Categorías especiales de datos personales en el ámbito de la relación de trabajo

Special categories of personal data in the labour relationship

ÁNGEL LUIS DE VAL TENA*

1. SOBRE EL TRATAMIENTO DE DATOS PERSONALES DEL TRABAJADOR EN EL MARCO DE UNA RELACIÓN LABORAL

El conocimiento de determinados datos personales del trabajador otorga a su empleador un poder más extenso cuando ha de tomar decisiones organizativas y de gestión de personal, además de orientar o ejecutar la actividad de control sobre la prestación de servicios, de manera más precisa e intensa[1].

Ciertamente, el "dato personal" –toda información sobre la persona trabajadora, como, por ejemplo, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social– y su "tratamiento" –cualquier operación o conjunto de operaciones, realizadas por el empresario o por un encargado suyo, sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción– cuando sea necesario para la génesis y posterior ejecución del contrato de trabajo, conjuntamente, aportan información relevante y de considerable valor para adoptar determinaciones, ordinarias o extraordinarias, sobre los recursos humanos, en aras a su optimización desde la perspectiva de los resultados empresariales.

Bajo esta premisa, las nuevas tecnologías[2], incorporadas también a la administración de la empresa, multiplican las posibilidades de obtener datos personales, además de profesionales, del trabajador y perfeccionan su tratamiento, amplificando las interrelaciones de unos datos con otros, de manera que provocan la "hiperdatificación"[3], si bien incrementan, al mismo tiempo, el riesgo de lesión de los derechos y libertades del interesado, de ahí la imperativa necesidad de adoptar nor-

* Catedrático de Derecho del Trabajo y de la Seguridad Social. Universidad de Zaragoza. ORCID: http://orcid.org/0000-0003-3276-5983

[1] *Vid.* VALDÉS DAL-RE, F.: "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", *Revista de Derecho Social*, núm. 79, 2017, p. 19.

[2] Así lo advierte MOLINA NAVARRETE, C.: "La «gran transformación» digital y bienestar en el trabajo: riesgos emergentes, nuevos principios de acción, nuevas medidas preventivas", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. extraordinario 1, 2019, p. 11.

[3] Ha destacado la "hiperdatificación" del lugar de trabajo, MERCADER UGUINA, J. R.: "El mercado de trabajo y el empleo en un mundo digital", *Información Laboral*, núm. 11, 2018, p. 4 (BIB 2018/13994).

mas que garanticen la protección de esos derechos y libertades a propósito del tratamiento de datos personales de los trabajadores en el ámbito laboral.

No se olvide que algunas notas identificativas de la relación jurídico-laboral inciden de manera particular en el tratamiento de los datos personales del trabajador, actualizando continuadamente aquellos riesgos, y así se ha subrayado[4], entre otras: su carácter personalísimo, que hace más complejo el tipo de datos a considerar; su perdurabilidad, que supone la necesaria conservación de los datos; y –habría que añadir– sus diversas proyecciones, individual y colectiva, que implican un aprovechamiento de los datos para evaluar diferentes realidades.

Como no han dejado de crecer las posibilidades de acumular datos de los trabajadores en "ficheros" –conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica– y de combinar esos datos para elaborar "perfiles" –forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física–, se ha de aplicar la normativa sobre protección de datos personales también a la empresa en relación con los datos conocidos de sus trabajadores para que su tratamiento alcance las mismas garantías que en otros escenarios jurídicos, de igual forma que se reconocen a otros interesados.

El trabajador, como ciudadano, también es titular del derecho fundamental a la protección frente al tratamiento de los datos personales –"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" [art. 18.4 Constitución Española (en adelante, CE)]–, que le garantiza "el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados" y se configura como "una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención"[5]. Aunque imbricado con otros derechos constitucionales, como el derecho a la intimidad (art. 18.1 CE), se considera un derecho autónomo e independiente, que consiste en "un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso"[6].

También la normativa comunitaria reconoce expresamente este derecho. Así, la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, CDFUE) recoge que "toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan" (art. 8.1 CDFUE) y el Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) dispone que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" (art. 16.1 TFUE), trasladando al Parlamento Europeo y al Consejo la obligación de establecer, con arreglo al procedimiento legislativo ordinario, "las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades

[4] *Vid.* DEL REY GUANTER, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la «intimidad informática» de trabajador)", *Relaciones Laborales*, T. II, 1993, pp. 135-160.

[5] STC 94/1998, de 4 de mayo.

[6] STC 292/2000, de 30 de noviembre.

comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos" (art. 16.2 TFUE).

Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión Europea, el Reglamento 2016/679/UE, de 27 de abril, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, RGPD), aplicable a partir del 25 de mayo de 2018, refuerza la seguridad jurídica y la transparencia en la provisión y gestión de los datos personales, con carácter general. Singularmente en el ámbito de las relaciones de trabajo[7], habilita a las disposiciones legislativas y a los convenios colectivos para establecer normas más específicas[8] que garanticen la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores, en particular "a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral" (art. 88.1 RGPD).

A nivel nacional, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, LOPDyGDD) adapta el ordenamiento español a la referida norma europea y completa sus disposiciones, aunque, desde la perspectiva exclusivamente laboral, no introduce novedades en cuanto al tratamiento de los datos de las personas trabajadoras y sí, en cambio, regula un conjunto de "derechos digitales"[9] de los trabajadores con la finalidad de garantizar su intimidad, fundamentalmente; y ello sin perjuicio del reconocimiento expreso del rol a desempeñar por la negociación colectiva para establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral (art. 91 LOPDyGDD). En esa línea, incorpora un nuevo artículo 20 bis al vigente texto refundido de la Ley del Estatuto de los Trabajadores (en adelante, TRLET), intitulado "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión", confirmando que "los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

No se pone en duda la aplicación de las normas sobre protección de datos personales en las relaciones de trabajo, que repercute en sus dimensiones individual y colectiva, en materia de prevención de riesgos laborales e, igualmente, en su vinculación con el sistema público de Seguridad Social. Como "interesado" o sujeto titular de los datos, el trabajador se beneficiará del conjunto de garantías articulado por la normativa sobre protección de

[7] Sobre las implicaciones que para las relaciones laborales, individuales y colectivas, tiene la aprobación del RGPD, *vid.* Miñarro Yanini, M.: "Implicaciones laborales del Reglamento comunitario de protección de datos: principales puntos críticos", en García Mahamut, R. y Tomás Mallén, B. (Edits.): *El Reglamento General de Protección de Datos*, Tirant lo blanch, Valencia, 2019, pp. 461 y ss.

[8] No necesariamente más protectora, como subrayan García Murcia, J. y Rodríguez Cardo, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo*, núm. 216, 2019, p. 11 (BIB 2019\1432).

[9] Son los siguientes: "Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral" (art. 87 LOPDyGDD), "Derecho a la desconexión digital en el ámbito laboral" (art. 88 LOPDyGDD), "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo" (art. 89 LOPDyGDD) y "Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral" (art. 90 LOPDyGDD).

datos. Ahora bien, según las recomendaciones de los órganos consultivos nacionales e internacionales en materia de protección de datos, la legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo y las prácticas laborales y tampoco estos, a su vez, pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos[10]. Ensamblar y armonizar ambos sectores del ordenamiento jurídico puede contribuir a aplicar soluciones que protejan convenientemente los derechos e intereses de los trabajadores, máxime cuando el terreno laboral se revela propicio para que surjan vulneraciones de los derechos, fundamentales o no, y actuaciones discriminatorias originadas por el conocimiento y tratamiento de datos personales[11].

Enlazar, asimismo, el interés legítimo del empresario en sacar provecho de las posibilidades que le ofrecen las nuevas tecnologías para conocer las señas de identidad, personales y profesionales, de sus trabajadores a la hora de desarrollar la actividad empresarial, en general, y la gestión del personal, en particular, con los derechos fundamentales –por supuesto, los inespecíficos también– de los asalariados en el seno de una relación laboral, no deviene en una tarea fácil, puesto que, más que buscar el equilibro[12] entre los derechos de uno y otro en juego, se deberá ponderar aquellos derechos según su valor constitucional.

El Reglamento comunitario y la legislación nacional sobre protección de datos personales aportan seguridad y salvaguardan la privacidad de los datos de trabajadores interesados. El nuevo ordenamiento sobre protección de datos personales distingue, sobre todo el conjunto, aquellas "categorías especiales de datos" a las que dedica un haz de cautelas sobre su tratamiento, por cuanto el riesgo no está implícito en el dato concreto, sino en su tratamiento[13] por el empleador responsable, resultando así datos especialmente sensibles y protegidos.

2. DATOS PERSONALES Y «CATEGORÍAS ESPECIALES» DE DATOS PERSONALES

La privacidad, más que la intimidad[14], como "escudo de protección" frente al tratamiento de los datos personales, deriva del derecho fundamental reconocido *ex* artículo 18.4 CE, formulado como garantía constitucional[15], que compele al legislador a limitar el uso de la informática –y de las nuevas tecnologías– para garantizar el honor y la intimidad personal de los ciudadanos y el pleno ejercicio de sus derechos. Dicho con otras palabras, se obliga a que la ley garantice la privacidad informática de la persona, que se traduce en el reconocimiento del "derecho a la autodeterminación informativa"[16], tendente a proteger jurídicamente la identidad personal; autodeterminación informativa que consiste en el control que ejerce el interesado sobre su información personal para preservar, en última instancia, la propia identidad, dignidad y libertad. Y es que solo cuando el sujeto titular puede determinar el alcance de la utilización de sus datos quedarán garantizados sus derechos.

---

[10] Lo ha destacado, acertadamente, MERCADER UGUINA, J. R.: "El mercado de trabajo y el empleo en un mundo digital", *cit.* p. 4.

[11] Al respecto, GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y de archivo de datos", en ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA R. (Coords.): *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Bomarzo, Albacete, 2004, p. 55.

[12] VALDÉS DAL-RE, F.: "Nuevas tecnologías y derechos fundamentales de los trabajadores", *Derecho de las Relaciones Laborales*, núm. 2, 2019, p. 130.

[13] *Vid.* TRONCOSO REIGADA, A.: "La protección de datos personales en el ámbito laboral", en VV.AA.: *La protección de datos personales en busca del equilibrio*, tirant lo blanch, Valencia, 2010, pp. 1563-1612.

[14] Con precisión, en relación con los datos genéticos, *vid.* ÁLVAREZ GONZÁLEZ, S.: "Derecho a la «privacidad» e información genética", en ÁLVAREZ GONZÁLEZ, S. y GARRIGA DOMÍNGUEZ, A. (Dirs.): *Un nuevo reto para los derechos fundamentales: los datos genéticos*, Dykinson, Madrid, 2017, pp. 22-26.

[15] STC 254/1993, de 20 de julio.

[16] LUCAS MURILLO DE LA CUEVA, P.: *Informática y protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1993, p. 33.

Sin llegar a establecer una clasificación directa de los datos personales, el Reglamento comunitario diferencia el "tratamiento de categorías especiales de datos personales" (art. 9. RGPD), lo que también tiene reflejo en nuestra legislación nacional[17] (art. 9 LOPDyGDD). De esa distinción se colige un doble nivel de protección aplicable a los datos personales según el bien jurídico tutelado[18]: por un lado, aquellos datos que se incluyen en las categorías especiales, estrechamente vinculados a la dignidad y personalidad humana, que reciben una protección reforzada, al quedar prohibido su tratamiento, salvo en los supuestos legalmente tasados; por otro, el resto de datos personales no incluidos en las categorías especiales. Quedan al margen los datos de naturaleza penal, es decir, los datos personales relativos a condenas e infracciones penales, que también son objeto de un particular tratamiento (art. 10 RGPD).

Entre los datos especiales por su tratamiento, también llamados "datos sensibles"[19], se identifican aquellos "datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical", así como también "datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física" (art. 9.1 RGPD).

No es nueva esta identificación separada de diversas categorías de datos, igualmente calificadas como "particulares"[20] o "especiales". La derogada Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos, enumeraba las siguientes categorías especiales de datos en cuanto a su tratamiento: "datos personales que revelen origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como (…) los datos relativos a la salud o a la sexualidad" (art. 8.1 Directiva 95/46/CE); obsérvese que no se recogían, de manera expresa e individualizada, los datos genéticos y los datos biométricos. En la misma línea, se calificaron como "datos especialmente protegidos", en la terminología de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, "los datos de carácter personal que revelen ideología, afiliación sindical, religión y creencias" y también "los datos de carácter personal que hagan referencia al origen racial (o étnico), a la salud y a la vida sexual" (art. 7.2 y 3 LO 15/1999).

2.1. Definición de datos personales

Con la técnica habitual del legislador de la Unión Europea, el RGPD incluye un precepto con definiciones, "a efectos del presente Reglamento", para facilitar la aplicación e interpretación de la norma.

En primer lugar, qué se entiende por dato personal: "toda información sobre una persona física identificada o identificable («el interesado»)" [art. 4.1) RGPD; tenor literal idéntico al derogado art. 2.a) Directiva 95/46/CE]. Se adopta un concepto amplio, quizá porque de-

[17] Desde la perspectiva del tratamiento, cabría diferenciar los datos sujetos a "tratamientos concretos", datos que tienen características singulares o que se manejan en contextos particulares. Al respecto, García Murcia, J. y Rodríguez Cardo, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 19.

[18] Rodríguez Escanciano, S.: "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. 423, 2018, p. 53.

[19] Cfr. Considerando 10 RGPD.

[20] El Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, incluye como "categorías particulares de datos" los de carácter personal que revelen "el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones", así como los datos de carácter personal relativos a "la salud o a la vida sexual" (art. 6).

finir el concepto de datos personales equivale a determinar lo que entra o queda fuera del ámbito de aplicación de las normas sobre protección de datos.

El –así llamado– "Grupo del artículo 29"[21] (en adelante, GT29), en su Dictamen 4/2007, de 20 de junio, sobre el concepto de datos personales, analiza esa definición de "datos personales" y concluye que el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona física: desde el punto de vista de su naturaleza, abarca información "objetiva" como, por ejemplo, la presencia de una determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones "subjetivas", como, por ejemplo, una valoración del trabajador; desde la perspectiva de su contenido, se incluyen todos aquellos datos que proporcionan información cualquiera, ya sea relativa a la vida privada y familiar del individuo *stricto sensu*, ya sea información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social; y en cuanto al formato o el soporte en que se dispone la información, se admite cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo.

Se puede considerar que la información versa "sobre" una persona física cuando se refiere a ella; así, los datos incluidos en el fichero de una persona guardado en el departamento de personal de su empresa están claramente relacionados con su situación como empleado de dicha empresa. Bien sea por su contenido, finalidad o resultado, el dato personal podrá estar referido a una persona o a varias.

Una persona física estará identificada cuando, dentro de un colectivo de personas, se la distingue de todos los demás miembros del grupo. En cambio, se considerará persona identificable "toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" [art. 4.1) RGPD][22]. Ciertamente, para que exista un dato de carácter personal –en contraposición con un dato disociado– no es imprescindible la plena coincidencia entre el dato y una persona concreta, sino que "es suficiente con que tal identificación pueda efectuarse sin esfuerzos desproporcionados"; y así para determinar si una persona es identificable "hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona"[23], en contraposición a aquellos datos anónimos, sin un nexo con una persona identificada o identificable.

Las normas de protección de datos personales se aplican a las personas físicas, según se deduce de la definición de datos personales que hace referencia solamente a ellas. La información relativa a las personas jurídicas no está, en principio, cubierta por aquellas normas, si bien nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la norma comunitaria a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello[24]. Distinto es el supuesto de aquella información referente a personas jurídicas que también pueda ser considerada, en función de sus características, como información "sobre" perso-

[21] Este Grupo se creó en virtud de lo dispuesto en el artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la Unión Europea, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad; sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

[22] La STJUE de 6 de noviembre de 2003, Asunto C-101/01, *Bodil Lindqvist*, señaló que el concepto de dato personal incluye, sin duda, la identificación de una persona por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones.

[23] SAN de 8 de marzo de 2002 (Rec. núm. 948/2000).

[24] STJUE de 6 de noviembre de 2003, Asunto C-101/01, *Bodil Lindqvist*.

nas físicas. Lo que sucede, por ejemplo, cuando la denominación de la persona jurídica tiene su origen en el nombre de una persona física.

Como se ha apuntado *ut supra*, no son personales, a estos efectos, los "datos anónimos", es decir, cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. En relación con ese tipo de datos, se acuñan los "datos anonimizados", que son aquellos datos anónimos que con anterioridad se referían a una persona identificable, pero cuya identificación ya no es posible. La anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible la identificación de una persona física, de manera que cualquier técnica de anonimización eficaz ha de impedir a todos singularizar a una persona en un conjunto de datos, vincular dos registros en un conjunto de datos –o dos registros pertenecientes a conjuntos diferentes– e inferir cualquier tipo de información a partir de dicho conjunto[25].

A diferencia de esas técnicas, la "seudonimización" conlleva el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable [art. 4.5 RGPD]. Si con la utilización de un seudónimo existe la posibilidad de seguir un rastro hasta llegar a la identidad de la persona, aunque solo en condiciones previamente definidas, consecuentemente los datos personales seudonimizados se deben considerar información sobre una persona física identificable, sin que se excluya para ellos ninguna medida relativa a la protección de datos por más que puedan reducirse los riesgos para los interesados afectados (considerando 26 RGPD); de modo que la aplicación de la seudonimización a los datos personales puede ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos (considerando 28 RGPD). Los datos cifrados son un paradigma[26] de técnica de seudonimización: la información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir, para establecer la correspondencia entre el código y los identificadores habituales de la persona –nombre, fecha de nacimiento, dirección, etc.– se guardan por separado.

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

Especial protección –según el certero criterio del legislador comunitario– merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento puede entrañar importantes riesgos para los derechos y las libertades fundamentales (considerando 51 RGPD). Por esta razón se identifica un conjunto de informaciones para su tratamiento diferenciado como "categorías especiales de datos personales". Lógicamente, pertenecen al género común de datos personales, esto es, constituyen información sobre una persona física identificada o identificable, si bien una parte

[25] Cfr. Dictamen 5/2014, de 10 de abril de 2014, sobre técnicas de anonimización, adoptado por el GT29. Igualmente, el documento "Orientaciones y garantías en los procesos de anonimización de datos personales", redactado por la Agencia Española de Protección de Datos (en adelante, AEPD) (https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf)

[26] Otros: función hash, función con clave almacenada, cifrado determinista o función hash con clave con borrado de clave, descomposición en tokens (Dictamen 5/2014, de 10 de abril de 2014, sobre técnicas de anonimización, adoptado por el GT29).

de esos datos se separan para aplicarles reglas específicas, de protección reforzada, cuando se proceda a su tratamiento. Valorando, principalmente, a su contenido, al tratar categorías especiales de datos personales se atenderá a la regulación particular, a modo de régimen excepcional, de su tratamiento, sin perjuicio de que deban aplicarse los principios generales y otras normas comunes, sobre todo en lo relativo a las condiciones de licitud del tratamiento, como más adelante expondremos.

Únicamente cuando establecen los requisitos específicos de ese tratamiento, se enumeran las categorías especiales de datos, a saber: datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud y datos relativos a la vida sexual o la orientación sexual de una persona física (art. 9.1 RGPD). Cabe anotar una mayor precisión respecto del listado recogido en la –ya derogada– Directiva 95/46/CE y también su ampliación con los datos biométricos y los genéticos, diferenciando estos últimos de los propios de la salud o de carácter médico.

En la legislación española vigente, al incorporar normas más definidas –*ex* artículo 6.2 RGPD– para garantizar la protección de los derechos y libertades en relación con el tratamiento lícito de categorías especiales de datos personales, asume la misma enumeración, sin mencionar qué datos se incluyen, ante la expresa remisión al precepto del Reglamento comunitario (art. 9 LOPDyGDD).

Por supuesto, algunas categorías especiales de datos, más que otras, tienen una notable incidencia sobre la persona trabajadora y su tratamiento en las relaciones laborales, significativamente –pero no solo– los datos que revelen la afiliación sindical, los datos biométricos dirigidos a identificar de manera unívoca a una persona y también datos relativos a la salud[27]. Ello no es óbice para que precisemos todos y cada uno de esos datos, máxime cuando la normativa en vigor no se ha ocupado de aportar una mínima descripción, en algún caso.

2.2.1. Datos sobre el origen racial o étnico

La información sobre el origen racial o étnico de un individuo revela un rasgo de la persona física. La prohibición general de tratamiento de datos personales de esta naturaleza trata de evitar situaciones discriminatorias, incluso lesivas de la dignidad de la persona, en particular en el acceso al empleo o durante la ejecución de la prestación de trabajo, señaladamente. El origen de una persona hay que ligarlo al lugar de nacimiento o a la pertenencia, en función del nacimiento, a un grupo social, donde tuvo principio su familia, que puede quedar reconocido por la raza o etnia de referencia.

La acepción más próxima del término raza es la que determina "cada uno de los grupos en que se subdividen algunas especies biológicas y cuyos caracteres diferenciales se perpetúan por herencia"[28]. Referido a las personas, en su concepción antropológica, designaría a cada uno de los cuatro grandes grupos étnicos en los que se suele dividir la especie humana, tomando ciertas características físicas distintivas, como el color de la piel, que se transmiten por herencia de generación en generación. La palabra etnia, por su parte, califica a una comunidad humana definida por afinidades raciales, lingüísticas, culturales, sociales o de otro tipo.

Aunque, en puridad, raza y etnia tienen significados propios, un reciente informe de la

[27] Por todos, García Murcia, J. y Rodríguez Cardo, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 10, y Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019, p. 128 y ss.

[28] Según el Diccionario de la Lengua Española, editado por la Real Academia Española de la Lengua (en adelante DRAE), otro significado es "casta o calidad del origen o linaje".

Comisión Europea[29], que analiza en profundidad el concepto del origen étnico o racial y su interpretación por parte de tribunales internacionales y nacionales, considera el origen racial o étnico como una categoría conceptual única, transversal y compuesta para aplicar el derecho antidiscriminatorio y como base jurídica útil para practicar la interpretación legal en el vacío actual de definiciones universalmente aceptadas.

En todo caso, el uso del término "origen racial" en el Reglamento europeo no supone aceptar por parte de la Unión Europea cualesquiera teorías que tratan de determinar la existencia de razas humanas separadas (considerando 51 RGPD). Simplemente, esos datos personales de carácter personal que revelen el origen racial o étnico, que existen y no pueden obviarse, se consideran merecedores de un tratamiento más garantista; y ello porque son datos que pueden usarse con fines discriminatorios.

No es preciso hacer referencia a normas internacionales o comunitarias, que también son muchas en el mismo sentido; basta recordar lo que dispone nuestra Constitución, que neutraliza toda discriminación "por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social" (art. 14 CE).

La legislación laboral, de idéntico modo, reconoce el derecho de todo trabajador "a no ser discriminados directa o indirectamente para el empleo, o una vez empleados, por razones de sexo, estado civil, edad dentro de los límites marcados por esta ley, origen racial o étnico, condición social, religión o convicciones, ideas políticas, orientación sexual, afiliación o no a un sindicato, así como por razón de lengua, dentro del Estado español" [art. 4.2.c) TRLET), e igualmente el derecho "al respeto de su intimidad y a la consideración debida a su dignidad, comprendida la protección frente al acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, y frente al acoso sexual y al acoso por razón de sexo" [art. 4.2.e) TRLET]. Como sanción legal, se entenderán nulos y sin efecto los preceptos reglamentarios, las cláusulas de los convenios colectivos, los pactos individuales y las decisiones unilaterales del empresario que den lugar en el empleo, así como en materia de retribuciones, jornada y demás condiciones de trabajo, (…) a situaciones de discriminación directa o indirecta por razón de sexo, origen, incluido el racial o étnico, estado civil, condición social, religión o convicciones, ideas políticas, orientación o condición sexual, adhesión o no a sindicatos y a sus acuerdos, vínculos de parentesco con personas pertenecientes a o relacionadas con la empresa y lengua dentro del Estado español" (art. 17.1 TRLET).

2.2.2. Datos sobre opiniones políticas o convicciones religiosas o filosóficas

En la misma dirección, sobre la base de la tutela antidiscriminatoria, la prohibición general de tratamiento se aplica a los datos que revelen opiniones, ideas o posicionamientos políticos, así como las convicciones religiosas, filosóficas y –añadimos nosotros– morales o éticas. La ideología la conforma el conjunto de ideas fundamentales que caracteriza el pensamiento de una persona[30] y la opinión política es el juicio o valoración que se forma una persona respecto de las distintas opciones políticas, no solo respecto de los partidos políticos.

Aquella prohibición alcanza a los datos que denotan posicionamientos individuales basados en convicciones religiosas o morales o fundados en preferencias personales conformadoras de un proyecto vital autónomo[31]. El

[29] Cfr. Informe de la Comisión Europea "The meaning of racial or ethnic origin in EU law: between stereotypes and identities" (http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54924)

[30] Definición tomada del DRAE.

[31] *Vid.* ALBERT, M.: "Convicciones religiosas y elecciones personales: derecho a la objeción de conciencia y autodeter-

derecho distingue "las convicciones en sentido estricto (articuladas en los términos del Convenio de Roma por la vía del artículo 9, que se ocupa de la libertad de pensamiento, conciencia y religión) de las preferencias, elecciones, opciones y proyectos vitales (articuladas, en cambio, por la vía del artículo 8, que garantiza el derecho a la vida privada personal y familiar)"[32]. Las convicciones implican un convencimiento íntimo, asentado sobre la fe o las creencias; no son simples expresiones de la autonomía personal o del libre desarrollo de la personalidad y tampoco son opiniones o ideas.

También la Constitución garantiza la libertad ideológica, religiosa y de culto de los individuos (art. 16.1 CE) y nadie puede ser obligado a declarar sobre su ideología, religión o creencias (art. 16.2 CE), preservando así la libertad de convicción de los individuos, sus creencias íntimas y el desarrollo y final del ser humano. Asimismo, reconoce y protege el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción [art 20.1. a) CE]. Y los ciudadanos tienen reconocido el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal (art. 23.1 CE).

Si a los trabajadores se les reconocen estos derechos, parece lógico que los datos personales que faciliten información sobre opiniones políticas o convicciones religiosas o filosóficas no puedan se tomados como referencia para adoptar decisiones empresariales. Su libertad de conciencia se manifiesta en opiniones políticas, creencias religiosas o planteamientos vitales que, aun conocidos por el empleador, no pueden ser tratados, como pauta general.

2.2.3. Datos sobre la afiliación sindical

De todas las categorías especiales de datos, la referida a la afiliación sindical es una información de contenido estrictamente laboral, a diferencia del otras que, siendo de carácter más general, pueden tener un incidencia transversal, también –claro está– en las relaciones de trabajo.

Es cierto que el Tribunal Constitucional concluyó que, "siendo los sindicatos formaciones con relevancia social, integrantes de la estructura pluralista de la sociedad democrática, no puede abrigarse duda alguna de que la afiliación a un sindicato es una opción ideológica protegida por el artículo 16 CE", que garantiza al ciudadano el derecho a negarse a declarar sobre ella[33]. Por consiguiente, la manifestación de la afiliación sindical es un derecho personal y exclusivo del trabajador, que deben respetar tanto el empresario como los propios sindicatos.

Por más que la afiliación a un sindicato lleve consigo cierta inclinación por determinados valores socio-políticos, esa afección solo en parte puede considerarse coincidente con lo que hemos definido como ideología en el caso de las organizaciones sindicales, por su vinculación directa a los intereses profesionales. En este contexto, el conocimiento de la afiliación sindical de la persona, cuando se produce en el ámbito laboral, solo se aproximaría a las convicciones socio-políticas de la persona.

Realmente, la protección deriva del derecho fundamental a la libertad sindical, derecho que se proyecta con relevancia incuestionable para los trabajadores en tanto les permite organizarse con fines de promoción y defensa de sus intereses profesionales[34]. Como derecho

minación individual en la jurisprudencia del Tribunal Europeo de Derechos Humanos", *Revista Persona y Derecho*, núm. 77, 2017, p. 251.

[32] ALBERT, M.: "Convicciones religiosas y elecciones personales: derecho a la objeción de conciencia y autodeterminación individual en la jurisprudencia del Tribunal Europeo de Derechos Humanos", *cit.*, p. 253.

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

[34] *In extenso*, GARCÍA MURCIA, J.: "El hecho sindical. La mayor representatividad. Asociacionismo profesional y empresarial. Balance y propuestas de reforma", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. 429, 2018, p. 63.

fundamental de amplio contenido –esencial y derechos y facultades adicionales[35]– reconocido en nuestra Constitución, que sigue la senda de las declaraciones internacionales –Convenios de la Organización Internacional del Trabajo núms. 87 y 98, señaladamente– sobre esta materia, la libertad sindical comprende "el derecho a fundar sindicatos y a afiliarse al de su elección", sin que la afiliación sea forzosa o imperativa, pues "nadie podrá ser obligado a afiliarse a un sindicato" (art. 28.1 CE). Tanto en su vertiente positiva –derecho a afiliarse– como en su vertiente negativa –derecho a no afiliarse–, el derecho a sindicarse libremente, su respeto, lleva aparejado el derecho del trabajador a no declarar su afiliación sindical al empresario, idéntica garantía propia de la libertad ideológica, religiosa y creencias (art. 16.2 CE), por cuanto quedan preservadas esas informaciones por el derecho a la intimidad o privacidad de la persona. Tampoco, en consecuencia, se podrá indagar sobre su pertenencia o vinculación a un sindicato.

Conocerá, obviamente, la afiliación el sindicato elegido por el trabajador, en el que libremente ingresa. La información del trabajador afiliado y el mismo dato de la afiliación constarán en los archivos y ficheros del sindicato, sin que esos datos personales puedan comunicarse a terceros sin el consentimiento del interesado. Para el desenvolvimiento de la relación de adhesión, serán tratados los datos por la organización sindical, pero únicamente con ese fin.

De manera voluntaria, el trabajador podrá hacer pública su afiliación y con su expreso consentimiento se podrá tratar ese dato por quien o quienes lo conozcan, siempre con una finalidad lícita[36]. Recuérdese que será nula cualquier decisión del empresario que de lugar en el empleo, así como en materia de retribuciones, jornada y demás condiciones de trabajo, a situaciones de discriminación directa o indirecta por razón –entre otras– de "adhesión o no a sindicatos y a sus acuerdos" (art. 17 TRLET).

El empleador puede conocer la afiliación del trabajador a un sindicato con motivo del descuento de la cuota sindical. El supuesto está regulado en la Ley Orgánica 11/1985, de 2 de agosto, de libertad sindical (en adelante, LOLS): "el empresario procederá al descuento de la cuota sindical sobre los salarios y a la correspondiente transferencia a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de este" (art. 11.2 LOLS). No se impone *ex lege* la obligación del trabajador de declarar su afiliación a un sindicato. Solamente si el trabajador afiliado quiere abonar su cuota al sindicato a través de la fórmula del descuento o retención en su recibo de salarios, podrá facultar al sindicato para que, su vez, pida formalmente al empresario que proceda, primero, al descuento de la cantidad correspondiente y, después, a su transferencia a la cuenta de la organización sindical. No cabe detraer la cuantía anticipadamente ni puede exigirse una manifestación negativa de voluntad al trabajador, pues ello presupone el conocimiento de su afiliación a un sindicato.

Por ser la afiliación sindical un dato sensible y, por tanto, protegido, no incumbe al sindicato solicitar el descuento directamente al empresario. Previo a ese trámite, ha de obtener

---

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

[36] Como se afirma en el Preámbulo de la LOPDyGDD, "la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores". Las –así llamadas– listas negras de sindicalistas o de trabajadores conflictivos [STS (Civil) de 12 de noviembre de 2015 (Rec. 899/2014)] se conforman con "la recogida y difusión de determinada información relativa a un determinado grupo de personas, elaborada de conformidad con determinados criterios dependiendo del tipo de lista negra en cuestión, que generalmente implica efectos adversos y perjudiciales para las personas incluidas en la misma, que pueden consistir en discriminar a un grupo de personas al excluirlas de la posibilidad del acceso a un determinado servicio o dañar su reputación" (Informe núm. 0201/2010 de la AEPD). *Vid.* CRUZ VILLALÓN, J.: *Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador*, Bomarzo, Albacete, 2019, p. 60.

la conformidad o el consentimiento, expreso, libre e indubitado, del trabajador afiliado, tanto para que el sindicato solicite a la empresa el descuento de la cuota como para que la empresa realice el descuento en la nómina. Solo así el empleador podrá demostrar que el trabajador consintió el tratamiento de ese dato personal (art. 7.1 RGPD)[37]. Será, en definitiva, el sindicato el que facilite a la empresa el dato de la afiliación, junto con el consentimiento explícito[38] del trabajador afiliado para realizar el descuento de la cuota sindical, y sobre esa base el empresario, sin necesidad de recabar una nueva manifestación de consentimiento[39], comunicará al sindicato el traspaso de la cantidad deducida al trabajador, con ningún otro dato adicional, más allá del que sea indispensable para su identificación, ya conocido evidentemente por el sindicato.

También por idéntico motivo, de producirse –conforme a las previsiones legales– el descuento de la cuota sindical, su reflejo en el recibo de salarios ha de ser una información neutra, es decir, no debe identificar que corresponde a su afiliación y, menos aún, el sindicato beneficiario. No debe aparecer el dato de la afiliación sindical, aun cuando haya dado su consentimiento el trabajador para proceder a la retención de esa cantidad a favor del sindicato, ni expresar en la nomina cualquier signo del que se pueda deducir la condición de trabajador afiliado a un sindicato.

La doctrina judicial ha considerado que el dato de afiliación sindical del trabajador reflejado en la nómina –se incluía en el recibo de nómina (entregado en sobre cerrado y personalmente al trabajador) la denominación de la organización sindical a la que se estaba transfiriendo la cuota sindical– no lesiona el derecho a la protección de datos, y ello porque "se trata de un documento estrictamente privado, dirigido exclusivamente a la persona a la que se abona el salario mensual, al que no se da ninguna publicidad y que puede ser mantenido o no en dicho ámbito reservado a voluntad del referido trabajador"[40]. Hay que subrayar que se llega a esa conclusión teniendo en cuenta, sobre todo, el ámbito privado y confidencial –una nómina– en la que se hace constar el dato de afiliación a un concreto sindicato.

Probablemente, la respuesta judicial hubiera sido otra si se hubiera considerado que la hoja de salarios es "un documento de uso común en el tráfico jurídico por su habitual presentación ante entidades públicas y privadas a múltiples efectos", ya que en tal supuesto "la inclusión en la nómina del trabajador de la mención del sindicato, al que pertenece y a cuyo favor se hace el descuento de la cuota sindical, revela la afiliación sindical del trabajador, de modo que un dato que, como hemos dicho, pertenece a la privacidad del trabajador, podría ser fácilmente conocido por terceros"[41]. Por tanto, tratándose de una situación de hecho que incide sobre derechos personales y exclusivos del trabajador, será necesario su consentimiento expreso para que se incorpore su afiliación sindical a la nómina.

---

[37] Anteriormente, se exigía, por el carácter especialmente protegido de la afiliación sindical, que el trabajador consintiera la cesión de ese dato de forma expresa y por escrito (art. 7.2 LO 15/1999).

[38] Documento de trabajo sobre las "listas negras", de 3 de octubre de 2002, elaborado por el GT29: "será necesario contar con el consentimiento expreso y por escrito del afiliado no solo para la comunicación al sindicato de los datos referidos al pago de la cuota sindical por parte del empresario, sino también para la comunicación previa efectuada por el sindicato al empresario de su condición de afiliado que solicita el descuento en la nómina de la citada cuota". *Vid.*, también, el Informe núm. 0434/2010 de la AEPD.

[39] Puede considerarse que "el trabajador lo ha prestado expresamente respecto de las cesiones de datos que hubieran de realizarse entre el empresario y el sindicato para garantizar la efectividad de la forma de pago que el propio trabajador ha elegido" (Informe núm. 0033/2010 de la AEPD). En la doctrina, *vid.* MERCADER UGUINA, J. R. y DE LA PUEBLA PINILLA, A.: "Protección de datos y relaciones colectivas", *Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros*, núm. 423, 2018, p. 72.

[40] SAN (C-A) de 14 de septiembre de 2005 (Rec. 458/2003).

[41] STSJ de Cataluña de 9 de noviembre de 2004 (Rec. 5369/2004).

Por otra parte, a cada sindicato se le faculta para el tratamiento del dato de la afiliación de los trabajadores que voluntaria y libremente han decidido pertenecer al mismo, siempre en el ámbito de sus actividades legítimas y con las debidas garantías y sin que puedan comunicar los datos personales de sus miembros a terceros sin el consentimiento de los interesados [art. 9.2.d) RGPD]. Así, los sindicatos asumen el papel de responsables del tratamiento de esos datos.

Podríamos pensar que ese consentimiento, como excepción, debe darse para que el empresario conozca sobre la constitución de una sección sindical *ex* artículo 10 LOLS y la designación de uno o más delegados sindicales. La mera constitución de la sección sindical solo denota la existencia de trabajadores afiliados a un sindicato, si bien indirectamente puede dar a conocer los concretos trabajadores afiliados y, de manera directa, saber la concreta afiliación del delegado o delegados sindicales, al ser elegidos "por y entre" los afiliados al sindicato en la empresa o en el centro de trabajo.

Igualmente, se requiere el consentimiento del trabajador afiliado para que se haga constar en la candidatura a delegado de personal o miembro del comité de empresa, si bien para ser elegible[42] no se exige estar afiliado al sindicato por el que un trabajador decida presentarse, bajos sus siglas[43]. En verdad, la afiliación es un dato no requerido puesto que en el modelo oficial de candidatura[44], tanto a delegados de personal como a miembros de comité de empresa, la columna que se refiere a "sindicato/grupo de trabajadores/coalición" solo que tiene efectos en cuanto a la atribución de resultados y posteriormente para medir la representatividad de los sindicatos. Tampoco debe incluirse la afiliación sindical de los trabajadores, si le consta al empresario, en el censo laboral[45] que este último debe facilitar a la mesa electoral, al no exigirse esa información (art. 6.3 RD 1844/1994).

Finalmente, se debe destacar que si el dato de la afiliación sindical[46] constara en alguna administración o entidad[47] a las que se le aplica las normas que regulan el derecho de acceso a la información pública, en los términos que establece la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, "únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso" (art. 15.1 Ley 19/2013).

2.2.4. Datos genéticos

Resulta una novedad, respecto de la normativa precedente, la inclusión de los datos genéticos como una categoría especial de

[42] Cfr. Art. 69.2 TRLET.

[43] Se podrán presentar candidatos para las elecciones de delegados de personal y miembros del comité de empresa por los sindicatos de trabajadores legalmente constituidos o por las coaliciones formadas por dos o más de ellos, que deberán tener una denominación concreta atribuyéndose sus resultados a la coalición; igualmente podrán presentarse los trabajadores que avalen su candidatura con un número de firmas de electores de su mismo centro y colegio, en su caso, equivalente, al menos, a tres veces el número de puestos a cubrir (art. 69.3 TRLET). En el primer supuesto, la candidatura es sindical, pero no es requisito de validez de la misma que los candidatos sean trabajadores afiliados; es más, si lo fueran y cambiaran su afiliación a otro sindicato, el resultado inicial no se modifica a efectos de atribuir los resultados obtenidos en la elección, es decir, "el cambio de afiliación del representante de los trabajadores, producido durante la vigencia del mandato, no implicará la modificación de la atribución de resultados" (art. 12.3 RD 1844/1994, de 9 de septiembre, por el que se aprueba el Reglamento de elecciones a órganos de representación de los trabajadores en la empresa).

[44] Cfr. Modelo 8 del anexo RD 1844/1994.

[45] Cfr. Modelo 2 del anexo RD 1844/1994.

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

[47] No se incluye, sin embargo, a las organizaciones sindicales, puesto que a estas, como a los partidos políticos y a las organizaciones empresariales, solamente se les aplica el Capítulo II, que desarrolla la "publicidad activa", del Título I de la Ley; por lo tanto, no el Capítulo III, que regula el "derecho de acceso a la información pública", del mismo Título I. Cfr. Art. 3.a) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (BOE de 10 de diciembre de 2013).

datos personales. Se ha podido defender su coincidencia, en su régimen jurídico, o proximidad con los datos relativos a la salud o con los datos médicos. Sin embargo, nada hay que objetar sobre la pertenencia de los datos genéticos al grupo de los datos sensibles, de forma separada o individualizada, sobre todo porque no todos los datos genéticos deben ser considerados datos de salud o deben asimilarse a estos últimos, sino porque "todo dato genético es, por la naturaleza de la información que revela o pudiera revelar, un dato merecedor de protección reforzada"[48].

Por su especificidad respecto de otras categorías especiales de datos y por la limitación que ha conllevado su asimilación a los datos de salud, es acertada la referencia a los datos genéticos, por cuanto merecen una protección autónoma[49]. Y quizá por presentarse como nueva categoría especial, el vigente Reglamento comunitario aporta una definición: "datos personales relativos a las características genéticas, heredadas o adquiridas, de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona" [art. 4.13) RGPD], en particular "a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente" (considerando 34 RGPD).

Previamente, la Recomendación núm. R 5 (97), de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros, sobre protección de datos médicos, ya había aportado un concepto autónomo de dato genético, entendiendo que se refiere a "todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no". Asimismo, la Declaración Internacional sobre los Datos Genéticos Humanos, de 16 de octubre de 2003, aprobada por la 32ª sesión de la Conferencia General de la UNESCO, define los datos genéticos como "información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos".

En nuestro ordenamiento jurídico, la noción de "dato genético de carácter personal" fue introducida por la Ley 14/2007, de 3 de julio, de investigación biomédica (en adelante, LIB), como la "información sobre las características hereditarias de una persona, identificada o identificable, obtenida por análisis de ácidos nucleicos u otros análisis científicos" [art. 3.j) LIB].

Como se observa, la definición de dato genético que aporta el Reglamento comunitario es más amplia y precisa que las anteriores, siendo coincidente en su núcleo esencial. Abarca todas las informaciones sobre la fisiología y la salud de la persona física, obtenida a través de la analítica de una muestra biológica, cualquier análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN) u otro elemento que permita obtener información equivalente[50].

En concreto, las técnicas de análisis de ADN revelan el carácter único[51] de la persona

[48] GÓMEZ SÁNCHEZ, Y.: "La protección de los datos genéticos: el derecho a la autodeterminación informativa", *Derecho y Salud*, vol. 16, núm. extraordinario 1, 2008, p. 62.

[49] ROMEO CASABONA, C. M.: "El tratamiento y la protección de los datos genéticos", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): *Gen-Ética*, Ariel, Barcelona, 2003, p. 240.

[50] *Vid.* LEWIS R.: *Human Genetics: Concepts and Applications*, 12ª ed., McGraw-Hill Science, NewYork (EE.UU.), 2017, *passim*.

[51] *Vid.* CLAYTON, E. W., EVANS, BARBARA J., HAZEL, JAMES W. y ROTHSTEIN, MARK A.: "The law of genetic privacy: applications, implications, and limitations", *Journal of Law and the Bioscien-*

–a excepción de los gemelos monocigóticos[52]– y su configuración genética, por ende tiene un carácter dual: "proporcionan información sobre el cuerpo humano y permiten la identificación inequívoca de una, y solo una, persona"[53]. Esa información genética obtenida permite al propio sujeto obtener información sobre su configuración genética, las consecuencias presentes o futuras de tal configuración y le posibilita la adopción de decisiones y el ejercicio de sus derechos y libertades; permite identificar a la persona, viva o muerta, y relacionarla con otros sujetos; permite conocer a la persona su estado de salud actual y prever la propensión a padecer enfermedades futuras; permite detectar predisposiciones genéticas de los individuos y capacidad de diversa naturaleza; aporta datos relevantes que superan el ámbito individual; aporta información que puede ser utilizada en muy diversos campos de la organización de la sociedad, entre ellos el ámbito laboral, y, por último, aporta información que podrá valorarse en el futuro[54].

No solo por el contenido de la información que aporta, también su singularidad está determinada por las características[55] de la información genética, fundamentalmente dos: permanencia e inalterabilidad, con independencia de la voluntad del individuo, y vinculación biológica con los demás miembros de un grupo familiar o étnico.

Sobre la base de lo expuesto, se deriva la especial naturaleza que poseen los datos genéticos. La más perfecta, en el sentido de exclusiva, relación entre la persona física y la información obtenida, que permite la identificación de aquella a través de esos datos, además de dar a conocer datos relativos a cuestiones estrechamente unidas al núcleo de la personalidad y de la dignidad humanas, hace que tengan especial incidencia en la vida privada, en el ejercicio de las libertades o ante el riesgo de prácticas discriminatorias[56]. De ahí, en suma, la calidad del dato personal, su calificación como dato sensible y su fundamento como categoría especial de dato personal.

El peligro de difundir datos personalísimos y el riesgo de adoptar decisiones discriminatorias en la esfera de las relaciones laborales y en otros –sanitario o de los seguros, por ejemplo– campos, si duda, es cierto, de ahí la interdicción general de tratamiento de los datos genéticos y su reserva, excepto en los supuestos amparados por el legislador. Por la complejidad y la sensibilidad de la información genética, existe un peligro cierto de que el responsable del tratamiento haga un uso indebido de la misma o la reutilice con fines no autorizados. Además, toda discriminación por razón de características genéticas debe quedar prohibida con carácter general[57].

Se ha de recordar, por último, que si el dato genético[58] constara en alguna administración o entidad a las que se le aplica las normas que regulan el derecho de acceso a la información pública, en los términos que establece la –ya citada– Ley 19/2013, "el acceso solo se podrá

ces, vol. 6, núm. 1, 2019, p. 1 (https://academic.oup.com/jlb/article/6/1/1/5489401).

[52] LACADENA, J. R.: "Individualización y mismidad genética en el desarrollo humano", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): *Gen-Ética*, Ariel, Barcelona, 2003, p. 116.

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

[54] Son las conclusiones que presenta GÓMEZ SÁNCHEZ, Y.: "La protección de los datos genéticos: el derecho a la autodeterminación informativa", *cit.*, p. 61.

[55] Las apunta ROMEO CASABONA, C. M.: *Los genes y sus leyes. El derecho ante el genoma humano*, Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, Comares, Granada, 2002, p. 63.

[56] *Vid.* ÁLVAREZ GONZÁLEZ, S.: "Derecho a la «privacidad» e información genética", *cit.*, p. 20, y la bibliografía que cita.

[57] Cfr. Considerando 23 Directiva (UE) 2016/680, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[58] El mismo criterio se aplica para datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, los datos biométricos y a los relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública al infractor.

autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley" (art. 15.1 Ley 19/2013).

2.2.5. Datos biométricos

Ex lege, "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" [art. 4.14) RGPD], son datos biométricos e, igualmente, se encuadran entre las categorías especiales de datos personales cuando identifican –se insiste– de manera unívoca a una persona (art. 9.1 RGPD).

Estos datos se han definido como "propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad"[59]. Ejemplos típicos de datos biométricos "identificadores", al corresponder a una única persona, son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces y también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento, como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc. En particular, el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física (considerando 51 RGPD).

Una peculiaridad de los datos biométricos –como sucede, por cierto, con los genéticos– es que se les puede considerar tanto como contenido de la información sobre una determinada persona –el trabajador X tiene estas huellas dactilares– como un elemento para vincular una información a una determinada persona física –este dispositivo lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden al trabajador X; por lo tanto el trabajador X ha tocado este dispositivo–.

A través de sistemas que utilizan información o datos biométricos, se puede identificar a un trabajador, ya sea mediante el análisis de aspectos físicos y morfológicos de la persona –huellas dactilares, patrones de la mano, reconocimiento facial, características de la retina, geometría del iris, rasgos de la voz, estructuras venosas, pulsaciones, ondas cerebrales o estado de atención–, ya sea por la valoración de sus comportamientos o habilidades –comprobación de su escritura, firma o presión sobre las teclas del ordenador–. Con ellos se permite al empleador controlar toda la actividad del trabajador, desde su inicio, pasando por el desempeño de sus funciones durante el tiempo de trabajo, hasta su conclusión. Dicho con otras palabras, el empresario, con los sistemas biométricos, puede controlar la presencia y ubicación precisa de los empleados en sus instalaciones, conociendo con exactitud la hora de entrada y de salida o el tiempo efectivo dedicado a la actividad profesional, lo que permite diferenciar y valorar el tiempo productivo e improductivo, particularmente útil en organizaciones con horario flexible o con jornadas irregulares[60].

Al respecto, el Tribunal de Justicia de la Unión Europea ha confirmado que "un registro del tiempo de trabajo, que incluye la indicación de las horas en que cada trabajador

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

[60] Así lo expone, con razón, RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, p. 158.

inicia y finaliza la jornada, así como de las pausas o periodos de descanso correspondientes, queda comprendido en el concepto de «datos personales»"[61].

También, de modo destacado, son particularmente útiles[62] para garantizar el acceso de los empleados a determinadas dependencias o a la utilización de equipamientos, bien sea por el tipo de actividad desarrollada o por el valor y las posibles consecuencias que los medios materiales –instrumentos, máquinas, etc.– pueden acarrear para el propio trabajador o para terceros. La principal ventaja de estos medios de control es que no permiten la suplantación de la persona física sujeta a control o vigilancia.

Un uso adicional, por último, que permite la evolución tecnológica posibilita la puesta en marcha de procesos de encuadramiento de los individuos en grupos o divisiones, de cara a la elaboración de perfiles y "con fines claramente decisionales"[63].

Para el reconocimiento biométrico del trabajador, el paso previo es proceder a captar, por medio de un sensor específico para cada tipo de técnica biométrica, uno o más rasgos específicos de la persona, y su transformación en una secuencia numérica, conformando una plantilla que queda registrada en una base de datos. Después, la utilización del sistema biométrico requerirá, en cada uso, la comparación entre la plantilla almacenada y la muestra biométrica que se vuelve a tomar para verificar su equivalencia[64].

Esa recogida primera y el tratamiento posterior de datos biométricos puede poner en riesgo los derechos fundamentales de los trabajadores, pues de esos datos se pueden deducir otras informaciones que pertenecen a su esfera de privacidad[65]. Por ello, la licitud del uso de estos modelos de identificación personal se somete al juicio de proporcionalidad[66] por parte de los tribunales cuando han de valorar aquella en supuestos controvertidos. Así, sobre el control horario basado en un método que consiste en la lectura biométrica, basado en el reconocimiento tridimensional de la mano –largo, ancho y espesor– para verificar la identidad biométrica de la persona, se analiza el objetivo propuesto, "objetivo que no es otro que el de lograr un mayor nivel de eficacia en la Administración pública, eficacia que pasa por un control efectivo del cumplimiento de sus obligaciones por parte de los empleados públicos, obligaciones que se inician en el momento del puntual acceso a sus puestos de trabajo y en una estricta observancia de la jornada laboral". Respecto del juicio de rigurosa necesidad, aún existiendo otros sistemas, "hay dos realidades que no pueden negarse, de un lado la lógica posibilidad de incorporación a la Administración pública de las nuevas tecnologías como método de control y, de otro, el notorio carácter imperfecto de los sistemas de control más comúnmente usados, tanto el sistema

[61] STJUE de 30 de mayo de 2013, Asunto C-342/12, *Worten – Equipamentos para o Lar, S. A.*

[62] *Vid.* Goñi Sein, J. L.: "Intimidad del trabajador y poderes de vigilancia y control empresarial", en García Murcia, J. (Coord.): *Jornada sobre derechos fundamentales y contrato de trabajo*, Principado de Asturias, Oviedo, 2017, p. 61.

[63] Baz Rodríguez, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, Bosch Wolters Kluwer, Barcelona, 2019, p. 244.

[64] *Vid.* Poquet Catalá, R.: *El actual poder de dirección y control del empresario*, Cuadernos de Aranzadi Social, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2013, p. 285.

[65] En este sentido, Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, p. 159, pone de relieve esos riesgos para la persona del trabajador, "no en vano –y como mero ejemplo– el iris puede revelar el consumo de drogas y de alcohol o el padecimiento de enfermedades como hipertensión o diabetes".

[66] Como sintetizan las SSTC 66/1995, de 8 de mayo, 55/1996, de 28 de marzo, 207/1996, de 16 de diciembre, y 37/1998, de 17 de febrero, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

de firma, por su posible manipulación, como el sistema de reloj y ficha, por no impedir la sustituibilidad en su cumplimiento". Por último, "la implantación del sistema puede reportar más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto, máxime cuando nos encontramos ante la imposición de una obligación a un colectivo vinculado a la Administración mediante una relación de sujeción especial"[67].

Sin embargo, aplicando ese mismo principio de proporcionalidad, más cuestionable –incluso "deplorable"[68]– resulta la implantación de chips subcutáneos, las pulseras de movimientos o las etiquetas de identificación por radiofrecuencia. La Recomendación 2009/387/CE, de 12 de mayo de 2009, de la Comisión Europea, sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia, insiste en que el trabajador conozca el modelo empleado como sistema de control, imponiendo a las empresas la obligación de elaborar y publicar información[69] precisa y fácil de comprender sobre el uso de cada aplicación, que como mínimo debe incluir: a) la identidad y el domicilio de los operadores; b) la finalidad de la aplicación; c) los datos que procesa la aplicación, en particular si se trata de datos personales, y si se controla la localización de las etiquetas; d) un resumen de la evaluación del impacto sobre la protección de datos y la intimidad; y, e) los posibles riesgos para la intimidad, si existen, relacionados con el uso de etiquetas en la aplicación y las medidas que pueden adoptar las personas para reducirlos.

Sobre el tratamiento de las expresiones faciales del trabajador por medios automatizados, de la misma manera se advierte el riesgo de un uso desproporcionado –incluso en el trabajo a distancia, pues ello lo permite las nuevas tecnologías– por su incidencia sobre los derechos y libertades de los trabajadores. Se ha considerado ilegal, en general, y los empresarios, por consiguiente, deben abstenerse de utilizar tecnologías de reconocimiento facial, aunque puede haber algunas excepciones marginales a esta regla, sin que tales escenarios puedan utilizarse para invocar una legitimación general del uso de estas tecnologías[70]. Asimismo, debido a los riesgos particulares asociados a los datos biométricos, antes de comenzar el tratamiento de las imágenes digitales a los fines del reconocimiento facial, se requerirá el consentimiento informado de la persona[71].

2.2.6. Datos relativos a la salud

El Convenio 108, de 28 de enero de 1981, del Consejo de Europa, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, entre las "categorías particulares de datos" refiere los de carácter personal –entre otros– relativos a "la salud" (art. 6). Asimismo, la Recomendación núm. R 5 (97), de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros, sobre protección de datos médicos, señala que la expresión "da-

[67] SSTSJ de Cantabria (C-A) de 21 de febrero (Rec. 763/2002) y de 14 marzo de 2003 (Rec. 893/2002). De igual manera, sobre la implantación de un sistema de huella dactilar con lector biométrico en el centro de trabajo para el acceso a las instalaciones, cfr. STSJ de Murcia de 25 de enero de 2010 (Rec. 1071/2009) y STSJ de la Comunidad Valenciana de 8 de febrero de 2017 (Rec. 3489/2016); en la doctrina, Goñi Sein, J. L.: *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018)*, Bomarzo, Albacete, 2018, p. 47.

[68] Así de contundente se expresa Rodríguez Escanciano, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, p. 161.

[69] La Guía sobre seguridad y privacidad de la tecnología RFID (*Radio Frequency IDentification*), elaborada por la AEPD y el Instituto Nacional de Tecnologías de la Comunicación, recomienda informar a los trabajadores sobre la existencia del tratamiento de forma clara y accesible, indicando la localización de las etiquetas, la existencia de lectores, su posible monitorización y el modo de desactivación.

[70] Dictamen 02/2017, de 8 de junio, sobre el tratamiento de datos en el trabajo, adoptado por el GT29.

[71] Dictamen 02/2012, de 22 de marzo, sobre reconocimiento facial en los servicios en línea y móviles, adoptado por el GT29.

tos médicos" se refiere "a todos los datos personales relativos a la salud de un individuo", esto es, "a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos" (art. 1).

Repite esa idea la –tantas veces citada y derogada– Directiva 95/46/CE, que enumeraba los datos relativos a la salud –característicos de su "identidad física, fisiológica o psíquica" [art. 2.a) Directiva 95/46/CE]– dentro de las categorías especiales de datos personales en cuanto a su tratamiento (art. 8.1 Directiva 95/46/CE), siendo preciso dar una interpretación amplia a la expresión "datos relativos a la salud", de modo que comprenda "la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona"[72]. Al respecto, el GT29, en el Anexo a la Carta "*Health data in apps and devices*", identifica los criterios relevantes para determinar cuándo los datos procesados por las aplicaciones y dispositivos de estilo de vida y bienestar deben considerarse "datos de salud"; así cuando: los datos son inherente o claramente de carácter médico; los datos son datos sin procesar del sensor que se pueden usar en sí mismos o en combinación con otros datos para sacar una conclusión sobre el estado de salud actual o el riesgo para la salud de una persona; se sacan conclusiones sobre el estado de salud o el riesgo para la salud de una persona, independientemente de si estas conclusiones son precisas o inexactas, legítimas o ilegítimas, adecuadas o inadecuadas.

Son "datos especialmente protegidos", según la anterior Ley Orgánica 15/1999, "los datos de carácter personal que hagan referencia a la salud", junto a otros (art. 7.2 y 3 LO 15/1999). Respecto de su tratamiento, además, decía que "las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad" (art. 8 LO 15/1999). Es su norma reglamentaria[73] de desarrollo la que define los "datos de carácter personal relacionados con la salud" como "las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética" [art. 5.1.g) RD 1720/2007].

En el presente, el Reglamento 2016/679/UE define los datos sobre la salud como "los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" [art. 4.15) RGPD]. Antes, en su parte expositiva afirma que entre los datos personales referentes a la salud "se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro"; específicamente "se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un mé-

[72] STJUE de 6 de noviembre de 2003, Asunto C-101/01, *Bodil Lindqvist*.

[73] RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

dico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica *in vitro*" (considerando 35 RGPD).

La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, asegura, *ab initio*, que "la dignidad de la persona humana, el respeto a la autonomía de su voluntad y su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica" (art. 2.1 Ley 41/2002) y, reafirma que "toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley" (art. 7.1 Ley 41/2002).

En el ámbito laboral, sin duda, la alteración de la salud puede afectar al trabajador, disminuyendo su rendimiento o, en muchas ocasiones, impidiéndole prestar servicios de manera temporal. Incluso ante las situaciones de riesgo para la salud o cuando ya se haya modificado la salud del trabajador, la intervención de la empresa podrá estar justificada bien para prevenir el desarrollo de enfermedades o patologías o bien para verificar el estado de salud del trabajador[74].

En efecto, por un lado, el empresario "podrá verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico" y la negativa del trabajador a dichos reconocimientos –como sanción– "podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones" (art. 20.4 TRLET), como podrían ser las mejoras voluntarias sobre las prestaciones económicas del sistema público de Seguridad Social, concretamente la prestación de incapacidad temporal.

Se trata, en definitiva, de someter al trabajador a controles médicos adicionales a los efectuados por los servicios públicos de salud y las entidades gestoras y colaboradoras de la Seguridad Social, mediante el servicio médico de empresa o a través del recurso a servicios sanitarios externos, pero sin que sea posible realizar pruebas diagnósticas que no tengan "como finalidad la mejora o estudio de su estado de salud"[75] o utilizar las informaciones obtenidas para fines distintos a los habilitados *ex lege*[76].

De esta extensión del poder de control del empresario, según el Tribunal Constitucional, no se deriva la posibilidad de crear un fichero automatizado denominado "absentismo con baja médica", por cuanto requeriría que mediase el consentimiento expreso de los afectados o que, por razones de interés general, así lo dispusiera una ley; como ninguno de dichos requisitos concurren en el supuesto enjuiciado, ello determina que la creación de esa base de datos vulnera el artículo 18 CE, el derecho a la intimidad personal de los titulares de la información en ella conservada, en relación con el artículo 18.4 CE[77].

Por otro lado, la Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales (en adelante, LPRL), obliga al empresario a garantizar a los trabajadores a su servicio "la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo" (art. 22.1, párrafo primero, LPRL). La vigilancia y control de la salud de los trabajadores,

[74] *Vid.*, con detalle y finura jurídica, RODRÍGUEZ ESCANCIANO, S.: *Derechos laborales digitales: garantías e interrogantes*, *cit.*, pp. 138-157.

[75] STS de 25 de enero de 2018 (Rec. 249/2016).

[76] STSJ del País Vasco de 6 de julio de 2004 (Rec. 1232/2004), donde se calificó el reconocimiento médico como desproporcionado y realizado con intención de constituir una prueba a esgrimir en un procedimiento judicial posterior.

[77] STC 202/1999, de 8 de noviembre. *Vid.* GARCÍA MURCIA, J.: "Derecho a la intimidad y contrato de trabajo: la anotación de las bajas médicas (Comentario a la STC 202/1999, de 8 de noviembre)", *Repertorio Aranzadi del Tribunal Constitucional*, núm. 2, 2000, pp. 1937-1956.

siendo una obligación empresarial, se llevarán a cabo por personal sanitario con competencia técnica, formación y capacidad acreditada (art. 22.6 LPRL).

Esta vigilancia, en principio, solo se puede realizar cuando el trabajador preste su consentimiento. De este carácter voluntario únicamente se exceptúan, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para él mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad (art. 22.1, párrafo segundo, LPRL).

En todo caso, las medidas de vigilancia y control de la salud de los trabajadores se llevarán a cabo respetando siempre el derecho a la intimidad y a la dignidad de la persona del trabajador y la confidencialidad de toda la información relacionada con su estado de salud (art. 22.2 LPRL). En efecto, respecto de los datos relativos a la salud obtenidos en los reconocimientos médicos de los trabajadores, rige el principio básico de confidencialidad, como proyección del derecho a la intimidad, lo que supone su "reservabilidad", el mantenimiento en secreto hacia personas que no tienen un interés legítimo para justificar su conocimiento[78]. Ahora bien, esa confidencialidad parece graduarse según la información se presente en forma de resultados o en forma de conclusiones: para los resultados de la vigilancia de la salud la confidencialidad es máxima –modulable solo por el consentimiento del trabajador o un interés legítimo, como el perjuicio a terceros–, mientras que la confidencialidad es mínima para las conclusiones obtenidas, por el tipo de información que incorpora y el mayor número de destinatarios, "bien entendido que en ningún caso debe trascender de la empresa o de los sujetos con responsabilidades en materia de prevención"[79].

Los resultados de la vigilancia de la salud se comunican a los trabajadores afectados (art. 22.3 LPRL) y el acceso a toda la información médica de carácter personal se limita al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador (art. 22.4 párrafo segundo, LPRL). No obstante la anterior prohibición, el empresario y las personas u órganos con responsabilidades en materia de prevención deben ser informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva (art. 22.4 párrafo tercero, LPRL).

Como garantía conexa, más allá del derecho a la protección de los datos relativos a la salud, la información médica de los trabajadores obtenida en los procesos de vigilancia de su salud con fines preventivos, que excede del estricto ámbito de los riesgos profesionales[80], no podrá ser usada "con fines discriminatorios ni en perjuicio del trabajador" (art. 22.4 LPRL). Esos son, perfectamente identificados por el legislador, los riesgos para el trabajador que el conocimiento de datos sobre su salud deriva en el ámbito del empleo y las relaciones laborales.

[78] PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*, núm. 138, 2018, pp. 168-169.

[79] Así, PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *cit.*, p. 169.

[80] BLASCO PELLICER, A.: "El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador", en BORRAJO DACRUZ, E. (Dir.): *Trabajo y libertades públicas*, La Ley, Madrid, 1999, p. 257.

En definitiva, el cumplimiento del deber de vigilancia de la salud conlleva para el personal sanitario encargado la obtención de resultados y elaboración de diagnósticos, mientras que para el empresario comporta el depósito de una muy amplia información sobre los trabajadores que será necesario conservar y organizar a través de ficheros, con su actualización periódica, aunque no tenga acceso a la totalidad de los datos contenidos; responsable del tratamiento de los datos que conformen resultados sobre la salud de los trabajadores será el servicio de prevención ajeno, encargado de la vigilancia de la salud, o la empresa si se encarga de ella un servicio de prevención propio o mancomunado, si bien, como esta no puede tener acceso a esos datos, se tendrán que establecer distintos perfiles y facultades de acceso para evitar su conocimiento por el propio empleador; en cambio, sobre las conclusiones entregadas por el personal sanitario será la empresa[81]. Bien entendido que todos los datos sobre la salud deberán tener un tratamiento informático separado[82] de los otros datos disponibles de los trabajadores, y en todo caso se deberán adoptar medidas adecuadas de seguridad técnica y organizativa para evitar que personas extrañas al servicio médico del empleador tengan acceso a tales resultados.

2.2.7. Datos sobre la vida sexual o la orientación sexual

La norma comunitaria incluye en su listado de categorías especiales de datos personales, por último, los "datos relativos a la vida sexual o a la orientación sexual de la persona física" (art. 9.1 RGPD), modificando así la referencia pretérita a los datos relativos "a la sexualidad" (art. 8.1 Directiva 95/46/CE). En el contexto nacional, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, se refería a los datos que hagan referencia "a la vida sexual" (art. 7.3 y 4 LO 15/1999), mientras la legislación en vigor se refiere genéricamente a la "orientación sexual" (art. 9.1 LOPDyGDD).

En cuanto al concepto, la orientación sexual es una atracción emocional, romántica, sexual o afectiva duradera hacia otra persona y se distingue fácilmente de otros componentes de la sexualidad, como el sexo biológico, la identidad sexual –el sentido psicológico de ser hombre o mujer– y el rol social del sexo –respeto de las normas culturales de conducta femenina y masculina–. La atracción puede ser hacia personas del sexo opuesto –heterosexualidad–, hacia personas del mismo sexo –homosexualidad– o hacia personas de su mismo sexo y del sexo opuesto –bisexualidad–.

La orientación sexual es diferente de la vida sexual o de la conducta sexual, mientras la primera se refiere a los sentimientos y al concepto de uno mismo, la segunda, por el contrario, puede o no expresar su orientación sexual. También se diferencia de la identidad de género, que no se relaciona con la atracción hacia otra persona, sino con quién eres: hombre, mujer, transgénero, intergénero, etc.

No se pretende describir todas las variantes acerca de la orientación sexual de las personas físicas, incluso las hay que no sienten ningún tipo de atracción sexual por nadie. La exposición precedente trata de exponer una realidad sobre la que se proyectan múltiples comportamientos discriminatorios conocida la orientación sexual de una persona, señaladamente en el ámbito de las relaciones de trabajo, ya sea en el acceso al empleo, en las condiciones de trabajo o en la extinción del contrato. Las diferencias de trato basadas en la orientación sexual se deben, sin duda, a los prejuicios sociales contra el comportamiento

[81] Sobre los sujetos intervinientes en el tratamiento, *in extenso*, *vid.* PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *cit.*, pp. 175-178.

[82] MERCADER UGUINA, J. R.: "La protección de datos personales del trabajador. La obligación del empresario de informar al trabajador sobre sus condiciones de trabajo", en CASAS BAAMONDE, M. E. y GIL ALBURQUERQUE, R. (Dirs.): *Derecho Social de la Unión Europea. Aplicación por el Tribunal de Justicia*, Francis Lefebvre, Madrid, 2018, p. 776, que cita la Recomendación núm. 2015 (2) del Consejo de Europa.

sexual de los colectivos que no son heterosexuales, jugando las restantes opciones personales como causas de discriminación. Dicho con otras palabras, el ámbito de la discriminación incluirá "cualquier conducta que comporte una tratamiento diferencial peyorativo como consecuencia de la orientación sexual que el individuo ha escogido libremente", si bien los colectivos no heterosexuales son los que requerirán "una mayor protección y una tutela efectiva frente a actitudes discriminatorias"[83].

Aunque la orientación sexual no se encuentra prevista dentro de las causas discriminatorias enumeradas –"por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social"– en el artículo 14 CE, de ser considerada como tal al ser una enumeración abierta y que alude a cualquier otra condición o circunstancia personal o social.

Encuentra plena justificación, por tanto, la mención expresa a la orientación sexual entre las categorías especiales de datos personales, pues cualquier decisión basada en el conocimiento de esa información especialmente sensible puede resultar discriminatoria, quedando prohibido su tratamiento, como regla general, y sin que sea suficiente el consentimiento del concernido para levantar esa interdicción, resultando de aplicación otras circunstancias excepcionales.

3. EL TRATAMIENTO DE LAS CATEGORÍAS ESPECIALES DE DATOS PERSONALES

La especial protección que se debe otorgar a los datos personales que son particularmente sensibles en relación con los derechos y las libertades fundamentales se materializa en un régimen propio para su tratamiento, por cuanto este, de aceptarse, podría entrañar riesgos ciertos para aquellos derechos y las libertades. Esta es la razón ultima que justifica un tratamiento diferenciado de las categorías especiales de datos, que –a tenor del Reglamento comunitario, como se expondrá en breve– no deben ser tratados, a menos que se permita en situaciones delimitadas y contempladas por el legislador, habida cuenta también de que los Estados miembros pueden ordenar disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del Reglamento. Así, se han establecido de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras circunstancias cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas.

No obstante, además de los requisitos particulares de ese tratamiento, deben aplicarse los principios generales y otras normas, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento (considerando 51 RGPD). Se recuerda que el tratamiento solo será lícito si se cumple, al menos, una de las siguientes condiciones: a) que el interesado haya dado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) que el tratamiento sea necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación, a petición de este, de medidas precontractuales; c) que el tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona física; e) que el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) que el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales (art. 6.1 RGPD).

[83] CHACARTEGUI JÁVEGA, C.: *Discriminación y orientación sexual del trabajador*, Lex Nova, Valladolid, 2001, p. 24.

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

3.1. Prohibición general de tratamiento

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, se puede deber al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular –pero no solo– cuando los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual (considerando 75 RGPD). De ahí que el legislador europeo consagre un principio general en relación con las categorías especiales de datos: la prohibición de tratamiento.

En términos taxativos, "quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física" (art. 9.1 RGPD).

Como a continuación se listan, como excepciones, hasta diez circunstancias causales o situaciones jurídicas que permiten el tratamiento total o parcial de las categorías especiales de datos personales (art. 9.2 RGPD), se podría pensar que la garantía para los interesados es absoluta, cuando realmente no es así, siendo muchas y amplias las salvedades.

Precisamente sobre tales excepciones, el legislador nacional interviene conforme a las posibilidades que abre la norma comunitaria, bien sea por el llamamiento, en general, a enervar o concretar los supuestos de tratamiento excepcional [art. 9.2.a) y b) RGPD] o por el reenvío, solo respecto del tratamiento de datos genéticos, datos biométricos o datos relativos a la salud, a los ordenamientos de los Estados miembros para mantener o introducir condiciones adicionales, inclusive limitaciones (art. 9.4 RGPD).

La prohibición, "a fin de evitar situaciones discriminatorias" (art. 9.1 LOPDyGDD), abarca a un conjunto de datos que revelan rasgos de la persona o de su determinación social, cuyo conocimiento puede provocar, en mayor o menor medida, prejuicios sociales, una posición de desventaja en muchos ámbitos, entre los que incluimos la relaciones de trabajo, e incluso resulta contraria a la dignidad de la persona (art. 10.1 CE). Lo que caracteriza a la prohibición de discriminación, frente al principio genérico de igualdad, "es la naturaleza particularmente odiosa del criterio de diferenciación utilizado, que convierte en elemento de segregación, cuando no de persecución, un rasgo o una condición personal innata o una opción elemental que expresa el ejercicio de las libertades más básicas, resultando así un comportamiento radicalmente contrario a la dignidad de la persona y a los derechos inviolables que le son inherentes"[84].

Eliminado, de raíz, el tratamiento de las categorías especiales de datos personales se imposibilitaría cualquier modo de actuar o decidir que resulte contrario a los principios y derechos fundamentales. El marco jurídico regulador del tratamiento de datos, empero, no es tan estricto por la extensión de las limitaciones que incorpora.

3.2. Excepciones: el tratamiento permitido

Se autorizan excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre

[84] STC 62/2008, de 26 de mayo.

que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, así como cuando sea en interés público (considerando 52 RGPD).

Desde el punto de vista del tratamiento de los datos personales, en el global de datos, los especialmente sensibles forman una categoría con identidad propia, diferenciando dentro de estos últimos dos subcategorías[85]:

– Una, el tratamiento de datos cuya finalidad principal es identificar su origen racial o étnico, ideología, afiliación sindical, religión, creencias u orientación sexual, respecto de los que "el solo consentimiento del afectado no bastará para levantar la prohibición" (art. 9.1 LOPDyGDD), pero que no impedirá su tratamiento al amparo de los restantes supuestos contemplados en el artículo 9.2 RGPD, cuando así proceda.

– Otra, el tratamiento de datos genéticos, datos biométricos y datos relativos a la salud, al que se aplican todos los supuestos excepcionales –incluido el consentimiento del interesado– del artículo 9.2 RGPD que levantan la prohibición general. Además, sobre estos datos y su tratamiento, los Estados miembros pueden mantener o introducir condiciones adicionales, incluso limitaciones (art. 9.4 RGPD).

La regla general que prohíbe el tratamiento de las categorías especiales de datos personales conoce, en total, diez excepciones, supuestos enumerados en el artículo 9.2 RGPD, aunque no todos tienen la misma relevancia laboral[86].

[85] De género y dos especies diferentes habla, respecto de las categorías especiales de datos, MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, 3ª ed., Francis Lefebvre, Madrid, 2019, p. 27.

[86] La doctrina coincide en destacar tres o cuatro de las circunstancias excepcionales que permiten el tratamiento de categorías especiales de datos. *Vid.* GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 10, y BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, pp. 117-119.

[87] Cfr. Preámbulo de la LOPDyGDD.

3.2.1. El consentimiento explícito del trabajador como interesado

En primer lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado" [art. 9.2.a) RGPD]. Y así, en efecto, la ley española establece un matiz importante puesto que, a fin de evitar situaciones discriminatorias, "el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico", si bien respecto de esos concretos datos no se impide su tratamiento conforme a los restantes supuestos excepcionales (art. 9.1 LOPDyGDD).

Por ejemplo[87], siendo uno de los datos especialmente protegidos el de la afiliación sindical, la prestación del consentimiento por parte del trabajador afiliado no da cobertura a la creación de "listas negras" de sindicalistas, si bien eso no significa que pueda tratarse este dato –como se comprueba de seguido– por el empresario para hacer posible el ejercicio de los derechos de los trabajadores [art. 9.2.b) RGPD] o por los propios sindicatos [art. 9.2.d) RGPD].

Como pauta común, el consentimiento del interesado aporta la garantía de licitud sobre el tratamiento de sus datos personales [art. 6.1.a) RGPD]; en otros términos, para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho. El consentimiento debe darse mediante

un acto afirmativo y claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito[88], admitiéndose por medios electrónicos, o una declaración verbal[89] (considerando 32 RGPD), aunque esta alternativa puede acarrear problemas para probar la voluntad de la persona. En verdad, el consentimiento debe proceder de una declaración o de una clara acción afirmativa del afectado, lo que excluye –así se conocía– el "consentimiento tácito".

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines; caso de que el tratamiento tenga una pluralidad de finalidades, debe darse el consentimiento, de manera específica e inequívoca, para todos ellas. En el supuesto de que el consentimiento del interesado se haya solicitado por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

Cobra aquí especial relevancia la obligación del responsable del tratamiento de proporcionar información sobre el fin y fines perseguidos con esa acción, al igual que sobre los derechos subjetivos de los que dispone, desde la posibilidad de negarse a prestar el consentimiento hasta su rectificación o retirada en cualquier momento (art. 7.3 RGPD).

En suma, el consentimiento explícito es una característica cualificada[90] del "consentimiento informado"[91]. Sucede, sin embargo, que en el terreno de las relaciones laborales no siempre el consentimiento se puede entender dado válida y libremente, por lo que "en la mayoría de los casos de tratamiento de datos de los trabajadores, la base jurídica de dicho tratamiento no puede y no debe ser el consentimiento de los trabajadores, por lo que se requiere una base jurídica diferente"[92]. Ello como consecuencia de la relación de subordinación entre el trabajador y el empleador, puesto que para garantizar que el consentimiento se ha dado libremente, "este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento" (considerado 43 RGPD).

El legislador nacional es coherente con la conclusión anterior y, en consecuencia, prohíbe que el consentimiento del trabajador sea bastante para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar –entre otras informaciones– la afiliación sindical del trabajador. El solo consentimiento del trabajador afiliado no podrá ser la base jurídica de dicho tratamiento.

3.2.2. El cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social

En segundo lugar, la prohibición de tratamiento de cualquier categoría especial de dato

[88] Una manera evidente de garantizar que el consentimiento es explícito es confirmar de manera expresa dicho consentimiento en una declaración escrita; cuando proceda, el responsable podría asegurarse de que el interesado firma la declaración escrita, con el fin de eliminar cualquier posible duda o falta de prueba en el futuro (Directrices sobre el consentimiento en el sentido del Reglamento 2016/679/UE, adoptadas el 28 de noviembre de 2017, revisadas por última vez y adoptadas el 10 de abril de 2018, por el GT29).

[89] Contrasta esta posibilidad con el criterio más restricto de la –derogada– Ley 15/1999: "solo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias" (art. 7.2 Ley 15/1999).

[90] Así lo subraya MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, *cit.*, p. 48.

[91] TASCÓN LÓPEZ, R.: *El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión*, Civitas, Madrid, 2005, p. 103.

[92] Dictamen 02/2017, de 8 de junio, sobre el tratamiento de datos en el trabajo, adoptado por el GT29.

personal no se aplica cuando "el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado" [art. 9.2.b) RGPD].

La deficiente traducción al castellano –falta la conjunción disyuntiva "o" entre "el Derecho de la Unión" y "de los Estados miembros o un convenio colectivo"– siembra la duda interpretativa, que se resuelve por el contexto y que, asimismo, despeja la norma en su introducción explicativa: "deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones (considerando 52 RGPD).

Interesa destacar el rol que asumen las disposiciones legales y el convenio colectivo en la regulación de los derechos y obligaciones concernientes a la relación laboral (art. 3 TRLET). A estas fuentes de regulación de la relación laboral se refiere el Reglamento comunitario como "títulos de legitimación"[93] del tratamiento de las categorías especiales de datos personales, emplazando al convenio colectivo a asumir esa función ordenadora. El Derecho nacional, a través de disposiciones legislativas o de convenios colectivos, puede establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de la ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo (art. 88 RGPD). El reenvío al convenio colectivo, como regulación específica[94], se debe entender hecho al convenio colectivo estatutario[95], como norma jurídica[96] con eficacia *erga omnes*, de cualquier ámbito, "incluidos los «convenios de empresa»" (considerando 155 RGPD).

No se consiente, si más, el tratamiento de estas categorías especiales cuando deban cumplirse obligaciones o ejercer derechos reconocidos en el ordenamiento laboral y de seguridad y protección social, puesto que se requiere una "autorización" para ese tratamiento por parte de una norma jurídica, ya se encuentre esta en el seno del Derecho de la Unión Europea, en el Derecho interno o, como fuente propia del sector normativo referenciado, en un convenio colectivo, siendo dicha norma jurídica la que debe establecer las garantías suficientes

[93] Así lo subraya MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, *cit.*, p. 49.

[94] Advierten, con sumo acierto, GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", *cit.*, p. 11, que esta llamada a la negociación colectiva parece oportuna y razonable, "por su proximidad al terreno y su origen en la autonomía de las partes interesadas", pero desde la perspectiva española de negociación colectiva "tal vez sea más un reto que una probabilidad inmediata, a la vista del contenido que habitualmente revisten los convenios en nuestra experiencia". *Vid.*, al respecto, SERRANO GARCÍA, J. M.: *La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia*, Bomarzo, Albacete, 2019, pp. 17-26, 34-36 y 85-88.

[95] Entre otros, MERCADER UGUINA, J. R.: "Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre: una aproximación desde la protección de datos", *Trabajo y Derecho*, núm. 52, 2019, pp. 112-113, y BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit.*, p. 43.

[96] El convenio colectivo estatutario, una vez negociado "adquiere eficacia normativa, se incardina en el sistema de fuentes del Derecho y se impone a las relaciones de trabajo incluidas en su ámbito sin precisar el auxilio de técnicas de contractualización ni necesitar el complemento de voluntades individuales" (STC 177/1988, de 10 de octubre).

para preservar los derechos fundamentales e intereses del trabajador.

El Reglamento comunitario admite la licitud del tratamiento de datos cuando "es necesario para la ejecución de un contrato en el que el interesado es parte" [art. 6.1.b) RGPD] y cuando "es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento" [art. 6.1.c) RGPD]. Así, cuando sea necesario en el contexto de un contrato de trabajo, será lícito el tratamiento de los datos personales, de manera que en el ámbito laboral "el consentimiento del trabajador pasa, por tanto, como regla general a un segundo plano pues el consentimiento se entiende implícito en la relación negocial, siempre que el tratamiento de datos de carácter personal sea necesario para el mantenimiento y el cumplimiento del contrato firmado por las partes"[97]. Regla general que cede ante algunas categorías especiales de datos –cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico (art. 9.1 LOPDyGDD)– por no bastar el consentimiento del trabajador para anular la prohibición del tratamiento.

Por ende, más que "requerir situaciones específicas de prestación del consentimiento"[98], respecto del dato relativo a la afiliación sindical se impone una habilitación legal que marcará las garantías y condiciones adiciones para su tratamiento[99]. Así ocurre, como se ha descrito, con el descuento de la cuota sindical, pues el empresario únicamente puede proceder al descuento sobre los salarios y a la correspondiente transferencia, a solicitud del sindicato del trabajador afiliado y previa conformidad, siempre, de este (art. 11.2 LOLS). Es, entonces, el cumplimiento de una obligación legal, el descuento de la cuota sindical, la base jurídica que ampara el tratamiento del dato referente a la afiliación sindical.

3.2.3. La necesidad de proteger intereses vitales del interesado o de otra persona física

En tercer lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento" [art. 9.2.c) RGPD]. Coincide con una de las condiciones para considerar lícito el tratamiento [art. 6.1.d) RGPD].

En efecto, el tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida o la integridad física del concernido o la de otra persona física, cuando no está en condiciones de dar su consentimiento. Ahora bien, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente (considerando 46 RGPD).

La incapacitación jurídica de la persona, mediante una declaración judicial fundada en enfermedades o deficiencias persistentes de carácter físico o psíquico que impidan a la persona gobernarse por sí misma (arts. 199 y 200

[97] STC 39/2016, de 3 de marzo.

[98] LÓPEZ ÁLVAREZ, L. F.: *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016, p. 114.

[99] El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento 2016/679/UE, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento 2016/679/UE (art. 8.1 LOPDyGDD). Se impone, por consiguiente, una reserva de ley; *vid.* MERCADER UGUINA, J. R.: *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, *cit.*, p. 44.

Código Civil), o el deterioro físico o psíquico de la persona, sin la previa incapacitación judicial, justifican el tratamiento de datos relativos a la salud para proteger intereses vitales del interesado. Pensemos en un paciente que, según el criterio del médico que le asiste, carece de capacidad para entender la información a causa de su estado físico o psíquico; en ese supuesto, "la información se pondrá en conocimiento de las personas vinculadas a él por razones familiares o de hecho" (art. 5.3 Ley 41/2002). Por ejemplo, la comunicación de la historia clínica[100] de una persona que padece una enfermedad degenerativa o se encuentra en estado de coma, que le impida dar el consentimiento para la realización de una prueba o intervención en situación de urgencia vital.

De igual modo, el tratamiento de datos relativos a la salud puede responder a los intereses vitales del interesado o a motivos de interés público como, por ejemplo, cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o provocadas por el hombre.

3.2.4. Fundaciones, asociaciones u organizaciones políticas, filosóficas, religiosas o sindicales, sin ánimo de lucro

En cuarto lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados" [art. 9.2.d) RGPD].

Se excepciona el tratamiento de categorías especiales de datos cuando se vincule a necesidades específicas de fundaciones, asociaciones u organizaciones políticas, filosóficas, religiosas o sindicales, sin ánimo de lucro, en concreto cuando el tratamiento se realiza en el marco de sus actividades, tomando en consideración que su objetivo es permitir el ejercicio de las libertades fundamentales (considerando 51 RGPD). Afecta, fundamentalmente, a datos sobre el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o, específicamente en el ámbito laboral, a la afiliación sindical.

La referencia, desde un punto de vista subjetivo, se reduce a las organizaciones ideológicas o de tendencia, en sentido estricto, que incluye a aquellas organizaciones que tienen como rasgo más específico el ser creadoras o sustentadoras de una determinada ideología o concepción del mundo –llamada "tendencia"– y en función de la misma existen[101], definición en la que se encuadran los partidos políticos, los sindicatos y las confesiones religiosas. Asimismo, se vincula, desde una perspectiva objetiva, al tratamiento –*ad intra*, exclusivamente– de datos personales de los miembros actuales o antiguos de tales organismos o de personas que mantengan contactos regulares con ellos en relación con sus fines; por ello, se exige el consentimiento de los interesados para comunicar o transferir esos datos fuera de la organización de tendencia.

[100] Dictamen 36/2018, de 28 de junio de 2018, de la Autoridad Catalana de Protección de Datos, en relación con una consulta sobre la autorización para el acceso de terceros a la historia clínica.

[101] Sobre este tema, *vid.* APARICIO TOVAR, J.: "Relación de trabajo y libertad de pensamiento en las empresas ideológicas", en VV.AA.: *Derecho del Trabajo en homenaje a los profesores BAYÓN CHACÓN y DEL PESO CALVO*, Universidad Complutense, Madrid, 1980, p. 293. También, DE VAL TENA, A. L.: "Las empresas de tendencia ante el Derecho del Trabajo: libertad ideológica y contrato de trabajo", *Revista Proyecto Social*, núm. 2, 1994, p. 178-180.

No se refiere tanto a los datos personales de los cargos representativos, profesionales y trabajadores de partidos políticos, sindicatos o confesiones religiosas, aunque también, como a los datos personales de su militantes, afiliados o miembros de organizaciones de tendencia, así como de terceras personas ajenas con las que se relacionan. Efectivamente, el dato de la afiliación sindical no se podrá facilitar –insistimos– ni siquiera al empleador para solicitar el descuento de la cuota sindical, salvo previo consentimiento para ello del trabajador afiliado (art. 11.2 LOLS)

3.2.5. Los datos personales públicamente manifestados por interesado

En quinto lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos" [art. 9.2.e) RGPD]. Que el dato sea "manifiestamente" público significa que expresa, indudable y visiblemente se quiere revelar, mostrar o dar a conocer ese dato, que con esa acción de su titular sale del ámbito privado o de los confines de su privacidad.

No se encuentra esta circunstancia entre las condiciones de licitud del tratamiento de datos personales (art. 6 RGPD), por lo que no cabe concluir que es una condición intrínseca aplicable a todos los datos personales, sean categorías especiales de datos o no. Reparando en ello, la conclusión debe ser que también, respecto de los datos hechos públicos de manera voluntaria por el interesado, se requiere cumplir una de las condiciones legales, al menos, para que el tratamiento sea lícito[102], por ejemplo, cumplir una obligación legal o que el afectado de su consentimiento expreso, si bien –no hay que olvidarlo– ese consentimiento no es válido para eliminar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico (art. 9.1 LOPDyGDD).

Se puede disponer de la información, es decir, conocer el dato, pero no se permite su tratamiento por el simple hecho de que el interesado lo haya hecho manifiestamente público o expuesto de manera pública. Si, además concurre una causa o condición de licitud *ex* artículo 6.1 RGPD, se admitirá su tratamiento. Sería el caso de exigir al empresario, que pretende despedir disciplinariamente a un trabajador afiliado a un sindicato, el cumplimiento de la obligación legal de dar audiencia previa a los delegados sindicales de la sección sindical correspondiente a dicho sindicato, si bien habrá que probar que le consta esa información (art. 55.1, párrafo cuarto, TRLET). No hay la menor duda, al empresario le consta ese dato si el trabajador afiliado ha consentido el descuento de la cuota sindical, como se ha explicado *ut supra*.

3.2.6. La formulación, el ejercicio o la defensa de reclamaciones o la actuación de los tribunales en el ejercicio de su función jurisdiccional

En sexto lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial" [art. 9.2.f) RGPD]. A título excepcional, igualmente, se autoriza el tratamiento de las categorías especiales de datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial (considerando 52 RGPD).

Al respecto, son de aplicación los preceptos sobre "protección de datos de carácter personal en el ámbito de la Administración de Jus-

[102] Cfr. Dictamen 757/2017, de 26 de octubre de 2017, del Consejo de Estado, sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

ticia", que se incorporaron a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ), por la Ley Orgánica 7/2015, de 21 de julio, con el objetivo de intensificar la protección de datos en el ámbito de los Tribunales, que carecía hasta entonces de una regulación completa y actualizada. En principio, no será necesario el consentimiento del interesado para que los Tribunales procedan al tratamiento de los datos en el ejercicio de la potestad jurisdiccional, ya sean estos facilitados por las partes o recabados a solicitud del propio Tribunal, sin perjuicio de lo dispuesto en las normas procesales para la validez de la prueba[103] (art. 236 quáter LOPJ).

Es de interés esta excepción en las relaciones laborales, por su traslación a los procedimientos de solución judicial o extrajudicial de conflictos, tanto individuales o como colectivos; en particular, también, a los procedimientos de conciliación, mediación o arbitraje[104].

3.2.7. Por motivo de un interés público esencial

En séptimo lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2.g) RGPD]. La excepción viene a delimitar, cuando se tratan categorías especiales de datos, la condición de licitud justificada en "el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" [art. 6.1.e) RGPD].

En todo caso, el tratamiento de las categorías especiales de datos personales por este motivo excepcional –al igual que para los dos siguientes– deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad (art. 9.2 LOPDyGDD). Se consagra, por tanto, el principio de reserva de ley, previsión que no alcanza solo a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto del tratamiento de datos relacionados con la salud y de datos genéticos[105].

Así pues, se pueden igualmente imponer "condiciones especiales"[106] al tratamiento de las categorías especiales de datos –considerados sensibles– sobre esta base jurídica, tales como la adopción de medidas suplementarias de seguridad u otras, cuando ello derive del ejercicio de potestades públicas, que solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable si deriva de una competencia atribuida por la ley. Se pretende, en fin, reforzar la licitud del tratamiento, fijando de manera más precisa requisitos específicos[107] de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo.

---

[103] *Vid.* Castro Argüelles, M. A.: "Los derechos fundamentales inespecíficos en el proceso laboral", en VV.AA.: *Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social*, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Ed. Cinca, Madrid, 2014, pp. 15-17.

[104] Así –*v. gr.*– el procedimiento arbitral obligatorio *ex lege* en materia de elecciones sindicales (art. 76 TRLET).

[105] Cfr. Disposición adicional decimoséptima RGPD.

[106] Cfr. Preámbulo de la LOPDyGDD.

[107] Se habilita formalmente al Derecho de los Estados miembros para introducir disposiciones específicas, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo (art. 6.3 RGPD).

El responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado (considerando 45 RGPD).

Sobre el uso de la videovigilancia con fines de interés público, por ejemplo, "las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones" (art. 22.1 LOPDyGDD).

En el ámbito laboral[108], se permite a los empleadores el tratamiento de las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores previstas en el artículo 20.3 TRLET, "siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo" (art. 89.1 LOPDyGDD). Al respecto, se impone a los empleadores la obligación legal de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores y, en su caso, a sus representantes, acerca de esta medida. De haberse captado la comisión flagrante de un acto ilícito por los trabajadores, se considera cumplido el deber de informar cuando se haya colocado "un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 RGPD" o se incluya en ese dispositivo informativo "un código de conexión o dirección de internet a esta información" (art. 89.2, párrafo segundo, LOPDyGDD, en relación con el art. 22.4 LOPDyGDD).

En ningún caso se admite la instalación de sistemas de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos (art. 89.12 LOPDyGDD).

3.2.8. Fines médicos y sanitarios

En octavo lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario" [art. 9.2.h) RGPD].

Esta excepción únicamente es oponible si el tratamiento de cualquier categoría de dato personal, fundamentalmente –por su contenido– los datos relativos a la salud, es realizado "por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes" (art. 9.3 RGPD). Todos los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase

[108] *Vid.* GOÑI SEIN, J. L.: *La videovigilancia empresarial y la protección de datos personales*, Civitas, Cizur Menor (Navarra), 2007, *passim*. Recientemente, RODRÍGUEZ ESCANCIANO, S.: "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales", *Diario La Ley*, núm. 9328, 2019, pp. 1-9; BAZ RODRÍGUEZ, J.: *Privacidad y protección de datos de los trabajadores en el entorno digital*, *cit*., pp. 191-214; y GARCÍA SALAS, A. I.: "Videovigilancia y control empresarial del trabajador: su regulación en la nueva Ley Orgánica de Protección de Datos", en DE LA PUEBLA PINILLA, A. y MERCADER UGUINA, J. R. (Dirs.): *Tiempo de reformas: en busca de la competitividad empresarial y de la cohesión social*, tirant lo blanch, Valencia, 2019, pp. 537-560.

de este, están sujetas al deber de confidencialidad; obligación que resulta complementaria del deber de secreto profesional exigible en determinadas actividades profesionales.

Ese deber de secreto sobre la información médica del trabajador incumbe al personal y a las autoridades sanitarias que conocen los resultados –datos personales relativos a la salud– de la vigilancia de la salud (art. 22.4, párrafo segundo, LPRL); secreto que se proyecta frente al resto de personas relacionadas, directa o indirectamente, con dicha obligación preventiva y también respecto de terceros[109]. Deber de secreto, en fin, que se extiende sobre los resultados y sobre todo aquello que el trabajador haya confiado[110] al personal responsable o que este haya conocido con ocasión del desarrollo de sus funciones[111].

3.2.9. Razones de interés público en el ámbito de la salud pública

En noveno lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional" [art. 9.2.i) RGPD].

El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública, pero siempre sujeto a medidas adecuadas y específicas con el fin de proteger los derechos y libertades de las personas físicas (considerando 54 RGPD). En ese contexto, "salud pública" debe interpretarse según la definición del Reglamento núm. 1338/2008/CE, de 16 de diciembre, del Parlamento Europeo y del Consejo, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo: "todos los elementos relacionados con la salud, a saber, el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad" [art. 3.c) Reglamento núm. 1338/2008/CE].

Recalcamos que este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como los empresarios, traten los datos personales con otros fines.

A nivel estatal, la Ley 33/2011, de 4 de octubre, general de salud pública, establece que "las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población", quedando obligadas las personas públicas o privadas a ceder a la autoridad sanitaria, cuando así se las requiera, "los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública, de conformidad con lo establecido en la LO 15/1999, de 13 de diciembre, de protección de

[109] *Vid.* PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *cit.*, p. 171.

[110] Como señala SÁNCHEZ TORRES, E.: "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales", *Relaciones Laborales*, T. II, 1997, p. 113, la comunicación de ciertos hábitos –consumo de drogas– o comportamientos –actividad sexual– personales.

[111] Sobre el secreto médico, extensamente, FERNÁNDEZ-COSTALES MUÑIZ, J.: "El secreto médico profesional y el deber de sigilo de los delegados de prevención en el ámbito del tratamiento y protección de datos de la salud", *Revista Técnico Laboral*, núm. 133, 2012, pp. 360-373.

datos de carácter personal –entiéndase la referencia hecha a la LO 3/2018–" (art. 41.2 y 3 Ley 33/2011).

En consecuencia, el legislador no ha previsto que todo tipo de dato personal relacionado con la salud pueda ser –libremente y sin restricciones– cedido o transmitido entre administraciones públicas, sino exclusivamente por razones imprescindibles, de modo que no será necesario el consentimiento de las personas afectadas para la cesión de datos personales relacionados con la salud por razones de salud pública o por razones epidemiológicas[112].

3.2.10. Otros fines: archivo en interés público, investigación científica o histórica y estadísticos

Finalmente y en décimo lugar, la prohibición de tratamiento de cualquier categoría especial de dato personal no se aplica cuando "el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2.j) RGPD].

Dos precisiones iniciales. Una, primera, el tratamiento de datos personales con fines de investigación científica debe interpretarse de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado; entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública (considerando 159 RGPD) o, en general, en la investigación en salud (disp. adic. decimoséptima LOPDyGDD).

Otra, segunda, por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos; por cierto, los resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica (considerando 162 RGPD). El resultado del tratamiento con fines estadísticos no puede alumbrar datos personales, sino datos agregados, sin que el resultado o los datos personales se puedan utilizar para respaldar medidas o decisiones relativas a personas físicas concretas.

El tratamiento de datos personales con tales fines está supeditado a unas garantías adecuadas para los derechos y libertades del interesado, aplicando medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos, atendiendo a los principios de proporcionalidad y necesidad (considerando 156 RGPD).

Se permite el tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siempre que el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas, como, por ejemplo, la "seudonimización" de datos.

Corresponde a los Estados miembros establecer esas garantías adecuadas, bajo condiciones y procedimientos específicos, para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, sin que, en caso de que el tratamiento sirva también, al mismo tiempo, a otro fin, sea aplicable la excepción (art. 89.3 y 4 RGPD).

[112] Cfr. Informe 0121/2018 del Gabinete Jurídico de la AEPD, sobre la legitimación para el tratamiento de datos en materia de salud pública.

Pueden ser relevantes, respecto de la actividad laboral, el tratamiento de algunas categorías especiales de datos personales, de manera singular los datos relativos a la salud, cuando se realicen estudios de investigación científica o puramente estadísticos sobre enfermedades profesionales o sobre las consecuencias para la salud o la integridad física de los accidentes de trabajo. Asimismo, otros estudios de investigación histórica o estadísticos sobre la afiliación sindical, dado el importante rol constitucional que desempeñan los sindicatos en un sistema democrático (arts. 7 y 28.1 CE).

3.3. Obligaciones en el tratamiento de categorías especiales de datos

En el articulado del Reglamento europeo se recogen algunas obligaciones que afectan exclusivamente a los responsables y encargados del tratamiento de cualquier dato personal que pertenezca a las categorías especiales de datos. Se exponen, a continuación, algunas.

Como pauta general, todo interesado tiene derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, excepto si la decisión (i) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, (ii) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o (iii) se basa en el consentimiento explícito del interesado. Pues bien, esas excepciones a aquella primera regla general "no se basarán en las categorías especiales de datos personales" contempladas en artículo 9.1 RGPD, salvo que se aplique el artículo 9.2, letras a) –consentimiento explícito del interesado– o g) –el tratamiento es necesario por razones de interés púbico esencial–, y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado (art. 22.4 RGPD).

Sobre el registro de actividades de tratamiento y las obligaciones que se establecen *ex lege*, no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, excepto si el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o "incluya categorías especiales de datos personales", o datos personales relativos a condenas e infracciones penales (art. 30.5 RGPD).

En cuanto a la obligación de realizar una evaluación[113] del impacto de las operaciones de tratamiento en la protección de datos personales por parte del responsable, dicha evaluación se exige cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas y –en particular– siempre que se lleve a cabo un "tratamiento a gran escala de las categorías especiales de datos" (art. 35.3 RGPD).

Por último, el responsable y el encargado del tratamiento han de designar un delegado de protección de datos siempre que las actividades principales de aquellos "consistan en el tratamiento a gran escala de categorías especiales de datos personales", o datos personales relativos a condenas e infracciones penales [art. 37.1.c) RGPD].

[113] En la evaluación se debe hacer referencia a las operaciones de tratamiento previstas, a la necesidad y proporcionalidad de dichas operaciones, a los riesgos para los derechos y libertades de los interesados y a las medidas previstas para hacer frente a dichos riesgos. *Vid.* PRECIADO DOMÈNECH, C. H.: *El derecho a la protección de datos en el contrato de trabajo*, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017, pp. 150 y ss.

4. A MODO DE VALORACIÓN ÚLTIMA: SOBRE LAS GARANTÍAS MÁS INTENSAS EN EL TRATAMIENTO DE DATOS SENSIBLES DEL TRABAJADOR QUE SE RECONOCEN *EX LEGE* COMO CATEGORÍAS ESPECIALES DE DATOS

Hay una nítida línea de continuidad en el régimen jurídico que se viene aplicando a determinados datos personales del interesado, el trabajador que se convierte en titular del amplio conjunto de garantías delineado por la normativa –internacional, comunitaria y nacional– sobre protección de datos. Llámense –como antes– "categorías especiales de datos" (art. 8 Directiva 95/46/CE) por ser "datos especialmente protegidos" (art. 7 LO 15/1999), o –como ahora– "categorías especiales de datos", sin más precisiones (art. 9 RGPD y, también, LOPDyGDD), lo cierto es que han merecido especial protección aquellos datos personales que, por su naturaleza o su contenido, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que su tratamiento por el empleador u otro responsable puede suponer notables riesgos para esos derechos y las libertades fundamentales.

Ante todo, con su identificación se quiere impedir cualquier efecto discriminatorio sobre las personas físicas, desde la perspectiva de nuestro análisis en los trabajadores, por motivos de raza u origen étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, condición genética, estado de salud u orientación sexual. De ahí que el tratamiento de esos datos, las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deban permitirse en condiciones específicas o tratándose de categorías especiales de datos personales sencillamente no puedan ser autorizadas, salvo excepciones acotadas por el legislador.

Con ocasión de la revisión de la normativa sobre protección de datos personales, primero a nivel europeo y seguidamente a nivel estatal, las categorías especiales de datos personales han merecido un mayor grado de atención, con la finalidad de otorgarles una más y mejor protección cuando se permita su tratamiento, pues la base de su tutela es que tales datos personales no deben ser tratados, a menos que se permita su tratamiento en supuestos o ante circunstancias tasadas, sobre el consentimiento del titular o la concurrencia de otros derechos o intereses merecedores de ser atendidos o preservados. De máxima trascendencia en el tratamiento de las categorías especiales de datos es que, además de los requisitos específicos, deben aplicarse los principios generales relativos al tratamiento de los datos personales y otras reglas comunes, pero sobre todo las condiciones generales de licitud.

A la prohibición general de tratamiento de esas categorías especiales de datos, se enlazan, de forma explícita y muy delimitada, supuestos en los que excepcionalmente decae aquella limitación. Se puede calificar como prohibición relativa, al ser numerosas las hipótesis que habilitan el tratamiento, ciertamente encadenadas algunas a lo dispuesto en el Derecho de la Unión Europea o, principalmente, en el Derecho de los Estados miembros, y ello porque, según los datos a tratar o los supuestos, se reenvía a los ordenamientos nacionales para introducir condiciones adicionales, incluso limitaciones, pero siempre con la finalidad de establecer medidas adecuadas y específicas para proteger los intereses, derechos y libertades de la persona.

Precisamente el tratamiento en el ámbito laboral, permite a los legisladores estatales, bien en las disposiciones legislativas, bien en los convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguri-

dad en el trabajo, protección de los bienes de empleados o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral (art. 88.1 RGPD). Normas que incluirán medidas adecuadas y singulares para preservar la dignidad humana de los interesados, así como sus intereses legítimos y sus derechos y libertades fundamentales, prestando especial atención a la transparencia del tratamiento.

En el ejercicio de esa competencia reguladora, se impone que el solo consentimiento del trabajador no sirve para remover la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico (art. 9.1 LOPDyGDD), si bien se permite el tratamiento de los referidos datos personales al amparo de los restantes supuestos, por ejemplo, cuando el interesado ha hecho manifiestamente públicos alguno de esos datos o, inclusive, cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea en un procedimiento judicial o en un procedimiento administrativo o extrajudicial.

Uno de los datos que se reconoce como categoría especial, la afiliación sindical, y, al menos, dos circunstancias, de un resultado de diez, se presentan con una clara vinculación: el tratamiento de la afiliación sindical se permite cuando sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en tanto así lo autorice el Derecho de la Unión, el Derecho de los Estados miembros o un convenio colectivo, siempre que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del trabajador; también cuando sea efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por la organización sindical, siempre que el tratamiento se refiera exclusivamente a sus miembros actuales o antiguos, quedando prohibía su comunicación externa sin el consentimiento del interesado.

Otros datos, los relativos a la salud y, al menos, cuatro circunstancias, del total de listadas, presentan una evidente conexión: el tratamiento de los datos sobre la salud –en sentido amplio– del trabajador cuando sea necesario para proteger sus intereses vitales, cuando sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, cuando se necesario por razones de interés público en el ámbito de la salud pública y cuando resulte necesario con fines de investigación científica.

Pero no solo esas categorías especiales de datos y esas circunstancias que permiten su tratamiento, de igual manera otros datos personales merecen la tutela intensificada del legislador respecto de su tratamiento a fin de evitar situaciones discriminatorias y las mismas u otras circunstancias excepcionales posibilitarán su tratamiento, también con una incidencia, no meramente tangencial, en las relaciones de trabajo, más en el contexto de la creciente utilización de las nuevas tecnologías en la empresa al servicio de los poderes de dirección y control atribuidos al empleador.

BIBLIOGRAFÍA

ALBERT, M.: "Convicciones religiosas y elecciones personales: derecho a la objeción de conciencia y autodeterminación individual en la jurisprudencia del Tribunal Europeo de Derechos Humanos", Revista Persona y Derecho, núm. 77, 2017.

ÁLVAREZ GONZÁLEZ, S.: "Derecho a la «privacidad» e información genética", en ÁLVAREZ GONZÁLEZ, S. y GARRIGA DOMÍNGUEZ, A. (Dirs.): Un nuevo reto para los derechos fundamentales: los datos genéticos, Dykinson, Madrid, 2017.

APARICIO TOVAR, J.: "Relación de trabajo y libertad de pensamiento en las empresas ideológicas", en VV.AA.: Derecho del Trabajo en homenaje a los profesores BAYÓN CHACÓN y DEL PESO CALVO, Universidad Complutense, Madrid, 1980.

BAZ RODRÍGUEZ, J.: Privacidad y protección de datos de los trabajadores en el entorno digital, Bosch Wolters Kluwer, Barcelona, 2019.

BLASCO PELLICER, A.: "El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador", en BORRAJO DACRUZ, E. (Dir.): Trabajo y libertades públicas, La Ley, Madrid, 1999.

CASTRO ARGÜELLES, M. A.: "Los derechos fundamentales inespecíficos en el proceso laboral", en VV.AA.: Los derechos fundamentales inespecíficos en la relación laboral y en materia de protección social, XXIV Congreso Nacional de Derecho del Trabajo y de la Seguridad Social, Ed. Cinca, Madrid, 2014.

CHACARTEGUI JÁVEGA, C.: Discriminación y orientación sexual del trabajador, Lex Nova, Valladolid, 2001.

CLAYTON, E. W., EVANS, BARBARA J., HAZEL, JAMES W. y ROTHSTEIN, MARK A.: "The law of genetic privacy: applications, implications, and limitations", Journal of Law and the Biosciences, vol. 6, núm. 1, 2019 (https://academic.oup.com/jlb/article/6/1/1/5489401).

CRUZ VILLALÓN, J.: Protección de datos personales del trabajador en el proceso de contratación: facultades y límites a la actuación del empleador, Bomarzo, Albacete, 2019.

DE VAL TENA, A. L.: "Las empresas de tendencia ante el Derecho del Trabajo: libertad ideológica y contrato de trabajo", Revista Proyecto Social, núm. 2, 1994.

DEL REY GUANTER, S.: "Tratamiento automatizado de datos de carácter personal y contrato de trabajo (Una aproximación a la «intimidad informática» de trabajador)", Relaciones Laborales, T. II, 1993.

FERNÁNDEZ-COSTALES MUÑIZ, J.: "El secreto médico profesional y el deber de sigilo de los delegados de prevención en el ámbito del tratamiento y protección de datos de la salud", Revista Técnico Laboral, núm. 133, 2012.

GARCÍA MURCIA, J.: "Derecho a la intimidad y contrato de trabajo: la anotación de las bajas médicas (Comentario a la STC 202/1999, de 8 de noviembre)", Repertorio Aranzadi del Tribunal Constitucional, núm. 2, 2000.

GARCÍA MURCIA, J.: "El hecho sindical. La mayor representatividad. Asociacionismo profesional y empresarial. Balance y propuestas de reforma", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. 429, 2018.

GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito de trabajo: una aproximación desde el nuevo marco normativo", Nueva Revista Española de Derecho del Trabajo, núm. 216, 2019 (BIB 2019\1432).

GARCÍA SALAS, A. I.: "Videovigilancia y control empresarial del trabajador: su regulación en la nueva Ley Orgánica de Protección de Datos", en DE LA PUEBLA PINILLA, A. y MERCADER UGUINA, J. R. (Dirs.): Tiempo de reformas: en busca de la competitividad empresarial y de la cohesión social, tirant lo blanch, Valencia, 2019.

GÓMEZ SÁNCHEZ, Y.: "La protección de los datos genéticos: el derecho a la autodeterminación informativa", Derecho y Salud, vol. 16, núm. extraordinario 1, 2008.

GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y de archivo de datos", en ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA R. (Coords.): Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo, Bomarzo, Albacete, 2004.

GOÑI SEIN, J. L.: La videovigilancia empresarial y la protección de datos personales, Civitas, Cizur Menor (Navarra), 2007.

GOÑI SEIN, J. L.: "Intimidad del trabajador y poderes de vigilancia y control empresarial", en GARCÍA MURCIA, J. (Coord.): Jornada sobre derechos fundamentales y contrato de trabajo, Principado de Asturias, Oviedo, 2017.

GOÑI SEIN, J. L.: La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa (incluido el Real Decreto-Ley 5/2018), Bomarzo, Albacete, 2018.

LACADENA, J. R.: "Individualización y mismidad genética en el desarrollo humano", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): Gen-Ética, Ariel, Barcelona, 2003.

LEWIS R.: Human Genetics: Concepts and Applications, 12ª ed., McGraw-Hill Science, NewYork (EE.UU.), 2017.

LÓPEZ ÁLVAREZ, L. F.: Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo, Francis Lefebvre, Madrid, 2016.

LUCAS MURILLO DE LA CUEVA, P.: Informática y protección de datos personales, Centro de Estudios Constitucionales, Madrid, 1993.

MERCADER UGUINA, J. R. y DE LA PUEBLA PINILLA, A.: "Protección de datos y relaciones colectivas", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. 423, 2018.

MERCADER UGUINA, J. R.: "El mercado de trabajo y el empleo en un mundo digital", Información Laboral, núm. 11, 2018 (BIB 2018/ 13994).

MERCADER UGUINA, J. R.: "La protección de datos personales del trabajador. La obligación del empresario de informar al trabajador sobre sus condiciones de trabajo", en CASAS BAAMONDE, M. E. y GIL ALBURQUERQUE, R. (Dirs.): Derecho Social de la Unión Europea. Aplicación por el Tribunal de Justicia, Francis Lefebvre, Madrid, 2018.

MERCADER UGUINA, J. R.: Protección de datos y garantía de los derechos digitales en las relaciones laborales, 3ª ed., Francis Lefebvre, Madrid, 2019.

MERCADER UGUINA, J. R.: "Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre: una aproximación desde la protección de datos", Trabajo y Derecho, núm. 52, 2019.

MIÑARRO YANINI, M.: "Implicaciones laborales del Reglamento comunitario de protección de datos: principales puntos críticos", en GARCÍA MAHAMUT, R. y TOMÁS MALLÉN, B. (Edits.): El Reglamento General de Protección de Datos, tirant lo blanch, Valencia, 2019.

MOLINA NAVARRETE, C.: "La «gran transformación» digital y bienestar en el trabajo: riesgos emergentes, nuevos principios de acción, nuevas medidas preventivas", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. extraordinario 1, 2019.

PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", Revista del Ministerio de Trabajo, Migraciones y Seguridad Social, núm. 138, 2018.

POQUET CATALÁ, R.: El actual poder de dirección y control del empresario, Cuadernos de Aranzadi Social, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2013.

PRECIADO DOMÈNECH, C. H.: El derecho a la protección de datos en el contrato de trabajo, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2017.

RODRÍGUEZ ESCANCIANO, S.: "El derecho a la protección de datos personales en el contrato de trabajo: reflexiones a la luz del Reglamento europeo 2016/679", Revista de Trabajo y Seguridad Social, Centro de Estudios Financieros, núm. 423, 2018.

RODRÍGUEZ ESCANCIANO, S.: "Videovigilancia empresarial: límites a la luz de la Ley Orgánica 3/2018, de 5 diciembre, de protección de datos personales y garantía de los derechos digitales", Diario La Ley, núm. 9328, 2019.

RODRÍGUEZ ESCANCIANO, S.: Derechos laborales digitales: garantías e interrogantes, Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2019.

ROMEO CASABONA, C. M.: Los genes y sus leyes. El derecho ante el genoma humano, Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, Comares, Granada, 2002.

ROMEO CASABONA, C. M.: "El tratamiento y la protección de los datos genéticos", en MAYOR ZARAGOZA, F. y ALFONSO BEDATE, C. (Coords.): Gen-Ética, Ariel, Barcelona, 2003.

SÁNCHEZ TORRES, E.: "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales", Relaciones Laborales, T. II, 1997.

SERRANO GARCÍA, J. M.: La protección de datos y la regulación de las tecnologías en la negociación colectiva y en la jurisprudencia, Bomarzo, Albacete, 2019.

TASCÓN LÓPEZ, R.: El tratamiento por la empresa de datos personales de los trabajadores. Análisis del estado de la cuestión, Civitas, Madrid, 2005.

TRONCOSO REIGADA, A.: "La protección de datos personales en el ámbito laboral", en VV.AA.: La protección de datos personales en busca del equilibrio, tirant lo blanch, Valencia, 2010.

VALDÉS DAL-RE, F.: "Doctrina constitucional en materia de videovigilancia y utilización del ordenador por el personal de la empresa", Revista de Derecho Social, núm. 79, 2017.

VALDÉS DAL-RE, F.: "Nuevas tecnologías y derechos fundamentales de los trabajadores", Derecho de las Relaciones Laborales, núm. 2, 2019.

RESUMEN

La rápida evolución tecnológica ha planteado nuevos retos para la protección de los datos personales. Sin duda, la tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades, y ha de facilitar aún más la libre circulación de datos personales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

A nivel europeo, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. La Carta de los Derechos Fundamentales de la Unión Europea (art. 8.1) y el Tratado de Funcionamiento de la Unión Europea (art. 16.1) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

No obstante, el derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión Europea y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, ha sido necesario un Reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento. Por ello, se ha aprobado el Reglamento 2016/679/UE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

Dicho Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos, protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales. Se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

Al respecto, se considera "datos personales" toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; y "tratamiento", cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Entre los datos personales, especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. En verdad, la norma europea regula el tratamiento de las categorías especiales de datos ("datos sensibles"). Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca

a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas. Pero, además de los requisitos singulares de ese tratamiento, deben aplicarse los principios generales y otras normas del Reglamento europeo, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento.

Las excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales son:

a) El interesado ha dado su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada no puede ser levantada por el interesado. Precisamente, la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, establece que el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas, la afiliación sindical o la orientación sexual.

b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión, de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.

c) El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

d) El tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados.

e) El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

f) El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial.

g) El tratamiento es necesario por razones de un interés público esencial.

h) El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.

i) El tratamiento es necesario por razones de interés público en el ámbito de la salud pública.

j) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Se estudia, por un lado, el concepto de cada una de las categorías especiales de datos personales y, por otro, las excepciones a la prohibición general de tratar.

Palabras clave: Datos personales; categorías especiales de datos; origen étnico o racial; opiniones políticas; convicciones religiosas o filosóficas; afiliación sindical; datos genéticos; datos biométricos; datos relativos a la salud; orientación sexual; tratamiento de categorías especiales de datos.

ABSTRACT Rapid technological developments have brought new challenges for the protection of personal data. No doubt, technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities, and should further facilitate the free flow of personal data, while ensuring a high level of the protection of personal data.

At the European Union level, the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provides that everyone has the right to the protection of personal data concerning him or her.

Nevertheless, the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality

In order to ensure a consistent level of protection for natural persons throughout the European Union and to prevent divergences hampering the free movement of personal data within the internal market, a Regulation is necessary to provide legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and to provide natural persons in all Member States with the same level of legally enforceable rights and obligations and responsibilities for controllers and processors. For this reason, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, has been adopted, which repeals Directive 95/46/EC.

This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing of other not by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

In this regard, “personal data” means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; and “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Indeed, the European standard regulates the processing of special categories of personal data (“sensitive data”). Those personal data should include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited.

Such personal data should not be processed, unless processing is allowed in specific cases. But, in addition to the specific requirements for such processing, the general principles

and other rules of this Regulation should apply, in particular as regards to the conditions for lawful processing. The derogations from the general prohibition for processing such special categories of personal data are:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where the European Union or Member State law provides that the prohibition referred may not be lifted by the data subject. Precisely, Organic Law 3/2018, of 5 December, on the protection of personal data and guarantee of digital rights, establishes that the only consent of the affected party will not be enough to lift the prohibition on the processing of data whose disclosure racial or ethnic origin, political opinions, religious beliefs, trade union membership, or sexual orientation.

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by the European Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

(e) Processing relates to personal data which are manifestly made public by the data subject.

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) Processing is necessary for reasons of substantial public interest.

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

(i) Processing is necessary for reasons of public interest in the area of public health.

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

On one hand, this paper analyses the concept of each of the special categories of personal data and, on the other hand, the derogations from the general prohibition on processing special categories of personal data.

Keywords: Personal data; special categories of personal data; racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health data; sexual orientation; processing of special categories of personal data.