qué un método menos intrusivo (por ejemplo, una credencial o clave) no resulta suficiente. Finalmente, la empresa necesitará documentar su decisión.

Estrechamente relacionados con la esencia del derecho fundamental de protección de datos son los derechos de acceso, rectificación, oposición y supresión del trabajador. En este punto, se identifican en el artículo aquellas experiencias de negociación colectiva que han desarrollado algo más el contenido de estos derechos en materia de control horario. Igualmente, se abordan las medidas de seguridad que el empresario debe cumplir para preservar la confidencialidad de los datos recabados y evitar brechas de seguridad. El estudio se cierra con una referencia al régimen sancionador específico en materia de protección de datos de carácter personal y se pone el acento en su compatibilidad con las sanciones previstas en la LISOS.

En definitiva, el presente trabajo ofrece una perspectiva integrada de la obligación laboral de registro y el cumplimiento de los principios y garantías del derecho fundamental de protección de datos de carácter personal. Se identifican también los principales problemas jurídicos a que el empresario podría enfrentarse en función de la elección del método de registro así como también los derechos que los trabajadores podrían ejercitar de cara a rechazar alguno de los métodos impuestos por el empresario.

Palabras clave: Registro; jornada de trabajo; trabajador; tecnología; derecho de protección de datos.

ABSTRACT The new obligation of record the daily working hours of the employees has arisen some questions concerning the right to personal data. Some authors have studied only the labour approach. However, it is necessary to analyse the labour issues and the personal data protection right. It should be pointed out that the right to personal data protection is a human right. It means that the evidence of an employee misconduct (for example, be late for work) may be null (with the consequences of unfair dismissal) if the employer violates the mentioned human right. In this paper it is analysed the content and the scope of the employer's obligations in this matter in order to avoid the invalidity of the evidence. In addition, the employer may be sanctioned with very high finacial penalties.

Both perspectives are studied jointly: on the one hand, the content of the article 34.9 of the Workers' Statute and on the other hand, the Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and the article 18.4 of the Spanish Constitution such as the Law 3/2018, Personal Data Protection and the reports and resolutions of the Spanish Agency of Personal Data Protection (AEPD). In particular the reading of the reports and resolutions of the AEPD are very useful.

In the paper it is established that the consent of the employee is not necessary in order to process his personal data of the daily working hours due to those data are necessary to carry out the duties of the employer and are not data with a special protection. The employer has legitimate reasons in order to process the personal data of employees. However, the employer must inform employees in advance on the record and the purpose of the processing of his personal data. The compliance of the information duty is very relevant according to the Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The paper mentions that the article 34.9 of the Workers Statute do not establish a specific type of record. The type of record will be developed by the collective agreements or Enterprise agreements. In addition, the monitoring systems are studied such as the control based on the fingerprint and the facial recognition. In this sense, three categories of record are established: firtly, the non-controversial systems of record because they comply with the proportionality principle. The proportionality principle is a fundamental issue in matter of human rights. There are many examples into the the first category like signature sheets, computer applications, ID cards, etc. The employer may use anyone of them. Secondly, the prohibited systems of record based on the electronic devices of the employee's ownership. This practice is called "Bring your own device" (BYOD). It means that the employee uses his electronic devices in order to access the Enterprise applications like the email or data base and processes profesional data from the employer or the customers. The paper defends that this practice is prohibited when the employee is obligated to do that. The mentioned processing of data will not comply with the personal data protection regulation. In this sense, it is necesarry the consent of the employee. Finally, the systems of record linked to biometric data of the employees (fingerprint and facial recognition). The paper concludes that in Spain the judicial cases have focused on the fingerprint. However we do not have judicial cases on facial recognition yet. The Spanish personal data agency has stablished that the employer may use the record based on fingerprints and that the facial recognition is very exceptional.

The paper provides other solutions given by the comparative law such as the French experience. In France, the French Data Protection Agency (CNIL) has approved some rules on the facial reconigtion. According to the French regulation, the employer must comply the following criteria in order to use the facial recognition: i) To justify the reasons to use the facial recognition and not other less agressive methods; ii) To take security measures to protect the biometric data; iii) To make an impact assessment.

Concerning the first criteria, the companies should provide an specific context or reason which require the use of biometric data. For example, in the case of employees who use dangerous machines or access large sums of money. In addition, the company should prove that a less agressive method (for example: a pasword) is not enough. The company should document the measure. The French experience may be useful for the application of the new duty of record in Spain.

The rights to access, rectification, erasure and opposition of the personal data are at the heart of the right to personal data. The paper analyzes some examples of colllective agreements what have agreed the content of those rights in order to improve the protection of the record the daily working hours. In this matter, the collective agreements have a very relevant role. In addition, the security measures are studied due to its relevance to guarantee the confidentiality of the data and to avoid the security breaches. Finally, the penalties in matter of personal data protection are discussed focusing on the compatibility with the penalties regulated in the Law 5/2000, 4 August, in matter of the infringements and the penalties in the employment relationship.

Indeed, the paper provides an integrated approach of the working day monitoring and the compliance of the principles and guarantees of right to personal data. The research identifies the main legal issues for the employer taking into account the chosen method of record. In special the paper points out the exceptional use in the case of facial recognition showing the French case. Therefore other methods would be less risky like the signature sheets, computer aplications, ID cards, etc. In addition the employees' rights are explained.

Keywords: Record; working time; technology; employee; right to personal data.

Gestión y aplicación empresarial de las exigencias sobre protección de datos personales

Business management and implementation of personal data protection requirements

EVA MARÍA BLÁZQUEZ AGUDO*

1. INTRODUCCIÓN. NUEVAS NORMAS, NUEVOS TIEMPOS, PERO SIEMPRE CON EL DERECHO DE INTIMIDAD COMO LÍMITE

Como bien se conoce, el contexto legal de la protección de datos ha sido modificado en profundidad en los últimos dos años. En primer lugar, el 25 de mayo de 2018 entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), que de acuerdo con la técnica legislativa elegida es de aplicación directa a todos los Estados miembros de la Unión Europea. Con el objeto de adaptar la normativa española a esta modificación, un tiempo después se ha aprobado la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (BOE 6 de diciembre de 2018), en adelante LOPD en sustitución de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD de 1997)[1]. Esperada era esta nueva ley por dos motivos fundamentales: en primer lugar, como su propia Exposición de Motivos señala, con el fin de "*eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo*"; pero, asimismo, con otro importante fundamento como es la adaptación de este acervo normativo a las exigencias que la nueva sociedad digital que difícilmente podrían ser atendidas con una ley que tenía ya más de 20 años.

Si bien la Ley de Protección de Datos Personales anterior, la de 1997, tenía en paralelo un desarrollo normativo que ofrecía a través del RD 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, la vigente no tiene este desarrollo todavía. Es esperable que no se tarde diez años como ocurrió con la anterior legislación, y se apruebe lo antes posible una nueva normativa más concreta que venga a resolver algunas cuestiones que ahora se plantean en la aplicación práctica de la Ley Orgánica, cuestiones que se reseñarán en este análisis, especialmente en el ámbito laboral.

* Profesora Titular de Derecho del Trabajo y de la Seguridad Social (en servicios especiales) Universidad Carlos III de Madrid

[1] Esta norma procedió a la transposición de las nuevas directrices europeas marcadas por la Directiva 95/46/CE, de 24 de octubre de 1995, del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos.

1.1. El reducido avance legislativo en materia laboral

Aterrizando en el ámbito laboral, mientras que en la LOPD de 1997 no se recogía ninguna referencia a este sector, en la nueva norma sí se regulan algunas cuestiones en la materia, rompiendo con la inercia de aplicar las reglas generales sobre la protección de datos personales a un entorno regulatorio con tantas peculiaridades como el laboral. El avance ha sido propiciado por el RGPD que ya en su Considerando 115 determina que los Estados miembros de la Unión Europea tienen que establecer normas específicas relativas al tratamiento de datos personales de los trabajadores. Después de esta declaración de intenciones, en su artículo 88, se avanza en esta cuestión, especificando que en esta normativa es preciso determinar las condiciones de tratamiento de los datos personales sobre la base del consentimiento del trabajador, los fines de la contratación, la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

Además, hay que poner de manifiesto que en el RGPD se recogen expresamente otras dos cuestiones sobre derecho laboral: una relativa a la regulación de las situaciones de trasferencia de datos entre los grupos de empresa o uniones de empresas dedicadas a una actividad económica conjunta, fomentando el desarrollo de políticas corporativas, entre las cuales se encuentran los tratamientos aplicables a los datos personales de los trabajadores; y una segunda, sobre la regulación de los sistemas de supervisión en el lugar de trabajo, entre los cuales se encuentra principalmente la videovigilancia y el control informático. En este contexto, se pone de manifiesto, habrá que avanzar en los sistemas nacionales, pero siempre con unos límites claros como son, en general, todo el acervo comunitario en la materia, como no podía ser de otra manera, pero también el respeto a los derechos y libertades de los trabajadores, en concreto a la dignidad humana de los interesados, así como a sus intereses legítimos y a sus derechos fundamentales.

En resumen, el RGPD recoge la necesidad de crear un cuerpo de normas aplicables al concreto ámbito las relaciones laborales, adaptado a sus particularidades, tal y como se pone en evidencia en el articulado de la normativa europea. En primer lugar, las diferencias se imponen porque no es preciso el consentimiento del trabajador para tratar sus datos personales en el ámbito del contrato de trabajo como sí lo es en general para el resto de los tratamientos. Y, además, es preciso valorar en todo momento el equilibrio entre el necesario tratamiento de los datos y los derechos fundamentales de los empleados.

De acuerdo con estas bases indicadas en el RGPD, se regula esta cuestión en el ámbito nacional en la nueva LOPD. No obstante, y antes de seguir avanzando, hay que poner de manifiesto que se echa de menos una verdadera regulación en el ámbito de las relaciones laborales que vaya analizando pormenorizadamente los diferentes contextos que menciona la norma europea o, por lo menos, que dibuje los principales elementos precisos para desarrollar el tratamiento de los datos personales de las personas trabajadoras de forma segura. Es decir, que, en contra de lo que determina el artículo 88 de la RGPD, en la LOPD no se determinan ni las condiciones de tratamiento de los datos personales en este entorno sobre la base del consentimiento del trabajador, ni los fines de la contratación, ni la ejecución del contrato laboral, ni la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como tampoco los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la

relación laboral. De modo que, sin este desarrollo, en la mayoría de los supuestos se está aplicando las mismas reglas generales que ya se empleaban con anterioridad, aunque eso sí, atemperados por los principios generales de la nueva regulación europea.

1.2. Los no tan nuevos derechos digitales

Lo que sí se recoge la regulación de la LOPD son los nuevos derechos digitales en el ámbito de las relaciones laborales, que ha introducido modificaciones tanto en el Texto Refundido de la Ley del Estatuto de los Trabajadores como en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público. De los dieciocho artículos que se dedican en la LOPD a dichos derechos digitales, cinco de ellos se refieren al sector aquí analizado.

Así, se reconoce el derecho a la intimidad en el uso de dispositivos digitales; el derecho a la desconexión digital; el derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo; el derecho a la intimidad ante la utilización de sistemas de geolocalización y los derechos digitales en la negociación colectiva. Además, se añade alguna otra cuestión sobre la protección especial de delegado de protección de datos (artículo 36 de la LOPD) que es aplicable al régimen de relación laboral de quien ostente esta figura y el responsable del tratamiento, así como una alusión a los datos de afiliación sindical en la Exposición de Motivos de la LOPD.

Fuera de estas cuestiones nada aporta la nueva LOPD a las relaciones laborales, tal y como aquí se adelantó. Esta conclusión lleva a sustentar que en la práctica las reglas que se empleaban con anterioridad a la aprobación de la RGPD siguen en parte aplicándose en el entorno laboral en la mayoría de las situaciones. El único cambio real es el reconocimiento expreso de los derechos digitales, que principalmente imponen límites a través del reconocimiento del derecho a la intimidad de las personas trabajadoras en el desarrollo del tratamiento de sus datos personales. Y se dice expreso, dado que no significa una novedad, en cuanto a que ya desde el reconocimiento constitucional del derecho a la intimidad y su aplicación en el ámbito laboral, se ha creado una amplia jurisprudencia en la materia determinando dicho derecho como límite del tratamiento de datos personales en el ámbito de las relaciones laborales.

Al margen de lo señalado en la LOPD, los derechos fundamentales de los trabajadores deben ser respetados a tenor de lo establecido en la Constitución Española, con lo cual, como se ha señalado, las declaraciones sobre el derecho a la intimidad de las personas trabajadoras realmente no son necesarias con el fin de que se respeten dichas prerrogativas, dado que existía ya un compendio de jurisprudencia que desarrolla sus límites. Si bien es verdad que no se podía establecer el punto concreto de equilibrio entre los derechos de las partes, y había que estar al examen de cada caso concreto, la nueva normativa tampoco da un paso más en el asunto, sino que sigue siendo de aplicación la misma solución. Es tan difusa esta cuestión, que la propia LOPD anima a modificar estos derechos fundamentales de acuerdo con los nuevos tiempos. Y, como a continuación se pasa a analizar, ese debería ser el camino que seguir con el fin de aclarar los límites de los derechos fundamentales de las personas trabajadoras en este ámbito.

1.3. Otra vez girando en la órbita del juicio de ponderación

Pasando a analizar someramente los límites del tratamiento de los datos personales de los trabajadores, el primer límite se encuentra en el derecho a la autodeterminación informativa que, aunque se reconoce como un derecho fundamental autónomo en el párrafo cuarto del artículo 18 de la Constitución Española, sin embargo, su ejercicio siempre está vinculado a otros derechos, principalmente en el

ámbito analizado, al derecho a la intimidad. Es decir, no actúa de forma independiente, sino vinculado a otros. En esta línea, la LOPD no lo recoge, sino que cuando impone los límites de los derechos fundamentales en la materia hace referencia solamente al derecho a la intimidad.

Así, el artículo 87 de la LOPD recoge el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral. Posteriormente, el 89 del mismo cuerpo legislativo menciona la aplicación de este derecho al ámbito del uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo. Y, por último, su artículo 90 menciona la aplicación del mismo derecho fundamental, pero esta vez aplicable a la utilización de los sistemas de geolocalización en este ámbito laboral.

En definitiva, el derecho fundamental a la intimidad de los trabajadores sigue siendo el principal límite aplicable al tratamiento de los datos personales en este contexto. Y algo que no parece cambiar en el tiempo son los vaivenes jurisprudenciales sobre el punto de equilibrio entre dicho derecho y el poder de dirección empresarial. La LOPD no va más allá de reconocer que hay que respetar unos estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente, pero después de esta declaración programática, no determina los límites concretos de dicho derecho. Así, de nuevo la pelota está en el tejado del conocido juicio de ponderación, interpretado de forma a veces caprichosa por las cambiantes decisiones de los tribunales. Dicho de otro modo, habrá que estar casi a cada caso concreto para determinar cuál es el límite que respetar en este ámbito.

Sin entrar en la materia, simplemente recordar, como no puede ser de otra forma en cualquier introducción de un estudio en materia de protección de datos personales en el ámbito laboral, los pasos seguidos en la comprobación del principio de ponderación. En resumen, son el juicio de idoneidad (la actuación empresarial únicamente debe perseguir el ejercicio estricto de su poder empresarial), el principio de mínima intervención (el análisis de que no hay otra posible actuación empresarial, que sea menos agresivo con los derechos fundamentales de los trabajadores[2], y el juicio de proporcionalidad (valorar los beneficios y desventajas de la medida adoptada)[3].

En los últimos tiempos, varias han sido las sentencias del Tribunal Europeo de Derechos Humanos en relación con esta cuestión que han pivotado alrededor de dos casos concretos. En primer lugar, la sentencia de 12 de enero de 2016 (caso Bârbulescu vs. Romania) examinó un supuesto donde existía una política empresarial de uso de las comunicaciones limitada a finalidades de la prestación de servicios, de forma que cuando la empresa detecta la mala utilización para fines personales, despide al trabajador. El Tribunal se interroga sobre la existencia de una expectativa razonable de intimidad en el uso de la mensajería en el momento de puesta disposición de los medios de la empresa al trabajador y su interiorización del posible control de la empresa. Se concluye que se ha ejercido el poder empresarial de forma proporcionada y limitada a la finalidad perseguida, y que, por tanto, no se ha violado el derecho a la intimidad personal del trabajador. No obstante, más tarde la Gran Sala del TEDH, en la sentencia 5 de septiembre de 2017, vuelve a examinar el mismo asunto y concluye de distinta forma. Es preciso valorar si el empresario ha informado de forma previa a los trabajadores sobre la posibilidad de que sus comunicaciones sean vigiladas en cualquier momento y, además, es necesario que la empresa justifique la razón de este tipo de control y valore sus consecuencias[4]. De modo

[2] COMMITTEE OF MINISTERS, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, abril 2015, p. 1.

[3] Estos pasos se pueden analizar a través de la STC 39/2016, de 3 de marzo.

[4] MOLINA NAVARRETE, C., "De Bârbulesku II a López Ribalta: ¿qué hay de nuevo en la protección de los trabajadores?" en *Revista de Derecho del Trabajo y de la Seguridad Social, CEF*, núm. 419/2018.

que como no se ha comprobado si el trabajador ha recibido la información previa, ni se ha analizado los límites del control, ni el grado de intrusión en la vida privada del empleado, el Tribunal entiende que hay que indemnizar al trabajador, ya que los tribunales nacionales correspondientes no han cumplido su función de garante de los derechos del demandante ante terceros.

La segunda jurisprudencia europea para analizar la recoge la STEDH de 9 de enero de 2018 (caso López Ribalda y otros vs. España), donde se examina un supuesto en el que se instalan cámaras en una empresa, unas visibles para controlar posibles robos de los clientes, y otras ocultas para vigilar los posibles incumplimientos de las personas trabajadoras. En base a los ilícitos captados por las segundas, se despide a un grupo de trabajadores. Los tribunales españoles concluyeron que el medio de control había sido apropiado con la finalidad perseguida, necesario y proporcionado. El Tribunal Europeo de Derecho Humanos declara que como la videovigilancia en el lugar de trabajo significa una intromisión en la vida privada, es preciso informar sobre su uso para evitar la vulneración del derecho a la intimidad de los trabajadores. No obstante, cuando este supuesto ha sido de nuevo analizado por la Gran Sala, en su sentencia de 17 de octubre de 2019, se ha modificado la resolución. Así, a través del análisis del juicio de ponderación se concluye que el derecho de intimidad de las personas trabajadoras no ha sido vulnerado. La sospecha de los ilícitos justifica la utilización de la videovigilancia sin necesidad de informar previamente a las personas trabajadoras. En resumen, el punto de equilibrio se traslada hacia el poder de dirección de las empresas.

Estas dos sentencias ponen de manifiesto, una vez más, la necesidad de una regulación clara y segura sobre el límite entre los derechos fundamentales de las personas trabajadoras en el desarrollo de su prestación y, en concreto, en el ámbito de la protección de los datos personales, que sigue dependiendo del examen del supuesto concreto a través del juicio de ponderación. En definitiva, la empresa en la gestión del tratamiento de los datos personales de sus trabajadores deberá valorar si se desarrolla con respeto a sus derechos fundamentales, en especial el de intimidad, y en su caso, si se cumple el juicio de ponderación en la puesta en marcha de sus políticas en el contexto de la protección de datos.

2. LA POSICIÓN DE LA EMPRESA COMO RESPONSABLE EN EL TRATAMIENDO DE DATOS DE SUS TRABAJADORES. EN ESPECIAL SU RELACIÓN CON EL ENCARGADO Y CON EL DELEGADO DE PROTECCIÓN

El artículo 28 de la LOPD determina las obligaciones de los responsables y encargados, sin incluir una definición de estas figuras, dado que a estos efectos se remite al RGPD. Además, existe otra figura que es el delegado de protección de datos, cuyo nombramiento es preceptivo en algunas empresas.

2.1. El responsable del tratamiento

El responsable del tratamiento, aunque parezca repetitivo, es quien tiene la responsabilidad de que durante el tratamiento de los datos personales se cumpla estrictamente la norma aplicable. En la empresa obviamente será el empresario o persona en quien este delegue, asumiendo tanto el RGPD como la LOPD la posibilidad de que exista una corresponsabilidad, es decir, que existan varios responsables del tratamiento. En este contexto, el RGPD asume la definición de grupo empresarial como aquel constituido por una empresa que ejerce el control y sus empresas controladas y, además, declara que en estos supuestos el responsable será la empresa que tiene la posición dominante, por ejemplo, por propiedad, por participación financiera, entre otras. Su establecimiento principal será el de la empresa que ejerce el control, excepto

cuando los fines y medios del tratamiento los determine otra empresa. La determinación de la empresa principal a efectos de responsabilidad es fundamental para determinar la normativa estatal a aplicar al tratamiento de los datos.

A la empresa responsable del tratamiento se le va a exigir una responsabilidad proactiva a los efectos de controlar todas las cuestiones relativas al tratamiento de los datos personales de sus trabajadores. Tendrán que adoptarse medidas técnicas y organizativas apropiadas para garantizar su licitud en el momento del tratamiento, pero, asimismo, deberá valorar con anticipación los posibles riesgos para los derechos y libertad de los avances tecnológicos de forma consciente, diligente y proactiva[5]. Es decir, no solamente tiene que resolver las cuestiones que vayan surgiendo en la materia, sino que deberá anticiparse y tener preparada la respuesta a las situaciones que se vayan planteando.

Lo primero que tendrá que decidir la empresa es si debe hacer una evaluación previa de impacto del tratamiento, valorando de acuerdo con el artículo 28 de la LOPD, si se pueden generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados; de privación a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales; de tratamiento generalizado de categorías especiales de datos; de evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos; de utilización de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad; de tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales; o de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

En general, parece que la empresa tendrá obligación de desarrollar esta evaluación de impacto cuando queden afectados de forma importante los derechos fundamentales de sus trabajadores. Retomando las sentencias que se analizaron a propósito de la aplicación del juicio de ponderación, habrá que concluir que cuando sea posible afectar al derecho a la intimidad a través del uso de medios informáticos o de videovigilancia para el control de sus empleados será precisa tal evaluación. En todo caso, no será obligatorio en el supuesto de tratamientos basados en obligaciones legales y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral[6].

Además de la posible evaluación previa, la responsabilidad activa, como se ha señalado, determina que el responsable deba diseñar la política de tratamiento de los datos que se adapte a las finalidades perseguidas en el tratamiento; las medidas que valoren los riesgos del tratamiento de forma continua, estimando los efectos del avance de las tecnologías; y el catálogo de medidas de seguridad que debe aplicar en cada caso según la naturaleza de los datos personales. Estas obligaciones pueden ser objeto de un protocolo desarrollado

[5] AEPD/APDECAT/ Agencia Vasca de Protección de Datos, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*, 2017, p. 3.

[6] AEPD, *Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5 RGPD*, 2019.

por la empresa, que vaya siendo adaptado a la evolución de la tecnología.

2.2. El encargado del tratamiento, una posición de confianza

El responsable, esto es, la empresa, nombrará al encargado, que estará sometido al primero, quien establece las instrucciones de actuación del encargado, y con el que tendrá una relación de confianza. El encargado del tratamiento tiene una obligación fundamental que consiste en velar por el cumplimiento de la normativa de protección de datos. Además, el RGPD establece que es el encargado del registro de las actividades del tratamiento y debe determinar las medidas de seguridad.

El encargado puede ser un trabajador o un externo, en todo caso, de acuerdo con el artículo 28 del RGPD, el responsable y el encargado deben siempre firmar un contrato escrito, donde se establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable y se haga mención a su deber de confidencialidad.

Siempre bajo las instrucciones del responsable, tendrá que apoyarle en el cumplimiento de la responsabilidad proactiva, especialmente en la evaluación del impacto del tratamiento; en el desarrollo de los derechos reconocidos a los interesados sobre el tratamiento de sus datos personales; así como definir las relaciones con las autoridades competentes en la materia.

El artículo 33 de la LOPD determina que el responsable del tratamiento decidirá si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado. Se recoge una excepción en la norma. No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

2.3. El delegado de protección de datos (el DPD)

El RGDP ha incluido una nueva figura en esta materia que es el delegado de protección de datos, que deberá ser designado por el responsable y el encargado del tratamiento. No siempre es obligatorio su nombramiento. La LOPD determina, de acuerdo con la norma europea, en qué supuestos es obligatorio su nombramiento. Se basa en el tipo de actividad empresarial que se desarrolla, generalmente relacionadas con el tratamiento de categorías de datos especiales o de un número importante de datos (seguridad privada, centros sanitarios, entre otros). En todo caso, si se está al margen de estos supuestos tasados, pero, se decide nombrar un DPD, la normativa aplicable a su relación y obligaciones es la misma que la general. De acuerdo con la LOPD, si se nombra un DPD, habrá que informar a la AEPD o a las correspondientes de las distintas comunidades autónomas en el plazo de diez días desde su designación. En todo caso, continua la norma, todas las agencias tendrán listas accesibles de posibles delegados de protección de datos.

El DPD podrá ser una persona física o jurídica, pudiendo formar parte tanto de la plantilla del responsable como del encargado del tratamiento a través de una relación laboral o mediante la externalización del servicio. Puede ser a tiempo completo o parcial en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Al DPD se le exigen dos requisitos. En primer lugar, ciertas cualidades profesionales, en particular, es preciso contar con conocimientos especializados del Derecho y la práctica en materia de protección de datos, así como capacidad para desempeñar las funciones propias de la figura. Por tanto, deberá designarse a alguien

que tenga conocimiento suficiente en el tratamiento de datos personales y no podrá ser alguien técnico, sino alguien que conozca las normas de funcionamiento y los efectos posibles en caso de incumplimiento[7]. Estas condiciones, señala la LOPD, que pueden demostrarse por mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos[8].

Una segunda condición es la garantía de independencia dentro de la organización, debiendo evitarse cualquier conflicto de intereses[9]. La LOPD señala que cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. En este sentido, se reconoce una especial indemnidad como la que asiste a los representantes unitario o sindicales frente a la sanción empresarial. Así, en caso de despido se presume que el motivo el puesto desarrollado y, por tanto, es discriminatorio y debe ser calificado como nulo.

Una vez determinadas sus características, habrá que precisar cuáles son sus funciones. En primer lugar, son informar y asesorar sobre cualquier cuestión relativa al tratamiento de la protección de datos, así como servir de vínculo entre los interesados y las autoridades competentes. Para poder ejercer correctamente estas ocupaciones, la empresa y el encargado tendrán que informarle de todas las cuestiones relativas a esta materia, de modo que, por ejemplo, tendrán que participar en las reuniones de los cuadros directivos altos y medios; así como estar presente en todas las tomas de decisiones relacionadas con esta materia. Pero, en ningún caso quedará bajo sus instrucciones, dado que debe ejercer sus tareas de forma independiente.

En materia de asesoramiento, el RGPD señala como funciones para el delegado de protección de datos el control de las obligaciones normativas sobre el tratamiento de los datos personales; la vigilancia del cumplimiento de dichas obligaciones y de las políticas que se están llevando a cabo en cada entidad, pudiendo participar en la formación y concienciación del personal que participa en el tratamiento, así como en las auditorias; y el asesoramiento en la evaluación de los riesgos del tratamiento.

En la parte de intermediación, actúa como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos a tenor

[7] Entre sus cualidades personales, debería incluir, por ejemplo, la integridad y un nivel elevado de ética profesional; y el interés por la promoción de una cultura de protección de datos dentro de la organización y el cumplimiento de los elementos esenciales del RGPD. *Vid.* GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre los delegados de protección de datos (DPD), op. cit.*, pp. 12 y ss.

[8] Para obtener la certificación del DPD, la AEPD y se exigen como prerrequisitos: a) la experiencia profesional de, al menos, cinco años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos; b) la experiencia profesional de, al menos, tres años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos, y una formación mínima reconocida de sesenta horas en relación con la materia; c) la experiencia profesional de, al menos, dos años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD en materia de protección de datos, y una formación mínima reconocida de cien horas en relación con la materia; d) la formación mínima reconocida de ciento ochenta horas en relación con la materia. Quien cumpla estos requisitos, podrá acceder a un examen. El modelo de evaluación se complementa con la prueba de la práctica en la materia. *Vid.* Unidad de Evaluación y Estudios Tecnológicos de la AEPD, *Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de datos,* 2 de octubre de 2017.

[9] Ejemplo de conflicto son ciertos puestos de alta dirección (tales como director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI); otros cargos inferiores en la estructura organizativa, si tales cargos o puestos llevan a la determinación de los fines y medios del tratamiento; o si representa al responsable o encargado de tratamiento en los tribunales. *Vid.* GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Directrices sobre los delegados de protección de datos (DPD*), *op. cit.*, pp. 11, 12 y 17.

del artículo 36 de la LOPD que desarrolla lo indicado al respecto en el RGPD. Con este fin el delegado podrá inspeccionar el cumplimiento de la empresa y emitir recomendaciones en el ámbito de sus competencias. Por otra parte, el afectado por una vulneración en el tratamiento de sus datos personales, podrá, con carácter previo a la presentación de una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame. En este caso, el delegado tendrá que comunicarle su valoración sobre la cuestión presentada en el plazo de dos meses. Si el afectado no hubiese consultado con el delegado, la autoridad competente podría enviarle la consulta sobre el asunto que deberá contestar en el plazo de un mes. Con el objeto de facilitar el cumplimiento de esta cuestión, es aconsejable que las organizaciones informen a sus empleados sobre el nombre y datos de contacto del DPD a través de la intranet de la organización, el directorio telefónico interno o el organigrama[10].

3. LOS PRINCIPIOS APLICABLES A LA GESTIÓN DE LOS DATOS PERSONALES. EN ESPECIAL EL TRATAMIENTO DEL CONSENTIMIENTO

El RGPD determina qué principios deben aplicarse al tratamiento de los datos de las personas físicas identificadas o identificables en general y, por tanto, también en el caso de la gestión de los datos de las personas trabajadoras en el ámbito de desarrollo de las relaciones laborales. El artículo 5 del RGPD recoge los principios de licitud, lealtad y transparencia; la minimización del dato, la limitación de la finalidad del tratamiento y la exactitud de los datos, que se vincula al derecho de los interesados de rectificación; la limitación de la conservación de los datos recogidos; la integridad y confidencialidad y la responsabilidad proactiva. Así, todo ellos son límites directos del tratamiento de los datos personales de los empleados[11].

3.1. Las distintas vías de licitud del tratamiento de los datos de las personas trabajadoras

Como regla general, el tratamiento de los datos personales solamente es lícito cuando existe consentimiento del afectado de forma libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. No obstante, existen excepciones a esta regla general y una de las más importantes es la regulada en el ámbito de las relaciones laborales. En el artículo 6 del RGPD se recoge la excepción, sin que sea ninguna novedad. La LOPD de 1999 señalaba que no era preciso el consentimiento cuando los datos se refieran a las partes de un contrato o precontrato de una relación laboral y sean necesarios para su mantenimiento o cumplimiento de esta relación, dado que se entiende implícito dicho consentimiento en el momento de la firma del contrato laboral. A sensu contrario, sí lo es cuando se va más allá del contenido de la relación laboral y, por tanto, en estos supuestos habrá que recabar consentimiento de las partes. Nada recoge en este sentido expreso la LOPD actual, de forma que habrá que estar a lo que determina el RGPD. En conclusión, la licitud del tratamiento sin consentimiento llega hasta los límites de la finalidad del contrato de trabajo, esto es, todo aquello que queda amparado por el normal desenvolvimiento de la relación laboral. El contenido de cada contrato es lo que enmarca esta cuestión. Todo

[10] Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Directrices sobre los delegados de protección de datos (DPD)*, *op. cit.*, p. 14.

[11] Article 29 data Protection Working Party, *Opinion 2/2017 on data processing at work*, junio 2017, p. 5.

lo que exceda deberá ser consentido expresamente por el trabajador[12].

Al contrario que la LOPD, el RGPD hace una mención expresa al derecho a la información de la empresa en el ámbito laboral. Si la comunicación de datos personales es un requisito contractual, o una condición necesaria para suscribir un contrato, el trabajador no solo no precisa verter consentimiento para el tratamiento de sus datos personales, sino que tendrá incluso que aportar dichos datos, por lo que habrá que informarle de esta obligación y de las posibles consecuencias de no hacerlo. Dicho de otro modo, se impone un deber de aportar los datos personales a la empresa con el fin de facilitar el normal desenvolvimiento de las relaciones laborales. Así, no solamente se admite el tratamiento de los datos personales sin precisar consentimiento, sino que incluso es obligatorio aportarlos.

Además, en ocasiones incluso es lícita la trasmisión de los datos de las personas trabajadoras a terceros, sin su consentimiento, en base a las obligaciones reguladas en la ley. El artículo 8 de la LOPD señala que el tratamiento de datos personales podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley. Es el caso, por ejemplo, de la obligación empresarial de ceder datos a la agencia tributaria para el cumplimiento de las obligaciones de pago del IRPF[13], o a la TGSS para el abono de las cotizaciones sociales. Asimismo, queda amparado legalmente la cesión de datos a la inspección de trabajo o tributaria con el fin de colaborar en el cumplimiento de sus labores investigadoras. Pero, incluso, queda justificada en el caso de subcontratación con terceros de servicios de confección de nóminas y boletines de cotización. Por otro lado, la Disposición Adicional Primera del Real Decreto Legislativo 1/2002, de 29 de noviembre, por el que se aprueba el texto refundido de la Ley de Regulación de los Planes y Fondos de Pensiones, señala que los compromisos por pensiones asumidos por las empresas deberán instrumentarse mediante contratos de seguros y para cumplir esta obligación la empresa queda habilitada para la cesión de los datos personales de los trabajadores a la entidad con quien va a contratar, sin necesidad de solicitar consentimiento de los beneficiarios[14].

3.2. El deber complementario de informar al trabajador

Si bien es verdad que en el ámbito laboral el tratamiento de los datos personales de las personas trabajadoras por la empresa no precisa el consentimiento de los interesados e incluso se pueden ceder datos a terceros amparados en diversas disposiciones legales, esto no es suficiente. Para que el tratamiento sea lícito es preciso cumplir una obligación accesoria como es la información. En este ámbito se diferencia entre la obligación de la empresa en el caso de que los datos hayan sido aportados por las personas trabajadoras o no lo hayan sido.

En este sentido, el Considerando 60 del RGPD señala que el responsable deberá aportar a estos toda la información complementaria que sea necesaria para garantizar un tratamiento leal y transparente[15]. Y, en el caso de que los datos personales se obtengan directamente de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran, tal y como ya se mencionó. Así, el artículo 11 de la LOPD, de acuerdo con el artículo 13 del RGPD, determina que cuando los

[12] Committee of Ministers, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 1 de abril de 2015, pág.2

[13] Informe Jurídico de la AEPD, núm. 0539/2009.

[14] Informe Jurídico de la AEPD, núm. 0039/2010.

[15] El Informe Jurídico de la AEPD, núm. 0325/2009, recomienda que la información sea concisa, sin excesos que dificulten el entendimiento del documento.

datos personales sean obtenidos del afectado, el responsable del tratamiento al afectado la información básica, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En este sentido, la LOPD recoge el principio de información por capas que subyace en el RGPD, que significa que, en primer lugar, existe obligación de aportar una información básica y resumida, y, posteriormente, se remitirá el resto de las informaciones de forma detallada, en un medio más adecuado para su presentación y comprensión[16].

El contenido esencial de la primera información será la identidad del responsable del tratamiento y de su representante; la finalidad del tratamiento y la posibilidad de ejercer los derechos relacionados con el tratamiento de los datos de acuerdo con lo señalado con la LOPD. En el RGPD, se entiende por información básica: los datos del responsable del tratamiento y del DPD, en su caso; los fines del tratamiento y su base jurídica (el contrato de trabajo o una disposición legal) y los destinatarios de los datos personales. A lo que la LOPD añade los derechos de los interesados, que la norma europea trata como complementarios.

La información sobre el tratamiento debe hacerse en el momento en el que la persona trabajadora aporta sus datos personales. Así, al principio de la relación laboral será preciso que el trabajador conozca que sus datos van a ser tratados con fines de desarrollo del propio contrato y también los que van a ser cedidos a terceros en el mismo contexto. Dicha información básica tendría que hacerse en el mismo momento de la contratación, siendo solo posterior si se añaden tratamientos que no se habían previsto.

La LOPD añade que cuando los datos personales no hubieran sido obtenidos del afectado, el responsable tendrá que facilitarle la información básica general, pero, además, tendrá que incluirse las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos. En concreto, el RGPD determina que habrá que incluir si el conocimiento de los datos procede de fuentes de acceso público.

En un segundo momento, en general, se complementa la información sobre el plazo de conservación de los datos, la categoría de los datos, la posibilidad de presentar reclamación ante la autoridad competente en caso estimar que el tratamiento sufre alguna incidencia y, en su caso, sobre las posibles finalidades futuras del tratamiento. Como ya se ha señalado, el interesado puede recibir la información complementaria a través de correo electrónico o similar.

En resumen, la información facilitada debe ser concisa y entendible, empleando un lenguaje claro y sencillo. Además, también gratuita, excepto, como señala la LOPD en su artículo 13 en relación con el derecho al acceso a los datos, cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte.

La información, en general, podrá ofrecerse en cualquier medio en el que quede constancia del cumplimiento de la obligación de informar por si la empresa tiene que acreditar el cumplimiento de dicho deber. Como se ha señalado, respecto a la complementaria se puede remitir vía correo electrónico o medio similar. El RGPD determina que, si es solicitada expresamente por los interesados que la información sea remitida a través de medios electrónicos, la respuesta, en la medida que sea posible, deberá ser en este sentido. En todo caso, se han entendido como indicios suficientes del cumplimiento del deber de información, la adjuntada con la nómina, la incluida en un documento como anexo al contrato de trabajo, en un e-mail de respuesta, en una notificación por correo certificado o a través de

[16] AEPD/ APDCAT/ Agencia Vasca de Protección de Datos, *Guía para el cumplimiento del deber de informar*, p. 5.

la Intranet de la empresa, incluso un tablón de anuncios de la empresa seguro, accesible y visible con facilidad por los afectados[17].

3.3. El especial tratamiento de los datos de categoría especial

Eso sí, el empresario no puede tratar sin consentimiento del trabajador los datos personales que son calificados como de categorías especiales. El artículo 9 del RGPD prohíbe el tratamiento de los datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física y, por tanto, también de las personas trabajadoras. Pero, además, admite que los Estados Miembros de la Unión Europea pueden limitar aún más su tratamiento, con independencia incluso del consentimiento del interesado. En este contexto, la LOPD determina que, a los efectos de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

En el ámbito que aquí se analiza, el RGPD reconoce expresamente la licitud del tratamiento de datos de categorías especiales en determinados supuestos, que a continuación se pasan a analizar, donde no se precisa el consentimiento del afectado. No obstante, no puede perderse de vista que, en todo caso, siempre existe la obligación de informar sobre el tratamiento como en los supuestos generales.

En primer lugar, cuando sea preciso 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, siempre que se establezcan medidas adecuadas que respeten los derechos fundamentales y de los intereses de los afectados. De nuevo, el equilibrio en este asunto hay que buscarlo en la ponderación de las necesidades del desarrollo de la actividad laboral y los derechos fundamentales de las personas trabajadoras, lo que viene a poner de manifiesto la necesidad de que se regulen los límites de estos derechos, en la medida de lo posible.

Otra excepción al consentimiento se aplica en los tratamientos con finalidad en la medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social. En este caso, también el RGPD permite cautelas de las legislaciones de los Estados miembros, y la LOPD recoge esta excepción cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Asimismo, es posible también la excepción cuando el tratamiento sea preciso para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial. Por ejemplo, cuando se precise para acreditar un despido. Tampoco será preciso el consentimiento del tratamiento cuando se refiere a datos personales que el interesado ha hecho manifiestamente públicos, por ejemplo, a través de las redes sociales.

3.3.1. Los datos médicos y sanitarios

En relación a los tratamientos con finalidad en la medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, la LOPD recoge

[17] Informe Jurídico de la AEPD, núm. 0325/2009.

la excepción del consentimiento, como ya se ha señalado, cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Si bien es verdad que el RGPD remite a la normativa de cada Estado la posibilidad de incluir nuevas condiciones a los efectos de tratar dichos datos genéticos, biométricos o relativos a la salud, también en su artículo 88 se recoge que la legislación nacional o los convenios colectivos podrán incluir ciertas especificaciones en materia seguridad en el lugar de trabajo, así como sobre la salud y seguridad en el trabajo en el ámbito laboral. Y de nuevo el límite es el mismo: los derechos y libertades de los trabajadores y la dignidad humana de los interesados. Pero, además, se podrá justificar el tratamiento de estos datos personales cuando tenga una finalidad de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social. En este caso, como ya se ha señalado, el RGPD permite cautelas de las legislaciones de los Estados miembros y en la nueva ley de protección de datos se señala que su utilización deberá, en su caso, venir amparada por una ley que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad, sobre todo en el ámbito de la salud o la ejecución de un contrato de seguro del que el afectado sea parte.

En este contexto, la cuestión fundamental en el desarrollo de las relaciones laborales se enmarca en la aplicación de la normativa de seguridad y salud laboral. El artículo 22 de la Ley de Prevención de Riesgos exigible el consentimiento de los trabajadores para poner en marcha la vigilancia periódica del estado de su salud en función de los riesgos inherentes al puesto de trabajo, quedando limitado el acceso a la información médica de carácter personal al personal médico y a las autoridades sanitarias que lleven a cabo dicha vigilancia[18]. De esta forma, el empresario no puede acceder a toda la información, sino solo a las conclusiones de los chequeos médicos, que consisten básicamente en saber si el trabajador es apto o no para el puesto de trabajo que desarrolla[19], que podrá complementarse cuando sea preciso la adaptación de dicho puesto a las circunstancias específicas de esa persona.

No obstante, acto seguido, se recogen ciertas excepciones, por ejemplo, cuando los reconocimientos sean imprescindibles para valorar los efectos del desarrollo de la prestación de servicios en el estado de salud del trabajador, siempre y cuando sea un peligro para sí mismo o para otros, o así se recoja en alguna normativa específica. Hay que tener en cuenta si se trata de un riesgo cierto, qué tipo de situaciones de peligro se pueden causar en el desarrollo de la prestación de servicios, cómo se pueden evitar y si los efectos son suficientemente graves como para imponer el tratamiento. En este sentido, se está ante dicha situación cuando se produce un riesgo para el resto de los trabajadores o terceros si el trabajador se dedica a la prevención o extinción de incendios [STS, sala de lo social, de 10 de junio de 2015 (Recurso 178/2014)]; de trabajos en altura [STSJ de la Comunidad de Madrid, sala de los social, de 12 de septiembre de 2016 (Recurso 535/2016)]; de conductor (en las dos sentencias anteriores); de barredoras en vías públicas [STSJ de Cataluña, sala de los social, de 31 de marzo de 2016 (Recurso 1915/2016)].

Hay convenios colectivos que incluyen directamente esta obligación de sometimiento a ciertas pruebas médicas con el fin señalado. Solamente es admisible cuando quede justificado de acuerdo con lo indicado

[18] El Informe Jurídico de la AEPD, núm. 0206/2010 señala que, aceptado el sometimiento al reconocimiento médico, no será preciso que se preste un consentimiento adicional para el tratamiento de los datos.

[19] SSTC 70/2009, de 23 de marzo y 159/2009, de 29 de junio.

en la norma de prevención[20], por sospecha de consumo de alcohol o estupefacientes[21], o en cualquier momento se puede someter al personal de vuelo y mantenimiento a controles de alcohol y drogas de manera aleatoria para preservar la seguridad en vuelo y evitar cualquier accidente[22]. Al contrario, no puede entenderse como una cuestión que se puede generalizar por el mero hecho de haber sido establecido por convenio colectivo, dado que siempre es preciso que se cumplan con los supuestos de excepcionalidad, tal y como se ha mantenido[23].

En otras ocasiones, el empresario precisa conocer datos de la salud de sus trabajadores con el fin de controlar las ausencias al puesto de trabajo, en horas que corresponden a días laborables dentro de la jornada laboral de trabajo. En primer lugar, la norma laboral permite a la empresa la verificación del estado de enfermedad o accidente del trabajador con el fin de controlar el motivo de esa baja por incapacidad mediante un reconocimiento médico, esto es, a través del tratamiento de sus datos de salud, llegando incluso a poder sancionar al interesado si se niega a ser sometido a reconocimientos médicos. Pero, además, esta obligación se relaciona con la regulación de la extinción del contrato de trabajo motivado por dichas ausencias que se recoge en la misma normativa. La STC 202/1999, de 8 de noviembre, ha declarado que estas actuaciones con un mero fin de controlar el absentismo no pasan el filtro del juicio de ponderación y la AEPD sí que lo permite cuando el chequeo médico tenga una doble finalidad, tanto verificar el estado de salud del trabajador como controlar el absentismo, pero siempre amparado por el consentimiento del trabajador[24].

A veces, los datos de salud que deben ser tratados por las empresas no son tanto los de sus trabajadores como lo de sus parientes con la finalidad de entender certificada las situaciones que abren los derechos al disfrute de los permisos retribuidos o reducciones de jornada relacionados con la salud de sus familiares. Si existe consentimiento por parte del familiar para la trasmisión de la información, no habrá ninguna cuestión que analizar, tampoco cuando se trate de menores de catorce años, si el titular de la patria potestad o tutela es el propio trabajador, de modo que puede consentir dicho tratamiento. En otros casos, la información deberá ser minimizada y, en la medida de lo posible, anonimizada. En este supuesto, el certificado solo podrá poner de manifiesto el carácter grave de la enfermedad padecida, la hospitalización o la intervención quirúrgica, sin añadir ninguna otra información, sin referencia a la concreta enfermedad padecida o la causa de la intervención[25]. En todo caso, si la función de la acreditación es el abrir el derecho a disfrutar el permiso o la reducción, comprobada la situación es recomendable destruir la certificación con el fin de garantizar la protección de estos datos especialmente sensibles de los parientes del trabajador, puesto que ya no existe causa que justifique la licitud del tratamiento.

3.3.2. Los datos de afiliación sindical

El artículo 9 del RGPD prohíbe el tratamiento de los datos que revelen la afiliación sindical, sin que esta declaración suponga una novedad en el tratamiento de estos datos, los cuales ya era reconocidos por la LOPD de 1999 como datos especialmente protegidos. El RGPD admite el tratamiento de este tipo de datos, siempre y cuando se den ciertas cir-

[20] STS, sala de lo social, de 10 de junio de 2015 (Recurso 178/2014).

[21] Por ejemplo, el Convenio Colectivo de Exeo Gestión Integral, SLU. (BOE núm. 53, de 24 de junio de 2014) y el Convenio Colectivo estatal de las empresas de seguridad (BOE núm. 10, de 12 de enero de 2015).

[22] Convenio colectivo de Inaer Helicópteros, SAU (BOE núm. 198, de 19 de agosto de 2015).

[23] STS, sala de los social, 28 de diciembre de 2006 (Recurso 140/2005).

[24] AEPD, *Guía de la protección de datos en las relaciones laborales*, p. 31.

[25] Informe Jurídico de la AEPD, núm. 0002/2012.

cunstancias, en especial cuando se haya obtenido el consentimiento expreso del afectado para un fin concreto. Pero, además, invita a los Estamos miembros de la Unión Europea a limitar legalmente su tratamiento, incluso cuando exista consentimiento del interesado, si así lo estiman conveniente.

La LOPD trata en concreto los datos de afiliación sindical en su Exposición de Motivos. Partiendo de la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, pone como ejemplo que la prestación del consentimiento no dará cobertura en ningún caso a la creación de «*listas negras*» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores o por los propios sindicatos, siempre respetando los límites de la regulación europea.

En definitiva, la licitud del tratamiento de estos datos debe basarse en el consentimiento del interesado y se entiende lógico el tratamiento de los datos por parte de los sindicatos y de la empresa con el fin de facilitar los derechos de afiliación de los trabajadores. Así, por ejemplo, ya la AEPD había entendido antes de la regulación del RGPD que era suficiente con el cumplimiento de una ficha por el interesado al darse de alta en el sindicato, donde autorice expresamente la comunicación de sus datos al empresario para facilitar el cobro de la cuota sindical para entender lícito tal tratamiento[26]. Asimismo, se puede entender que desde dicha autorización el tratamiento de los datos de afiliación también es lícito con efecto de proteger al trabajador frente a la sanción empresarial. La normativa laboral reconoce al trabajador afiliado a un sindicato la prerrogativa especial de que los delegados sindicales de la sección sindical correspondiente a dicho sindicato sean escuchados en audiencia previa antes de imponer dicha sanción. Si el empresario tiene conocimiento por razón del cobro de la cuota, podrá (más bien tendrá) que tratar los datos con los fines señalados en este último supuesto[27].

4. LOS DERECHOS DE LAS PERSONAS TRABAJADORAS EN EL DESARROLLO DEL TRATAMIENTO DE SUS DATOS PERSONALES

El artículo 12 de la LOPD desarrolla los derechos reconocidos en los artículos 15 a 22 del RGPD. Como se ha señalado con anterioridad, la empresa está obligada a informar a las personas trabajadoras sobre sus derechos en materia de protección de sus datos personales a través de medios accesibles, recayendo sobre la empresa la carga de la prueba de que así se ha hecho. En concreto, se contemplan los siguientes derechos: derecho de acceso, derecho de rectificación, derecho de supresión, derecho a la limitación del tratamiento, derecho a la portabilidad y derecho de oposición. Algunos de ellos van a ser analizados a continuación.

4.1. Derecho de acceso y rectificación

El derecho de acceso está vinculado al derecho a la información, dado que se reconoce al interesado cuando no ha recibido comunicación previa sobre el tratamiento de sus datos, organizándose como una especie de derecho complementario. Se reconoce el derecho a obtener confirmación sobre si sus datos personales están siendo sometidos a tratamiento y, en su caso, información básica sobre dicho tratamiento. Como ocurre con todos los derechos reconocidos en este ámbito, no es un derecho absoluto, dado que el RGPD señala que este derecho nunca podrá afectar negativamente a los derechos y libertades de otros.

[26] Informe Jurídico de la AEPD, núm. 0033/2010.

[27] Informe Jurídico de la AEPD *sobre la utilización del dato de afiliación sindical en los procedimientos de despido*, 2002.

En el RGPD no se establece la forma de ejercicio, pero sí en la LOPD. Si la empresa trata una gran cantidad de datos relativos al afectado y no se especifican cuáles se están solicitado, se le podrá solicitar tal especificación. Además, se entenderá cumplido cuando se facilita un sistema de acceso remoto, directo y seguro a los datos personales. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte.

El RGPD reconoce el derecho de rectificación de sus datos personales a los interesados cuando son inexactos y a completarlos cuando sean incompletos, incluso a través de una declaración adicional. Con el fin de llevar a cabo su ejercicio el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Asimismo, deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

4.2. Derecho de supresión u olvido y extinción de la relación laboral

Los trabajadores podrán ejercer su derecho de supresión o al olvido, sustituyendo al derecho a la cancelación, cuando los datos ya no sean necesarios para el fin para el cual fueron recogidos, cuando hayan sido tratados de forma inadecuada, cuando se retire el consentimiento previo (en este contexto solamente en relación con los datos personales de categoría especial o fuera del entorno de la relación laboral), cuando el interesado se opone al tratamiento en el ejercicio de su derecho de oposición en los mismos supuestos, cuando los datos personales han sido tratados ilícitamente o deben suprimirse de acuerdo con la norma aplicable; y cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información relacionado con menores.

El RGPD añade excepciones al ejercicio del derecho de olvido, a las cuales podrá referirse el responsable para denegar el derecho de supresión. En el ámbito aquí estudiado solamente serían aplicables, en supuestos de interés público en el ámbito de la salud pública o cuando sea sea preciso para la formulación, el ejercicio o la defensa de reclamaciones. Si es preciso mantener algunos datos personales de los trabajadores a los efectos de utilizarlos como prueba, entonces no se podrá atender al derecho de supresión.

Asimismo, como medida cautelar se regula el derecho del interesado a la limitación del tratamiento como derecho previo al ejercicio al derecho de supresión. El RGPD reconoce el derecho a la limitación del tratamiento en supuestos tales como cuando se impugne la exactitud de los datos, y sea preciso un tiempo para que el responsable verifique este particular; o cuando se entienda que el tratamiento es ilícito y el interesado prefiera la limitación de uso, por ejemplo, hasta que pueda probar dicha ilicitud a los efectos de sanciones; o cuando sea el responsable quien no necesite los datos personales, pero sí el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; o cuando el interesado se haya opuesto al tratamiento y es precisa la verificación de los motivos legítimos del responsable prevalecen sobre los del interesado. En el supuesto de que dicha limitación sea levantada, el responsable deberá informar al interesado que la solicitó.

Obviamente parece adecuado que el trabajador pudiese pedir la supresión del tratamiento de sus datos personales, cuando se extingue la relación laboral, lo que debería ser algo automático al perder la finalidad del tratamiento. Dicho derecho a la supresión de datos quedaría limitado, sin lugar a duda, cuando legalmente sea precisa la custodia de documentos. Desde que el contrato termina, la licitud del tratamiento de los datos personales de las personas trabajadoras pierde su licitud basada en el desarrollo del contrato de trabajo. No obstante, la supresión del tratamiento debería respetar la necesaria liquidación de

las deudas pendientes o, en su caso, la celebración de los actos prejudiciales y judiciales que diese lugar una extinción unilateral por parte de la empresa.

Hecha esta afirmación, sin embargo, hay que poner de manifiesto que no todos los datos personales podrán destruirse de acuerdo con la ley, puesto que la ley impone el deber de mantener ciertos documentos durante un mayor período de tiempo. Así, el art. 4 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social señala que las infracciones en el orden social prescriben a los tres años, en materia de Seguridad Social a los cuatro y hasta cinco años en materia de prevención de riesgos a contar desde la fecha de la infracción. A partir de este tenor se impone la conservación de ciertos documentos una vez finalizado en contrato de trabajo como, por ejemplo, el propio contrato, nóminas; expedientes disciplinarios, boletines de cotización, evaluación de los riesgos o expedientes de accidentes laborales o enfermedades profesionales. Por otra parte, la Ley 58/2003, de 17 de diciembre, General Tributaria, en su artículo 66 señala que prescribirán a los cuatro años derechos de la Administración para determinar la deuda tributaria mediante la oportuna liquidación; exigencia de pago de las deudas tributarias liquidadas y autoliquidadas; derecho a solicitar las devoluciones derivadas de la normativa de cada tributo, las devoluciones de ingresos indebidos y el reembolso del coste de las garantías; derecho a obtener las devoluciones derivadas de la normativa de cada tributo, las devoluciones de ingresos indebidos y el reembolso del coste de las garantías. Todas estas prerrogativas imponen el deber de conservar la documentación relativa a los justificantes de gastos e ingresos, tales como facturas o recibos que acrediten los costes[28].

En resumen, las personas trabajadoras pueden ejercer su derecho a la supresión de datos relacionados con el propio desenvolvimiento de la relación laboral solamente cuando termina esta, excepto respecto a los datos personales que estén relacionados con posibles infracciones futuras, dado que la propia prescripción de las sanciones llevará a que se impida el ejercicio del derecho hasta momento posteriores.

5. PROTOCOLOS EMPRESARIALES EN EL ÁMBITO DE LA PROTECCIÓN DE DATOS

Diversas son las obligaciones de las empresas en materia de protección de datos personales de sus trabajadores. Como se ha señalado, el tratamiento de dichos datos queda justificado por el propio desenvolvimiento del contenido de la prestación de servicios. Desde el inicio de las relaciones precontractuales hasta el momento de la extinción del contrato e incluso más allá de ella, como se ha podido comprobar, es preciso tener en cuenta las finalidades, los derechos y los límites de ese tratamiento. Todo ello desde la responsabilidad proactiva que se exige a la empresa en esta materia que va desde la evaluación previa de impacto, si es precisa; hasta el estudio de los posibles riesgos con el fin de determinar las medidas de seguridad. Con todas estas obligaciones lo más adecuado es que las empresas diseñen protocolos en este ámbito que recojan de forma conjunta todas las cuestiones afectadas por la protección de datos personales en la línea de la responsabilidad proactiva, y que su contenido sea dinámico a través de revisiones periódicas que recojan las evaluaciones tecnológicas.

Al margen de esta opción, existen ciertos ámbitos en la materia que sí deben ser protocolizados con el fin de cumplir las obligacio-

[28] Pero aún hay más. En algunos casos la obligación de conservar documentación se extiende hasta diez años en base al necesario cumplimiento de la Ley Orgánica 7/2012, de 27 de diciembre, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal y la Ley 10/2010, de 28 de abril, de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo.

nes de la empresa en materia de protección de datos personales de sus trabajadores, los que a continuación se van a analizar. En concreto referidos, al uso de instrumentos digitales y la implantación de la videovigilancia.

5.1. El protocolo de utilización de los medios digitales de comunicación e información

En las empresas se utilizan diferentes instrumentos tecnológicos como ordenadores de sobremesa o portátiles, tabletas, smartphone o móviles; así como soportes digitales de almacenamiento, tales como pendrives, discos duros y otros de mayor capacidad como la nube (Dropbox, Google drive, Microsoft OneDrive o iCloud, entre otros), donde se vuelcan una cantidad ingente de datos personales. Pero, también se intercambia información mediante correos electrónicos, intranet de la empresa, incluso, WhatsApp u otros sistemas de mensajería instantánea, así como mediante el uso de las redes sociales[29]. Los soportes informáticos o de comunicación son, en gran parte, portátiles, lo que significa que incluso se trasladan fuera del ámbito del centro de trabajo y más allá del horario de trabajo. Con los problemas añadidos que se pueden encontrar en el uso cada vez más extendido del teletrabajo.

La empresa puede controlar la prestación laboral a través de estos medios informáticos o de comunicación que puedan llevar a sancionar a las personas trabajadoras. El ejercicio de este poder empresarial choca frontalmente con el derecho a la protección de datos personales y de la intimidad de los trabajadores, donde media el juicio de ponderación en la línea mostrada con anterioridad. Antes este panorama, parece lógico que las empresas establezcan políticas corporativas, que se actualicen constantemente con el fin de recoger los cambios provocados por la evolución tecnológica[30].

El artículo 87 de la LOPD recoge el derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral que ponga a su disposición por su empleador, y avisa que la empresa solamente podrá vigilar los contenidos derivados de estos usos con el fin de controlar la prestación de servicios y la integridad de los propios dispositivos. De acuerdo con el tenor del artículo mencionado, la protocolización en este contexto ha dejado de ser una buena práctica para convertirse en una obligación. La utilización del verbo "deber" lleva a concluir que la protocolización del uso de los dispositivos digitales que ponga a disposición de sus trabajadores se impone como nuevo deber del empresario. En todo caso, se pone de manifiesto la necesidad que estos protocolos se diseñen con la participación de los representantes de los trabajadores con el fin de salvaguardar sus derechos fundamentales.

El propio artículo de la LOPD señala la necesidad de establecer criterios de utilización de los dispositivos digitales, es decir, se regula una especie de deber de protocolizar estos usos siempre respetando unos estándares mínimos de protección de la intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. Así, la regulación de su uso y control deben ser lo menos invasivos para los derechos fundamentales de las personas trabajadoras, sin que sea admisible un control permanente o monitorización continua[31]. De este modo, es fundamental la limitación del tiempo de control a lo necesario para probar el cumplimiento/incumplimiento

[29] De acuerdo con la *Encuesta sobre el uso de la TIC y comercio electrónico de las empresas* (INE), a octubre de 2019 en las empresas de menos de diez trabajadores tienen ordenadores a su disposición el 79,9 % (elevándose hasta un 99,26% en las de más de 10); y tienen conexión a internet un 76,3% (elevándose hasta un 98;39% en empresas de más de 10 trabajadores).

[30] COMMITTEE OF MINISTERS, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, 1 de abril de 2015, pág.7.

[31] En este sentido, se pronunció la sentencia del Tribunal Europeo de Derechos Humanos en el caso Bârbulescu vs. Romania.

y el de controladores que van a participar en la vigilancia.

5.1.1. La regulación de los usos privados

El precepto mencionado señala la necesidad de determinar los usos autorizados. Así, se determina que "*el acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados*".

Así, lo primero que hay que aclarar es cuál son los usos permitidos de estos instrumentos que son de propiedad de la empresa[32]. Muchas cuestiones son las que se plantean en este foro. ¿El correo electrónico puede utilizarse para fines privados? ¿Solamente se pueden consultar páginas de internet relacionadas con la actividad de la empresa? ¿Se pueden almacenar archivos privados? ¿Los medios de comunicación pueden emplearse para comunicarse con personas ajenas a la relación laboral? ¿Puede utilizarse fuera del horario de trabajo? ¿Cuál será su control en el ámbito del teletrabajo?

Lo más recomendable es limitar estrictamente el uso de los medios al ámbito de la actividad laboral[33], incluso utilizando medidas de desincentivación como, por ejemplo, la inclusión de filtros de acceso a ciertas páginas web[34] o la utilización de los ordenadores exclusivamente en el centro de trabajo. En todo caso, si se ha admitido su uso con fines privados, como señala la ley, se requerirá que se especifiquen de modo preciso los autorizados. Por otro parte, se añade la necesidad de establecer garantías para preservar la intimidad de los trabajadores, mediante la determinación de los períodos en que los dispositivos podrán utilizarse para dichos fines privados. Como regla aplicable podría, por ejemplo, proponerse que el uso fuera del horario de trabajo se entienda como privado.

Asimismo, respecto al almacenaje de información personal parece adecuado que se permita a las personas trabajadoras que puedan habilitar una carpeta privada que quede protegida de la vigilancia de la empresa, en ordenadores, móviles o, incluso, en la nube[35]. No significa ningún coste económico adicional para la empresa y puede evitar vulneración de derechos de las personas trabajadoras en el contexto del control empresarial[36].

5.1.2. La obligación de información a los usuarios

La LOPD señala que en este ámbito es precisa la información periódica a los trabajadores[37]. En este sentido, sería adecuado que se entregasen las reglas de utilización de los medios digitales en la propia firma del contrato y cada vez que se entregue alguno de estos instrumentos, determinado sus usos y límites, dejando constancia de dicha entrega a través de la firma de un recibí. O, asimismo la información se puede canalizar a través de otros medios, como avisos constantes sobre el limitado uso empresarial cuando se accede al dispositivo digital, su inclusión en el convenio colectivo de la empresa, o mediante documen-

[32] AEPD, *Guía de la protección de datos en las relaciones laborales*, p. 28.

[33] Committee of Ministers, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, abril de 2015, pág.7.

[34] Se aconseja utilizar este tipo de filtros u otros limitadores similares para evitar problemas de vulneración de derechos fundamentales. *Vid.* Committee of Ministers, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, abril de 2015, pág.7.

[35] Article 29 data Protection Working Party, *Opinion 2/2017 on data processing at work*, 8 de junio de 2017, p. 15.

[36] Blázquez Agudo, E.M., *Aplicación práctica de la protección de datos en las relaciones laborales*, Wolters Kluwer, 2018, p. 231.

[37] Article 29 data Protection Working Party, *Opinion 2/2017 on data processing at work*, 8 de junio de 2017, p. 14.

to sobre las obligaciones del personal, que se ponga a disposición de los empleados.

Pero, además, es fundamental que dicha información se vaya actualizando a través de la entrega periódica y actualizada de dicha información. Los retos de la evolución de la tecnología llevan a que estas reglas de actuación deban ser dinámicas. Necesitan ser revisadas periódicamente con el fin de incluir nuevas finalidades o tratamientos. En general, además de cuando se hayan producido modificaciones concretas, se recomienda la actualización, al menos, una vez al año para evitar la obsolescencia de los criterios.

5.1.3. La extensión del protocolo a la utilización del correo electrónico

Muy relacionado con el protocolo anterior está el del uso del correo electrónico, que debe ser una parte individualizada del primero. En este sentido, la sentencia del Tribunal Europeo de Derechos Humanos Copland vs. United Kingdom, de 3 de abril de 2007, puso de manifiesto que los correos electrónicos en el entorno laboral pueden considerarse como parte de la vida personal del trabajador, por lo que se entiende que es preciso informar de los controles sobre este medio y el tiempo de almacenamiento de la información. Además, el correo electrónico puede ser considerado por sí mismo como un dato personal, cuando más allá de ser un conjunto de signos o combinación alfanumérica, contiene información acerca de su titular, por ejemplo, su nombre y apellidos, la empresa en que trabajan o su país de residencia[38].

Es esencial que las personas trabajadoras puedan contar con un manual de información sobre uso correcto del correo electrónico, que debería ser entregado cuando se facilita la dirección. Como ocurre en general, es conveniente que la utilización sea para usos empresariales, evitando al máximo la utilización para fines particulares. Para esto, hay que promocionar el uso de cuentas corporativas, con el nombre del servicio y la empresa, más que las privadas donde aparezca el nombre del trabajador, con el fin de poner de manifiesto que es un medio de trabajo[39]. Podría, por otro lado, ponerse a disposición del trabajador otra dirección de correo con su nombre para su uso personal, cuyo contenido, obviamente, sí estará protegido por el derecho a la intimidad, limitando de forma absoluta el acceso de la empresa a su contenido[40].

Asimismo, es recomendable introducir cribas de destinatarios o de contenidos en los correos electrónicos[41]; y diseñar medidas para la desactivación automática de la cuenta del trabajador después de su cese en la empresa y la inclusión de forma automática de pies informativos en los correos enviados, donde se clarifique que su uso está adscrito a fines de la empresa en cuestión y amparado por la aplicación de las normas de protección de datos personales.

5.1.4. Una especial atención a la geolocalización

La aparición de nuevos métodos de control como es el de geolocalización (sobre la situación geográfica de los trabajadores mediante sistemas instalados, por ejemplo, en vehículos o dispositivos móviles) ha llevado a que la LOPD en su artículo 90 haya regulado el derecho a la intimidad de las personas trabajadoras en el uso de estos medios. Si utilización de ya venía reconociéndose por los tribunales,

[38] Informe Jurídico de la AEPD, de 15 de noviembre de 2005.

[39] Este uso empresarial tiene la ventaja de determinar el ámbito del control empresarial y también abre la posibilidad de su uso plural. Es decir, en caso de ausencia temporal del trabajador o extinción de la relación laboral, se permite la entrada al dominio y la tramitación de la prestación de servicio. *Vid.* Informe Jurídico de la AEPD, núm. 9262/2010.

[40] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 2/2017 on data processing at work*, 8 de junio de 2017, p. 14.

[41] *Vid.*, entre otros, el Informe Jurídico de la AEPD, núm. 0242/2008.

cuando se obtenían fotos a través de un programa de GPS instalado en el móvil del trabajador [STSJ Galicia, sala de lo social, de 14 de febrero de 2013 (Recurso 1248/2013)]; para verificar las visitas con clientes [STSJ de Castilla– León, sala de lo social, de 8 de mayo de 2013 (Recurso 453/201) y STSJ de Andalucía/ Granada, sala de lo social, de 15 de julio de 2015 (Recurso 1264/2015)].

La inclusión de este tipo de medios en el protocolo analizado lleva de nuevo a poner en evidencia la necesidad de que el control solo se ejerza sobre instrumentos de trabajo entregados por la empresa y durante la jornada de trabajo. Y, en su caso, si el instrumento a través del cual se desarrolla la geolocalización puede también emplearse para usos privados, tendrá que ponerse de manifiesto en el protocolo en qué horario y días se utiliza como instrumento de trabajo y en cuales como uso personal.

Obviamente su utilización no precisa del consentimiento del trabajador, pero sí tiene derecho a información sobre el uso de dichos sistemas. Por eso, la LOPD obliga a informar a los trabajadores de su utilización de forma previa, expresa, clara e inequívoca y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Asimismo, la información debe extenderse al contenido de los derechos de acceso, rectificación, limitación del tratamiento y supresión. No se ha mencionado esta cuestión en la regulación de los otros derechos digitales recogidos en la nueva norma de protección de datos personales, pero, se entiende que esta regla se debe extender a todos los supuestos del protocolo estudiado, dado que de forma general se aplica a cualquier tratamiento de datos personales de los trabajadores que se haga en la empresa.

5.2. El protocolo de la videovigilancia

En los últimos tiempos, se ha incrementado exponencialmente la utilización de los medios de videovigilancia en la empresa[42], con una doble función, la seguridad de la empresa ante actos de terceros, pero, igualmente como medio de control de la prestación de servicio del trabajador. En relación con este último fin es necesaria la protocolización de esta práctica empresarial, tal y como se lleva reivindicando mucho tiempo[43].

La LOPD ha incluido la regulación de los tratamientos con fines de videovigilancia de forma general en el artículo 22, remitiendo al artículo 89 el uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo, donde se reconoce el derecho de los empleadores a utilizar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control como parte de su poder de dirección. Pero, siempre, en el marco legal y con los límites inherentes al mismo, de forma que de nuevo habrá que estar a la aplicación del juicio de ponderación, que se analizó al principio. El artículo 89 de la LOPD extiende los límites de la videovigilancia en el ámbito empresarial a otros sistemas de grabación de sonidos, cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo, aplicando los principios de proporcionalidad, intervención mínima y demás garantías aplicables a la videovigilancia.

5.2.1. El deber de información a los trabajadores y a sus representantes

En este supuesto tampoco es preciso el consentimiento del trabajador a los efectos de

[42] Este incremento se debe, sin lugar a duda, a que es más económico que la vigilancia personal. *Vid.* GOÑI SEIN, J. *La videovigilancia empresarial y la protección de datos personales*, Thomson Cívitas, 2007, pp. 17 y ss.

[43] MIRÓ MORROS, D. / CRUZ DE PABLO, M., "El uso de la video vigilancia en el ámbito laboral" en *Actualidad Jurídica Aranzadi*, núm. 891/2014 y BLÁZQUEZ AGUDO, E.M., "La implantación de un protocolo de videovigilancia en el centro de trabajo" en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 43/2017.

entender lícito el tratamiento recogido por las cámaras en el desarrollo de la prestación de servicios, siendo suficiente la información sobre su utilización. En este sentido, la LOPD en su artículo 89 establece el deber empresarial de información previa, expresa, clara y concisa acerca de esta medida como suele ser habitual en los supuestos que ya han sido analizados.

La información aportada debe versar sobre la existencia del tratamiento de los datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; sobre las consecuencias de la obtención de los datos, sobre todo haciendo referencia a su utilización para acreditar incumplimientos laborales; y sobre el ejercicio de los derechos de acceso, rectificación, supresión y oposición. En todo caso, será suficiente con tener dicha información a disposición de los trabajadores a través de impresos informativos o en intranet. Más adelante se tratará si es suficiente con la mostrada por los carteles informativos.

Tradicionalmente ha estado en duda si esta obligación debe ser siempre respetada o existen posibles excepciones justificadas para utilizar cámaras ocultas con el fin de captar ilícitos en el desarrollo de la prestación de servicios. Se ha entendido que la comunicación sobre su utilización reduce la efectividad del control. Cuestión que parece ahora resuelta al incluir en un segundo párrafo en el precepto mencionado donde se señala que "*en el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica*"[44]. Es decir, es suficiente la información recogida a través de un dispositivo informativo en lugar suficientemente visible identificando, donde se informe, al menos, de la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos anexos al tratamiento de los datos, o, se incluya toda esta información a través de un código de conexión o dirección de internet. En todo caso, aquí surge la duda de a qué tipo de actos ilícitos se refiere. En la primera redacción se refería a actos delictivos, de modo que no se hubiesen incluido incumplimientos fuera de lo penal. No obstante, en el tenor elegido no se hace esta diferenciación y parece que también se incluirían los laborales[45].

El cartel informativo sobre el uso de las cámaras tendrá que exhibirse en lugar visible, y como mínimo, en los accesos a las zonas vigiladas (interiores o exteriores). Además, tendrá que informar sobre la existencia de la videovigilancia; la identidad del responsable del tratamiento o del sistema de videovigilancia, y la dirección del mismo; la posibilidad de ejercitar los derechos reconocidos en los artículos 15 a 22 del RGPD de acuerdo con la *Guía sobre el uso de videocámaras para seguridad y otras finalidades* de la AEPD. Respecto a las dimensiones mínimas del cartel informativo, no existe criterio de la Agencia, sino que depende del espacio en el que se vayan a ubicar. Tampoco es preciso que se coloque debajo de la cámara, basta con que se encuentre en un lugar visible y se informe a la entrada del edificio.

La información deberá darse asimismo "*a los representantes de los trabajadores*", lo cual es adecuado desde el derecho reconocido en el punto f) del artículo 64 del Estatuto de los Trabajadores a recibir información sobre la implantación y revisión de sistemas de control de trabajo para los representantes unitarios, derecho también extensible a los sindicales de acuerdo con el artículo 10 de la Ley

[44] Puede entenderse que este precepto no respeta los artículos 12 y siguientes del RGPD, aunque la LOPD señale que se respeta su tenor en la aplicación de esta excepción. La regulación europea sobre protección de datos se basa en el principio de transparencia y el derecho de información, lo que debe de tenerse en cuenta a la hora de establecer la videovigilancia, sin que quepa una excepción para la captación de ilícitos laborales.

[45] Serrano Olivares, R. "Los derechos digitales en el ámbito laboral: Comentario de urgencia a la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales" en *IUSLabor*, núm 3/2018, p. 223.

Orgánica de Libertad Sindical. En cualquier caso, la información de los representantes de los trabajadores puede ser imprescindible en el caso excepcional en el que no se informa al trabajador y se graba un ilícito[46]. Es recomendable que cuando se opte por grabar con cámaras ocultas a los efectos de comprobar este tipo de actuaciones, se informe a los representantes con el objetivo de garantizar los derechos fundamentales de los trabajadores, dado que, en caso contrario, podría entenderse que se está conculcando estas garantías. Incluso es recomendable su participación en la puesta en marcha de la política de la empresa en materia de videovigilancia, donde se recoja la regulación de estas cuestiones.

En cualquier caso, en este ámbito es importante recordar que, aunque en la información suministrada a los representantes de los trabajadores se ponga en su conocimiento datos personales de terceros (los empleados), no se exige el consentimiento expreso de los interesados. En este caso, la licitud de esta acción viene avalada por su derecho a la información que viene recogido en el Estatuto de los trabajadores para los representantes unitarios y en la LOLS para los representantes sindicales.

5.2.2. Sobre el lugar de instalación de las cámaras

El párrafo segundo del artículo 89 de la LOPD establece que "*en ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos*". Esta norma no es nueva, dado que cautelas similares se aplicaban con anterioridad al RGPD por extensión del artículo 6 de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la Utilización de Videocámaras por las Fuerzas y Cuerpos de Seguridad en Lugares Públicos, que prohíbe la utilización de las videocámaras en este tipo de entorno. Cuando se captan imágenes y/o conversaciones en estos lugares privados, la empresa debe destruirlas inmediatamente.

En esta línea, no se admitió la colocación de cámaras en el vestuario[47]; en una taquilla de una estación, cuando se enfoca una zona donde la trabajadora se cambia para ponerse el uniforme, y el aseo[48]; en un módulo de descanso del personal de asistencia en tierra de un aeropuerto[49]. En definitiva, solamente es posible la instalación en los lugares donde se desarrolla la prestación de servicios. Aunque sí se admite en otros espacios cuando no se identifica a las personas trabajadoras, dado que en este caso no hay un tratamiento de datos personales[50], por no estar estas identificadas o identificables. En este ámbito hay que valorar la instalación de cámaras orientables o con "*zoom*", que tienen un mayor riesgo de vulneración de los derechos fundamentales de los trabajadores[51]. Hay que tener un especial cuidado en su ubicación, asegurando que en su recorrido no se enfoque ninguno de los emplazamientos que se consideran como privados.

5.2.3. La supresión de las imágenes o el sonido en treinta días

En el último párrafo del artículo 89 de la LOPD se señala que la supresión de los sonidos conservados por los sistemas de grabación se realizará atendiendo a lo dispuesto en el

[46] COMMITTEE OF MINISTERS, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, abril 2015.

[47] STSJ Islas Canarias/ Las Palmas de Gran Canaria, sala de los social, de 27 de julio de 2001 (AS 4602, 2001).

[48] STSJ Comunidad de Madrid, sala de lo social, de 14 de abril de 2009 (AS 2009, 1656).

[49] STSJ de la Comunidad de Madrid, sala de lo social, de 20 de diciembre de 2006 (AS. 1069, 2006).

[50] STSJ de la Comunidad de Madrid, sala de lo social, de 14 de junio de 2006 (AS 3406, 2006).

[51] GUIDE FERNÁNDEZ, A., "La videovigilancia laboral y el derecho a la protección de datos de carácter personal" en *Revista de Derecho Político*, núm. 91/2014, p. 48.

apartado 3 del artículo 22 de esta ley, es decir, que los datos deberán ser suprimidos en el plazo máximo de un mes desde su captación como ocurre también en relación con las imágenes captadas mediante videovigilancia, manteniéndose el mismo límite temporal utilizada hasta ahora.

Asimismo, se mantienen las mismas excepciones que ya eran aplicables antes de la aprobación de la LOPD: será posible conservar las imágenes o sonidos, si son necesarios para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones, extensible al material que pudiese servir de prueba de un incumplimiento contractual en el ámbito laboral, que pueda servir para motivar un despido disciplinario. Aunque la norma no regula cómo se debe desarrollar esa custodia, parece que la vía más segura será su la entrega al órgano judicial donde se quisiese utilizar a los efectos probatorios, como prueba anticipada al procedimiento[52], en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

5.3. El Protocolo de los buzones internos de denuncias[53]

Los buzones internos de denuncias o "whistleblowing" se utilizan para recibir denuncias, esto es, "una revelación deliberada de información acerca de actividades no triviales que se creen peligrosas, ilegales, inmorales, discriminatorias o que de alguna otra manera incluyen una infracción en una organización, siendo tal revelación llevada a cabo por miembros actuales o pasados de la organización, que no tienen deberes de información o de vigilancia, y pudiendo ir dirigida a órganos de la propia organización o a terceras partes"[54]. El objetivo de este buzón en este ámbito es poner en conocimiento de la empresa, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

Antes de su regulación por la nueva LOPD, ya existían algunas manifestaciones legislativas al respecto en el ámbito de la prevención del acoso sexual y por razón de sexo, pero, también en el área de la protección de datos personales en la empresa[55]. Ahora el artículo 24 de la LOPD regula los sistemas de información de denuncias internas. Con posterioridad, a nivel europeo, se ha aprobado la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, cuyo objetivo es obligar a crear canales de denuncia a las entidades públicas y privadas comprendidas en su ámbito de aplicación.

Si los datos personales tratados en el ámbito del canal de denuncia tienen relación con la actividad laboral, podrán ser tratados sin necesidad del consentimiento de los afectados. En caso de que se vaya más allá de esta relación, habrá que comunicar el acto ilícito a la autoridad competente, ya que el empresario no podrá seguir con el procedimiento, sin consentimiento del denunciado. Obviamente al tratamiento de dichos datos habrá que aplicar todos los principios relacionados con su protección y el respeto a los derechos fundamentales de las personas trabajadoras.

Desde la entrada en vigor de la Directiva 2019/1937 es obligatorio que las empresas de

[52] Blázquez Agudo, E.M., *Aplicación práctica de la protección de datos en las relaciones laborales*, *op. cit.*, p. 196.

[53] Sobre esta cuestión, puede consultarse más extensamente, Blázquez Agudo, E.M., "El canal de denuncias o "Whistleblowing" en el ámbito laboral: un instrumento preciso a implantar en la empresa" en AA.VV., *Tiempos de reformas: en busca de la competitividad empresarial y de la cohesión social*, 2019, pp. 561– 586.

[54] Pérez Triviño, J.L.,"*Whistleblowing" en Eunomía. Revista en Cultura de la Legalidad,* núm. 14/2018, p. 287.

[55] Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Opinión 1/2006 sobre la aplicación de las normas de protección de Datos de la Unión Europea a los mecanismos internos de "Whistleblowing"*, febrero 2006.

más de 50 trabajadores establezcan canales de denuncia interna, de forma que el desarrollo de protocolos en esta materia viene a ser aún más necesarios con el fin de conseguir que se protejan los derechos fundamentales de las personas trabajadoras que están en juego. Por lo tanto, es adecuado diseñar políticas consensuadas entre la empresa y los representantes de los trabajadores, vía negociación o acuerdo colectivo, donde se desarrolle el canal de denuncias como instrumento fundamental para el control de las conductas ilícitas que se produzcan. Es recomendable crear protocolos claros y fácilmente comprensibles que otorgue confianza al trabajador para decidir el uso de los canales de denuncia[56], donde se proteja la normativa de protección de los datos personales tratados en su ámbito.

5.3.1. La información ofrecida a las personas trabajadoras

El artículo 24 de la LOPD impone como primera obligación que la empresa informe de la existencia del canal de denuncias a empleados y terceros, que puede hacerse a través de diversos mecanismos como, por ejemplo, mediante un anexo al contrato de trabajo, circulares informativas o a través de la intranet. Incluso parece beneficioso que se incluya en el protocolo como deber de las personas trabajadoras la denuncia de los ilícitos que conozca como parte de las obligaciones de los códigos éticos que se desarrollan en las empresas[57].

Con el fin de animar a la denuncia de los actos ilícitos de los que tengan conocimiento, se estima como adecuado que se recoja un listado concreto de posibles actuaciones denunciables que pueda servir de guía en la identificación de dichas conductas, aunque solo tendrá una función ejemplarizante. Además, en la información proporcionada debería incluirse quiénes pueden ser denunciados (otras personas trabajadoras y personas colaboradoras), quién gestiona el buzón (la empresa, o mediante un servicio externalizado), el procedimiento a seguir de forma clara y comprensible; así como las garantías que se ofrecen al denunciante.

El artículo 24 de la LOPD determina que el acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, dentro o fuera de la entidad (según la gestión del buzón se realice por la empresa o por un servicio externo), desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. De esta forma, en el protocolo tendrán que determinarse las personas que se encarguen de este sistema. Con independencia de esta cuestión, también habrá que poner de manifiesto que según el ilícito denunciado sea administrativo o penal, será preciso permitir el acceso a las denuncias a la autoridad competente; o a otras personas, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan; así como al personal de recursos humanos, cuando sea preciso adoptar medidas disciplinarias frente a un trabajador.

Por otra parte, de acuerdo con el artículo 19 de la Directiva 2019/1937 es necesario establecer medidas que eviten las represalias contra los denunciantes. Por ejemplo, que sean sancionados o despedidos[58], que pierdan posibilidades de promoción profesional, que sean modificadas sus condiciones de trabajo, que se les denieguen acciones formativas, o que sufran discriminaciones, acosos o daños en su reputación.

---

[56] Department for Business, Innovation & Skills, *Guidance for employers and Code of practice*, Reino Unido, 2015, p. 5.

[57] Algunos pronunciamientos judiciales han reconocido la procedencia del despido por no haber procedido de este modo. *Vid.* STSJ de Cataluña, sala de lo social, de 15 de febrero de 2010 (AS 2010, 1411) y STSJ de Aragón, sala social, de 6 de marzo de 2013 (JUR 2012, 115775).

[58] Deben calificarse como despidos nulos aquellos que han sufrido los denunciantes sin causa. *Vid.* STSJ de la Comunidad de Valencia de 2 de abril de 2019 (sentencia 1054/2019).

5.3.2. El proceso diligente de investigación

De acuerdo con la Directiva 2019/1937, las denuncias pueden hacerse por escrito, por correo, a través de un buzón físico destinado a recoger denuncias o mediante una plataforma en línea, ya sea en la intranet o en internet. O, incluso, se puede permitir que denuncien verbalmente, por una línea de atención telefónica o a través de otro sistema de mensajería vocal. Además, incluso se pueden admitir entrevistas breves con el fin de recoger la información necesaria.

Recibida la denuncia, se informará al denunciado sobre los hechos, los destinatarios de la información, el responsable de la gestión de la investigación y sus derechos en materia de protección de datos[59]. Además, deberían proponerse medidas cautelares, cuando sea preciso, a aplicar mientras se desarrolle el proceso de investigación, siempre y cuando sea preciso evitar daños irreparables; pero, también otras complementarias como nombrar asesores jurídicos que apoyen a los denunciantes. En todo caso, el procedimiento a seguir deberá ser diligente.

Es aconsejable que se prevea la evaluación del sistema para reparar disfuncionalidades y que para apoyar este fin se interrogue al denunciante sobre su grado de satisfacción con dicho procedimiento. Igualmente se entiende preciso tener un registro sobre sobre el número de denuncias, su naturaleza y su desarrollo, siempre respetando el principio de confidencialidad.

Por último, el artículo 24 de la LOPD establece el modo de conservación de los datos personales obtenidos en el funcionamiento del buzón. Así, los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados, sin determinar que se entiende cómo tal. Así, será adecuado que la empresa incluya en su protocolo los límites de conservación de estos datos personales. En todo caso, la ley establece un plazo máximo de tres meses desde su recogida para proceder a su supresión. A partir de ese momento solo se podrán conservar los datos necesarios para dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica o de forma anónima las denuncias que no hayan sido cursadas. En todo caso, fuera del sistema de denuncias pueden conservarse con el fin de continuar con la investigación de los hechos denunciados por cualquier de las partes involucradas en dicha investigación.

[59] Informe Jurídico de la AEPD núm. 0128/2007, sobre Creación de sistemas de denuncias internas en las empresas (mecanismos de "*whistleblowing*").

BIBLIOGRAFIA

AEPD/APDECAT/ Agencia Vasca de Protección de Datos, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento*, 2017.

AEPD/ APDCAT/ Agencia Vasca de Protección de Datos, *Guía para el cumplimiento del deber de informar*.

ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 2/2017 on data processing at work*, 8 de junio de 2017.

BLÁZQUEZ AGUDO, E.M., "La implantación de un protocolo de videovigilancia en el centro de trabajo" en *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 43/2017.

BLÁZQUEZ AGUDO, E.M., "El canal de denuncias o "Whistleblowing" en el ámbito laboral: un instrumento preciso a implantar en la empresa" en AA. VV., *Tiempos de reformas: en busca de la competitividad empresarial y de la cohesión social,* 2019.

COMMITTEE OF MINISTERS, *Recommendation CM/Rec (2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment*, abril 2015.

DEPARTMENT FOR BUSINESS, INNOVATION & SKILLS, *Guidance for employers and Code of practice,* Reino Unido, 2015.

GOÑI SEIN, J. *La videovigilancia empresarial y la protección de datos personales*, Thomson Cívitas, 2007.

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, *Opinión 1/2006 sobre la aplicación de las normas de protección de Datos de la Unión Europea a los mecanismos internos de "Whistleblowing"*, febrero 2006.

GUIDE FERNÁNDEZ, A., "La videovigilancia laboral y el derecho a la protección de datos de carácter personal" en *Revista de Derecho Político*, núm. 91/2014.

MIRÓ MORROS, D. / CRUZ DE PABLO, M., "El uso de la video vigilancia en el ámbito laboral" en *Actualidad Jurídica Aranzadi*, núm. 891/2014.

MOLINA NAVARRETE, C., "De Bârbulesku II a López Ribalta: ¿qué hay de nuevo en la protección de los trabajadores?" en *Revista de Derecho del Trabajo y de la Seguridad Social, CEF*, núm. 419/2018.

PÉREZ TRIVIÑO, J.L.,*"Whistleblowing" en Eunomía. Revista en Cultura de la Legalidad,* núm. 14/2018.

SERRANO OLIVARES, R. "Los derechos digitales en el ámbito laboral: Comentario de urgencia a la ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales" en *IUSLabor*, núm 3/2018.

UNIDAD DE EVALUACIÓN Y ESTUDIOS TECNOLÓGICOS DE LA AEPD, *Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de datos,* 2 de octubre de 2017.

RESUMEN

La nueva normativa de protección de datos personales ha introducido algunos cambios en el ámbito de las relaciones laborales. El tratamiento de los datos de las personas trabajadoras por la empresa es continuo en el marco del contrato de trabajo, sin que sea preciso el consentimiento del trabajador. Desde esta perspectiva, en este trabajo se analizan los elementos fundamentales del desenvolvimiento del derecho a la protección de datos y a la intimidad de los trabajadores en el ámbito del ejercicio del poder empresarial. Aunque la nueva LOPD se refiere al contexto laboral, sin embargo, no regula específicamente el desarrollo de ciertas cuestiones claves en este contexto, por lo que hay que aplicar las normas generales, adaptándolas a las necesidades concretas de esta actividad. La aportación concreta de la LOPD es el reconocimiento de derechos digitales, tales como el derecho a la intimidad en la aplicación de los medios digitales, de videovigilancia y de controles emergentes como la geolocalización.

De acuerdo con estas bases, tres son los grandes bloques de este trabajo. El primero trata de fijar el acerbo legislativo aplicable a la protección de datos de las personas trabajadoras en el marco de su contrato de trabajo de acuerdo con el nuevo Reglamento Europeo en la materia y la LOPD de diciembre de 2018. Una segunda parte se centrará en analizar la aplicación de los principios básicos y derechos regulados de forma general al ámbito estudiado. Por último, se pondrá acento en los protocolos que la empresa debe desarrollar con el fin de cumplir los deberes que se le imponen en este contexto.

Así, en primer lugar, se analiza el contexto legal de la protección de datos personales en España, poniendo en evidencia las carencias regulatorias en la materia laboral, sirviendo como primera valoración que se ha perdido una ocasión para establecer un verdadero marco en este ámbito, lo que lleva a que el contexto no hay cambiado profundamente con la publicación de la normativa europea y la ley orgánica española, esto es, los límites de la protección de los datos personales de los trabajadores siguen dependiendo del juicio de ponderación, el cual ha sido construido por la jurisprudencia a lo largo de los últimos años.

Establecida esta premisa, en un segundo gran bloque se pasa a analizar elementos esenciales regulados en el nuevo acerbo legislativo en materia de derecho de protección de datos personales y su afectación a las relaciones laborales. Así, se examina la situación de la empresa como responsable del tratamiento frente a los datos personales de sus trabajadores dentro del marco de la nueva responsabilidad proactiva y la regulación de las figuras del encargado y el delegado de protección. Este último tiene un posicionamiento estratégico en la empresa, en la que siempre debe mantener su independencia como figura interpuesta entre esta y la autoridad de control.

En esta línea, también se analiza la aplicación de los principios generales de protección de datos personales de los trabajadores en la empresa, teniendo en cuenta que en este ámbito se excluye el elemento esencial para convertir a un tratamiento en lícito como es el consentimiento del interesado. Dada la especial relación del trabajador con la empresa, no es exigible dicho consentimiento siempre que el tratamiento se haga en el marco del desarrollo de las relaciones laborales, aunque la empresa mantiene el deber complementario de información sobre dicho tratamiento. Hay una excepción en este contexto: el tratamiento de los datos de categorías especiales (los datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física y, por tanto, también de las personas trabajadoras). En estos casos sí se demanda el consentimiento, aunque de nuevo se determina excepciones en estos supuestos. En este sentido, se profundiza en el análisis del tratamiento de los datos médicos y sanitarios y de los datos de afiliación sindical en el marco del contrato de trabajo.

Por último, en este segundo bloque se propone el examen de los derechos de las personas trabajadoras en el desarrollo del tratamiento de sus datos personales en el ámbito de sus relaciones laborales. En concreto, el derecho de acceso y de rectificación, así como el derecho de supresión u olvido y su implicación en la extinción del contrato.

Determinado el desarrollo de los principios y derechos en materia de protección de datos personales de las personas trabajadoras en la empresa, la última parte de este trabajo se centra en los protocolos que la empresa debe poner en marcha con el objeto de cumplir los requisitos de la normativa en el ámbito estudiado.

El primero debe ser el protocolo de utilización de los medios digitales de comunicación e información en el ámbito de la actividad diaria de la prestación de servicios, siempre con respeto a los derechos fundamentales de las personas trabajadoras, en especial al derecho a la intimidad. Dos son las cautelas que deben tenerse en cuenta: la inclusión de los contornos de los usos privados de estos instrumentos y del deber de información a los usuarios sobre su control. Además, estos protocolos deben contemplar dos instrumentos de trabajo como son el correo electrónico, el más utilizado, y aquellos que permiten el control mediante la geolocalización, por ser los más intrusivos.

Un segundo protocolo es el de videovigilancia, donde se regularán los contornos del control empresarial de la prestación de servicios a través de este medio, cada vez más utilizado en la empresa en el ejercicio de su poder de dirección. Importante es incluir en ellos el deber de información a las personas trabajadoras y a sus representantes sobre cómo se va a realizar dicho control a través de carteles, pero también de forma individualizada con los límites recogidos por la jurisprudencia. Asimismo, tendrá que incluirse el lugar correcto de instalación de las cámaras y la forma de supresión de las imágenes en el plazo de 30 días.

Por último, la empresa debe desarrollar un protocolo en materia de puesta en marcha de los buzones de denuncia que se exige ahora desde la normativa europea. En dicho desarrollo es esencial valorar las implicaciones de los límites de la normativa en materia de protección de los datos personales de las personas trabajadoras.

Palabras clave: Protección de datos personales; derecho a la intimidad; empresa y protección de datos; relación laboral y protección de datos.

ABSTRACT The new regulations on the protection of personal data have introduced some changes in the field of industrial relations. The processing of the workers´ personal data is carried out daily in the context of the employment contract, without requiring the worker's consent. From this perspective, this paper analyses the fundamental elements of the development of the right to data protection and privacy of workers in the field of the exercise of business power. Although the new LOPD (the Organic Law of Personal Data protection, published in December of 2018) refers to the field of labor relations, however, it does not specifically regulate the development of some of their main fundamental elements, so the general rules must be used to. Particularly, the LOPD does refer to new digital rights such as the right to privacy in the control of digital instruments, videosurveillance and emerging controls such as the geolocation.

According to these bases, this paper is divided in three big blocks. The first one seeks how to establish the legislative framework which is applicated to the protection of workers' data under their employment contract in accordance with the new European Regulation (the new General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council) and the Organic Law of Personal Data protection, published in 2018. A second part focuses on the basic principles and rights in general manner and its concrete application in the studied field. Finally, the protocols, that the company must develop in order to fulfil the duties in this context, are analyzed as a special form to business power development.

Thus, first of all, the legal context of the protection of personal data in Spain is analyzed, highlighting the regulatory deficiencies in this area, serving as a first conclusion that an opportunity has been missed in order to establish a useful framework in this context. Then, it is possible to affirmative that their structure has not changed profoundly with the publication of European and Spanish new legislation. In summary, the limits of the protection of workers' personal data remain depending on the weighting and proportionality judgment, which has been built by jurisprudence over the past few years.

Established these elements, a second large block goes on analyzing the essential elements regulated in the new legislative framework (European and Spanish one) about the right to protection of personal data and its impact on industrial relations. Thus, it is essential to understand the situation of the company (the controller) as responsible of its workers personal data protections´ in the context of the new proactive responsibility and the regulation of the figures of the processor and the data protection officer, who has a strategic position in the company (between independence and his position as a interposed figure in front of the data protection authority).

In this area, the application of the general principles of the protection of workers' personal data in the labor relations is also analyzed, specially the absence of the necessity of consent. Given the special relationship among workers and company, such consent is not required when the processing is done in the context of the development of industrial relations, although the complementary duty of information is maintained for the employers. There is an exception in this context: the processing of data of special categories (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation). In these cases, consent is demanded, although again exceptions are determined. In this sense, it goes into the analysis of its involvement in the environment of the processing of medical and health data and trade union membership data.

Finally, this second block proposes the examination of the rights of workers in the development of the processing of their personal data in the field of their industrial relations. In particular, the right of access and rectification, as well as the right of erasure or to be forgotten and its involvement in the termination of the contract are treated.

Determined the development of the principles and rights regarding the workers´ protection of personal data in the labor context, the last part of this paper focuses on the protocols that the company must implement in order to comply with the requirements of regulations in the studied field.

The first protocol is about the use of communication and information digital instruments used in the day-to-day labor activities, always with respect to the worker´s fundamental rights. Two are the precautions to be considered for the companies: the inclusion of the regulation about its private uses and the duty of information about their control use. In addition, these protocols should include the regulation of two working instruments such as e-mail, as the most used one, and the limits of the geolocation control, as the most intrusive one.

A second protocol is about video surveillance, increased day by day, where the company control limits must be imposed according to the regulation. In this type of protocol, it is important to include the duty of information to workers and their representatives on how such control will be carried out through collective and individual information according to the limits set out by the case-law. The installation site of the cameras and the form of image suppression within 30 days must also be included in them according with the legislation rules.

Finally, companies must develop a protocol on the implementation of whistleblowing channel required from European legislation (EU Whistleblower Protection Directive, published recently in 2019). In its development it is essential to assess the implications of the limits of the legislation on the workers´ protection of their personal data.

Keywords: Personal data protection; right of privacy; companies and data protection; labor relation and data protection.

El papel de la negociación colectiva en el terreno de la protección de datos personales y garantía de los derechos digitales

The role of collective bargaining in relation to the personal data protection and the guarantee of digital rights

RAQUEL YOLANDA QUINTANILLA NAVARRO*

1. INTRODUCCIÓN

La creciente e imparable utilización de las tecnologías de la información y la comunicación en las empresas constituye una nueva realidad, que permite a los trabajadores disponer de recursos informáticos muy prácticos para su actividad laboral. Junto a esa ventaja, los trabajadores sufren, en ocasiones, los inconvenientes derivados de esa aplicación diaria de las nuevas tecnologías, pudiendo significar para ellos la limitación de derechos fundamentales. De ahí que tanto a las empresas como a los trabajadores se les exija responsabilidad en la aplicación y utilización de los dispositivos informáticos y electrónicos en el ámbito de las relaciones laborales.

Por un lado, el empresario, mediante su poder directivo[1] de control y su poder disciplinario de corrección, ha de asegurar sus sistemas informáticos frente al mal uso y las prácticas abusivas por los trabajadores. Aquél realiza una labor tanto preventiva, controlando esa utilización, como correctora, mediante sanciones de hechos abusivos llevados a cabo.

Por otro lado, para el trabajador, la utilización de los dispositivos digitales corporativos, el correo electrónico, etc., no puede suponer un menoscabo en el ejercicio de sus derechos. Por ello, resulta imprescindible la regulación de su utilización, mediante normas de actuación, que preserven los intereses del empresario, junto con los derechos de los trabajadores, garantizando un uso correcto de las tecnologías de la información y la comunicación[2].

* Profesora Titular de Derecho del Trabajo y de la Seguridad Social de la Universidad Rey Juan Carlos.

[1] De consulta obligada resulta la obra clásica del maestro MONTOYA MELGAR, A.: *El poder de dirección del empresario*, Estudios de Trabajo y Previsión, Instituto de Estudios Políticos, Madrid, 1965.

[2] *Vid.* SEMPERE NAVARRO, A. V., SAN MARTIN MAZZUCCONI, C.: *Nuevas tecnologías y relaciones laborales*, Colección Monografías, Aranzadi, Cizur Menor, 2002. SEMPERE NAVARRO, A. V., MATEOS Y DE CABO, O. I.: "Uso y control de herramientas informáticas en el trabajo (marco legal, pautas judiciales y convencionales)"; y SAN MARTIN MAZZUCCONI, C.: "EL derecho a la protección de datos personales de los trabajadores: criterios de la Agencia Española de Protección de Datos", en SAN MARTIN MAZZUCCONI, C. (Dir.): *Tecnologías de la información y la comunicación en las relaciones de trabajo: nuevas dimensiones del conflicto jurídico*, Eolas ediciones, León, 2014. MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Colección Claves Prácticas, 3ª edición, Francis Lefebvre, Madrid, 2019. CRUZ VILLALÓN, J.: *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites de la actuación del empleador*, editorial Bomarzo, Madrid, 2019. SERRANO GARCÍA, J. Mª.:

2. EL REGLAMENTO (UE) 2016/679 Y LOS CONVENIOS COLECTIVOS

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, regula con carácter general lo relativo al tratamiento de los datos personales en el ámbito laboral.

En concreto, el art. 88 del Reglamento UE 2016/679 en su apartado 1, prevé 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 la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral".

Por tanto, el Reglamento (UE) 2016/679 faculta a cada Estado miembro de la Unión Europea a dictar normas específicas que desarrollen las generales del Reglamento. El contenido de las normas específicas abarca cada etapa de la relación laboral, desde el paso previo a la contratación, pasando por el contenido de la ejecución del contrato y hasta la extinción de dicho contrato, ya que las tecnologías de la información y la comunicación se proyectan sobre todas las fases de la vida del contrato de trabajo.

Las normas específicas incluirán medidas adecuadas para preservar la dignidad humana de los interesados, sus intereses legítimos y sus derechos fundamentales. De ahí que deban centrarse en la transparencia del tratamiento, 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 Reglamento (UE) 2016/679).

En nuestro Derecho interno, el artículo 18.4 de la Constitución Española reconoce el derecho a la protección de los datos de carácter personal cuando dispone que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Como ha declarado el Tribunal Constitucional[3], se reconoce ese derecho con el rango de derecho fundamental de todo ciudadano. El derecho a la protección de los datos personales es un derecho fundamental inespecífico, puesto que el trabajador es titular del mismo como cualquier otro ciudadano, no por su condición de trabajador.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD) realiza la función de salvaguarda encomendada por el precepto constitucional al legislador. Acorde con el art. 1 LOPD, su objeto consiste en lo siguiente: a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679, y completar sus disposiciones. b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia, editorial Bomarzo, Madrid, 2019. CUADROS GARRIDO, E.: *Trabajadores tecnológicos y empresas digitales*, Aranzadi, Cizur Menor, 2018. BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, Bosch Wolters Kluwer, Madrid, 2019.

[3] SSTC 94/1998, de 4 de mayo y 292/2000, de 30 de noviembre.

El derecho fundamental de las personas físicas a la protección de sus datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en dicha ley orgánica. Precisamente, los artículos 87 a 91, ambos inclusive, se centran en la protección de los datos personales y la garantía de los derechos digitales en el ámbito laboral.

El papel que la negociación colectiva asume al respecto, se señala en el art. 91 LOPD, titulado "Derechos digitales en la negociación colectiva", que establece la posibilidad de que la negociación colectiva prevea garantías adicionales respecto de las reguladas en la ley: "Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral".

3. EL PAPEL RESERVADO POR LA LOPD A LA NEGOCIACIÓN COLECTIVA EN ESTA MATERIA

El Título X de la LOPD reconoce y garantiza un conjunto de derechos digitales de los ciudadanos conforme al mandato constitucional. En particular, son objeto de regulación los derechos y libertades relacionados con el entorno de internet, como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Asimismo establece la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Más concretamente, la LOPD 3/2018 se centra en la garantía de los derechos digitales en el ámbito laboral en sus artículos 87 a 91 ambos inclusive, cuyos títulos son los siguientes:

- Artículo 87. Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.
- Artículo 88. Derecho a la desconexión digital en el ámbito laboral.
- Artículo 89. Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.
- Artículo 90. Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.
- Artículo 91. Derechos digitales en la negociación colectiva.

En virtud del art. 91 LOPD, se atribuye expresamente un papel a la negociación colectiva de cara a la protección de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y de sus derechos digitales en el ámbito laboral. Ese papel consiste en servir de instrumento por medio del cual se establezcan garantías adicionales de esos derechos. Podemos identificar varias características del papel de la negociación colectiva en esta materia.

Una primera característica es que se trata de una función, la de la negociación colectiva, que permite sumar más contenidos protectores a los ya previstos en el propio texto legal. El reconocimiento de esa función tiene carácter facultativo, por lo que no se impone a la negociación colectiva la obligación reguladora, sino la posibilidad de ocuparse de esta materia si lo considera oportuno y conveniente.

La segunda característica a destacar es que el legislador no selecciona el tipo de instrumento negocial que se puede utilizar, por lo que deja margen para que esa regulación se pueda realizar por la vía del convenio colectivo estatutario tanto sectorial, como empresarial, o mediante acuerdo marco.

Como tercera característica, el contenido del art. 91 LOPD está recordando la función principal de la negociación colectiva como fuente jurídica que mejora el contenido legal laboral. Hace referencia a las garantías adicionales, expresión que destaca que el carácter básico o esencial se lo reserva la ley orgánica reguladora y, por tanto, que el convenio colectivo completa ese contenido legal adaptándolo a la situación específica del ámbito de aplicación del convenio colectivo en razón del tipo de actividad productiva a la que afecte y de otras circunstancias concretas.

La cuarta característica es la relativa a las garantías, esto es, los mecanismos o formas de asegurar el cumplimiento de las obligaciones del empresario y de sus trabajadores respecto del tratamiento de los datos personales de dichos trabajadores y de la garantía de los derechos digitales. Es una llamada a la responsabilidad conjunta de empresario y trabajador, en la aplicación diaria de esos recursos informáticos que facilitan la realización de las prestaciones laborales. A continuación analizamos el contenido, en este materia, de los convenios colectivos sectoriales y empresariales de los ámbitos territoriales estatal, autonómicos y provinciales publicados durante el año 2019.

3. EL PAPEL DE LA NEGOCIACIÓN COLECTIVA VIGENTE RESPECTO DE LA PROTECCIÓN DE DATOS PERSONALES DEL TRABAJADOR[4]

3.1. Disposiciones comunes

Son escasos los convenios colectivos que incorporan algún contenido relacionado con la materia de la protección de datos personales de los trabajadores.

Dentro de la estructura del texto negociado, las cláusulas convencionales sobre protección de los datos personales de los trabajadores suelen ubicarse bien en un capítulo autónomo[5], bien dentro del apartado de desarrollo del sistema de trabajo[6].

Como excepción a la regla general de escasez de contenidos, podemos mostrar el VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados, que regula los principios básicos en el tratamiento de datos[7]. En este sentido, se hace referencia a la obligación de las empresas del sector de garantizar que los datos personales de los trabajadores sean:

- Exactos y actualizables cuando corresponda, tratados de manera lícita, leal y transparente en relación con el interesado, y resulten idóneos y limitados a la finalidad para la que son tratados.
- Tratados con las medidas que garanticen su integridad y confidencialidad.
- Conservados durante el tiempo necesario, en función de la finalidad del tratamiento.

Esta obligación empresarial se asume desde el inicio de la relación laboral y hasta después de finalizar la misma. Precisamente se pueden observar cláusulas convencionales que regulan el tratamiento de los datos de carácter personal de los trabajadores cuyos contratos se han extinguido. En este sentido, destaca la siguiente cláusula de autorización

[4] Sobre las categorías especiales, *vid.* En este mismo número de la Revista, el artículo del profesor DE VAL TENA: "Categorías especiales de datos personales en el ámbito de la relación de trabajo".

[5] Capítulo XI Convenio colectivo marco de la Unión General de Trabajadores. Capítulo IX Convenio colectivo 2019-2022 para la empresa Ontex peninsular. Capítulo XV Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería. Art. 76 II Convenio colectivo de la Asociación Centro Trama.

[6] Art. 6.3 Convenio colectivo de Delver Logistics, SLU. Un lugar más secundario se adjudica a esta materia en el V Convenio colectivo de Consum, Sociedad Cooperativa Valenciana, en la que se regula en las Disp. Adic. 1ª y 2ª del texto convencional.

[7] Art. 71 VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados.

expresa a la extinción del contrato de trabajo[8], prevista en el Convenio colectivo 2019-2022 para la empresa Ontex peninsular[9], que establece que la empresa presumirá que los archivos que se reciban en la terminal del empleado que cesa, o que estén almacenados en la misma, son de uso profesional, por lo que la empresa tendrá libertad para su almacenamiento, registro, revisión o destrucción. Para acceder a esos datos, el trabajador, a la firma de su recibo de finiquito, deberá comunicar a la empresa las contraseñas o credenciales que tuviera de la terminal que se le hubiese asignado, al considerar que son propiedad de la empresa. Además, el convenio colectivo mencionado añade que la empresa no tendrá responsabilidad respecto de los contenidos de los correos que puedan recibirse con posterioridad al cese, ni tendrá obligación de comunicarlos[10].

La regulación de la protección de los datos de carácter personal en la negociación colectiva se realiza generalmente, mediante una cláusula en la que se hace mención a los derechos fundamentales que se tratan de proteger, como son la intimidad y la dignidad del trabajador[11]. Como ejemplo de ello, destacamos la siguiente cláusula: "Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales"[12].

Solo se trata de una cláusula recordatoria del reconocimiento de los derechos fundamentales en conflicto con la utilización de las tecnologías, remitiéndose a la legislación específica reguladora, e incluso remarcando la garantía de que cumplirán la legislación aplicable en los términos que la misma prevea[13].

También podemos encontrar cláusulas convencionales en las que se hace mención a la protección de los datos personales de los trabajadores de forma breve y muy genérica, indicando que estos últimos ya han sido informados de la incorporación de sus datos a los ficheros existentes en las empresas para el mantenimiento de su relación contractual y para las finalidades del propio cumplimiento de lo establecido en los distintos artículos del convenio[14]. Como vemos, este texto adolece de algunos defectos, puesto que no se ha previsto el previo consentimiento expreso del trabajador, sino que este último solo ha sido informado de que se producirá esa incorporación, y no se detallan las finalidades concretas de incluir sus datos personales en el fichero de la empresa.

En otros textos, se establece la obligación para el trabajador de dar una documentación básica a la empresa y actualizarla. Entre otros datos se hace referencia al e-mail donde poder remitir, con la confidencialidad exigida

[8] Art. 34 Convenio colectivo 2019-2022 para la empresa Ontex peninsular. En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[9] Art. 34 Convenio colectivo 2019-2022 para la empresa Ontex peninsular.

[10] Art. 34 Convenio colectivo 2019-2022 para la empresa Ontex peninsular. En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[11] En alguna ocasión, el contenido sobre protección de datos y confidencialidad se proyecta solo en relación con los teletrabajadores de la empresa. Es el caso del art. 78 del Convenio colectivo de la empresa "Páginas Amarillas Soluciones Digitales, Sociedad Anónima Unipersonal" (centro San Sebastián de los Reyes).

[12] *Idem* art. 31 Convenio colectivo de trabajo de ámbito provincial para la actividad de oficinas y despachos. Idem Art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería. Disp. Adic. 1ª y 2ª V Convenio colectivo de Consum, Sociedad Cooperativa Valenciana. Art. 47, Disp. Adic. 5ª y 8ª Convenio Colectivo del Grupo Acrismatic. Art. 6.3 Convenio colectivo de Delver Logistics, SLU.

[13] Art. 71.3 VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados.

[14] Art. 46 VI Convenio autonómico de Pompas Fúnebres de Galicia.

por la LOPD, cualquier tipo de información o documentación relacionada con su actividad laboral[15].

Avanza más la regulación convencional que, en vez de remitirse a la LOPD, opta por recordar y cumplir los mandatos de esa legislación específica, como nos muestra la cláusula convencional del Convenio colectivo Barna Porters[16], en virtud de la cual, y citando el Reglamento comunitario, se indica que la empresa Barna Porters informará y solicitará el consentimiento expreso[17], de acuerdo con la representación legal de los trabajadores[18], a las personas trabajadoras, de que los datos personales que han facilitado o faciliten voluntariamente a la empresa durante su relación contractual se incorporen a un fichero propiedad de la empresa con la única finalidad de mantener y dar cumplimiento a su contrato de trabajo y proceder a gestionar los recursos humanos, y la formación y promoción de los trabajadores de la empresa[19]. Se añade en dicho convenio colectivo, que los trabajadores podrán ejercitar su derecho de acceso, rectificación, cancelación y oposición a través de los canales establecidos, mediante solicitud al responsable del fichero.

Mediante dicha cláusula se informa a los trabajadores de que su consentimiento será requisito previo a la recogida de sus datos personales, y a la utilización de los datos recabados[20]. Se indica la única finalidad que se persigue con su recogida, lo que permite confirmar la conexión entre la información personal que se recaba y trata, y el legítimo objetivo para el que se solicita. Se informa de su incorporación a un fichero propiedad de la empresa. Recuerda, por último, los derechos –previstos legalmente– de acceso, rectificación, cancelación y oposición de los trabajadores y el procedimiento para ejercitar esos derechos[21].

Cuando se trata de datos de carácter personal relativos a la salud del trabajador, se garantiza el respeto del derecho a la intimidad y dignidad de los trabajadores, así como la confidencialidad de toda la información relacionada con su estado de salud[22].

Junto al Convenio colectivo Barna Porters, el Convenio colectivo marco de la Unión General de Trabajadores[23] muestra una de las regulaciones más completas, puesto que incluye un capítulo específico titulado "Los derechos digitales", en el que se establecen los principios comunes, así como la creación de una Comisión para la protección de los derechos digitales. Analicemos los detalles de ese contenido.

---

[15] Art. 8.1 Convenio colectivo de Delver Logistics, SLU.

[16] Art. 51 Convenio colectivo Barna Porters. También art. 46 VI convenio autonómico de Pompas Fúnebres de Galicia.

[17] *Idem* art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[18] *Idem* art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[19] *Idem* art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[20] "El tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona, requerirá el consentimiento de esta, salvo que ese tratamiento sea necesario para cumplir con la obligación del control diario de jornada": art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería. Sobre las categorías especiales, *vid.* en este mismo número de la Revista, el artículo del profesor DE VAL TENA: "Categorías especiales de datos personales en el ámbito de la relación de trabajo".

[21] Art. 51 Convenio colectivo Barna Porters. También art. 46 VI Convenio autonómico de Pompas Fúnebres de Galicia.

[22] Art. 43 II Convenio colectivo de la Asociación Centro Trama. Art. 75 I Convenio colectivo de Quirón Prevención, SLU. Se puede redactar con más detalle el contenido relativo a la vigilancia de la salud y la protección de los datos de carácter personal de los trabajadores, como se observa en el art. 61 Convenio colectivo estatal de tejas, ladrillos y piezas especiales de arcilla cocida. En el mismo se hace referencia al carácter secreto de la historia clínica y a que "cuando finalice la relación laboral, el servicio de prevención le entregará una copia del historial clínico laboral a petición del trabajador".

Sobre las categorías especiales, *vid.* en este mismo número de la Revista, el artículo del profesor DE VAL TENA: "Categorías especiales de datos personales en el ámbito de la relación de trabajo".

[23] Arts. 45, 46 y 47 Convenio colectivo marco de la Unión General de Trabajadores.

El Convenio mencionado, primero, recuerda la obligación de respeto y cumplimiento de lo previsto en los arts. 87 a 91 LOPD y normas de desarrollo[24]. En este sentido, exige a las secciones sindicales regionales que comuniquen sus propuestas de transformación digital o tecnológica de forma detallada en el plazo de un mes anterior a que adopten decisiones al respecto[25].

A continuación, señala una serie de disposiciones comunes relativas a la utilización de los dispositivos digitales y el tratamiento de datos obtenidos de su uso[26], que incluyen:

a) La comunicación a las secciones sindicales regionales de forma expresa, clara e inequívoca, de las medidas relativas a dicho uso, con carácter previo a su adopción. Las medidas a adoptar deben atender a un fin legítimo, y respetar los principios de proporcionalidad e intervención mínima.

b) Información a los trabajadores de los Organismos afectados por el ámbito funcional del Convenio, sobre los derechos a la protección de sus datos de carácter personal, así como sobre el contenido, los criterios de utilización de los dispositivos digitales en el ámbito laboral y el tratamiento de los datos obtenidos a través de dichos sistemas[27].

c) Idoneidad, necesidad y proporcionalidad entre el tratamiento de los datos personales y los fines para los que son tratados[28]. Al respecto, los trabajadores pueden ejercitar sus derechos de acceso, rectificación, limitación del tratamiento y supresión de datos.

d) Obligación de previa consulta a los trabajadores sobre decisiones a adoptar en materia de planificación, organización del trabajo en la empresa e introducción de nuevas tecnologías, en todo lo relacionado con las consecuencias que éstas pudieran tener para la seguridad y la salud de los trabajadores, derivadas de la elección de los equipos, la determinación y la adecuación de las condiciones de trabajo y el impacto de los factores ambientales en el trabajo.

Como novedad de este Convenio[29] también destaca la constitución de una Comisión paritaria para la protección de los derechos digitales. Este órgano de representación paritario está compuesto por dos personas nombradas por cada una de las partes (social y empresarial), y desempeña las competencias sobre las materias relacionadas con el fin de salvaguardar los derechos digitales en el ámbito laboral.

A la Comisión para la protección de los derechos digitales se le encomienda la negociación y aprobación del acuerdo sobre la materia, con los contenidos siguientes: utilización de los dispositivos digitales, garantías de los derechos relacionados con el tratamiento de datos personales de los trabajadores, desconexión digital, formación y sensibilización de los trabajadores respecto de sus derechos digitales, y demás garantías adicionales que tengan conexión con las materias mencionadas, junto con la articulación de los derechos de acceso, rectificación, limitación del tratamiento y eliminación.

El plazo, para alcanzar un acuerdo sobre la materia, se limita a la vigencia del convenio colectivo, y se incorporará en este último como anexo. Si no se alcanza un acuerdo al respecto, se prevén la mediación y el arbitraje para

[24] *Idem* art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[25] Art. 45 Convenio colectivo marco de la Unión General de Trabajadores.

[26] Art. 46 Convenio colectivo marco de la Unión General de Trabajadores.

[27] Esa información deberá ser clara e inequívoca, como señala el art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[28] Art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[29] Art. 47 Convenio colectivo marco de la Unión General de Trabajadores.

desbloquear la negociación y lograr el objetivo de regulación de esta materia.

Asimismo, la Comisión asume las funciones de vigilancia y control del cumplimiento de lo pactado en esta materia, y debe impulsar cuantas medidas sean convenientes de cara a observar la adecuación o la conveniencia de modificar los criterios de utilización pactados, o establecer salvaguardas.

3.2. Deber de confidencialidad, secreto profesional y acceso a los datos de carácter personal

Dado el carácter sensible de los datos a los que puedan tener acceso los trabajadores, estos están especialmente obligados al secreto profesional respecto de los datos de carácter personal en cuyo tratamiento intervengan, con independencia de que la empresa sea la responsable del fichero o la encargada de su tratamiento por cuenta de un cliente[30].

Del mismo modo, los trabajadores deben cumplir y respetar las medidas generales y específicas de seguridad que la empresa establezca en relación con los ficheros que contengan datos personales.

Respecto de esas medidas de seguridad que la empresa pueda determinar, en materia de protección de datos y confidencialidad, cabe destacar la regulación detallada prevista en el Convenio colectivo de Hollygood, SL[31]., que estipula todo lo relativo a la confidencialidad, el acceso a esos datos de carácter personal y la posible cesión de los mismos. En primer lugar, respecto de la confidencialidad y el secreto profesional dispone lo siguiente:

– Que los trabajadores se comprometen de manera expresa, tanto durante la vigencia de su prestación de servicios, como después de su extinción, a no difundir, transmitir, revelar a terceras personas cualquier información de la empresa o de los clientes/as de la misma, a la que tenga acceso como consecuencia del desempeño de su actividad laboral, ni a utilizar tal información en interés propio o de sus terceros.

– Esa prohibición mencionada se extiende a la reproducción en cualquier soporte de la información de la empresa a la que tenga acceso el trabajador sobre datos o clientes de la empresa, procedimientos y sistemas de organización, programas informáticos o cualquier otro tipo de información interna, salvo que tal información sea estrictamente necesaria para el desarrollo del contenido inherente a su puesto de trabajo y se realice dentro del ámbito de la empresa.

En los textos convencionales se reitera, a menudo, que son propiedad de la empresa todas las notas, informes y cualesquiera otros documentos (incluyendo los almacenados en dispositivos informáticos), elaborados por el trabajador durante la vigencia del contrato que lo relaciona con la empresa, y que se refieran a la actividad de la empresa. De ahí que sea la empresa la que custodie esa información y documentación[32].

El deber de confidencialidad está protegido en dicha empresa frente a su vulneración, considerándose infracción muy grave su incumplimiento, pudiendo motivar un despido disciplinario. Aparte de la extinción contractual, la empresa se reserva el derecho a reclamar el resarcimiento de daños y perjuicios, sin perjuicio de adoptar cualquier otra reclamación incluida la vía penal[33].

Respecto de la cesión de datos de carácter personal, el texto convencional mencionado[34]

[30] Art. 33 Convenio colectivo 2019-2022 para la empresa Ontex peninsular.

[31] Art. 13 Convenio colectivo de Hollygood, SL. De forma más breve y genérica se expresa este contenido en el art. 43 Convenio colectivo de Nokia Spain, SA.

[32] Art. 13 Convenio colectivo de Hollygood, SL.

[33] Art. 13 Convenio colectivo de Hollygood, SL.

[34] Art. 13 Convenio colectivo de Hollygood, SL.

recuerda que solo se puede producir esa cesión previa autorización del titular de los datos personales, que, como hemos señalado anteriormente, son propiedad de la empresa. En este sentido, se fijan las medidas de garantía en materia de cesión, que son las siguientes[35]:

– Se permite el acceso únicamente si fuese necesario para cumplir con la prestación de servicios, siendo el trabajador el único responsable de la custodia de las claves de acceso utilizadas para su trabajo, las cuales son personales e intransferibles.

Las credenciales que la empresa entrega para los accesos a los sistemas (usuarios y contraseñas) tienen carácter confidencial, por lo que se prohíbe revelarlas (salvo por autorización expresa de los responsables de su administración). Existen credenciales personales y colectivas. En caso de credencial personal, el trabajador se responsabiliza del uso que se haga de la misma. Se prohíbe el acceso a los sistemas a los que el trabajador no se esté debidamente autorizado, bien utilizando medios o técnicas que permitan vulnerar la seguridad o bien utilizando credenciales que no le correspondan[36].

Los criterios de acceso al contenido de dispositivos digitales de uso por los trabajadores y trabajadoras, requieren especificar de modo preciso los usos autorizados y que se establezcan garantías para preservar la intimidad de los trabajadores, y la determinación de los periodos en que los dispositivos podrán utilizarse para fines privados[37].

– Cuando se produzca el acceso, el trabajador utilizará esos datos exclusivamente para cumplir con sus obligaciones contractuales para con la empresa.

– Asimismo, el trabajador cumplirá las medidas de seguridad presentes y futuras necesarias para asegurar la confidencialidad, secreto e integridad de los datos de carácter personal a los que tenga acceso.

– En ningún caso podrá, el trabajador, ceder a terceras personas los datos de carácter personal a los que tenga acceso, ni tan siquiera a efectos de su conservación.

– También se podrá disponer, como medida de garantía, de cámaras de seguridad, que graben de forma constante las instalaciones de la empresa. Para la empresa HOLLYGOOD[38], esas grabaciones pueden ser utilizadas no solo con el fin de evaluar el rendimiento de los trabajadores, sino también como prueba de cara a justificar un despido o servir de prueba válida ante los tribunales de justicia.

3.3. Faltas laborales en materia de protección de datos de carácter personal

Son escasas las referencias específicas a comportamientos incumplidores en materia de protección de datos de carácter personal, a excepción de lo ya mencionado en relación con el deber de confidencialidad. Aun así, podemos destacar las siguientes faltas consideradas muy graves:

– Hacer públicos los datos personales y/o teléfonos de los usuarios o familiares o a personas ajenas[39].

– El uso de claves ajenas para el acceso a cualquier equipo informático, red, fichero, archivo o documentación, incluida cualquier tipo de visita a internet o uso indebido del correo electrónico[40].

[35] Seguimos exponiendo el contenido del art. 13 Convenio colectivo de Hollygood, SL.

[36] Art. 33 Convenio colectivo 2019-2022 para la empresa Ontex peninsular.

[37] Art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[38] Art. 13 Convenio colectivo de Hollygood, SL. De modo similar, Disp. Adic. 1ª V Convenio colectivo de Consum, Sociedad Cooperativa Valenciana.

[39] Art. 28.21 Convenio colectivo de clínicas y consultas de odontología y estomatología de la provincia de Ávila.

[40] Art. 42, apartados nº 22 Convenio Colectivo de Trabajo de ámbito provincial para las industrias de la Madera y Corcho.

– Violar el secreto de la correspondencia o documentos reservados de la empresa, o revelar a personas extrañas a la misma el contenido de éstos[41].

– También es falta muy grave, la extracción de información de la empresa a cualquier dispositivo de almacenamiento o por cualquier otro medio, sin permiso de esta; y revelar a terceros ajenos a la empresa datos de reserva obligada[42].

– El incumplimiento en materia de protección de datos[43], a veces, con el condicionante de que cause perjuicios graves al organismo[44].

– La violación de los secretos de obligada confidencialidad, el de correspondencia o documentos reservados de la empresa, debidamente advertida, revelándolo a personas u organizaciones ajenas a la misma, cuando se pudieran causar perjuicios graves a la empresa[45].

– El incumplimiento de las normas e instrucciones de la empresa referidas a la seguridad de la información, la confidencialidad y la utilización de los medios tecnológicos[46].

– Aquellos usos que impliquen la comisión de un acto ilícito o perjudicial de cualquier modo, incluyendo el envío o la comunicación de información difamatoria, escandalosa, amenazadora, acosadora o las que sean de carácter privado sin la autorización de las personas implicadas[47].

– Respecto del incumplimiento del respeto al derecho a la intimidad y dignidad del trabajador, en relación con la vigilancia de la salud en la empresa, puede conllevar el cese inmediato de la persona responsable, reservándose la dirección el derecho a emprender las acciones legales oportunas[48].

4. LOS DERECHOS A LA INTIMIDAD Y A LA DIGNIDAD EN LA UTILIZACIÓN DE LOS DISPOSITIVOS DIGITALES DE LA EMPRESA

4.1. Disposiciones comunes

Para el desempeño de las actividades y funciones relativas a su puesto de trabajo, el trabajador precisa cada vez con más frecuencia, de la utilización de dispositivos digitales corporativos, así como del correo electrónico y el sistema de mensajería proporcionados por la empresa y propiedad de la misma[49], las herramientas sociales y colaborativas. Los trabajadores que, por sus funciones, tengan acceso a internet, intranet y/o correo electrónico, deben hacer un uso razonable de los medios

Idem art. 30 Faltas muy graves Convenio Colectivo Provincial de Trabajo para las Industrias de Carpintería y Ebanistería.

[41] Art. 34. 8 Convenio colectivo del Grupo Acrismatic. art. 32.7 y .8 Convenio Colectivo de la empresa Alvarez Maderas y Envases S.L.

[42] Art. 34.19 y 25, respectivamente, del Convenio colectivo del Grupo Acrismatic. Art. 33 Convenio colectivo 2019-2022 para la empresa Ontex peninsular. En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[43] Art. 39.7 VI Convenio autonómico de Pompas Fúnebres de Galicia. Art. 48.b) 12 III Convenio colectivo de Puertos del Estado y Autoridades Portuarias. Art. 61.3.h) I Convenio colectivo de Quirón Prevención, SLU.

[44] Art. 48.c) 28 III Convenio colectivo de Puertos del Estado y Autoridades Portuarias.

[45] Art. 67.i) Convenio Colectivo del sector de la Industria Siderometalúrgica de Cantabria. art. 32.7 y .8 del Convenio Colectivo de la empresa Alvarez Maderas y Envases S.L.

[46] Art. 57 Convenio colectivo de Severiano Servicio Móvil, SA.

[47] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[48] Art. 43 II Convenio colectivo de la Asociación Centro Trama. Art. 75 I Convenio colectivo de Quirón Prevención, SLU. Art. 36.2 Convenio colectivo de trabajo de cueros, repujados, marroquinería y similares de Cataluña.

[49] Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca.

telemáticos, de acuerdo con los principios de la buena fe contractual[50].

En este sentido, en la negociación colectiva se estipulan los principios generales de utilización de internet y las nuevas tecnologías en la empresa, para que el uso de correo electrónico e internet, así como del resto de herramientas y medios técnicos puestos a disposición de los trabajadores por la empresa, se ajusten a lo dispuesto en el convenio colectivo, y a la regulación normativa vigente.

Esta regulación convencional debe partir de dos pilares fundamentales, como son, por un lado, el legítimo derecho de la empresa, de controlar el uso adecuado de las herramientas y medios técnicos que pone a disposición del trabajador para realizar su actividad; y, por otro lado, la salvaguarda del derecho a la intimidad y a la dignidad del trabajador.

La necesidad de esos instrumentos digitales no solo se enfoca a que el trabajador desarrolle sus tareas con eficacia, sino también a que pueda utilizar dichos medios electrónicos para su relación con las representaciones sindicales y unitarias de los trabajadores de la empresa.

Uno de los convenios colectivos más recientes que se ocupa de estos aspectos relativos a la protección de datos personales del trabajador y los derechos digitales, es el II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU[51], en cuyo Capítulo XVI se regula todo lo relativo a la utilización de dispositivos digitales corporativos, software y aplicativos, correo electrónico, sistema de mensajería y herramientas sociales y colaborativas, acceso a internet.

En contraste con el convenio anteriormente citado, en otras ocasiones, el convenio colectivo solo se remite a la regulación normativa legal sobre la garantía de los derechos digitales[52], señalando que las empresas articular**á**n los medios necesarios para el adecuado ejercicio y respeto de los derechos establecidos en los arts. 87 a 91 de la LOPD y en la normativa que la desarrolla o sustituya.

4.2. El poder directivo empresarial de control de los dispositivos digitales

Para el empresario resulta imprescindible marcar los límites en la utilización de esos instrumentos digitales, ejercitando su poder directivo, al mismo tiempo que determinar qué conductas son sancionables por haber sobrepasado los límites fijados. De ahí que la negociación colectiva, cuando regula el contenido sobre la utilización por los trabajadores de los instrumentos tecnológicos y digitales, suela incorporar una primera cláusula en la que recuerda que las facultades organizativas y directivas del empresario en defensa de sus intereses legítimos, le facultan para llevar a cabo el control del uso de los medios digitales que tienen disponibles sus trabajadores para realizar su actividad laboral[53]. En alguna ocasión se añade que el ejercicio de ese poder directivo concreto queda delimitado en lo regulado por el convenio colectivo aplicable a la empresa[54].

Resulta excepcional encontrar un convenio colectivo que proponga la negociación colecti-

[50] Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca.

[51] II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[52] Art. 83 Convenio colectivo estatal de tejas, ladrillos y piezas especiales de arcilla cocida.

[53] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[54] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

va de un protocolo de uso de los medios informáticos, pero un ejemplo de ello es el art. 56.d) Convenio Colectivo del Sector e Industria, Servicios e Instalaciones del Metal de la Comunidad de Madrid[55].

Como tales recursos son de carácter laboral, las empresas podrán ejercer sobre los mismos las medidas de dirección, gestión y control que fueran precisas, respetando el derecho a la intimidad y a la dignidad de las personas trabajadoras[56].

Para garantizar que ese control empresarial de las herramientas informáticas y medios técnicos se realice dentro de los parámetros legales, la negociación colectiva suele recordar que el control empresarial se realizará dentro del límite general y los límites específicos[57], refiriéndose el límite general al respeto de los derechos fundamentales de las personas trabajadoras. En ocasiones, se matiza que se pondrá especial atención en la protección de aquellos derechos más fácilmente vulnerables y, en particular, el derecho al secreto de las comunicaciones y a la intimidad y dignidad de los trabajadores[58]. Como límites específicos se prevé que esas medidas de control empresarial sean proporcionales al riesgo existente y necesario para alcanzar un propósito específico, explícito y legítimo.

Con carácter general, los convenios colectivos establecen el límite de que todos esos dispositivos digitales no sean utilizados para fines particulares[59], sino que esa utilización sea siempre por motivos y para fines laborales[60]. Así sucede, por ejemplo, en el II Convenio colectivo de la Asociación Centro Trama, que dispone lo siguiente: "Los trabajadores y trabajadoras podrán utilizar el correo electrónico, la intranet e internet con libertad y en el sentido más amplio posible, para el desempeño de las actividades de su puesto de trabajo"[61].

En algunos textos convencionales se determinan los instrumentos informáticos y sus usos para el desarrollo de la actividad laboral[62], indicando:

- Que el personal no utilizará programas propios ni de uso particular, ni introducirá datos particulares ni extraerá ningún tipo de datos del sistema informático para uso particular, así como no introducirá contraseñas privadas no autorizadas por la empresa.

- Que se obliga al personal a mantener conectado durante toda la jornada laboral el teléfono móvil propiedad de la empresa que le ha facilitado a fin de que ésta se pueda comunicar con el mismo en cualquier momento.

- Que no utilizará cualquier medio de comunicación vía intranet-internet, correo electrónico o cualquier otra modalidad que exista o pudiera existir en la empresa para uso particular o privado.

[55] También art. 57.d) Convenio Colectivo del Sector Industrias Siderometalúrgicas de Navarra. Art. 64.d) convenio colectivo de industrias siderometalúrgicas de Guadalajara. Art. 32.d) Convenio Colectivo de la empresa TSF Navarra de Técnicas de Soldadura y Fijación, S.L. de Arazuri-Orcoyen. Art. 66.d) Convenio Colectivo del sector de la Industria Siderometalurgica de Cantabria.

[56] Art. 33 Convenio colectivo 2019-2022 para la empresa Ontex peninsular. Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca.

[57] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[58] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[59] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU. Art. 40.2.19 Convenio colectivo estatal de tejas, ladrillos y piezas especiales de arcilla cocida.

[60] Art. 75 del II Convenio colectivo de la Asociación Centro Trama.

[61] Art. 76 II Convenio colectivo de la Asociación Centro Trama. Art. 71 Convenio colectivo de trabajo de cueros, repujados, marroquinería y similares de Cataluña.

[62] Art. 7.3, .4 y .5 Convenio colectivo de Delver Logistics, SLU.

Junto a esa regla general, se prevé la excepción de un uso particular, pero de carácter restringido, esto es, solo si cumple los siguientes requisitos[63]:

- Que esté justificado razonablemente en atención a necesidades familiares y domésticas, cuestiones de necesidad o urgentes, o para acceder esporádicamente a información que no esté prohibida por la entidad empresarial.
- Que no interfiera en el normal cumplimiento de las obligaciones laborales.
- Que no interfiera en el normal uso de los medios tecnológicos de la empresa.
- Solo durante el tiempo estrictamente indispensable.
- Que no se vulnere la confidencialidad de la información de la empresa, ni su reputación, ni sea un uso contrario a la ley o a la normativa corporativa empresarial.
- Tampoco se permitirá una utilización que ponga en riesgo la seguridad de la información, o de los instrumentos digitales que la empresa haya proporcionado a los trabajadores.
- Que se cuente con la autorización oportuna[64].

Cabe destacar, entre los requisitos establecidos, los de no vulneración de la confidencialidad de la información de la empresa, y la seguridad de la información.

En algún texto convencional, se señala el supuesto de que los trabajadores necesiten realizar un uso de estos medios que exceda de lo habitual, tengan o no relación con el desempeño profesional, para lo cual deben utilizar los cauces adecuados de acuerdo con su superior inmediato, a fin de no causar daños en el desarrollo normal de las comunicaciones y en el funcionamiento de la red interna[65].

Por otro lado, en algún convenio colectivo se hace constar que no está permitido el envío de mensajes o imágenes de material ofensivo, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, aquellos que promuevan el acoso sexual, así como la utilización de la red para juegos de azar, sorteos, descarga de video, etc., no relacionados con la actividad profesional[66].

Es frecuente que los textos convencionales destaquen, como lo hace el Convenio colectivo de Davigel España, que la empresa puede utilizar software de control automatizado para controlar el material creado, almacenado, enviado o recibido en la red de la empresa, así como controlar sitios visitados por sus trabajadores usuarios en internet, espacios de charla, revisar historiales descargados de la red de internet por los trabajadores, revisar historiales de mensajes, de correo electrónico enviados y recibidos por los trabajadores[67].

No obstante, y como hemos señalado, se debe garantizar el respeto a la dignidad e intimidad del trabajador, cuando existan indicios

[63] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[64] Esta circunstancia se añade tanto al calificar el comportamiento como falta leve, grave o muy grave, en los art. 39.2.1. l, 2.2.k, y 2.3.o del Convenio colectivo de recuperación y reciclado de residuos y materias primas secundarias. Idem art. 34.20 Convenio Colectivo del Grupo Acrismatic. Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca.

[65] Art. 76 II Convenio colectivo de la Asociación Centro Trama.

[66] Art. 76 II Convenio colectivo de la Asociación Centro Trama.

[67] Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca.

De modo similar, art. 33 Convenio colectivo 2019-2022 para la empresa Ontex peninsular, y arts. 68-70 VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados. Por su parte, el Convenio colectivo del Grupo de empresas Mercadona, SA, y Forns Valencians Forva, SA, Unipersonal incluye ese contenido al hilo de enumerar las faltas muy graves, en concreto, en el art. 33.C.3 del mismo.

de uso ilícito o abusivo por su parte y la entidad empresarial realice las comprobaciones oportunas, por ejemplo, en el ordenador del trabajador o en los sistemas que ofrecen el servicio. En este sentido, en el caso de que el empresario proceda a verificar esos indicios, se suelen incorporar en los convenios colectivos varias garantías de los derechos fundamentales anteriormente mencionados, como los siguientes:

- La garantía de la presencia del trabajador[68].
- La presencia de algún representante unitario o sindical si el trabajador así lo desea[69].
- La comprobación se hará en horario laboral[70].
- El acceso debe ser necesario para facilitar razonablemente las operaciones empresariales; si existen medios o mecanismos de menor impacto para el trabajador, la empresa deberá hacer uso de los mismos, para que sea una intervención mínima.
- La privacidad y la dignidad del trabajador deberá garantizarse, en cualquier caso[71].
- La denegación de acceso por parte del trabajador podrá dar lugar a la imposición de las sanciones disciplinarias correspondientes[72].

4.3. Los representantes de los trabajadores, los dispositivos digitales y la protección de datos de carácter personal de los trabajadores

Los textos convencionales hacen referencia a la participación de la representación legal de los trabajadores en materia de protección de los datos de carácter personal de los trabajadores:

- En la elaboración de los criterios de utilización de los dispositivos digitales[73].
- Como informadora pasiva, ya que se le comunicará la introducción de nuevas tecnologías en la empresa, que comporten un periodo de formación a las personas trabajadoras[74].
- Audiencia previa a la elaboración y adopción por la empresa de la política interna al respecto, en la que se especifiquen las modalidades de ejercicio del derecho a la desconexión, especialmente en el supuesto de trabajo a distancia o en su domicilio, así como las acciones de formación y de sensibilización sobre un uso razonable de las herramientas tecnológicas, con el fin de prevenir del riesgo de fatiga informática.

[68] La Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca, matiza que se inspeccione con la asistencia de los representantes legales de los trabajadores o, en su defecto, por otros trabajadores de Davigel España.

[69] Art. 76 II Convenio colectivo de la Asociación Centro Trama. Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca. En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[70] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[71] En este sentido, Art. 76 II Convenio colectivo de la Asociación Centro Trama. Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca. Art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[72] Disp. Adic. 3ª Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca.

[73] Art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

[74] Art. 85 Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería.

Por otro lado, para facilitar los derechos de información que legalmente tienen reconocidos los representantes de los trabajadores, se permite, en los convenios colectivos, que los miembros de comités de empresa, delegados de personal o delegados sindicales puedan hacer uso del correo electrónico para comunicarse entre sí o con sus respectivas organizaciones sindicales, así como con la dirección de la empresa[75], del mismo modo que puede tener a su disposición un tablón virtual a tal efecto[76], o una cuenta específica de correo electrónico[77].

Con esa misma finalidad facilitadora, se suele regular en la negociación colectiva que la empresa ponga a disposición de la representación de los trabajadores los medios para que pueda utilizar el correo electrónico en las comunicaciones con los trabajadores, disfrutando del acceso a las direcciones de correo de las que estos últimos dispongan en la empresa[78]. No obstante, se añade en esos textos convencionales, que las representaciones de los trabajadores, en el ejercicio del derecho que se les reconoce, deberán cumplir la normativa vigente en materia de protección de datos de carácter personal[79].

Otra garantía en favor de los representantes de los trabajadores que hemos encontrado en algún texto convencional, es la de excluir de la consideración como faltas graves determinados comportamientos si son realizados por representantes legales y sindicales de los trabajadores en el ejercicio de sus funciones, como se produce con los siguientes[80]:

– El uso del teléfono móvil (aun siendo propiedad del trabajador) para fines personales durante el tiempo efectivo de trabajo. El uso reiterado o el perjuicio generado por el mismo en el proceso productivo. Igual consideración tendrá el uso de aparatos reproductores multimedia durante el tiempo de trabajo.

– El uso no autorizado y con carácter personal de las herramientas de la empresa, dentro o fuera de la jornada laboral, para fines particulares. A estos efectos tendrán también la consideración de herramientas todos los equipos informáticos.

4.4. Ejercicio del poder disciplinario en caso de uso irregular de las nuevas tecnologías

El incumplimiento de las normas sobre utilización de los sistemas informáticos y herramientas tecnológicas a los que se hace referencia en los apartados anteriores, puede requerir revisar cualquier software dentro de la red empresarial, imponer las restricciones que se consideren oportunas en la utilización de estos medios, y aplicar el régimen disciplinario previsto en el convenio colectivo concreto[81].

Con frecuencia, los convenios colectivos se ocupan de estos contenidos en el apartado relativo al régimen disciplinario, clasificando los comportamientos sancionables como faltas leves, graves o muy graves.

En unos casos, el comportamiento prohibido se expresa de modo general y se limita en función de ciertas condiciones; si ha habido un uso particular, si ha ocasionado perjuicios a la empresa[82]. En otros casos, se detalla, por ejem-

[75] Art. 72 Convenio colectivo de trabajo de cueros, repujados, marroquinería y similares de Cataluña.

[76] Art. 93 I Convenio colectivo de Quirón Prevención, SLU.

[77] Art. 51 Convenio colectivo de Nokia Spain, SA.

[78] Art. 46 VI convenio autonómico de Pompas Fúnebres de Galicia.

[79] Art. 72 Convenio colectivo de trabajo de cueros, repujados, marroquinería y similares de Cataluña.

[80] Art. 30 Faltas graves letras U) y V) del Colectivo Provincial de Trabajo para las Industrias de Carpintería y Ebanistería. Art. 31 Convenio colectivo de la madera de la provincia de Cuenca. Art. 40.1.10 Convenio colectivo estatal de tejas, ladrillos y piezas especiales de arcilla cocida.

[81] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[82] Como muestra, el art. 42.3. letra r) del III Convenio colectivo de Activa Innovación y Servicios, SAU. califica como

plo, prohibiendo utilizar las herramientas corporativas para envíos masivos o uso abusivo que interfieran las comunicaciones del resto de personas trabajadoras o perturben el normal funcionamiento de la red empresarial[83].

Podemos encontrar, en los textos convencionales, los usos prohibidos distinguiendo, por un lado, aquellos que afectan a los derechos de los demás trabajadores o a terceros[84]. Por otro lado, aquellos que perjudican a la empresa[85].

Asimismo, se puede comparar el nivel de gravedad de la falta que el convenio colectivo prevé, en función de que concurran o no distintas circunstancias. Como muestra de ello, acudimos al Convenio colectivo de la ONCE:

- Faltas leves[86]:

– Efectuar modificaciones a los componentes físicos (hardware) de los equipos informáticos (ampliación de memoria, módems, teclado, añadir o quitar tarjetas, etc.).

– Utilizar recursos telemáticos, incluido internet y correo electrónico, para actividades no relacionadas directamente con el puesto de trabajo, siempre que no interfiera con la actividad laboral ni se produzca perjuicio para la ONCE.

- Faltas graves[87]:

– Compartir o facilitar el identificador de usuario y contraseña a otras personas (logon, login, etc.).

– Enviar mensajes de correo electrónico de forma masiva sin consentimiento de la empresa.

– Instalar cualquier tipo de software (programas, paquetes, etc.), sin la correspondiente autorización.

– Cambiar la configuración de los recursos informáticos corporativos.

– Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

– Leer, borrar, copiar, o modificar los mensajes de correo electrónico o archivos de otros usuarios. Enviar mensajes de correo electrónico de forma masiva sin consentimiento de la Organización.

- Faltas muy graves[88]:

– Acceder, o intentar acceder, a áreas restringidas de los sistemas informáticos

infracción muy grave la siguiente: "El uso de software ilegal o programas informáticos no autorizados por la Empresa así como la utilización de cualquier medio de comunicación internet-intranet, correo electrónico y otros para uso privado o particular o la introducción de contraseñas privadas y no autorizadas por el administrador del sistema de la Empresa, si se causa perjuicio a la Empresa".

[83] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU.

[84] En este sentido, por ejemplo, el art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU. Establece la siguiente prohibición: "Bajo ningún concepto podrán las personas trabajadoras falsificar mensajes de correo electrónico, enviar mensajes por correo o imágenes de material ofensivo, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc., o aquellos que promuevan el acoso sexual o moral o inciten a la violencia".

[85] En este sentido, el art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU. Prevé como sancionable "Evadir soluciones de seguridad, aprovechar potenciales vulnerabilidades de los sistemas o redes, emplear redes wifi o cualquier otro tipo de red de comunicación, para fines ilícitos que supongan un perjuicio para la Empresa o para el resto de personas trabajadoras de la Compañía".

[86] Art. 73.a apartados 8 a 10 XVI Convenio colectivo de la ONCE y su personal.

[87] Art. 73.b. apartados 15 a 20 XVI Convenio colectivo de la ONCE y su personal.

[88] Art. 73.c. apartados 24 a 30 XVI Convenio colectivo de la ONCE y su personal.

ONCE o aumentar el nivel de privilegios de un usuario.

– Introducir voluntariamente virus o cualquier otro software que produzca graves alteraciones en los sistemas.

– Copiar y transferir al exterior datos de carácter personal o confidencial obrantes en los ficheros propiedad de la ONCE, o utilizar este tipo de datos para usos propios o con fines lucrativos.

– Descifrar, o intentar descifrar, las contraseñas, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la empresa.

– Crear ficheros y bases de datos con datos personales sin la autorización exigida por la normativa vigente en cada caso.

– Usar programas informáticos sin la correspondiente licencia, así como usar, reproducir, ceder, transformar o comunicar públicamente cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

– No cumplir con el deber de confidencialidad o con las medidas de seguridad implantadas para los ficheros de datos o documentos de carácter personal, o dar a estos datos un fin inadecuado.

4.5. Clasificación de las faltas laborales en esta materia

Podemos sistematizar el contenido del régimen disciplinario que se prevé en los convenios colectivos en los supuestos de utilización irregular de las nuevas tecnologías de la información y la comunicación. En este sentido, se observa que algunos comportamientos sancionables figuran dentro del apartado de faltas graves en unos convenios colectivos, mientras que para otros convenios colectivos esas mismas faltas laborales son calificadas como muy graves.

Otro aspecto que destaca es que la misma conducta infractora se puede calificar por sí sola como falta laboral en un convenio colectivo, mientras que en otro convenio se exige que vaya acompañada de determinadas circunstancias, para poder obtener esa calificación de falta laboral, de modo que en ausencia de esas circunstancias no cabría considerar que se ha producido una falta laboral.

En ocasiones se ponen condicionantes que han de concurrir, aunque no simultáneamente, sino por separado, para considerar el comportamiento como falta muy grave, de modo que, si no se aprecian esos condicionantes, el comportamiento pasaría a calificarse como grave[89].

- Faltas leves

En los convenios colectivos analizados, se consideran faltas leves los comportamientos siguientes:

– Usar material de la empresa (medios telefónicos, telemáticos, informáticos, mecánicos o electrónicos) para asuntos particulares[90].

– El uso no autorizado y con carácter personal de las herramientas de la empresa, dentro o fuera de la jornada laboral, para fines particulares. A estos efectos tendrán también la consideración de herramientas todos los equipos informáticos, siempre y cuando su utilización exceda de la que cabe esperar de un medio moderno de comunicación e información[91].

– El uso inadecuado o para fines distintos de los autorizados de los sistemas

[89] Art. 61.3.p) I Convenio colectivo de Quirón Prevención, SLU.

[90] Art. 18.1.A).1 Convenio colectivo de Frit Ravich SL.

[91] Art. 72.11 Convenio colectivo del Grupo Prisa Radio. Art. 57 Convenio colectivo de Severiano Servicio Móvil, SA.

o herramientas informáticas, incluido internet, dispositivos móviles, que infrinja con carácter leve la normativa interna vigente en cada momento para esta materia en la empresa[92].

– El uso no autorizado de equipos informáticos, material y herramientas de Logirail para fines personales o de ocio, tanto dentro como fuera de la jornada laboral, siempre y cuando no comprometa la seguridad en la circulación o la de sus compañeros de trabajo[93].

– El uso de los teléfonos móviles particulares en el lugar de trabajo[94].

– Utilización del teléfono móvil personal durante la jornada laboral, cuando del tiempo empleado en esta utilización pueda inferirse una dejación o abandono de funciones inherentes al trabajo y siempre y cuando no obedezca a situaciones graves y de urgente necesidad para el trabajador[95].

– La utilización o manipulación de cualquier dispositivo electrónico, teléfono móvil, tableta o Smartphone, de titularidad personal, sin la autorización expresa del superior jerárquico durante la jornada de trabajo, excepto en salas y tiempo de descanso. Podrá ser tipificada de grave, si acarrean o conllevan consecuencias en materia de riesgos laborales para el titular o tercero[96].

[92] Art. 71.A. 9 Convenio colectivo del Grupo Parcial Cepsa. Art. 38.1. i) Convenio Colectivo de empresa para el personal laboral del Ayuntamiento de Cangas del Narcea.

[93] Art. 1.12 Anexo III Convenio colectivo de Logirail, SAU.

[94] Art. 45.7 V Convenio colectivo de Consum, Sociedad Cooperativa Valenciana.

[95] Art. 28.4 Convenio colectivo de clínicas y consultas de odontología y estomatología de la provincia de Ávila. Art. 56. J) Convenio colectivo sectorial de ámbito estatal de las administraciones de Loterías.

[96] Art. 32.12. del Convenio Colectivo de la empresa Álvarez Maderas y Envases S.L.

• Faltas graves

Como faltas graves, en los convenios colectivos objeto de estudio, se clasifican los siguientes incumplimientos laborales:

– Usar el teléfono de empresa para asuntos particulares sin la debida autorización, así como llevar desconectado reiteradamente el teléfono móvil que le facilita la empresa, propiedad de la misma, durante la jornada laboral impidiendo la comunicación de la empresa con el trabajador[97].

– El uso extraprofesional de internet y correo electrónico de la empresa puesto a disposición de los trabajadores para el desempeño de sus funciones, si el uso de los mismos estuvieran limitados[98].

– La utilización de los medios informáticos propiedad de la empresa (correo electrónico, internet, intranet, etc.), para fines distintos de los relacionados con el contenido de la prestación laboral[99], cuando del tiempo empleado en esta utilización pueda inferirse una dejación o abandono de funciones inherentes al trabajo[100].

– Aquellos usos que violen alguna ley o alguna normativa aplicable, incluyen-

[97] Art. 42.2. letra h) III Convenio colectivo de Activa Innovación y Servicios, SAU. Art. 38.2. p) Convenio Colectivo de empresa para el personal laboral del Ayuntamiento de Cangas del Narcea. Art. 47.B. 17 III Convenio colectivo de panadería y pastelería de la Comunitat Valenciana.

[98] Art. 47.2.0 VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados.

[99] Art. 32.16 Convenio Colectivo de la empresa Álvarez Maderas y Envases S.L.

[100] Art. 66.d) Convenio Colectivo del sector de la Industria Siderometalurgica de Cantabria. Art. 56.d) Convenio Colectivo del Sector e Industria, Servicios e Instalaciones del Metal de la Comunidad de Madrid. Art. 28.12 Convenio colectivo de clínicas y consultas de odontología y estomatología de la provincia de Ávila. Art. 64.d) Convenio colectivo de industrias siderometalúrgicas de Guadalajara. Art. 32.d) Convenio Colectivo de la empresa TSF Navarra de Técnicas de Soldadura y Fijación, S.L. de Arazuri-Orcoyen.

do, aunque no limitándose, a las leyes que regulan las actividades relativas a la publicidad, el alcohol, la protección de la infancia, las drogas, el cifrado, la alimentación, los servicios financieros, las armas de fuego, el juego y las apuestas, la importación, los sistemas de información, la propiedad intelectual, la obscenidad, la privacidad, la seguridad y las telecomunicaciones[101].

– El uso inadecuado o para fines distintos de los autorizados de los sistemas o herramientas informáticas, incluido internet y dispositivos móviles, que infrinja con carácter grave la normativa interna vigente en cada momento para esta materia en la empresa[102].

– En algún convenio colectivo se matizan más los requisitos para considerar grave la siguiente falta: utilización reiterada del teléfono móvil personal durante la jornada laboral, cuando del tiempo empleado en esta utilización pueda inferirse una dejación o abandono de funciones inherentes al trabajo y siempre y cuando no obedezca a situaciones graves y de urgente necesidad para el trabajador y ya hubiese sido sancionado el trabajador por esta conducta como falta leve[103].

– El uso del teléfono móvil (aun siendo propiedad del trabajador) para fines personales durante el tiempo efectivo de trabajo. El uso reiterado o el perjuicio generado por el mismo en el proceso productivo. Igual consideración tendrá el uso de aparatos reproductores multimedia durante el tiempo de trabajo[104].

– El uso no autorizado y con carácter personal de las herramientas de la empresa, dentro o fuera de la jornada laboral, para fines particulares. A estos efectos tendrán también la consideración de herramientas todos los equipos informáticos[105].

Como prerrogativa de los representantes sindicales y legales de los trabajadores de la empresa, se puede encontrar una cláusula como la del Convenio Colectivo de Trabajo de ámbito provincial para las industrias de la Madera y Corcho, que expresamente excluye de la calificación como falta grave, en caso de que la representación legal y sindical de los trabajadores hagan uso particular del teléfono móvil de la empresa, de los reproductores multimedia y de los equipos informáticos, sin autorización, si lo hacen en el ejercicio de sus funciones[106].

• Faltas muy graves

Se consideran faltas muy graves, principalmente por negligencia, disminución voluntaria del rendimiento, por mala fe y abuso de confianza, los siguientes comportamientos

[101] En este sentido, art. 168 II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU. También art. 57.d) Convenio Colectivo del Sector Industrias Siderometalúrgicas de Navarra. Art. 39.2.k Convenio Colectivo del Sector de Industrias Vinícolas de Navarra.

[102] Art. 71.B. 13 Convenio colectivo del Grupo Parcial Cepsa.

En otro Convenio colectivo se considera falta grave la utilización de los medios informáticos, telemáticos o tecnológicos puestos a disposición por la empresa de forma contraria a lo dispuesto en los códigos y protocolos de uso de dichos medios tecnológicos establecidos en cada empresa, y como muy grave si con ese comportamiento se produce un perjuicio grave a la empresa: Art. 41.2.l) y 41.3.i) del Convenio colectivo del sector Limpieza de Edificios y Locales de Zaragoza.

[103] Art. 28.11 Convenio colectivo de clínicas y consultas de odontología y estomatología de la provincia de Ávila.

[104] Art. 30 Faltas graves Convenio Colectivo Provincial de Trabajo para las Industrias de Carpintería y Ebanistería. Art. 31 Convenio colectivo de la madera de la provincia de Cuenca. Art. 41, apartados 21º y 22º Convenio Colectivo de Trabajo de ámbito provincial para las industrias de la Madera y Corcho.

[105] Art. 30 Faltas graves Convenio Colectivo Provincial de Trabajo para las Industrias de Carpintería y Ebanistería. Art. 41, apartados nº 21, y nº 22 Convenio Colectivo de Trabajo de ámbito provincial para las industrias de la Madera y Corcho.

[106] Art. 41, apartados nº 21, y nº 22 Convenio Colectivo de Trabajo de ámbito provincial para las industrias de la Madera y Corcho. Art. 31 Convenio colectivo de la madera de la provincia de Cuenca.

incumplidores previstos en los convenios colectivos que hemos consultado:

- El uso inadecuado o indebido[107] o para fines distintos de los autorizados al trabajo de los sistemas o herramientas informáticas, incluido internet y dispositivos móviles, que infrinja con carácter muy grave la normativa interna vigente en cada momento para esta materia en la empresa[108].

- La utilización de medios y equipos, incluidos los informáticos, para los que no se tenga autorización y que, con notorio beneficio personal, sean empleados para la realización de trabajos particulares o ajenos a la actividad contractual de la persona trabajadora[109].

- La reiteración en el uso indebido de internet y correo electrónico puestos por la empresa a disposición de los trabajadores para el desempeño de sus funciones, si el uso de los mismos estuvieran limitados[110].

- La utilización o instalación de programas de ordenador y la conexión a internet, de forma reiterada, sin la debida autorización, si con ello se causase un perjuicio importante a la empresa[111].

- La utilización para uso propio y particular de los medios materiales y elementos de comunicación de la empresa (en especial el teléfono, internet y correo electrónico)[112].

- El acceso, a través de internet, a páginas prohibidas por la Ley como por ejemplo, pornografía infantil[113], chats y juegos[114].

- La reiteración en el uso no autorizado y con carácter personal de las herramientas de la empresa, dentro o fuera de la jornada laboral, cuando el mismo sea contrario a los usos y costumbres comúnmente aceptados. En todo caso se considerará incluido el material pornográfico, de abuso de menores, terrorista y belicista, chats no relacionados con la actividad de la empresa y cualquier actividad con carácter lucrativo. A estos efectos tendrán también la consideración de herramientas los equipos informáticos[115].

- Usar el teléfono para asuntos particulares sin la debida autorización, así como llevar desconectado reiteradamente el teléfono móvil que le facilita la empresa, propiedad de la misma, durante la jornada laboral impidiendo la comunicación de la empresa con el personal[116].

- Violar el secreto de la correspondencia o documentos reservados a la empresa, así como el incumplimiento de la normativa de protección de datos[117].

- Revelar a elementos extraños a la Empresa datos de reserva obligada[118].

---

[107] Art. 30 Faltas muy graves, V) Convenio Colectivo Provincial de Trabajo para las Industrias de Carpintería y Ebanistería.

[108] Art. 71.C.7 Convenio colectivo del Grupo Parcial Cepsa.

[109] Art. 38.3. t) Convenio Colectivo de empresa para el personal laboral del Ayuntamiento de Cangas del Narcea.

[110] Art. 47.3.O) VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados.

[111] Art. 57 Convenio colectivo de Severiano Servicio Móvil, SA.

[112] Art. 47.C. 18 III Convenio colectivo de panadería y pastelería de la Comunitat Valenciana. Idem art. 44.12 Convenio Colectivo del sector Comercio Textil de la provincia de Castellón. Art. 47.15 V Convenio colectivo de Consum, Sociedad Cooperativa Valenciana. En este último precepto convencional, se faculta a la empresa para acceder a las comunicaciones con el objeto de verificar el fraude cuando existan indicios razonables de uso indebido de los mismos.

[113] Art. 39.2.k Convenio Colectivo del Sector de Industrias Vinícolas de Navarra.

[114] Anexo III apartado 3. 33 y 34 del Convenio colectivo de Logirail, SAU.

[115] Art. 47.C. 18 III Convenio colectivo de panadería y pastelería de la Comunitat Valenciana.

[116] Art. 30.3.17 Convenio colectivo de Delver Logistics, SLU.

[117] Art. 32.7 y .8 Convenio Colectivo de la empresa Alvarez Maderas y Envases S.L.

[118] Art. 32.7 y .8 Convenio Colectivo de la empresa Alvarez Maderas y Envases S.L.

5. DERECHO A LA DESCONEXIÓN DIGITAL

Las personas trabajadoras tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar. Pues bien, solo hemos encontrado algún convenio colectivo que regule la desconexión digital, y lo hace de forma muy vaga, esto es, incluyendo el término en el título del artículo, pero no detallando más aspectos de esa desconexión digital. La cláusula indica lo siguiente:

"Una vez finalizada la jornada laboral, y para gestionar mejor las cargas de trabajo de aquellas personas que dispongan de dispositivos portátiles para trabajar, teléfonos móviles, tabletas u ordenadores deberá respetarse el descanso entre jornadas de trabajo, el descanso semanal, los festivos, las vacaciones y cualquier tipo de ausencia justificada"[119].

Algo más añade el convenio colectivo de la empresa Autoamtax, que se apoya en el art. 88 LOPD, y dispone que la empresa, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que prevenga la fatiga informática, preservando el derecho a la desconexión digital en los casos de realización total o parcial del trabajo a distancia así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas[120].

[119] Art. 40 Convenio colectivo de Zurich Insurance PLC, Sucursal en España, Zurich Vida, Compañía de Seguros y Reaseguros, SA y Zurich Services, AIE.

[120] Art. 26 I Convenio colectivo de la empresa AUTOAMTAX, S.C.A.

6. CONCLUSIONES

Regulada por la LOPD la protección de datos y la garantía de los derechos digitales como derecho fundamental del ciudadano, surge la pregunta de qué espacio regulador queda asignado a la negociación colectiva. Partiendo de que es un derecho fundamental, su contenido esencial está fijado en la propia Ley orgánica. Sería, pues, el contenido adicional el que quedaría como posible objeto de regulación mediante los convenios colectivos.

El legislador hace referencia en el art. 91 LOPD a que los convenios colectivos podrán establecer "garantías adicionales". Por tanto, el papel de la negociación colectiva es secundario.

Con carácter general, la negociación colectiva no se ha ocupado más que escasamente, de las garantías adicionales para proteger los datos de carácter personal de los trabajadores y sus derechos digitales. Esa escasez se constata a pesar de que la materia abordada tiene carácter transversal, y afecta a todos los trabajadores, en mayor o menor medida, sea cual sea el tipo de actividad productiva que se desarrolle en la empresa.

De los convenios colectivos que se detienen a regular esa materia, lo más frecuente es que únicamente se centren en prever como faltas leves, graves y muy graves, los incumplimientos en materia de protección de datos de carácter personal, y en la utilización de las herramientas digitales y las nuevas tecnologías. Los convenios colectivos se centran en determinar los comportamientos sancionables, más que ocuparse de prever garantías para la protección de los datos de carácter personal de los trabajadores y de los derechos digitales de los trabajadores en el ámbito laboral.

De nuevo son escasos los convenios colectivos que detallan cómo se deben utilizar los instrumentos electrónicos en la empresa, aunque se puedan extraer algunas pautas a partir de las prohibiciones y de las faltas laborales expresadas en los textos convencionales.

La negociación colectiva tiene encomendado un papel menor en esta materia, pero es un papel normativo relevante, en la medida en que permite adaptar los contenidos legales a las más diversas situaciones en las empresas. Sería deseable que la negociación colectiva se mostrase más activa en esta materia, desarrollando contenidos protectores de los derechos fundamentales a la intimidad y la dignidad, y limitando de forma equilibrada las funciones de organización, vigilancia y control del empresario.

Anexo.
CONVENIOS COLECTIVOS CITADOS

Resolución de 23 de octubre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el II Convenio colectivo de empresas vinculadas para Telefónica de España, SAU, Telefónica Móviles España, SAU y Telefónica Soluciones de Informática y Comunicaciones de España, SAU. «BOE» núm. 273, de 13 de noviembre de 2019.

Resolución de 20 de diciembre de 2018, de la Dirección General de Trabajo, por la que se registra y publica el III Convenio colectivo de Activa Innovación y Servicios, SAU. (Boletín Oficial del Estado núm. 9 de 10/01/2019).

Resolución de 21 de diciembre de 2018, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo del Grupo Prisa Radio. BOE Núm. 21, de 24 de enero de 2019.

Resolución de 27 de diciembre de 2018, de la Dirección general de Trabajo, disponiendo la inscripción en el Registro y publicación del Convenio Colectivo del sector de la Industria Siderometalúrgica de Cantabria, para el periodo 2017-2020. (Boletín Oficial de Cantabria núm. 5 de 08/01/2019).

Resolución disponiendo la inscripción en el Registro y publicación del Convenio Colectivo de la empresa Álvarez Maderas y Envases S.L., para el periodo 2012-2021. Boletín Oficial de Cantabria nº 20, de 29/01/2019.

Resolución de 16 de febrero de 2018, de la Dirección General de Empleo, por la que se registra y publica el Convenio colectivo del Grupo Parcial Cepsa. Publicado en: «BOE» núm. 52, de 28 de febrero de 2018,

Resolución de 21 de diciembre de 2018, de la Consejería de Empleo, Industria y Turismo, por la que se ordena la inscripción del Convenio Colectivo de empresa para el personal laboral del Ayuntamiento de Cangas del Narcea en el Registro de convenios y acuerdos colectivos de trabajo dependiente de la Dirección General de Trabajo.

Resolución de 21 de diciembre de 2018, de la Consejería de Empleo, Industria y Turismo, por la que se ordena la inscripción del Convenio colectivo de empresa para el personal laboral del Ayuntamiento de Cangas del Narcea en el Registro de convenios y acuerdos colectivos de trabajo dependiente de la Dirección General de Trabajo. BOP Asturias nº 21, de 31 enero 2019.

Resolución de 15 de enero de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Davigel España, SAU, para sus centros de trabajo de Las Palmas de Gran Canaria, Madrid, Málaga y Palma de Mallorca. BOE nº 28, de 1 febrero 2019.

Resolución de la Oficina Territorial de Trabajo de Segovia por la que se ordena la inscripción y publicación del Convenio colectivo 2019-2022 para la empresa Ontex peninsular. BOP Segovia nº 14, de 1 de febrero de 2019.

Resolución de 22 de enero de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Severiano Servicio Móvil, SA. BOE nº 34, de 8 de febrero de 2019.

Resolución de 22 de enero de 2019, de la Dirección General de Trabajo, por la que se registra y publica el VII Convenio colectivo estatal del sector de fabricantes de yesos, escayolas, cales y sus prefabricados. Publicado en: «BOE» núm. 38, de 13 de febrero de 2019.

Resolución de 14 de enero 2019, de la Dirección General Trabajo, por la que se registra y publica el Convenio Colectivo del Sector e Industria, Servicios e Instalaciones del Metal de la Comunidad de Madrid, suscrito por la Asociación de Empresarios del Comercio de Industria del Metal de Madrid (AECIM) y las organizaciones sindicales CC OO de Industria e Madrid y Federación e Industria, Construcción y Agro de Madrid de UGT. BO. Comunidad de Madrid 14 febrero 2019, núm. 38.

Resolución de 4 de febrero de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo del Grupo de empresas Mercadona, SA, y Forns Valencians Forva, SA, Unipersonal. BOE nº 42, de 18 de febrero de 2019.

Resolución de 6 de febrero de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Hollygood, SL. BOE nº 43, de 19 de febrero de 2019.

Resolución de 9 de enero de 2019, de la Dirección General de Trabajo de la Consejería de Economía, Empleo y Hacienda, sobre registro, depósito y publicación del convenio colectivo de la empresa "Páginas Amarillas Soluciones Digitales, Sociedad Anónima Unipersonal" (centro San Sebastián de los Reyes) (código número 28102282012019).BOCM nº 44, de 21 de febrero de 2019.

Resolución 9C/2019, de 10 de enero, de la Directora General de Política Económica y Empresarial y Trabajo, por la que se acuerda el registro, depósito y publicación en el Boletín Oficial de Navarra del Convenio Colectivo del Sector Industrias Siderometalúrgicas de Navarra. BO Navarra de 26 de febrero de 2019.

Resolución de 16 de marzo 2019, del Servicio Provincial de Economía y Empleo de Zaragoza, por la que se registra y publica el convenio colectivo del sector Limpieza de Edificios y Locales de Zaragoza BO. Zaragoza 27 marzo 2019, núm. 70.

Resolución de 18 de febrero de 2019, de la Dirección General de Trabajo, por la que se registra y publica el V Convenio colectivo de Consum, Sociedad Cooperativa Valenciana.BOE nº 52, de 1 de marzo de 2019.

Resolución de 1 de marzo de 2019, de la Oficina territorial de Trabajo de la Delegación territorial de la Junta de Castilla y León en Ávila, por la que se dispone la inscripción en el registro de convenios y acuerdos colectivos de trabajo y la publicación en el boletín oficial de la provincia de Ávila del "convenio colectivo de clínicas y consultas de odontología y estomatología de la provincia de Ávila".

Resolución de 21 de febrero de 2019, de la Subdirección General de Relaciones Laborales, por la que se dispone el registro y publicación del texto del III Convenio colectivo de panadería y pastelería de la Comunitat Valenciana. Diario Oficial de la Comunitat Valenciana nº 8505, de 13 de marzo de 2019.

Resolución de 18 de marzo de 2019, de la Delegación Territorial de Jaén, de las Consejerías de Empleo, Formación y Trabajo Autónomo y de Economía, Conocimiento, Empresas y Universidad, por la que se dispone el registro y publicación del Convenio Colectivo de Trabajo de ámbito provincial para las industrias de la Madera y Corcho. Años 2019 y 2020.BOP de Jaén nº 56, de 22 de marzo de 2019.

Resolución de 8 de enero de 2018, de la Dirección General de Empleo, por la que se registra y publica el XVI Convenio colectivo de la ONCE y su personal. BOE nº 16, de 18 de enero de 2019.

Resolución de 19 de marzo de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de recuperación y reciclado de residuos y materias primas secundarias. BOE nº 76, de 29 de marzo de 2019.

Resolución de 19 de marzo de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Zurich Insurance PLC, Sucursal en España, Zurich Vida, Compañía de Seguros y Reaseguros, SA y Zurich Services, AIE. BOE nº 76, de 29 de marzo de 2019.

Resolución de 19 de marzo de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo del Grupo Acrismatic. BOE nº 76, de 29 de marzo de 2019.

Resolución de 20 de marzo de 2019, de la Dirección Territorial de Economía Sostenible, Sectores Productivos, Comercio y Trabajo, por la que se dispone el registro y publicación del Convenio Colectivo del sector Comercio Textil de la provincia de Castellón. BOP Castellón de la Plana nº 42, de 2 de abril de 2019.

Resolución TSF/773/2019, de 20 de febrero, de la Dirección General Relaciones Laborales y Calidad en el Trabajo, por la que se dispone la inscripción y la publicación del Convenio colectivo de trabajo de cueros, repujados, marroquinería y similares de Cataluña. Boletín Oficial de la Generalitat de Cataluña nº 7847, de 4 de abril de 2019.

Resolución de 19 de marzo de 2019, de la Dirección General de Trabajo, por la que se registra y publica el II Convenio colectivo de la Asociación Centro Trama. BOE nº 85, de 9 de abril de 2019.

Resolución de 18 de marzo de 2019, de la Secretaría General de Empleo, por la que se dispone la inscripción en el registro y la publicación del VI convenio autonómico de Pompas Fúnebres de Galicia. DOG nº 73, de 15 de abril de 2019.

Resolución 25C/2019, de 27 de febrero, de la Directora General de Política Económica y Empresarial y Trabajo, por la que se acuerda el registro, depósito y publicación en el Boletín Oficial de Navarra del Convenio Colectivo del Sector de Industrias Vinícolas de Navarra. BO de Navarra nº 74, de 16 de abril de 2019.

Resolución de 12 de abril de 2019, de la Consejeria de Economía, Empresas y Empleo de la Junta de Comunidades de Castilla– La Mancha en Guadalajara, por la que se registra y publica el Convenio colectivo de industrias siderometalurgicas. BOP de Guadalajara, nº . 75, de 16 de Abril de 2019

Resolución de 4 de abril de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Logirail, SAU. BOE nº 96, de 22 de abril de 2019.

Resolución 20C/2019, de 19 de febrero, de la Directora General de Política Económica y Empresarial y Trabajo, por la que se acuerda el registro, depósito y publicación en el Boletín Oficial de Navarra del Convenio Colectivo de la empresa TSF Navarra de Técnicas de Soldadura y Fijación, S.L. de Arazuri-Orcoyen. BO Navarra nº 76, de 23 de abril de 2019.

Resolución de 15 de abril de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Frit Ravich SL. BOE nº 104, de 1 de mayo de 2019.

Resolución de 26 de abril de 2019, de la Delegación Territorial de Empleo, Formación, Trabajo Autónomo, Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía en Huelva, por la que se acuerda el registro, depósito y publicación del I Convenio colectivo de la empresa AUTOAMTAX, S.C.A. BO de Huelva nº 92, de 16 de mayo de 2019.

Resolución de fecha 6 de mayo de 2019 del Jefe de la Oficina Territorial de Trabajo de Burgos, por la que se dispone la inscripción y publicación del convenio colectivo de trabajo de ámbito provincial para la actividad de oficinas y despachos. BOP Burgos nº 93, de 17 de mayo de 2019.

Resolución de 16 de mayo de 2019, de la Delegación Territorial Delegación Territorial de Empleo, Formación, Trabajo Autónomo, Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía por la que se dispone el registro y publicación del Convenio Colectivo de la empresa EUI IT Global Services A.I.E. BOP de Sevilla nº 135, de 13 de junio de 2019.

Resolución de 13 de junio de 2019, de la Dirección General de Trabajo, por la que se registra y publica el III Convenio colectivo de Puertos del Estado y Autoridades Portuarias. BOE nº 143, de 15 de junio.

Resolución de 5 de junio de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo sectorial de ámbito estatal de las administraciones de loterías. BOE nº 146, de 19 de junio de 2019.

Resolución de 13 de junio de 2019, de la Dirección General de Trabajo, por la que se registra y publica el I Convenio colectivo de Quirón Prevención, SLU. BOE nº 151, de 25 de junio de 2019.

Resolución, de 31 de octubre de 2019, de la Oficina Territorial de Trabajo de la Delegación Territorial de la Junta de Castilla y León en Ávila por la que se dispone la inscripción en el Registro de Convenios y Acuerdos Colectivos de Trabajo y la publicación en el Boletín Oficial de la Provincia de Ávila del Convenio Colectivo de "CASTA SALUD, S.L. – centro de trabajo de Arévalo".

Resolución, de 25 de julio de 2019, de la Oficina Territorial de Trabajo de Ávila por la que se dispone la inscripción en el Registro de Convenios y Acuerdos Colectivos de Trabajo y su publicación en el Boletín Oficial de la Provincia de Ávila del Convenio Colectivo Provincial de Trabajo para las Industrias de Carpintería y Ebanistería. BOP Ávila nº 148, de 1 de agosto de 2019.

Resolución de 21 de agosto de 2019, de la Dirección Provincial de la Consejería de Economía, Empresas y Empleo, por la que se dispone el registro y la publicación del Convenio colectivo de la madera de la provincia de Cuenca vigencia para los años 2.018-2.019. BOP Cuenca nº 98, de 26 de agosto de 2019.

Resolución de 13 de septiembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo marco de la Unión General de Trabajadores 2019-2020. BOE nº 237, de 2 de octubre de 2019.

Resolución de 30 de septiembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo estatal de tejas, ladrillos y piezas especiales de arcilla cocida. BOE nº 245, de 11 de octubre de 2019.

Resolución de 13 de septiembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo estatal para las industrias del curtido, correas y cueros industriales y curtición de pieles para peletería (2019-2021). BOE nº 237, de 2 de octubre de 2019.

Resolución de 7 de octubre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Nokia Spain, SA. BOE nº 251, de 18 de octubre de 2019.

Resolución de 5 de noviembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Acuerdo de modificación del II Convenio colectivo de las entidades públicas empresariales Administrador de Infraestructuras Ferroviarias y Administrador de Infraestructuras Ferroviarias de Alta Velocidad. BOE nº 270, de 9 de noviembre de 2019.

Resolución de 12 de noviembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo de Delver Logistics, SLU. BOE nº 283, de 25 de noviembre de 2019.

Resolución de 12 de noviembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Acuerdo de prórroga de la ultraactividad del Convenio colectivo de Compañía Trasmediterránea, SA, y su personal de flota. BOE nº 280, de 21 de noviembre de 2019.

Resolución de 22 de noviembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo del Grupo Santander. BOE nº 290, de 3 de diciembre de 2019.

Resolución de 26 de noviembre de 2019, de la Dirección General de Trabajo, por la que se registra y publica el Acuerdo de prórroga de ultraactividad del Convenio colectivo de CTC Externalización, SL. BOE nº 292, de 5 de diciembre de 2019.

RESUMEN

El Reglamento (UE) 2016/679 faculta a cada Estado miembro de la Unión Europea a dictar normas específicas que desarrollen las generales del Reglamento. El contenido de las normas específicas abarca cada etapa de la relación laboral, desde la contratación, pasando por el contenido de la ejecución del contrato y hasta la extinción de dicho contrato, ya que las tecnologías de la información y la comunicación se proyectan sobre todas las fases de la vida del contrato de trabajo.

La LOPD 3/2018 prevé, en su art. 91, que los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral. El legislador hace referencia en el art. 91 LOPD a que los convenios colectivos podrán establecer "garantías adicionales".

El papel de la negociación colectiva es secundario y su función tiene carácter facultativo, y no obligatorio. Por medio de la regulación convencional, se puede aumentar el contenido protector de los derechos de los trabajadores, en este caso, en relación con la protección de sus datos de carácter personal, así como garantizar de modo más eficaz los derechos digitales de aquellos.

Por otro lado, el legislador no selecciona el tipo de instrumento negocial que se puede utilizar, por lo que deja margen para que esa regulación se pueda realizar por la vía del convenio colectivo estatutario tanto sectorial, como empresarial, o mediante acuerdo marco.

El presente trabajo profundiza en el papel que la negociación colectiva vigente ha asumido al respecto. Para ello, se han analizado los convenios colectivos de los ámbitos territoriales estatal, autonómicos y provinciales, y tanto sectoriales como de empresa publicados en 2019. Resultado de dicha labor investigadora, se han extraído los contenidos que los convenios colectivos han previsto en esta materia.

Como conclusión principal del estudio de investigación realizado, se ha comprobado la escasez del tratamiento y regulación de esta materia en la negociación colectiva actual.

Por un lado, la protección de los datos de carácter personal de los trabajadores se atiende por la negociación colectiva con el fin de proteger la intimidad y dignidad de los trabajadores. En este sentido, los convenios colectivos regulan los principios básicos de esa protección en la empresa, el deber de confidencialidad, el secreto profesional y la limitación del acceso a esos datos. Asimismo se incorporan determinados comportamientos dentro del listado de faltas laborales en sus distintas categorías de leves, graves y muy graves.

Los textos convencionales suelen utilizar una cláusula general, en la que se recuerda la necesidad de proteger los derechos fundamentales en conflicto con la utilización de las tecnologías en la empresa. En este sentido, se indica que los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, así como se reconoce el derecho a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización, para, a continuación, remitirse a la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.

Aspectos tan relevantes para la protección de los datos de carácter personal de los trabajadores que no son abordados más que excepcionalmente en los convenios colectivos, son los siguientes: el consentimiento previo y expreso del trabajador respecto de la recogida de sus datos personales que la empresa custodia y sobre los que esta última adquiere la propiedad incluso una vez finalizada la relación laboral, la finalidad concreta con la que se

recopilan, administran y custodian esos datos; la conexión entre la información personal que se recaba y trata, y el legítimo objetivo para el que se solicita, o el procedimiento para que el trabajador pueda ejercitar su derecho de acceso, rectificación, cancelación y oposición.

Más interés se muestra en la regulación del deber de confidencialidad cuando se tiene acceso a esos datos personales y se utilizan, de modo que se limita su utilización al tiempo estrictamente imprescindible y solo para la finalidad concreta establecida, sancionándose el incumplimiento de ese deber.

Por otro lado, el empresario pone a disposición de los trabajadores, dispositivos informáticos y digitales propiedad de la empresa, para que desempeñen su trabajo de manera más eficaz, al mismo tiempo que otras herramientas digitales le sirven al empresario para establecer determinadas medidas de control y vigilancia del cumplimiento de las obligaciones laborales de sus trabajadores. La negociación colectiva regula las normas de utilización de esos dispositivos y herramientas electrónicos por los trabajadores y por los representantes de los trabajadores.

Resulta excepcional encontrar un convenio colectivo que proponga la negociación colectiva de un protocolo de uso de los medios informáticos. Como tales recursos son de carácter laboral, las empresas podrán ejercer sobre los mismos las medidas de dirección, gestión y control que fueran precisas, respetando el derecho a la intimidad y a la dignidad de las personas trabajadoras

En este sentido, la regulación convencional se detiene en la tipificación de las faltas laborales cometidas por los trabajadores en la utilización de esos dispositivos con fines particulares y no laborales, o vulnerando los deberes de confidencialidad y secreto profesional.

Con carácter general, la negociación colectiva no se ha ocupado más que escasamente, de las garantías adicionales para proteger los datos de carácter personal de los trabajadores y sus derechos digitales. Esa escasez se constata a pesar de que la materia abordada tiene carácter transversal, y afecta a todos los trabajadores, en mayor o menor medida, sea cual sea el tipo de actividad productiva que se desarrolle en la empresa.

La negociación colectiva tiene encomendado un papel menor en esta materia, pero es un papel normativo relevante, en la medida en que permite adaptar los contenidos legales a las más diversas situaciones que pueden producirse en las empresas. Sería deseable que la negociación colectiva se mostrase más activa en esta materia, para desarrollar contenidos protectores de los derechos fundamentales a la intimidad y la dignidad, y limitar de forma equilibrada las funciones de organización, vigilancia, control del empresario.

Resulta imprescindible la regulación de su utilización, mediante normas de actuación, que preserven los intereses del empresario, junto con los derechos de los trabajadores, garantizando un uso correcto de las tecnologías de la información y la comunicación.

Palabras clave: Negociación colectiva; protección; datos de carácter personal; intimidad; dignidad; derechos digitales; poder directivo empresarial; faltas laborales; desconexión digital.

ABSTRACT Regulation (EU) 2016/679 empowers each Member State of the European Union to issue specific rules that develop the general rules of the Regulation. The content of the specific norms covers each stage of the labour relationship, from hiring, through the content of the contract execution and until the termination of said contract, since information and communication technologies are projected on all phases of the life of the employment contract.

The LOPD 3/2018 provides, in its art. 91, that collective agreements may establish additional guarantees of rights and freedoms related to the processing of workers' personal data and the safeguarding of digital rights in the workplace. The legislator makes reference in art. 91 LOPD that collective agreements may establish "additional guarantees".

The role of collective bargaining is secondary and its function is optional, and not mandatory. Through conventional regulation, the protective content of workers' rights can be increased, in this case, in relation to the protection of their personal data, as well as more effectively guarantee the digital rights of those.

On the other hand, the legislator does not select the type of negotiation instrument that can be used, so it leaves room for that regulation to be carried out through the statutory collective agreement, both sectoral and business, or through a framework agreement.

This work deepens the role that collective bargaining in force has assumed in this regard. To this end, collective agreements have been analyzed in the state, regional and provincial territorial areas, and in both sector and company areas published in 2019. As a result of this research work, the contents that the collective agreements have foreseen in this matter have been extracted.

As a main conclusion of the research study carried out, the lack of treatment and regulation of this matter in the current collective bargaining has been verified.

On the one hand, the protection of personal data of workers is served by collective bargaining in order to protect the privacy and dignity of workers. In this sense, collective agreements regulate the basic principles of such protection in the company, the duty of confidentiality, professional secrecy and the limitation of access to such data. Likewise, certain behaviours are included in the list of work offenses in their different categories of mild, serious and very serious.

Conventional texts often use a general clause, which recalls the need to protect fundamental rights in conflict with the use of technologies in the company. In this regard, it is indicated that workers have the right to privacy in the use of digital devices made available to them by the employer, as well as the right to digital disconnection and privacy in the face of the use of video surveillance devices and geolocation, and then refer to current legislation on the protection of personal data and guarantee of digital rights.

Aspects so relevant for the protection of personal data of workers that are not addressed more than exceptionally in collective agreements, are the following: the prior and express consent of the worker regarding the collection of their personal data that the company keeps and on which the latter acquires the property even after the end of the employment relationship, the specific purpose with which these data are collected, managed and guarded; the connection between the personal information that is collected and processed, and the legitimate objective for which it is requested, or the procedure so that the worker can exercise his right of access, rectification, cancellation and opposition.

More interest is shown in the regulation of the duty of confidentiality when such personal data is accessed and used, so that its use is limited to the strictly essential time and only for the specific purpose established, sanctioning the breach of that duty.

On the other hand, the employer makes available to the workers, computer and digital devices owned by the company, to perform their work more efficiently, while other digital tools serve the employer to establish certain control measures and monitoring compliance with the labour obligations of its workers. Collective bargaining regulates the rules of use of these electronic devices and tools by workers and by workers' representatives.

It is exceptional to find a collective agreement that proposes the collective negotiation of a protocol for the use of computer media. As such resources are of a labour nature, companies may exercise the necessary management, management and control measures, respecting the right to privacy and dignity of working people.

In this sense, the conventional regulation stops in the typification of the labour faults committed by the workers in the use of these devices with particular and non-labour purposes, or violating the duties of confidentiality and professional secrecy.

In general, collective bargaining has dealt only with additional guarantees to protect the personal data of workers and their digital rights. This shortage is confirmed despite the fact that the subject matter is transversal, and affects all workers, to a greater or lesser extent, regardless of the type of productive activity carried out in the company.

Collective bargaining is entrusted with a minor role in this matter, but it is a relevant normative role, insofar as it allows the legal content to be adapted to the most diverse situations that may happen in companies. It would be desirable for collective bargaining to be more active in this area, to develop protective contents of fundamental rights to privacy and dignity, and to limit in a balanced way the functions of organization, surveillance, control of the employer.

It is essential to regulate its use, through rules of action, that preserve the interests of the employer, together with the rights of the workers, guaranteeing a correct use of the information and communication technologies.

Keywords: Collective bargaining; protection; personal data; right to privacy and right to dignity; digital rights; corporate management; labour breaches; digital disconnection.

SUMARIO

ISSN 2660-4647
00148
9 772660 464706