LA PROTECCIÓN DE DATOS PERSONALES EN LOS PROCESOS DE SELECCIÓN DE LOS TRABAJADORES; EN PARTICULAR, AQUELLOS DATOS ESPECIALMENTE SENSIBLES*

Ángel Luis de Val Tena**
Universidad de Zaragoza

SUMARIO: –1. Premisa: el marco jurídico (texto y contexto general) aplicable a los trabajadores, también a los demandantes de empleo. –2. La licitud del tratamiento de los datos personales en los procesos de selección. 2.1. Cuando el tratamiento es necesario para la aplicación de «medidas precontractuales». 2.2. Cuando el interesado da su consentimiento para el tratamiento de sus datos personales con uno o varios fines específicos. –3. Propuesta de clasificación de los datos personales y consecuencias sobre su tratamiento. 3.1. Una clasificación: datos personales y «categorías especiales de datos personales». 3.1.1. Definición de datos personales. 3.1.2. Datos particularmente sensibles: las «categorías especiales de datos personales». A) Datos sobre la afiliación sindical. B) Datos biométricos. C) Datos relativos a la salud. 3.2. Limitaciones al tratamiento de las «categorías especiales de datos personales» con el fin de seleccionar trabajadores. 3.2.1. Prohibición general de tratamiento. 3.2.2. Excepciones: el tratamiento permitido. A) El consentimiento explícito del interesado. B) Los datos personales públicamente manifestados por el interesado. C) Fines médicos y sanitarios. –4. Conclusiones.

RESUMEN

En los procesos de selección de personal para ocupar un puesto de trabajo, también resulta de aplicación la normativa –europea y nacional– sobre protección de datos personales.

Se considera "datos personales" toda información sobre una persona física identificada o identificable 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.

ABSTRACT

In the staff selection process, regulations -European and national- on protection of personal data also apply.

Is "personal data" any information relating to an identified or identifiable natural person and is "processing" 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.

Palabras clave: Procesos de selección de personal, datos personales, categorías especiales de datos, afiliación sindical, datos biométricos, datos relativos a la salud, tratamiento de categorías especiales de datos.

Key words: Staff selection process, personal data, special categories of personal data, trade union membership, biometric data, health data, processing of special categories of personal data.

* Recibido el 29 de marzo de 2020. Aceptado el 17 de abril de 2020.
** Catedrático de Derecho del Trabajo y de la Seguridad Social. ORCID: http://orcid.org/0000-0003-3276-5983

1. PREMISA: EL MARCO JURÍDICO (TEXTO Y CONTEXTO GENERAL) APLICABLE A LOS TRABAJADORES, TAMBIÉN A LOS DEMANDANTES DE EMPLEO

El trabajador, como ciudadano, es titular del derecho fundamental a la protección frente al tratamiento de sus datos personales *ex* artículo 18.4 Constitución Española[1] (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"[2]. 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"[3].

La privacidad, más que la intimidad[4], 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[5], 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"[6], 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.

Igualmente, el ordenamiento jurídico de la Unión Europea reconoce expresamente aquel 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 le 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 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 que puede asumir 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).

No se pone en duda la aplicación de las normas sobre protección de datos personales en las relaciones de trabajo, que repercute tanto en su dimensión individual como 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 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].

[1] Artículo 18.4 CE: "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".
[2] STC 94/1998, de 4 de mayo.
[3] STC 292/2000, de 30 de noviembre.
[4] 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.
[5] STC 254/1993, de 20 de julio.
[6] LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales,* Centro de Estudios Constitucionales, Madrid, 1993, p. 33.
[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,* nº 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).
[10] Lo ha destacado, acertadamente, MERCADER UGUINA, J. R., "El mercado de trabajo y el empleo en un mundo digital", *Información Laboral,* n.º 11, 2018, 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.

Tampoco cabe cuestionar la vigencia de ese conjunto de reglas jurídicas sobre el tratamiento de datos personales cuando se facilitan o recogen los mismos en un proceso de selección iniciado ya sea directamente por un empresario, ya sea por un intermediario en el proceso de colocación, habilitado *ex lege* para desarrollar esa función. El empleador y, de igual manera, los servicios públicos de empleo, agencias de colocación u otras entidades colaboradoras de aquellos, al participar en la intermediación laboral, "someterán su actuación en el tratamiento de datos de los trabajadores a la normativa aplicable en materia de protección de datos" [art. 34.1, párrafo segundo, RD-Leg. 3/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley de Empleo (en adelante, LE)]. En particular, se subraya la obligación de las agencias de colocación de "respetar la intimidad y dignidad de los trabajadores y cumplir la normativa aplicable en materia de protección de datos" [art. 33.4.b) LE], y ello en un contexto más amplio que les exige garantizar, en su ámbito de actuación, el principio de igualdad en el acceso al empleo, no pudiendo establecer discriminación alguna, directa o indirecta, basada en motivos de origen, incluido el racial o étnico, sexo, edad, estado civil, religión o convicciones, opinión política, orientación sexual, afiliación sindical, condición social, lengua dentro del Estado y discapacidad [art. 33.4.f) LE].

Sin ser necesaria tal remisión expresa para que resulten aplicables las normas sobre protección de datos personales, aquella aporta mayor seguridad jurídica, más aún porque el demandante de empleo, sin duda, se encuentra en una posición débil, más acentuada que la de un trabajador ya contratado[12], y de mayor vulnerabilidad, por lo tanto. Probablemente, el empleador requerirá el conocimiento y tratamiento de datos profesionales, cuando no otros estrictamente personales, de cada uno de los candidatos a ocupar el puesto de trabajo ofertado, y la negativa a facilitarlos supondrá *de facto* un inconveniente[13] para participar, con reales posibilidades de éxito, en el proceso de selección.

Las nuevas tecnologías[14], incorporadas también al desarrollo de los procesos de selección de personal, multiplican las posibilidades de obtener datos personales, además de profesionales, de los demandantes de empleo y perfeccionan su tratamiento, amplificando las interrelaciones de unos datos con otros, de manera que provocan la "hiperdatificación"[15]. Pero, y es cierto, no cabe desconocer que al mismo tiempo incrementan el riesgo de lesión de los derechos y libertades del interesado, de ahí la imperativa necesidad de respetar las normas que garantizan la protección de esos derechos y libertades a propósito del tratamiento de los datos personales.

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 [art. 4.6) RGPD]– 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, intere-

[12] Por todos, GOÑI SEIN, J. L., *El respeto a la esfera privada del trabajador,* Civitas, Madrid, 1988, p. 39.
[13] Como ha descrito 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, pp. 9 y 10, quien busca un empleo "es plenamente consciente de que sus expectativas de lograr ser contratado se desvanecerían de manera inmediata en cuanto ponga algún tipo de resistencia o reticencia a transmitir la información completa que se le pueda solicitar al efecto de parte de su potencial empleador.
[14] Así lo advierte, con carácter general, 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,* n.º extraordinario 1, 2019, p. 11.
[15] Ha destacado la "hiperdatificación" del lugar de trabajo, MERCADER UGUINA, J. R., "El mercado de trabajo y el empleo en un mundo digital", cit., p. 4 (BIB 2018/13994).

ses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física [art. 4.4) RGPD]–, se ha de aplicar la normativa sobre protección de datos personales también a la empresa y a los agentes, públicos o privados, de intermediación en el proceso de colocación, en relación con los datos conocidos de los candidatos, para que su tratamiento alcance las mismas garantías que en otros escenarios jurídicos, de igual forma que se reconocen a otros interesados.

2. LA LICITUD DEL TRATAMIENTO DE LOS DATOS PERSONALES EN LOS PROCESOS DE SELECCIÓN

Ensamblar el interés legítimo del empresario para conocer las señas de identidad, personales y profesionales, de los participantes en un proceso de selección de personal con los derechos fundamentales –por supuesto, también los inespecíficos– de los interesados en ocupar un puesto de trabajo no deviene en una tarea fácil, puesto que, más que buscar el equilibro[16] entre los derechos de uno y otros en juego, se deberá ponderar aquellos derechos según su valor constitucional.

El Reglamento europeo y la legislación nacional sobre protección de datos personales, en perfecta coordinación normativa, aportan seguridad jurídica y salvaguardan la privacidad de los datos de los interesados. Se ha denunciado, sin embargo, el "precario"[17] marco normativo especializado que resultaría aplicable a la actuación del empleador en el desarrollo del proceso de colocación, no sin reconocer que el conjunto normativo, jurisprudencial y administrativo de carácter general resulta de plena aplicación a las fases de selección previas a la contratación laboral. Sea o no precario, en el doble sentido –habría que entender– de transitorio e insuficiente o escaso, lo cierto es que el legislador nacional no ha implementado previsión alguna sobre la protección de datos en las fases de selección y colocación de los demandantes de empleo, pese a que aquel reglamento habilita a las disposiciones legislativas y a los convenios colectivos para establecer normas más específicas[18] que garanticen la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores, en particular –entre otros– "a efectos de contratación de personal" (art. 88.1 RGPD).

Siendo así, es obligado analizar ese marco jurídico común para corroborar la licitud del 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 [art. 4.2) RGPD]– de los datos personales en los procesos de selección, para posteriormente abordar las singularidades que refieren a los datos especialmente sensibles.

2.1. Cuando el tratamiento es necesario para la aplicación de «medidas precontractuales»

Entre las condiciones que permiten el tratamiento licito de los datos personales, una es que resulte 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"* [art. 6.1.b) RGPD]. Sobre la base

[16] VALDÉS DAL-RE, F., "Nuevas tecnologías y derechos fundamentales de los trabajadores", *Derecho de las Relaciones Laborales,* n.º 2, 2019, p. 130.
[17] CRUZ VILLALÓN, J., *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador,* cit., p. 23.
[18] 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", cit., p. 11 (BIB 2019\1432).

de considerar a los procesos de selección y colocación como una fase precontractual, se busca, en esta causa de licitud, asidero legal para facilitar la recogida y el tratamiento de los datos personales de quienes participan como demandantes de empleo.

Ab initio, hay que reparar en el muy distinto alcance que supone diferenciar, por un lado, el tratamiento de los datos personales para facilitar o adoptar "medidas precontractuales" [art. 6.1.b) RGPD] y, por otro, admitir específicamente la posibilidad de tratar datos personales "a efectos de contratación de personal" (art. 88.1 RGPD), y ello en la misma norma. Más aun cuando en el ámbito laboral se distingue claramente el proceso de selección de los trabajadores y, en su caso, el precontrato de trabajo[19], esto es, el compromiso formal de las partes de celebrar un contrato de trabajo[20], subordinado o no al cumplimiento de determinadas condiciones. Siendo ambas fases previas a la contratación, con consecuencias jurídicas radicalmente desiguales para las partes interesadas, ni siquiera los datos que se precisan del demandante de empleo y del trabajador seleccionado, con el que se formaliza el precontrato, serán coincidentes en su totalidad.

En la doctrina, no obstante, encontramos posiciones favorables a justificar la licitud del tratamiento de los datos personales cuando sea necesario para la aplicación, a petición del interesado, de medidas precontractuales.

Así, tomando como referencia, inicialmente, la Recomendación núm. R (89) 2, de 18 de enero de 1989, del Comité de Ministros del Consejo de Europa a los Estados miembros, sobre la protección de los datos de carácter personal con fines de empleo, donde –así se dice– "la expresión con fines de empleo se refiere a las relaciones entre trabajadores y empresarios en materia de reclutamiento de los trabajadores", y, después, la Recomendación CM/Rec (2015) 5, de 1 de abril de 2015, del Comité de Ministros del Consejo de Europa, relativa al tratamiento de datos personales en el entorno laboral, que precisa el alcance de esa misma manifestación referida "a la relación entre empleadores y empleados en relación con la contratación", se considera que la redacción del artículo 6.1.b) RGPD "es clara y solventa toda discrepancia al respecto", concluyendo que "no es preciso el consentimiento para la aplicación de medidas precontractuales adoptadas a petición del interesado"[21], lo que no excluye la obligación de información[22].

Obsérvese que el tratamiento de datos personales en las relaciones precontractuales ha sido el ámbito identificado por el Reglamento europeo, siempre a petición del interesado; no la más amplia expresión que posibilitaría la recogida y el tratamiento de datos de carácter personal con fines de empleo, que sí incluiría los procesos de selección de personal.

Con mayor precisión, según se ha subrayado, la licitud de la obtención y el tratamiento de datos personales al amparo de la aplicación de "medidas precontractuales" se justifica bajo el cumplimiento de dos requisitos: que ese tratamiento sea "necesario" y que se lleve a cabo "a

[19] Aunque no contiene el vigente texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, TRLET) una regulación del precontrato de trabajo, la posibilidad de concertarlo debe ser admitida y "el silencio de dicha norma ha de ser suplido, a tenor del art. 4.3 del Código Civil, por lo previsto en las disposiciones de este, que, en su artículo 1255 y concordantes, admite una amplia libertad contractual que permite que las partes se comprometan a un ulterior otorgamiento del contrato, mediante una oferta en tal sentido aceptada" [STS de 15 de marzo de 1991 (Rec. 1106/90)].
[20] Por todas, SSTS de 23 de octubre de 1986 (RJ 1986, 5889) y de 23 de mayo de 1988 (RJ 1988, 4271).
[21] MERCADER UGUINA, J. R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales,* 3.ª ed., Francis Lefebvre, Madrid, 2019, p. 84.
[22] Cfr. Recomendación primera del documento de la Agencia Española de Protección de Datos (en adelante, AEPD) "Selección de personal a través de internet", Plan de Inspección de Oficio, Informe de conclusiones y recomendaciones, de 17 de noviembre de 2005.

petición de este (el interesado)", es decir, del demandante de empleo, lo que exige –y no puede interpretarse de otro modo– "el consentimiento del demandante de empleo"[23]. Se acierta al diferenciar, empero, el tratamiento necesario de datos con vistas a la ejecución del contrato, que no requiere consentimiento del interesado, del tratamiento necesario para adoptar medidas precontractuales, que sí exige el consentimiento del interesado, por lo que, en definitiva, no cabe interpretar que el artículo 6.1.b) RGPD "está permitiendo al empleador obtener y tratar esos datos por propia iniciativa sin el correlativo consentimiento del trabajador"[24].

Alcanzada esa conclusión, ciertamente poco añadiría, respecto de las "medidas precontractuales", ese apartado sobre el primero del mismo precepto, en tanto se considera lícito el tratamiento de datos personales cuando el interesado haya dado su consentimiento para uno o varios fines específicos [art. 6.1.a) RGPD]; en el supuesto referido, sería al objeto de participar en un proceso de selección. La exigencia de que sea necesaria la obtención y el tratamiento de los datos con ese fin no supone, en realidad, un requisito, puesto que uno de los principios generales del tratamiento es que los datos personales sean "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" [art. 5.1.c) RGPD].

En definitiva, bien sea –principalmente– por el preciso alcance de la referencia normativa a las "medidas precontractuales", que no incluye el tratamiento de datos personales "a efectos de contratación de personal", bien sea –como argumento secundario– por la condición o requisito añadido de exigir la petición del interesado para aplicar dichas medidas precontractuales, petición que se ha identificado con el consentimiento del demandante de empleo interesado, lo cierto es que resulta inadecuado justificar la licitud del tratamiento de datos personales del interesado que participa voluntariamente en un proceso de selección de personal *ex* artículo 6.1.b) RGPD, más aún, y sobre todo, porque ello puede conllevar, por una acción interpretativa de la norma, menores garantías para el demandante de empleo.

2.2. Cuando el interesado da su consentimiento para el tratamiento de sus datos personales con uno o varios fines específicos

Como regla general, el consentimiento del interesado aporta la garantía de licitud sobre el tratamiento de sus datos personales [art. 6.1.a) RGPD]; dicho con otras palabras, para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado.

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 los datos de carácter personal que le conciernen, como una declaración por escrito[25], admitiéndose por medios electrónicos, o una declaración verbal[26] (considerando 32 RGPD), aunque esta segunda 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".

[23] CRUZ VILLALÓN, J., *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador,* cit., pp. 25-28.
[24] CRUZ VILLALÓN, J., *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador,* cit., p. 27.
[25] 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).
[26] 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).

Asimismo, 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 todas 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[27] del "consentimiento informado"[28]. 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"[29]. 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). De igual manera, aquel riesgo lo advertimos en los procesos de selección del personal, donde la posición débil del demandante de empleo, como ya se ha expuesto *ut supra*, se intensifica.

Pues bien, definido el consentimiento del interesado como "toda manifestación de voluntad 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" [art. 4.11) RGPD], corresponde, por ende, al legislador establecer un conjunto de garantías que asegure la validez jurídica del consentimiento del interesado para que se reconozca como causa lícita del tratamiento de los datos personales.

Así, de la aplicación coordinada del Reglamento europeo y la legislación española, deducimos el requisito de demostrar que el interesado consintió el tratamiento de los datos (art. 7.1 RGPD), para lo que la declaración escrita y firmada es, sin duda, el mejor medio de prueba, debiendo ser clara y precisa en sus términos, singularmente identificando el fin o los fines específicos para los que se otorga dicho consentimiento [art. 6.1.a) RGPD]; cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades es preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas (art. 6.2 LOPDyGDD). Es más, si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso, y utilizando un lenguaje claro y sencillo (art. 7.2 RGPD). Además, al evaluar si el consentimiento se ha dado 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 del tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato (art. 7.4 RGPD); o dicho en otros

[27] Así lo subraya MERCADER UGUINA, J. R., *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, cit., p. 48.
[28] 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.
[29] Dictamen 02/2017, de 8 de junio, sobre el tratamiento de datos en el trabajo, adoptado por el GT29.

términos más concluyentes, 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 (art. 6.3 LOPDyGDD). En todo caso, se considera infracción muy grave no solo "el tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679", sino también "el incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento" (arts. 72.1.b) y c) LOPDyGDD].

Todas esta previsiones particulares sobre la validez del consentimiento –junto a las de general aplicación previstas en el Código Civil[30], que lo consideran nulo si prestado con error, violencia, intimidación o dolo– pretenden asegurar el tratamiento lícito de los datos personales. Obviamente, todas esa garantías proyectadas sobre el consentimiento del interesado son trasladables a la aquiescencia manifestada por el demandante de empleo que participa en un proceso de selección en cuanto a la obtención y tratamiento de sus datos personales, incluidos los profesionales.

Consideramos, en fin, que el tratamiento lícito de esos datos en el proceso de selección se debe basar en el consentimiento del interesado, manifestando –sin error, violencia, intimidación o dolo– al respecto su voluntad libre, específica, informada e inequívoca, mediante –mejor– una declaración expresa, que pueda probarse, o una nítida acción afirmativa.

De las restantes causas de licitud del tratamiento de datos personales, enumeradas en el artículo 6 RGPD, ninguna, en su tenor literal, resulta aplicable a este supuesto, y en particular, como se ha argumentado, la referida al tratamiento necesario para la aplicación de medidas precontractuales a petición del interesado [art. 6.1.b) RGPD], al tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento [art. 6.1.c) RGPD] o al tratamiento necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, puesto que sobre dichos intereses prevalecen los intereses o los derechos y libertades fundamentales del interesado que requieren la protección de datos personales [art. 6.1.f) RGPD].

Es relevante esta conclusión puesto que el tratamiento de los datos personales, según sea su clasificación, se sujeta a condiciones, límites o prohibiciones, atendiendo a la naturaleza o contenido de los datos. Por esa razón, es preciso, a continuación, desarrollar aquella clasificación y las consecuencias jurídicas que de ella se derivan para el tratamiento de los datos personales.

3. PROPUESTA DE CLASIFICACIÓN DE LOS DATOS PERSONALES Y CONSECUENCIAS SOBRE SU TRATAMIENTO

3.1. Una clasificación: datos personales y «categorías especiales de datos personales»

Sin llegar a establecer una clasificación directa de los datos personales, el Reglamento europeo diferencia el "tratamiento de categorías especiales de datos personales" (art. 9. RGPD), lo que también tiene relejo en nuestra legislación nacional[31] (art. 9 LOPDyGDD).

[30] Cfr. Artículos 1262 y ss. Código Civil.
[31] 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.

De esa distinción se colige un doble nivel de protección aplicable a los datos personales, según el bien jurídico tutelado[32]: 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"[33], 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"[34] 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).

3.1.1. 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, establece 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 definir 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"[35] (en adelante, GT29), en su Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, analiza esa definición de "datos personales"

[32] 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*, n.º 423, 2018, p. 53.
[33] Cfr. Considerando 10 RGPD.
[34] 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).
[35] 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.

y concluye que el concepto de datos personales comprende 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.

Como afirma el Tribunal de Justicia de la Unión Europea (en adelante, TJUE) el concepto de dato personal tiene "un significado muy amplio, que no se ciñe a los datos confidenciales o relacionados con la intimidad, sino que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean «sobre» la persona en cuestión"[36].

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 le 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][37]. 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"[38], en contraposición a aquellos datos anónimos, sin un nexo con una persona identificada o identificable.

Como antes se ha apuntado, 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

[36] STJUE de 20 de diciembre de 2017, Asunto C-434/16, *Peter Nowak*.
[37] 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.
[38] SAN de 8 de marzo de 2002 (Rec. núm. 948/2000).

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[39].

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[40] 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.

3.1.2. Datos particularmente sensibles: las «categorías especiales de datos personales»

Especial protección –según el certero criterio del legislador europeo– 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 mismos (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 de esos datos se separan para aplicarles reglas específicas, de protección reforzada, cuando se proceda a su tratamiento. Valorando, principalmente, 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 lo relativo a las condiciones de licitud del tratamiento, como más adelante expondremos.

Únicamente cuando establece 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 –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.

[39] 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 AEPD (https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf)

[40] 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).

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 europeo (art. 9 LOPDyGDD).

Por supuesto, algunas categorías especiales de datos, más que otras, tienen una notable incidencia sobre la persona trabajadora –también cuando es candidata en un proceso de selección– 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, los datos relativos a la salud[41].

A) 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, desde los estados previos hasta su finalización.

Al respecto, 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[42].

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.

Con mayor certeza, 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[43]. Como derecho fundamental de amplio contenido –esencial y derechos y facultades adicionales[44]– 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, 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.

[41] 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. pp. 128 y ss.

[42] SSTC 292/1993, de 18 de octubre, 94/1998, de 4 de mayo, y 145/1999, de 22 de julio.

[43] *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*, n.º 429, 2018, p. 63.

[44] Entre otras muchas, SSTC 132/2000, de 16 de mayo, 76/2001, de 26 de marzo, y 281/2005, de 7 de noviembre.

Conocerá la afiliación, obviamente, 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.

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, a 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 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)[45]. Será, en definitiva, el sindicato el que facilite a la empresa el dato de la afiliación, junto con el consentimiento explícito[46] 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[47], 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.

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.

Finalmente, se debe destacar que si el dato de la afiliación sindical constara en alguna administración o entidad[49] a las que se le aplica las normas que regulan el derecho de acceso a

[45] 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).

[46] 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.

[47] 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*, n.º 423, 2018, p. 72.

[48] El mismo criterio se aplica para los datos que revelen la ideología, religión o creencias.

[49] 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",

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).

De manera voluntaria, el trabajador podrá hacer pública su afiliación, si bien, como se dirá más adelante, su expreso consentimiento no bastará para tratar ese dato por quien o quienes lo conozcan (art. 9.1 LOPDyGDD).

Interesa afirmar, en cualquier caso, "el derecho del trabajador a no sufrir, por razón de su afiliación o actividad sindical, menoscabo alguno en su situación profesional o económica en la empresa"[50]. Se consagra, en definitiva, una "garantía de indemnidad"[51] que prohíbe cualquier diferencia de trato por razón de la afiliación sindical o la actividad sindical, que se traduce –en lo que interesa al objeto de este estudio– en la prohibición de discriminación sindical en la admisión al empleo, resultando ilícitas la circulación de "listas negras" que incluyan trabajadores a los que, por razones sindicales, se juzga conveniente no contratar. De igual manera, resultan contrarias al derecho del trabajador a la libertad sindical, en su vertiente negativa, las llamadas "cláusulas de seguridad sindical", incluidas en convenios u otros instrumentos colectivos, que pretenden obligar al empresario a contratar solo trabajadores afiliados, como "taller cerrado" (*closed shop*), taller sindicado (*unión shop*), empleo preferencial (*preferential hiring*), entre otras[52].

B) 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"[53]. 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).

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.

[50] STC 74/1998 de 31 de marzo de 1988.

[51] SALA FRANCO, T., *Derecho sindical*, 2.ª ed., tirant lo blanch, Valencia, 2017, p. 35.

[52] Vid., por todos, OJEDA AVILÉS, A., *Compendio de derecho sindical*, 3.ª ed., Tecnos, Madrid, 2014, p. 58.

[53] Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, adoptado por el GT29.

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.

También, de modo destacado, son particularmente útiles[54] 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.

Por último, un uso adicional, de interés para nuestra tema de estudio, que permite la evolución tecnológica es 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"[55].

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[56].

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[57]. Por ello, la licitud del uso de estos modelos de identificación personal se somete al juicio de proporcionalidad[58] por parte de los tribunales cuando han de valorar aquella en supuestos controvertidos.

[54] 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.
[55] BAZ RODRÍGUEZ, J., *Privacidad y protección de datos de los trabajadores en el entorno digital,* Bosch Wolters Kluwer, Barcelona, 2019, p. 244.
[56] 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.
[57] 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".
[58] 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).

C) Datos relativos a la salud

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 médico 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[59].

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"[60] o utilizar las informaciones obtenidas para fines distintos a los habilitados *ex lege*[61].

[59] Vid., con detalle y finura jurídica, RODRÍGUEZ ESCANCIANO, S., *Derechos laborales digitales: garantías e interrogantes,* cit., pp. 138-157.
[60] STS de 25 de enero de 2018 (Rec. 249/2016).
[61] 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.

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, 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 presta 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).

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[62], 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.

En definitiva, el cumplimiento del deber de vigilancia de la salud conlleva unas tasadas obligaciones –secreto profesional– para el personal sanitario encargado de 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 conforman 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[63]. Bien entendido que todos los datos sobre la salud deberán tener un tratamiento informático separado[64] 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.

Cuantas cautelas se han expuesto en relación a los datos relativos a la salud de los trabajadores que prestan servicios en la empresa, resultan trasladables, en su justa dimensión, a los datos sobre la salud de los demandantes de empleo conocidos en las fases de intermediación, selección y colocación. Así, por medio de la realización de test psicotécnicos y psicoló-

[62] 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.
[63] Sobre los sujetos intervinientes en el tratamiento, *in extenso,* vid. PEDROSA ALQUÉZAR, S. I., "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social,* n.º 138, 2018, pp. 175-178.
[64] 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.

gicos se pueden conocer datos personales especialmente sensibles[65], algunos de los cuales cabe calificarlos como datos de salud[66]. De igual manera, cuando se requiera la realización de un reconocimiento previo a la contratación laboral, a los efectos de determinar la aptitud del aspirante, los datos conocidos gozarán de idénticas garantías en cuanto a su protección, pudiendo conocerse la valoración final[67], esto es, la condición de apto o no apto, pero no los resultados concretos.

3.2. Limitaciones al tratamiento de las «categorías especiales de datos personales» con el fin de seleccionar trabajadores

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 libertades. Esta es la razón ultima que justifica un tratamiento diferenciado de las categorías especiales de datos, que –a tenor del Reglamento europeo, 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).

El artículo 9 del RGPD y también de la LOPDyGDD concretan ese régimen particular y excepcional que se aplica al tratamiento de las categorías especiales de datos personales.

3.2.1. Prohibición general de tratamiento

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, se pueden 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.

[65] Como ha subrayado CRUZ VILLALÓN, J., *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador,* cit., p. 53, debe tenerse en cuenta que los test psicológicos, por lo general, van más allá del análisis del estado de salud de la persona, por ello "han de entenderse como ilícitos, por carente de fundamento y desproporcionados, cuando por su contenido pretendan efectuar una indagación en la personalidad del demandante de empleo, no justificada de manera objetiva y solvente como requisito necesario a efectos del desarrollo de la actividad profesional para la que va a ser contratado".
[66] Vid. Informe núm. 0445/2009 de la AEPD, que recoge lo señalado en un informe previo de 20 de mayo de 2002: "resulta evidente que los datos objeto de consulta referentes a la evaluación médico psicológica para determinar la aptitud o no de …, son datos relacionados con la salud de las personas".
[67] El Informe núm. 0203/2006 de la AEPD concluye que el tratamiento de los resultados de un reconocimiento médico, más allá de la condición de apto o no apto del aspirante, puede resultar excesivo en relación con la finalidad que justifica su tratamiento.

En términos suficientemente 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).

Se podría pensar que la garantía para los interesados es absoluta, cuando realmente no es así, siendo muchas y amplias las salvedades (art. 9.2 RGPD).

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 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 empleo o de trabajo, e incluso resulta contraria a la dignidad de la persona (art. 10.1 CE).

Eliminando, 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.

3.2.2. 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 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[68]:

- 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).

[68] 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,* cit., p. 27.

La regla general que prohíbe el tratamiento de las categorías especiales de datos personales conoce, en total, diez excepciones, enumeradas en el artículo 9.2 RGPD, aunque no todas tienen la misma relevancia, de ahí que destaquemos solo algunas.

A) El consentimiento explícito del 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[69], 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"[70] de sindicalistas, si bien eso no significa que pueda tratarse ese dato 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].

B) Los datos personales públicamente manifestados por el interesado

Asimismo, 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[71], 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).

[69] Cfr. Preámbulo de la LOPDyGDD.
[70] 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).
[71] 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.

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*.

C) Fines médicos y sanitarios

Cabe destacar, por último, que 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 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[72]. Deber de secreto, en fin, que se extiende sobre los resultados y sobre todo aquello que el trabajador haya confiado[73] al personal responsable o que este haya conocido con ocasión del desarrollo de sus funciones[74].

4. CONCLUSIONES

La persona que participa en un proceso de selección con el fin de acceder a un empleo, sin duda, queda amparada por la normativa sobre protección de datos personales. Se ha destacado, con razón, la especial vulnerabilidad que caracteriza la posición que ocupa el demandante de empleo, incluso más débil que la del trabajador ya contratado por un empleador. El trabajador desempleado, cuando tiene voluntad de acceder a un puesto de trabajo, probable-

[72] Vid. PEDROSA ALQUÉZAR, S. I., "Vigilancia de la salud laboral y protección de datos", cit., p. 171.
[73] 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.
[74] 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*, n.º 133, 2012, pp. 360-373.

mente necesite una mayor defensa a la hora de proteger sus datos personales. Por el momento, no ha sido esa la percepción del legislador, europeo o nacional, lo que obliga a enfocar esa tutela conforme al marco común regulador de la protección de datos personales.

Son aplicables, por consiguiente, los principios generales relativos al tratamiento de datos personales, así como sus reglas de licitud, si bien reparando en la singularidad de los procesos de selección de personal. En efecto, también en los procesos de selección de personal los datos personales serán tratados por el responsable –el propio empleador o el órgano de intermediación– de manera lícita, leal y transparente en relación con el interesado, que es el demandante de empleo; serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados; serán exactos y, si fuera necesario, actualizados; 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; y, por último, 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 RGPD).

También, por supuesto, se requiere una causa que aporte garantía de licitud al tratamiento de los datos personales. Esta será el consentimiento del interesado para el tratamiento de sus datos personales para un fin determinado [art. 6.1.a) RGPD], esto es, el consentimiento libre, específico, informado e inequívoco, manifestado mediante una declaración o acción afirmativa, que exprese la voluntad de permitir el tratamiento de los datos personales con el objeto de participar en un proceso de selección para cubrir una oferta de empleo. Ese consentimiento será igualmente exigible, bajo las mismas condiciones, cuando se empleen las nuevas tecnologías de la información y la comunicación, como los –así llamados– portales de empleo. Es más, como ha establecido recientemente el TJUE, se requiere que el consentimiento sea previo y que se haya dado después de haber facilitado al interesado una información clara y completa, en particular sobre los fines del tratamiento de los datos[75].

Al responsable del tratamiento se le exige una "responsabilidad proactiva", en tanto será garante del cumplimiento de la normativa especial y deberá ser capaz de demostrarlo, singularmente capaz de demostrar que el interesado consintió el tratamiento de sus datos personales.

Sobre esta premisa, tras haber argumentado la inaplicación de otra condición de licitud por no ser los procesos de selección de trabajadores propiamente "medidas precontractuales", el consentimiento no permite tratar cualesquiera datos personales del demandante de empleo; y ello porque el consentimiento del interesado, como causa de licitud del tratamiento, se sujeta a condiciones y a limitaciones. Unas, las primeras, se refieren a la propia manifestación de voluntad. Otras, las segundas, mencionan términos o confines en cuanto a los posibles efectos jurídicos del mismo consentimiento.

En principio, el tratamiento de "categorías especiales de datos personales" queda prohibido. Por ser datos particular o especialmente sensibles, esa interdicción afecta a los 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 (art. 9.1 RGPD). Pese a quedar –literal– prohibidos, no es de aplicación esa regla en un amplio conjunto de supuestos (art. 9.2 RGPD); entre las excepciones, el consentimiento explícito del interesado o que el propio interesado haya hecho manifiestamente públicos esos datos personales.

[75] STJUE de 29 de julio de 2019, Asunto C-40/17, *Fashion ID GmbH & Co. KG.*

Pudiéramos pensar que, como el consentimiento del demandante de empleo es la condición de licitud del tratamiento de sus datos personales durante el desarrollo de un proceso de selección, el propio consentimiento podría amparar también el tratamiento de todas las categorías especiales de datos personales. Esa conclusión, empero, resulta contraria a lo dispuesto por el legislador español porque –*a contrario sensu*– ha establecido, a fin de evitar situaciones discriminatorias, que "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). Estas concretas categorías especiales de datos, en cambio, sí podrán ser tratadas al amparo de los restantes supuestos contemplados en el artículo 9 RGPD, por ejemplo cuando el tratamiento se refiera a datos personales que el interesado ha hecho manifiestamente públicos o con fines médicos o sanitarios.

En todo caso, resulta obligado recordar que los datos a obtener y tratar en un proceso de selección, conforme al principio de "minimización de datos", han de ser adecuados, pertinentes y limitados a los necesarios en relación con ese único fin, por lo algunos datos personales –y los profesionales, objetivos y subjetivos, lo son– sí cumplirán esa caracterización, pero otros muchos no, como la mayoría de los datos incluidos en las categorías especiales de datos, especialmente sensibles.