CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS EN LA VIGILANCIA DE LA SALUD DE LOS TRABAJADORES: BASES PARA UNA PREVENCIÓN DE CALIDAD

Núm. 21/2004

SONIA ISABEL PEDROSA ALQUÉZAR

Profesora Ayudante de Derecho del Trabajo y de la Seguridad Social. Universidad de Zaragoza

Extracto:

TOMANDO como punto de referencia la Ley de Prevención de Riesgos Laborales (LPRL) y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), este trabajo quiere poner de manifiesto qué supone el principio de confidencialidad en relación con los datos derivados de la medida preventiva de vigilancia de la salud, principio corolario de otros como el de finalidad, veracidad o conservación limitada, de derechos tales como el de información sobre el tratamiento de esos datos, acceso, cancelación o rectificación, o de medidas de seguridad imprescindibles con los avances de las nuevas tecnologías, que hacen posible una vigilancia de la salud de calidad informatizada, y son base de la protección de un nuevo derecho con sustantividad propia: el derecho a la libertad frente a las potenciales agresiones a la intimidad, la dignidad de la persona y otros derechos provenientes del uso ilegítimo del tratamiento automatizado de datos.

Sumario:

I. INTRODUCCIÓN

La vigilancia de la salud puede definirse como un instrumento parte de un sistema de prevención cuyo objetivo es detectar los problemas de salud físicos y psíquicos que el trabajo puede generar en la salud de quienes lo desempeñan.

Su base jurídica se encuentra, fundamentalmente, en los artículos 14 y 22 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales (LPRL) [1] –regulándola como un derecho del trabajador y un deber del empresario–, 37 del Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención [2] (RSP) y en diversos Reglamentos sobre riesgos específicos.

El mecanismo utilizado por este instrumento preventivo es el de los exámenes de salud consistente en pruebas de diversa índole capaces de detectar alguna anomalía en el bienestar del trabajador. Estas pruebas deben estar relacionadas con los riesgos existentes en el concreto puesto de trabajo y practicarse respetando los derechos fundamentales del trabajador –dignidad, intimidad y no discriminación señala específicamente la LPRL–. Los encargados de la misma, aunque la obligación sea de la empresa, van a ser, conforme a las prescripciones del RSP, médicos y enfermeros especialistas en Medicina o Enfermería de empresa –ayudados por auxiliares clínicos y personal administrativo si se cree conveniente– y, aunque la normativa de prevención de riesgos no se manifieste al respecto, parece que debería entenderse que la práctica de una vigilancia de la salud de carácter psicológico debería llevarse a cabo por personal especializado en Psicología o Sociología Industrial.

Todos ellos forman parte de un servicio de prevención como órgano encargado de organizar y gestionar las actividades preventivas en la empresa que puede ser de tres clases: propio, creado por la propia empresa de la que formarán parte sus trabajadores (arts. 14 y 15 del RSP); externo, como empresa a la que recurre aquella que necesita la organización y gestión de la prevención (arts. 16 a 20 RSP); y mancomunado, cuyo régimen jurídico se asimila al propio pero que se crea entre varias empresas con características comunes como desarrollar simultáneamente actividades en un mismo centro de trabajo, edificio o centro comercial (art. 21 RSP).

1 BOE de 10 de noviembre.

2 BOE de 31 de enero.

El sometimiento a esta vigilancia es, en principio, voluntario para el trabajador salvo que se dé alguno de los supuestos de obligatoriedad regulados en el artículo 22.1 de la LPRL: 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 la salud del trabajador puede constituir un peligro para él mismo, para los demás trabajadores o para otras personas relacionadas con la empresa –en estos dos casos previo informe de los representantes de los trabajadores–, o cuando así esté establecido en una disposición legal en relación con la protección de riesgos y actividades de especial peligrosidad.

Sobre la base de estas ideas genéricas, este trabajo quiere poner de manifiesto, tomando en consideración la LPRL y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [3] (LOPD), qué supone el principio de confidencialidad en relación con la medida preventiva de vigilancia de la salud cuyo respeto va a coadyuvar al logro de un sistema preventivo empresarial de calidad.

II. LA CONFIDENCIALIDAD COMO PRINCIPIO IMPRESCINDIBLE EN LA ELABORACIÓN, TRATAMIENTO Y COMUNICACIÓN DE LOS DATOS RELACIONADOS CON LA VIGILANCIA DE LA SALUD

Sin duda uno de los principios fundamentales de un sistema adecuado de tratamiento de datos es que consiga un escrupuloso respeto a la confidencialidad de los mismos, en la medida en que ésta forma parte inescindible del derecho a la intimidad, y se cree siguiendo las prescripciones de la normativa de protección de datos.

1. La comunicación de los datos.

El derecho a la intimidad supone, en general, la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás que, por un lado, implica la exclusión del conocimiento ajeno de cuanto hace referencia a la propia persona y, por otro, el control por su titular de los datos e información relativos a sí mismo [4]. Estos aspectos se concretan, en el ámbito de la vigilancia de la salud, en el contenido de sus exámenes que deberán realizarse de forma y con medios que no supongan una intrusión no razonable en la vida privada o íntima del trabajador, y en la exigencia

[3] BOE de 14 de diciembre.

[4] Por todas, STC 142/1993, de 22 de abril (BOE de 28 de mayo), donde se pone de manifiesto que «el atributo más importante de la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos».

de confidencialidad sobre los datos obtenidos en la práctica de los mismos a las personas encargadas de su realización –y también a la empresa y otros sujetos con responsabilidades preventivas– sólo revelables cuando exista un interés legítimo [5].

El respeto a la intimidad a través de la confidencialidad de los datos obtenidos en el examen de salud va a colisionar con el derecho a la información que tiene la empresa respecto de esos datos para cumplir con su obligación preventiva, de ahí que la LPRL articule mecanismos de equilibrio entre ambos derechos [6] garantizando la intimidad de los trabajadores, pero, a su vez, las exigencias de protección de la salud individual, colectiva y de terceros relacionados con la empresa a través del derecho a la información que, como expresa el artículo 20.4 de la CE, tiene su límite en el respeto, especialmente, al derecho al honor, a la intimidad y a la propia imagen, límite que el Tribunal Constitucional ha hecho recíproco [7].

Que un dato sea confidencial supone su reservabilidad, el mantenimiento en secreto hacia personas que no tienen un interés legítimo en su conocimiento. El artículo 22 de la LPRL distingue varios tipos de datos o, más correctamente, documentación de datos estructurados en función de dos fines diferentes, y con una distinta exigencia de confidencialidad. Para los resultados de la vigilancia la confidencialidad es máxima –sólo modulable por el consentimiento expreso del trabajador o un interés legítimo como el perjuicio para terceros–, mientras que para las conclusiones la confidencialidad es mínima por el tipo de datos que incorporan y la mayor cantidad de sujetos a los que se comunican, bien entendido que en ninguno de los dos casos debe trascender de la empresa o de los sujetos –incluida la Administración sanitaria– con responsabilidades en materia de prevención.

Efectivamente, el artículo 22 de la LPRL después de establecer el principio de confidencialidad, como manifestación del derecho a la intimidad, en los datos derivados de la práctica de la salud, lo modula en función de la documentación de esos datos según esté articulada en forma de resultados o en forma de conclusiones.

1.1. Resultados.

Los resultados de la vigilancia de la salud son los documentos que contienen los datos personales referidos a la salud del trabajador derivados de la práctica de las diferentes pruebas a las que ha sido sometido para detectar el efecto que los riesgos de su puesto de trabajo provocan en su salud.

---

5 *Vid.* artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE de 14 de mayo).

6 Pues se trata de conseguir una «tutela de la salud» y no un «poder sobre la salud» (CIACCI, G.: «Problemi e iniziative in tema di tutela dei dati personali, con particolare riguardo ai dati sanitari», *Política del Diritto*, núm 4, 1991, pág. 690).

7 *Vid.*, para esta reciprocidad de límites, las sentencias recogidas en LACRUZ BERDEJO, J.L.; SANCHO REBULLIDA, F.; LUNA SERRANO, A.; DELGADO ECHEVERRÍA, J.; RIVERO HERNÁNDEZ, F.; RAMS ALBESA, J.: *Elementos de Derecho Civil I. Parte General. Volumen Segundo. Personas*, Madrid, Dykinson, 2001, págs. 81-108. También, el Capítulo IV –Buena Fe y Libertades de Expresión e Información en la Jurisprudencia del Tribunal Constitucional– de la monografía de NARANJO DE LA CRUZ, R.: *Los límites de los derechos fundamentales en las relaciones entre particulares: la buena fe.* Madrid, BOE-Centro de Estudios Políticos y Constitucionales, 2000, págs. 325-447.

La LPRL se refiere a ellos en su artículo 22.3 y, también, en el artículo 22.4.2.º párrafo, con los términos información médica –se entiende también la referida a los exámenes de salud psico–social– de carácter personal. Deben incorporar el diagnóstico, pronóstico, y, en su caso, el tratamiento que debe seguir el trabajador o la remisión a su Médico de familia o especialista, así como todos los aspectos relacionados con su puesto de trabajo o actividad con precisión y claridad [8] poniendo de manifiesto si la alteración de su salud tiene origen laboral, si puede verse agravada como consecuencia de las funciones que desempeña o si su estado de salud le impide o dificulta el normal desarrollo de su actividad laboral, afecta a otros trabajadores o a otras personas en la empresa [9]. Además la información podrá ser continuada si el trabajador está sujeto a tratamiento o a período de observación [10].

Entiendo, así, que esta información médica de carácter personal –que identifico con el contenido de los resultados– incluye tanto información sobre salud que tenga que ver con el puesto de trabajo como aquella que no la tiene pero ha surgido de la práctica del examen de salud y opto, de esta forma, por una acepción amplia del término información médica de carácter personal a diferencia de otros autores como FERNÁNDEZ DOMÍNGUEZ y RODRÍGUEZ ESCANCIANO que consideran que la acepción información médica de carácter personal sólo se refiere a los datos relativos a la salud del trabajador «detectados en un reconocimiento médico que poca o ninguna relación tuvieran con la actividad laboral por él desarrollada o con el riesgo derivado de su trabajo (tal sería el caso de defectos congénitos o enfermedades comunes), los cuales, en consecuencia, deben quedar preservados de cualquier injerencia salvo la del personal médico asistencial encargado de velar por la salud del trabajador y las autoridades sanitarias» [11].

Cosa distinta es que, a partir de esa información, tengan que extraerse unas conclusiones en relación, única y exclusivamente, con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de mejorar o introducir medidas de prevención o protección. Conclusiones para las que, como se ha adelantado, la LPRL relaja la exigibilidad de confidencialidad porque, efectivamente, convertirán una parte de la información médica personal en información pública o, más correctamente, en «colectiva limitada» para que no se conozcan los datos más íntimos sobre la salud.

Así, cuando el artículo 22 se refiere a la información médica de carácter personal se está refiriendo a los resultados que derivan de la práctica de esa vigilancia que, por pertenecer a la esfera íntima del trabajador en cuanto se refieren a su salud, son sólo accesibles para el personal médico o autoridades sanitarias que han llevado a cabo la vigilancia. Para elaborar las conclusiones, que se entregarán al empresario con el fin de que cumpla correctamente con su obligación preventiva, se

8 SEMPERE NAVARRO, A.; GARCÍA BLASCO, J.; GONZÁLEZ LABRADA, M.; CARDENAL CARRO, M.: *Derecho de la Seguridad y salud en el trabajo*, Madrid, Civitas, 2001, pág. 226.

9 BLASCO PELLICER, A.: «El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador», VV.AA., BORRAJO DACRUZ, E. [Dir.]: *Trabajo y Libertades Públicas*, Madrid, La Ley-Actualidad, 1999, pág. 274.

10 Ibídem.

11 FERNÁNDEZ DOMÍNGUEZ, J.J.; RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Madrid, Agencia de Protección de Datos, 1997, pág. 200. En sentido similar, PURCALLA BONILLA, M.A.: «Vigilancia de la salud de los trabajadores: claves interpretativas de su régimen jurídico», *Aranzadi Social*, volumen V, 1997, pág. 703.

utilizará –pero no se incorporará– lo más relevante de esa información médica en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o para adoptar medidas de protección o prevención más eficaces.

Estos resultados deberían ser comunicados al trabajador directamente por los miembros del Servicio de Prevención con el que la empresa tenga concertada o contratada la práctica de esta medida preventiva. Deben entregarse por escrito, con exclusión de las posibles anotaciones subjetivas que se hayan realizado en el transcurso de la práctica de la vigilancia, en la medida en que las mismas forman parte –como pone de manifiesto el art. 18.3 de 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 [12]– del derecho a la intimidad del médico o, en este caso, también del psicólogo o sociólogo. Deberá entregarse en sobre cerrado para evitar cualquier atentado a la confidencialidad, permitiendo la atención posterior a su conocimiento para la resolución de cualquier duda al respecto. Además, también deberán comunicarse de palabra, cumpliendo con los principios éticos de actuación recogidos en los diversos Códigos Deontológicos de los profesionales intervinientes en la vigilancia de la salud, cuando se haga necesario por la especial trascendencia de los resultados [13]. Así, puede hacerse personalmente, si se hace necesario, o enviando al trabajador los datos por correo especificando en el sobre el carácter confidencial de la información y con el sello del servicio de prevención.

Con el avance de las nuevas tecnologías, si se adoptan las medidas necesarias para garantizar el respeto a la confidencialidad e integridad de esos datos –medidas que se analizarán posteriormente–, podrían comunicarse los resultados por correo electrónico o dejarlos archivados en una página de Internet facilitando al trabajador una clave o la posibilidad de que él mismo pudiera crearse esa clave con la que pudiera tener acceso a ellos.

Ahora bien, el sobre cerrado y sellado en su apertura por el servicio de prevención en el que expresamente figure la palabra «confidencial» parece que garantiza de forma más eficaz la confidencialidad que unas claves informáticas que expertos afines a la empresa podrían descifrar.

No obstante estas garantías del soporte papel, debería evitarse que los sobres fueran remitidos a la empresa y ésta los distribuyera directamente a sus trabajadores. Es preferible optar por el envío directo a cada uno de ellos dentro de la empresa o a su domicilio particular, pues la LPRL señala que, salvo que el trabajador lo autorice –y aunque no lo establezca, también si existe un interés legítimo, conforme a la regulación del derecho a la intimidad por la Ley Orgánica 1/1982, de 5 de mayo–, la empresa sólo tendrá acceso a las conclusiones y debe evitarse, por tanto, cualquier tentación de filtración de datos que pudiera suponer un perjuicio para el trabajador al que se refirieran los concretos resultados.

12 BOE de 15 de noviembre.

13 Por ej., por haberse detectado una grave enfermedad.

De estos resultados también tendrán conocimiento, obviamente, los concretos profesionales que practican la vigilancia de la salud, si bien, sólo deberían conocerlos los que intervienen directamente en la práctica de esas pruebas y los documentalistas que los incorporan a soporte informático y papel, no los ayudantes de esos profesionales –auxiliar técnico sanitario, por ejemplo–, salvo en el caso de que este conocimiento resulte imprescindible. Así parece deducirse del artículo 22.4.2.º donde se establece que «el acceso a la información médica de carácter personal se limitará al personal médico…», entendiendo que el término médico incluye los propios médicos –licenciados en Medicina y Cirugía y su correspondiente especialidad– enfermeros –en cuanto a la necesidad establecida normativamente de que los servicios de prevención dispongan de ellos–, pero no ayudantes de este personal médico. Para la vigilancia de la salud de tipo psicosocial el personal que tendrá acceso a estos resultados serán los psicólogos y sociólogos directamente encargados de esa vigilancia. Además, también podrán tener acceso a los mismos las Autoridades Sanitarias, entendiendo por tales las que tengan competencia en materia de prevención de riesgos laborales y, en determinados supuestos, las competentes en materia de salud pública cuando se trate de enfermedades de declaración obligatoria o cuando la información derivada de la vigilancia de la salud tenga trascendencia en el ámbito de sus competencias. Este acceso es necesario para el correcto funcionamiento del Sistema de Información en Salud Laboral y para obtener datos de vigilancia epidemiológica [14] y, por tanto, limitado a los datos imprescindibles para que dichas Autoridades puedan ejercer correctamente sus responsabilidades [15].

Tanto personal como Autoridades Sanitarias deben, conforme a esa obligada confidencialidad recogida en el artículo 22.2 de la LPRL, guardar secreto sobre el contenido de esos resultados frente al resto de las personas relacionadas de alguna forma con la obligación preventiva de vigilancia de la salud (empresario, representantes de los trabajadores…) y también respecto de terceros, salvo que de la no revelación de esos datos pudiera derivarse un perjuicio para la salud de otros trabajadores o de terceros relacionados con la empresa o que, por imperativo legal, se establezca lo contrario, pues, como se ha puesto de manifiesto, el límite de los derechos individuales se encuentra, según el Tribunal Constitucional (TC), en el respeto al derecho de los otros y en lo que puedan determinar las leyes. Un secreto que no alcanza solamente a lo que pueda extraerse de esos resultados, sino también a todo aquello que el trabajador haya podido confiar al médico o a cualquiera de las personas involucradas en esa vigilancia [16], así como todo lo que esas personas hayan visto, oído o comprendido con ocasión del desarrollo de sus funciones.

---

14 Efectivamente, esta alusión a las Autoridades Sanitarias deriva del protagonismo que tienen en la vigilancia de la salud, tanto por la regulación específica del artículo 10 de la LPRL en el que se hace referencia a la realización de protocolos, a la implantación de ese Sistema de Información en Salud Laboral –con la expresión «implantación de sistemas de información adecuados»–, a la realización de estudios epidemiológicos e investigaciones en salud laboral, y a la supervisión de la formación que, en materia de prevención y promoción de la salud laboral, deba recibir el personal sanitario actuante en los servicios de prevención autorizados. Este protagonismo ya venía reconocido en el Capítulo IV de la LGS en el que a estos efectos destaca el artículo 10.3, que fija el deber de mantener la confidencialidad de toda la información relacionada con el proceso realizado en instituciones sanitarias que colaboren con el sistema público respecto a la salud laboral. *Vid.* también artículos 38 y 39 del RSP sobre colaboración de los servicios de prevención con el Sistema Nacional de la Salud.

15 BLASCO PELLICER, A.: «El deber empresarial de vigilancia de la salud y el derecho a la intimidad del trabajador», *op. cit.*, pág. 275.

16 Pues, ciertas enfermedades pueden investigarse a partir del conocimiento de determinados hábitos sociales, como el consumo de drogas o ciertas prácticas sexuales, o deducirse a partir de enfermedades concurrentes (en este sentido, SÁNCHEZ TORRES, E.: «El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales», *Relaciones Laborales*, octubre 1997, pág. 113).

Esta entrega de los resultados de la vigilancia forma parte del derecho a la intimidad como confidencialidad de los datos que forman parte de la propia persona y que deben ser conocidos por su titular quien, como manifestación de su libertad, puede decidir no conocerlos expresándolo por escrito. Esta renuncia al conocimiento no exime a los trabajadores de la obligación de cooperar con el empresario para que éste puede garantizarles unas condiciones de trabajo que sean seguras y no entrañen riesgos para su seguridad y su salud (art. 29 de la LPRL) y, en consecuencia, las medidas que los servicios de prevención recomienden adoptar o se exijan en las conclusiones de esos resultados deberán ser cumplidas por el trabajador, ya se trate de vigilancia de la salud obligatoria o voluntaria, con la consecuencia de sanción disciplinaria en caso de incumplimiento, salvo que, obviamente, esas medidas sean abusivas o atenten directamente contra los derechos fundamentales de los trabajadores.

Podría pensarse que en el caso de una vigilancia voluntaria también deberían ser voluntarias las medidas a adoptar. Sin embargo, debe señalarse que cuando un trabajador toma la decisión de someterse a esa vigilancia asume, salvo en los casos de desproporcionalidad o abuso en las pruebas o en las medidas a adoptar, las consecuencias derivadas de esa vigilancia en relación con los riesgos soportados y las medidas que pueden adoptarse. Aunque también es cierto que esta obligación se relativiza puesto que los riesgos a los que está sometido un trabajador al que se le practica una vigilancia voluntaria son menos perjudiciales para su salud que los que exigen una vigilancia obligatoria y, por tanto, será más fácil que el empresario cumpla con las obligaciones inherentes a la vigilancia de la salud, aun cuando el trabajador no adopte las prescripciones de los servicios de prevención. En este caso tiene más peso la autonomía de la voluntad, que puede llevar a flexibilizar el cumplimiento de esas medidas.

Por otra parte, debe advertirse que, conforme a lo dispuesto en el artículo 22.4.2.º párrafo, el trabajador podrá disponer que la información sobre el estado de salud contenida en los resultados sea facilitada al empresario o a otras personas –relacionadas o no con la prevención– con su consentimiento expreso –y aunque no lo diga expresamente la LPRL, por escrito, y señalando concretamente a qué personas, físicas o jurídicas, quiere facilitar esos datos–. Sólo él, exceptuando los supuestos de perjuicios para terceros o cuando así esté establecido por una ley, puede romper la confidencialidad para que el conocimiento de su estado de salud por la empresa o terceros no se considere intromisión ilegítima [17].

Esta regulación del acceso a los resultados supone la necesidad de adaptación a la LPRL de algunas normas anteriores a la misma sobre riesgos específicos que establecen la obligación para los empresarios de que sean ellos los que transmitan la información.

Además, respecto de estos resultados que se están analizando, debe señalarse que el artículo 37.3.f) del RSP autoriza al personal encargado de la vigilancia de la salud a analizar dichos resultados con criterios epidemiológicos para investigar y analizar las posibles relaciones entre la exposición a los riesgos profesionales y los perjuicios para la salud con el fin de proponer medidas encaminadas a mejorar las condiciones y medio ambiente de trabajo. Resalta, de este modo, el ámbito de acción colectiva de la vigilancia de la salud que trata de recopilar, sobre la base de la vigilan-

17 Conforme al artículo 2.2 de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad y a la Propia Imagen, «no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado su consentimiento expreso».

cia individual, datos epidemiológicos, es decir, datos que reflejen la distribución de enfermedades en cuanto a sus determinantes de origen laboral que sirven, a su vez, para descubrir nuevos agentes que pueden perjudicar a la salud o para identificar condiciones de trabajo que son responsables de generar enfermedades en los trabajadores o de favorecer o agravar dolencias que padecen [18].

1.2. Conclusiones.

Las conclusiones pueden definirse como la información final derivada de los datos de los resultados de los exámenes de salud físicos o psico-sociales practicados que señalan la aptitud o inaptitud del trabajador para el desempeño de un determinado puesto de trabajo y/o la necesidad de introducir o mejorar las medidas de protección y prevención.

Estas conclusiones sobre los resultados de la vigilancia de la salud [19], conforme a las orientaciones establecidas por la Organización Internacional del Trabajo (OIT) en la Recomendación número 171 de 1985 sobre los servicios de salud en el trabajo [20], no deberían contener información de índole médica o, más bien, podría decirse, de índole clínica [21]. Las conclusiones no pueden reflejar la concreta enfermedad o problema de salud que el trabajador tiene, evitando, de este modo, posibles tendencias empresariales hacia la discriminación. Ahora bien, si deben expresarse las condiciones de trabajo que están contraindicadas al determinado trabajador, temporal o permanentemente –información obligada para el cumplimiento del principio de adaptación del trabajo al trabajador (art. 15 LPRL)–, puede ser fácil determinar qué tipo de enfermedad tiene el mismo. Por eso es loable la decisión de la LPRL de establecer expresamente el derecho a la no discriminación en la práctica y consecuencias de la vigilancia de la salud. No obstante, los responsables de la práctica de esta vigilancia deben ser cautos en la utilización de sus palabras para dar a conocer la aptitud o no del trabajador para el concreto puesto de trabajo o función, en aras de evitar posibles suspicacias del empresario en perjuicio de los trabajadores.

Es así que para determinar el grado de aptitud en el trabajo en relación con la salud del trabajador, de forma adecuada y garantista con los derechos fundamentales del mismo, deben tenerse en cuenta los protocolos de actuación de la vigilancia en la medida que recogen criterios de valoración para determinar si una persona es apta o no, criterios que dejan un margen subjetivo a los responsables de los servicios de prevención ya que pueden adaptar el protocolo a las circunstancias de la empresa y/o circunstancias del trabajador [22].

---

18 FERNÁNDEZ, A.: «Epidemiología Laboral», VV.AA., BENAVIDES, F.; RUIZ FRUTOS, C.; GARCÍA, A.M. [Coords.]: *Salud Laboral. Conceptos y Técnicas para la prevención de riesgos laborales.* Barcelona, 2.ª ed. Masson, 2000, pág. 439.

19 De las que los servicios de prevención deberán hacer copia para facilitarlas al empresario y a otros encargados de tareas preventivas a los que, como se verá, la LPRL concede el derecho a conocerlas.

20 Apartado 16 de la Recomendación citada. Puede encontrarse el texto en *http://www.ilo.org*

21 Incluyendo, con más facilidad en este término, la dimensión psíquica de la salud.

22 El Protocolo del Plomo, por ej., establece, dentro de su apartado 6 –Conducta a seguir ante las alteraciones que se detecten–, los criterios de inaptitud para el trabajo con este material: «En el examen previo, la existencia de alguna de las patologías, que se citan a continuación debe ser considerada como un criterio absoluto de inaptitud para los puestos de trabajo expuestos al plomo: enfermedades congénitas como la talasemia o el déficit de G-6-PD; insuficiencia renal; insu-

Además de esos criterios, hay que tener en cuenta, tal y como recomiendan los Principios Directivos Técnicos y Éticos relativos a la Vigilancia de la Salud de los Trabajadores [23], en primer lugar, que, desde el punto de vista de salud en el trabajo, no existe una aptitud general para el empleo, ya que por su propio carácter relativo debe determinarse respecto de un empleo particular o una determinada tarea, y, así, se ha de procurar que la ineptitud para los mismos sea causa de adaptación en otro puesto de trabajo [24]. En segundo lugar, que la aptitud se refleja en la relación entre las demandas de una tarea específica y las capacidades del trabajador en un momento determinado; así, el tiempo puede hacer cambiar estos dos factores y, por tanto, toda aptitud o ineptitud debería permanecer –salvo en casos que no admitan duda– abierta a la posibilidad de su revisión. En tercer lugar, la conveniencia de proceder con precaución en aquellos supuestos en los que una persona enferma o físicamente discapacitada es examinada en relación con su aptitud en el empleo –trabajadores cuya atención preventiva se encuentra recogida en el art. 25 de la LPRL (trabajadores sensibles a determinados riesgos) que debe ser interpretado teniendo en cuenta lo dispuesto en el art. 22 de la LPRL– pues, esa discapacidad puede generar dos riesgos que deberían evitarse: por un lado, dar demasiada importancia a la discapacidad funcional y no permitir ninguna adaptación del trabajo al trabajador, con lo que, seguramente, se estará ante un supuesto de discriminación. Por otro, sobrevalorar la capacidad de una persona decidida para superar una discapacidad y conseguir resultados satisfactorios en un empleo que podría estar más allá de sus posibilidades.

La decisión última sobre esa aptitud debería adoptarse, así, a la luz de las interacciones entre la capacidad, la ergonomía y la rehabilitación profesional desde las tres dimensiones de la salud y, para ello, es necesario que, además de esas recomendaciones, se apliquen los baremos del concreto protocolo, reglamento, convenio colectivo o plan de empresa de forma fundada, rigurosa [25] y técnica [26] en

ficiencia hepática, trastornos neuropsiquíatricos, patología derivada del alcohol». A continuación señala, y ahí es donde entra el criterio subjetivo del personal encargado de realizar la vigilancia que «se valorará cuidadosamente la existencia de patologías que pueden suponer una contraindicación relativa o temporal, como la HTA, anemia, diabetes, cardiopatía, insuficiencia respiratoria, así como respiración nasal defectuosa».

23 OIT.: *Principios Directivos Técnicos y Éticos relativos a la vigilancia de la salud de los trabajadores.* Ginebra, OIT, 1998.

24 Pues, al contrario de lo que afirma la STSJ de Asturias de 11 de junio de 1999 (Ar. 1984), el objetivo principal de la vigilancia de la salud no es conseguir a un trabajador sin tacha médica alguna presente o previsiblemente futura, sino procurar una adaptación a sus posibilidades.

25 Así, la STSJ de Andalucía-Granada, de 6 de abril de 1998 (RJCA 1146), en un caso de ingreso en el Cuerpo de la Guardia Civil, puso de manifiesto que «aun aceptando que una cifra de colesterol superior al máximo permitido pudiera calificarse como una enfermedad o anomalía endocrino metabólica, no podría considerarse, en el caso concreto que analizamos la existencia de tal enfermedad, a los efectos de declarar la ineptitud física del recurrente, puesto que para que el colesterol pueda considerarse como factor de riesgo cardiovascular, debe detectarse una cifra superior a 250 mg/100 ml, sin que una cifra aislada tenga valor diagnóstico ni pronóstico cuando se encuentra en límites cercanos a la normalidad, máxime si se tiene en cuenta, que en los análisis practicados al recurrente posteriormente, se apreció una cifra más baja, por lo tanto, no siendo admisible una interpretación extensiva de las causas de exclusión por indiciaria de futuros riesgos cardio-circulatorios que sea la cantidad de colesterol en sangre del actor, lo procedente es la nulidad de los actos impugnados», abogando por una rigurosidad en el baremo que, en otro caso, puede vulnerar el derecho de acceso al empleo en condiciones de igualdad.

26 De este modo, aunque un determinado trastorno como el daltonismo no hubiera impedido la prestación laboral al inicio de la misma, si posteriormente, en virtud de pacto colectivo, se llegó a la conclusión de que obstaba objetivamente dicha prestación, atendidas las exigencias técnicas y de productividad del servicio de prevención y extinción de incendios, tal acuerdo lícito al amparo del artículo 82.2 del Estatuto de los Trabajadores (ET), permite a la empresa acordar la resolu-

función del concreto puesto de trabajo [27, 28]. En cualquier caso, si no se está de acuerdo con la aptitud determinada, puede acudirse a otros profesionales sanitarios competentes para comparar diagnósticos y atribuir mayor fuerza de convicción a alguno de ellos [29].

Las conclusiones, además de a los trabajadores, deben comunicarse a otros sujetos relacionados con la prevención, fundamentalmente al empresario. Pueden ser individuales, referenciando la aptitud para cada trabajador aunque se entreguen en documento conjunto, o colectivas. Estas últimas dan una visión genérica del estado de salud de todos los trabajadores en conjunto, aconsejando las medidas de protección que deban adoptarse, siempre que los resultados no determinen la necesidad de ofrecer a la empresa y a otros sujetos de la acción preventiva unas conclusiones individualizadas [30].

Las personas que pueden tener acceso a las conclusiones, según lo dispuesto en el artículo 22.4 de la LPRL, son, por un lado, la empresa y, por otro, las personas y órganos con responsabilidad en materia de prevención para que «puedan desarrollar correctamente sus funciones» respecto a la misma; luego, el uso de la información derivada de las conclusiones se limita, así, a lo estrictamente necesario para el correcto desempeño de sus funciones.

Esos sujetos con responsabilidades preventivas son, en primer lugar, los delegados de prevención, en cuanto que entre sus funciones, recogidas en el artículo 36 de la LPRL, está la de colaborar con la dirección de la empresa en la mejora de la acción preventiva y, expresamente, en cuanto a sus competencias, la de tener acceso a la información y documentación relativa a las condiciones de trabajo que sean necesarias para el ejercicio de sus funciones, con las limitaciones previstas en el artículo 22.4 de la LPRL. En segundo lugar, el Comité de Seguridad y Salud, como «órgano paritario y colegiado de participación destinado a la consulta regular y periódica de las actuaciones de la empresa en materia de prevención de riesgos» (art. 39 LPRL) a quien la LPRL le atribuye la competencia de conocer cuantos documentos e informes relativos a las condiciones de trabajo sean necesarios para el cumplimiento de sus funciones [art. 39.2.b)], así como la de conocer y analizar los daños producidos en la salud o en la integridad física de los trabajadores, al objeto de valorar sus causas y proponer las medidas preventivas oportunas [art. 39.2.c)]. En tercer lugar, la representación

---

ción de la relación laboral al amparo y con las consecuencias del artículo 52 del ET (STSJ de Castilla y León, Valladolid, de 17 de febrero de 1998, Ar. 5145. En sentido similar, STSJ de Castilla y León, Burgos, de 7 de enero de 1998, Ar. 33, sobre un caso de deuteranopia –anormalidad rojo-verde–).

27 Concreto puesto de trabajo que permite no considerar discriminatoria la extinción de un contrato de trabajo por embarazo cuando éste, en relación con el puesto o tareas concretas del mismo, supone un riesgo para la salud y seguridad de otras personas (STSJ de Madrid, de 3 de octubre de 2000, JUR 2001/20581, en relación con una piloto embarazada).

28 Además, esta relación de la aptitud con el concreto puesto de trabajo puede llegar a convertir en válida una condición resolutoria del contrato de trabajo si, como consecuencia del reconocimiento médico, se detecta alguna ineptitud para el desempeño del concreto puesto de trabajo, como la de un futbolista a quien se le detectó «gonartrosis incipiente femorotibial medial y femoropateral, con leve claudicación del miembro inferior derecho a la carrera y limitación de últimos grados de flexión en rodilla derecha», considerando, de este modo, esa rodilla derecha como factor de riesgo para realizar una actividad deportiva (STSJ de Andalucía-Sevilla, de 7 de abril de 2000, Ar. 1050).

29 Mayor fuerza de convicción que se valorará en función de criterios tales como la autoridad de su autor, su imparcialidad o el tipo de pruebas efectuadas (STSJ de Castilla y León, Valladolid, de 9 de diciembre de 1997, Ar. 5215).

30 Por ejemplo, porque en una empresa, todos los trabajadores son aptos para desempeñar sus respectivos puestos.

unitaria y sindical de los trabajadores en cuanto que los artículos 19.3, 64.1.8) y 64.1.9) del ET, así como el 18 de la LPRL les atribuye funciones preventivas y, a mayor abundamiento, tienen que elaborar informe en algunos supuestos de vigilancia obligatoria.

Además, considero que también tienen derecho al conocimiento de las conclusiones los trabajadores designados para tareas preventivas (arts 10 y 12 del RSP), que complementarán las labores de los servicios de prevención, y los integrantes de los servicios de prevención que, salvo circunstancias excepcionales, no tienen acceso a los resultados como auxiliares técnicos sanitarios o integrantes diferentes a los que tienen la función de vigilancia. En estos dos casos, sólo cuando los que realizan la vigilancia de la salud lo consideren necesario en función de las circunstancias de la empresa, carácter de los riesgos en la misma y funciones atribuidas a esos colectivos. Por otro lado, también la Autoridad Laboral, en virtud de su derecho de acceso a la documentación sobre práctica de los controles del estado de salud de los trabajadores y conclusiones obtenidas de los mismos recogido en el artículo 23.1.d) de la LPRL y, unida a ella, la Inspección de Trabajo y Seguridad Social, siempre que solicite esas conclusiones para cumplir con su función de asistencia técnica o de vigilancia y exigencia del cumplimiento de las normas laborales [31].

Todos ellos están sometidos a un deber de confidencialidad entendiendo que cuando el artículo 22.2 de la LPRL dice «las medidas de vigilancia y control de la salud se llevarán a cabo respetando… la confidencialidad de toda la información relacionada con su estado de salud» hace referencia no sólo a los datos incorporados a los resultados y que llevarán a las conclusiones, sino también a las conclusiones mismas en cuanto documento final que resuelve sobre si el estado de salud del trabajador es el correcto para el desempeño del concreto puesto de trabajo.

Además, el artículo 36.2.b) prevé el respeto a la confidencialidad de las conclusiones para los Delegados de Prevención y la normativa sobre Inspección de Trabajo [32] regula un deber de sigilo o secreto que recoge también el ET en sus artículos 62.2 y 65.2 para los representantes de los trabajadores. Por otro lado, los trabajadores designados para tareas preventivas y los miembros de los servicios de prevención se encuentran sometidos también a un deber de sigilo de prevención conforme al artículo 30.4 de la LPRL que puede definirse como un secreto o prudencia concreta respecto a la información relativa a la empresa de la que tuvieran conocimiento como consecuencia del desempeño de sus funciones preventivas y en el que no hace falta reunir ningún requisito de profesionalidad para su exigencia –información relativa a la empresa que puede incluir la aptitud o no de sus trabajadores para el desempeño de ciertos trabajos y a la que se le puede atribuir el carácter de reservada por causa justa [33] como puede ser evitar la discriminación en el empleo, discriminación que justifi-

31 *Vid.* Ley 42/1997, de 14 de noviembre, de Ordenación de la Inspección de Trabajo y de la Seguridad Social (BOE de 15 de noviembre) y Real Decreto 138/2000, de 4 de febrero, por el que se aprueba el Reglamento de Organización y Funcionamiento de la Inspección de Trabajo y Seguridad Social (BOE de 16 de febrero).

32 *Vid.*, artículo 12 de la Ley 42/1997, de 14 de noviembre citada y artículo 10 del Real Decreto 138/2000, de 4 de febrero citado.

33 La empresa no puede atribuir a una información cualquiera ese carácter reservado. Éste debe determinarse de manera individualizada y objetiva, caso por caso y utilizando criterios de carácter objetivo, como la justa causa, con los que se llegue a concluir que una determinada información tiene carácter reservado. En la determinación de esos criterios tendrá un papel fundamental la negociación colectiva de empresa que, en función de las circunstancias de la misma, podrá

ca, a su vez, junto con el deber de no perjudicar al trabajador, la confidencialidad respecto a las conclusiones exigidas al empresario [34].

La confidencialidad empresarial también viene justificada por las exigencias de la buena fe contractual (art. 20.2 del ET) y del deber que se incorpora al tipo infractor del artículo 13.5 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social (TRLISOS) [35].

Debe señalarse, además, que los miembros del servicio de prevención no encargados directamente de la vigilancia a quienes le son comunicadas las conclusiones tienen obligación de respetar la confidencialidad de los datos relacionados con la misma por prescripción de los artículos 15.2, para los servicios de prevención propios, y 18.3, para los servicios de prevención externos, del RSP cuya aplicación debe hacerse extensiva no sólo a los encargados de la actividad sanitaria –física, psíquica y social–, sino también a otros miembros del servicio de prevención en virtud del deber de coordinación entre sus componentes, también recogido en estos dos artículos.

Los miembros del Comité de Seguridad y Salud también se encuentran sometidos a este deber de confidencialidad, que puede justificarse en el deber de sigilo del artículo 30.4 en la medida en que sus miembros son sujetos con obligación de sigilo: Delegados de Prevención y representantes de los empresarios. Los que no integran pero participan en las reuniones de este órgano no tendrán acceso a estas conclusiones, salvo que por otras funciones desempeñadas esté justificado el acceso a las mismas (Delegados sindicales) [36], aunque sí que serán informados de las medidas adoptadas a partir de la práctica de la vigilancia.

Los Reglamentos sobre riesgos específicos anteriores a la LPRL –plomo, amianto, etc.– ofrecían una solución más práctica exigiendo directamente a todos los implicados en la vigilancia un deber de confidencialidad. Así, el Reglamento sobre trabajos con riesgo de amianto, en su artículo 15.7, limita la utilización de los datos de la vigilancia a fines médico-laborales y orientativos para la mejora del ambiente de trabajo sobre la base de esa confidencialidad, al igual que lo hace el artícu-

---

dar orientaciones sobre lo que debe tener carácter reservado en ella (*Vid.*: PEDROSA ALQUÉZAR, S.: «Ámbito de actuación y responsabilidades de los servicios de prevención en la Administración General del Estado», *Revista de Trabajo y Seguridad Social*. CEF, número 223, 2001, págs 147-148 con base en GARRIDO PÉREZ, E.: *La información en la empresa. Análisis jurídico de los poderes de información en los representantes de los trabajadores*, Madrid, CES, 1995, págs. 331-362). *Vid.*, alcance de ese carácter reservado en STC 213/2002, de 11 de noviembre, que recuerda que no es suficiente con que el empresario califique unilateralmente como confidencial cierta información, sino que es necesario también que «desde un plano objetivo efectivamente lo sea» (FJ 9).

34 PURCALLA BONILLA, M.A.: «Vigilancia de la salud de los trabajadores: claves interpretativas de su régimen jurídico», *op. cit*, pág. 704.

35 BOE de 8 de agosto. Su artículo 13.5 establece que se considerará infracción muy grave incumplir el deber de confidencialidad en el uso de los datos relativos a la vigilancia de la salud de los trabajadores.

36 Además, también puede venir justificado en la propia garantía de confidencialidad general de los datos sanitarios y en la obligación de circunscribirse a las funciones preventivas que el ordenamiento le encomienda como criterios suficientes para asentar un implícito deber de sigilo al órgano como tal, independientemente de sus miembros, que, si se vulnera, permite al trabajador reclamar las responsabilidades que procedan.

lo 11.6 del Reglamento para la prevención de riesgos y protección de la salud por la presencia de cloruro de vinilo monómero en el ambiente de trabajo o el artículo 13.6 del Reglamento para la prevención y protección de la salud de los trabajadores por la presencia de plomo metálico y sus componentes iónicos en el centro de trabajo [37].

Respecto a si las propuestas preventivas incorporadas a las conclusiones son o no vinculantes para el empresario, algunos autores niegan tal carácter en la medida en que la decisión última la tiene éste en virtud de sus poderes organizativos [38]. Si bien, las responsabilidades en las que puede incurrir el empresario por una vigilancia inadecuada, además de la necesidad de considerar la vigilancia como una totalidad de práctica de exámenes de salud y medidas derivadas de esos exámenes que la LPRL encomienda a los servicios de prevención –aunque como manifestación de la obligación empresarial–, son motivo para poder afirmar que el cumplimiento de esas medidas propuestas no debería quedar a disposición del empresario. Tiene la obligación de asumirlas, pues la LPRL articula este deber de vigilancia a través del servicio de prevención. La empresa tiene obligación de poner en marcha la infraestructura adecuada, a través de los servicios de prevención, para llevar a cabo esa vigilancia que trae consigo unas consecuencias que forman también parte de esa obligación y, salvo, claro está, que el criterio del servicio de prevención vulnerara directamente alguno de los derechos fundamentales del trabajador sin ninguna justificación con el consiguiente perjuicio para el mismo [39], debe cumplir con todas las implicaciones derivadas de ese deber [40].

En refuerzo de esta línea argumental, debe señalarse que, en general, la normativa tanto anterior como posterior a la LPRL ponen de manifiesto este planteamiento obligando al empresario a adoptar las medidas recogidas en las conclusiones. Así, el Reglamento sobre Enfermedades

37 La Orden de 9 de abril de 1986, por la que se aprueba el Reglamento para la Prevención de Riesgos y Protección de la Salud por la presencia de cloruro de vinilo monómero en el ambiente de trabajo (BOE de 6 de mayo de 1986) ha sido derogada por el Real Decreto 665/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo (BOE de 24 de mayo de 1997). La Orden de 9 de abril de 1986, por la que se aprueba el Reglamento para la Prevención de Riesgos y Protección de la Salud de los Trabajadores por la presencia de plomo metálico y sus compuestos iónicos en el ambiente de trabajo (BOE de 24 de abril de 1986) ha sido derogada por el Real Decreto 374/2001, de 6 de abril, sobre la protección de la salud y seguridad de los trabajadores contra los riesgos relacionados con los agentes químicos durante el trabajo (BOE de 1 de mayo de 2001 y corrección de errores de 30 de mayo y 22 de junio).

38 *Vid.* SEMPERE NAVARRO, A.; GARCÍA BLASCO, J.; *et alt. Derecho de la Seguridad…, op. cit.*: «Las propuestas realizadas no son vinculantes para el empresario, de modo que la decisión empresarial entra en la esfera de sus poderes organizativos, si bien no puede desconocerse que una negativa a seguir las conclusiones formuladas puede determinar un incumplimiento empresarial…» (pág. 229).

39 Si esta circunstancia se diera, habría que comentar la situación con ese servicio y adoptar otro tipo de medidas.

40 Como pone de manifiesto MATEO BEATOS, «el examen médico está concebido dentro de una organización sanitaria en la que se integra no sólo el conocimiento médico sobre el estado de salud del trabajador, sino que abarca aspectos de la organización preventiva de la empresa; por ello las conclusiones ofrecidas al empresario no sólo se refieren al estado de salud sino a la aptitud expresa del trabajador para desarrollar la actividad laboral en un ámbito específico; en este sentido, el informe o conclusión médica, además de ser operativo, termina siendo casi decisorio, puesto que deja escaso margen de maniobra al empresario sobre la elección del trabajador en relación al puesto de trabajo y, además, está facultado para entrar en el ámbito del poder de dirección del empresario, en cuanto que puede plantear medidas concretas de carácter preventivo que, en caso de ignorarse por el empresario, comprometen la responsabilidad» MATEOS BEATO, A: *Diccionario de Seguridad y Salud Laboral: Conceptos de la Ley de Prevención de Riesgos Laborales*, Valladolid, LexNova, 2002, pág. 1.168.

Profesionales, aprobado por Orden de 9 de mayo de 1962, establece en su artículo 46 que las empresas están obligadas a cumplir con los dictámenes médicos sobre traslado de los trabajadores afectos de síntomas de enfermedad profesional sin incapacidad temporal; el Real Decreto 665/1997, de 12 de mayo, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo [41] obliga al empresario a revisar la evaluación y las medidas de prevención y de protección colectivas e individuales adoptadas «cuando se hayan detectado alteraciones de la salud de los trabajadores que puedan deberse a la exposición a agentes cancerígenos o mutágenos, o cuando el resultado de los controles periódicos, incluidos los relativos a la vigilancia de la salud, ponga de manifiesto la posible inadecuación o insuficiencia de las mismas» (art. 8.4); y, el Real Decreto 374/2001, de 6 de abril, sobre la protección de la salud y seguridad de los trabajadores contra los riesgos relacionados con los agentes químicos [42] establece, además, la obligación de «tener en cuenta las recomendaciones del médico responsable de la vigilancia de la salud al aplicar cualesquiera otras medidas necesarias para eliminar o reducir los riesgos…incluida la posibilidad de asignar al trabajador otro trabajo donde no exista riesgo de una nueva exposición» [art. 6.8.c)].

1.3. Comunicación en los supuestos de Empresas de Trabajo Temporal.

Mención especial requiere la comunicación de resultados en el ámbito de las Empresas de Trabajo Temporal (ETT). La normativa sobre este tipo de empresas obliga a que sean ellas las que realicen la vigilancia de la salud y no las empresas usuarias, obligación discutible sobre todo en el supuesto de una vigilancia de la salud periódica en la medida en que el trabajo se realiza en esa concreta empresa usuaria. Una vez practicada y habiendo comunicado los servicios de prevención correspondientes las conclusiones a la ETT, será ésta la que remita la información, por iniciativa propia o a petición de la interesada, a la empresa o empresas usuarias con las que haya concertado un contrato de puesta a disposición para que éstas puedan cumplir con la obligación recogida en el artículo 4 del Real Decreto 216/1999, de 5 de febrero, por el que se establecen disposiciones mínimas de seguridad y salud en el trabajo en el ámbito de las ETT [43].

Además, como el trabajador de la ETT que desempeña sus funciones en la empresa usuaria tiene reconocido el derecho de poder dirigirse en todo momento al servicio de prevención de la misma y el Real Decreto citado exige, además, en su artículo 6.3, la coordinación de ese servicio con el de la ETT para garantizar una protección adecuada de la salud y seguridad de los trabajadores puestos a disposición, resulta indudable la comunicación de los resultados entre esos dos servicios de prevención, ahora bien, siempre que, como pone de manifiesto el último párrafo de ese precepto, sea relevante para la protección de la salud de los trabajadores en misión y con estricto respeto a la con-

41 BOE de 24 de mayo.

42 BOE de 1 de mayo.

43 BOE de 24 de febrero. El artículo 4 señala lo siguiente: «La empresa usuaria deberá recabar la información necesaria de la empresa de trabajo temporal para asegurarse de que el trabajador puesto a su disposición reúne las siguientes condiciones: a) Ha sido considerado apto a través de un adecuado reconocimiento de su estado de salud para la realización de los servicios que deba prestar en las condiciones en que hayan de ser efectuados, de conformidad con lo dispuesto en el artículo 22 de la Ley de Prevención de Riesgos Laborales y el artículo 37.3 del Reglamento de los Servicios de Prevención».

fidencialidad de los datos contenidos tanto en los resultados como en las conclusiones que pueden utilizarse. Para contribuir a ese respeto, la comunicación de datos entre estos dos servicios de prevención deberá realizarse siempre entre ellos mismos, sin pasar por ninguna de las dos empresas, salvo, como se ha afirmado, la comunicación de las conclusiones de la vigilancia, necesaria para poder contratar de acuerdo con la ley al trabajador puesto a disposición.

2. El tratamiento de los datos.

2.1. Introducción.

Las conclusiones, los resultados y el seguimiento continuado del estado de salud del trabajador suministran una serie de datos que se documentan y están sujetos a una elaboración y, posteriormente, a un proceso de archivación y puesta a disposición para su custodia y tutela. Fases, estas, del tratamiento de datos sobre vigilancia de la salud en las que rige el principio de confidencialidad unido a otros que se analizan *infra*.

Este tratamiento de datos se realizará, normalmente, en soporte informático, por sus posibilidades de almacenamiento, elaboración y transmisión de ingentes masas de datos. Este tipo de soporte adquiere especial importancia en un mundo en el que la evolución tecnológica está redefiniendo la realidad socioeconómica afectando también, por tanto, a las relaciones laborales articulando nuevos escenarios de conflicto entre distintos intereses como el poder de dirección empresarial y el derecho a la intimidad del trabajador [44]. Y es que la informática, con todas esas posibilidades que ofrece, permite controlar la información y puede llegar a convertirse en un instrumento de presión y control empresarial [45]. Además, la transferencia de datos telemática entre ordenadores permite el cruce de ficheros y registros informáticos, con su correspondiente proceso y tratamiento automático de la información mediante los programas adecuados, de tal modo que la persona titular de los datos puede perder, prácticamente en su totalidad, el control sobre su utilización y su tratamiento.

Así, todos estos datos, organizados mediante los sistemas de almacenamiento y recuperación de la información, deben estar protegidos de manera que no sea posible el acceso –malintencionado o no– de quienes no estén autorizados para ello. La protección se realiza, por tanto, sobre los datos en sí –para que no puedan ser tratados o elaborados y convertidos en información, salvo para fines adecuados y por personas autorizadas– y va a suponer un límite a la utilización de la informática ante el temor de que pueda agredir a la intimidad [46], en este caso, de los trabajadores.

---

44 Por todos, GARCÍA BLASCO, J.; DE VAL TENA, A.: «Incidencia de las nuevas tecnologías en las relaciones laborales», *Monografías de la Revista Aragonesa de Administración Pública IV*, 2001, pág. 320.

45 Control de correo electrónico, control telefónico, control de descansos, control, incluso, de actitudes y gestos (por todos, *vid*. MERCADER UGUINA, J.: «Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿Hacia una empresa panóptica?», *Relaciones Laborales*, núm. 10, 2001).

46 *Vid.* DAVARA RODRÍGUEZ, M.A.: *La protección de datos en Europa: principios, derechos y procedimiento*, Madrid, Asnef-Equifax, 1998, pág. 16.

De este modo, el tratamiento automatizado de datos, en cuanto puede suponer que el perfil de una persona sea conocido por otros en cualquier momento y en cualquier lugar y, en consecuencia, configurar una determinada reputación o idea del individuo cuya valoración desfavorable afecte a sus más diversas actividades públicas o privadas –como puede ser la obtención de un empleo o la admisión a determinados colectivos [47]–, lleva inherente un derecho a la protección jurídica de datos de carácter personal –entre los que se incluyen los referidos a la salud– para evitar atentados directos a su intimidad o una limitación del ejercicio de sus derechos siendo así su objeto parcialmente coincidente con esa intimidad como control por su titular de los datos e información relativos a su propia persona [48]. Tiene su base jurídica en el artículo 18.4 de la Constitución en el que se establece que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Esta consolidación del derecho a la protección jurídica de datos se hace especialmente necesaria en el ámbito empresarial en la medida en que, como se ha señalado, la informática otorga un gran poder de control de la prestación laboral a la empresa y, por tanto, la forma en que se traten los datos en la misma puede afectar de forma más agresiva a los derechos fundamentales del trabajador que puede llegar a convertirse en individuo vulnerable «en grado impredecible» [49], especialmente si la empresa combina datos erróneos, inexactos y utilizados con finalidades ilícitas o diferentes a las que fueron obtenidas, o se transmiten arbitrariamente por el empresario [50].

Para conocer actualmente cómo debe articularse el tratamiento de datos relacionados con la salud y aplicados a la obligación de su vigilancia en el ámbito laboral, debe prestarse atención a la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos [51], que supuso la modificación de la LORTAD para cumplir con su transposición dando lugar a la Ley Orgánica 15/1999, de 13 de diciembre, de LPDP por la que se rige actualmente el tratamiento automatizado de esos datos en nuestro país, e incluso, también, como se verá, de los no automatizados. Además, habrá que tener en cuenta el Reglamento de desarrollo de la LORTAD, Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de las Medidas de Seguridad de los Ficheros Automatizados (RMSFA) que contengan datos de carácter personal, declarado vigente por la disposición transitoria tercera de la LOPD en lo que no se oponga a la misma.

---

47 Exposición de motivos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD) (BOE de 31 de octubre).

48 El TC, en su Sentencia 292/2000, de 30 de noviembre, basándose, sobre todo, en la idea de que prácticamente todos los derechos de una persona pueden resultar afectados por el tratamiento indebido de datos, afirma su separabilidad del derecho a la intimidad, aunque su objeto sea parcialmente coincidente, y lo considera en sí mismo un derecho o libertad fundamental.

49 Por todos, FERNÁNDEZ DOMÍNGUEZ, J.J.; RODRÍGUEZ ESCANCIANO, S.: *Utilización* y *control de datos laborales..., op. cit.*, pág. 107.

50 Especialmente peligroso cuando se refiere a datos relacionados con la salud del trabajador, pues las tendencias empresariales a medir todo en términos económicos pueden suponer que el trabajador tenga especiales dificultades en encontrar un trabajo por el mero hecho, por ejemplo, de su propensión a contraer afecciones gripales. FERNÁNDEZ DOMÍNGUEZ, J.J.; RODRÍGUEZ ESCANCIANO, S.: *Utilización* y *control de datos laborales..., op. cit.*, pág. 108.

51 DOCE núm. L 281, de 23 de noviembre de 1995.

Este Reglamento resulta de gran interés en lo que se refiere a la protección de datos en materia de vigilancia de la salud por considerarse de especial sensibilidad, de modo que los ficheros que contengan esos datos deben reunir las máximas garantías de seguridad para evitar el posible acceso o manipulación de los mismos en contra del derecho a la intimidad del trabajador.

También hay que tomar en consideración la Recomendación de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados Miembros Sobre Protección de Datos Médicos [52], así como el documento «Ethical Issues of Healthcare in the Information Society. Opinion of the European Group in Ethics in Science and New Technologies to the European Commission», de 13 de julio de 1999 [53]. Este último pone de manifiesto la importancia que puede tener la sociedad de la información y las nuevas tecnologías en un avance respecto al cuidado de la salud, que debe ofrecer todas las garantías precisas para no vulnerar los derechos fundamentales de los ciudadanos y, por extensión, de los trabajadores. Dentro de estas garantías se encuentra el tratamiento adecuado de datos sobre la salud sometido a principios como el de seguridad, control del trabajo de los profesionales de la salud, confidencialidad, etc.

Todas estas normas deben ser interpretadas a la luz del Convenio del Consejo de Europa núm. 108, de 28 de enero de 1981, sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal [54], que ha contribuido a consagrar, en el ámbito internacional, unos principios básicos «que deberán ser respetados en las transmisiones de datos, bien se realicen dentro de la frontera de los Estados, bien se transmitan los datos a otros Estados» [55].

2.2. La aplicación de la regulación sobre protección de datos de carácter personal.

2.2.1. Introducción.

Antes de comenzar a analizar las características de esta norma y de cómo se articula la protección de datos relacionados con la vigilancia de la salud al amparo de la misma, debe señalarse que el artículo 23.1.d) de la LPRL impone al empresario la obligación de elaborar y conservar a disposición de la autoridad laboral la documentación relativa a la práctica de los controles del estado de salud de los trabajadores previstos en el artículo 22 y las conclusiones obtenidas de los mismos.

Así, aunque de este artículo podría deducirse que es el empresario el que debe elaborar y conservar la documentación relativa a los resultados de la salud, es, en realidad, el servicio de prevención quien asume esta función porque es el personal que practica la vigilancia el único que, conforme al artículo 22.4 de la LPRL, tiene acceso, junto a las autoridades sanitarias, a los resultados que

52 Puede consultarse el texto en http//:www.comz.es

53 Véase nota anterior.

54 Ratificado por instrumento de 27 de enero de 1984 y publicado en BOE de 15 de noviembre de 1985.

55 *Cfr.* FERNÁNDEZ DE GATTA SÁNCHEZ, D.: «El régimen jurídico de la protección de datos personales: aspectos internacionales, comunitarios e internos», *Noticias de la Unión Europea*, núm. 149, 1997, pág. 75.

contienen la información médica de carácter personal. El empresario simplemente tendrá que comprobar la efectiva custodia y conservación, pero sin poder acceder a los mismos –quizá mediante certificado expedido por los servicios de prevención– a pesar de que puede ser responsable directo por no documentar esos resultados.

Respecto a las conclusiones, aunque pueda tener acceso a las mismas, va a ser también el servicio de prevención quien las elabore. Ahora bien, una vez elaboradas, sí que debería el empresario disponer de un fichero informático o manual donde se guardaran dichas conclusiones y al que él pudiera tener acceso. Además, podrá ser la empresa la encargada directa de entregar esas conclusiones a las autoridades sanitarias o laborales cuando así lo soliciten, derecho que no puede ejercer en el caso de los resultados ya que no puede disponer de ellos y entrar en la base de datos donde estén incorporados o acceder a los ficheros manuales donde estén guardados, puesto que este acceso está limitado al personal interviniente en esa vigilancia y los documentalistas que ordenan los datos derivados de la misma.

Se pueden distinguir, así, dos fases en el tratamiento de datos de la vigilancia de la salud; por un lado, la fase de elaboración y, por otro, la fase de archivación y custodia de esos datos. De la primera fase se van hacer cargo en todo caso, sean resultados o conclusiones, los servicios de prevención. En la de archivación y custodia se harán cargo, por un lado, estos servicios de prevención respecto de los resultados –frente a los que el empresario tiene, salvo excepciones, prohibido el acceso– y, respecto de las conclusiones, una vez ya entregadas al empresario, y aunque consten en los ficheros de los servicios de prevención, la empresa. Así, podría decirse que habría tres bases de datos: una de resultados y otra de conclusiones a cargo de los servicios de prevención, aunque con alguna responsabilidad de la empresa, y otra más de conclusiones a cargo directo de la empresa. Frente a todas ellas rige el principio de confidencialidad unido a otros principios derivados de la aplicación de la LOPD.

La aplicación de esta Ley a los supuestos de documentación de datos en vigilancia de la salud queda fuera de toda duda en la medida en que se aplica a los «datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado», incluyendo, así, los ficheros y tratamientos automatizados y no automatizados [56] utilizables o elaborados por las empresas, con exclusión de los que contengan datos utilizables por personas físicas «en el ejercicio de actividades exclusivamente personales o domésticas», los sometidos a «la normativa sobre protección de materias clasificadas» y «los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada» (art. 2.2).

56 Los ficheros manuales deben adecuarse a la LOPD, como dispone su disposición adicional primera, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados. El plazo de adaptación es el de doce años a contar desde el 24 de octubre de 1995, así, hasta el 24 de octubre de 2007. Esta prescripción se ha realizado sobre la base del artículo 32.2 de la Directiva 95/46/CE en el que se autoriza a los Estados miembros para establecer que el tratamiento de datos que ya se encuentren incluidos en ficheros manuales en la fecha de entrada en vigor de las disposiciones nacionales en aplicación de esa directiva debe ajustarse a lo dispuesto en los artículos 6 [principios relativos a la calidad de datos], 7 [principios relativos a la legitimación del tratamiento de datos] y 8 [tratamiento de categorías especiales de datos] en un plazo de doce años a partir de la adopción de la misma permitiendo, no obstante, los derechos de rectificación, cancelación y acceso. Esta inclusión de los ficheros no automatizados resulta de relevancia para evitar que las pequeñas empresas, justificando la falta de recursos para la obtención y conservación de recursos informáticos, puedan vulnerar los derechos de los trabajadores en la elaboración y tratamiento de datos relacionados con la salud.

La LOPD entiende por fichero «todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso» [art. 3.b)] y por tratamiento de datos «las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias» [art. 3.c)].

La LOPD considera a los datos relacionados con la salud datos especialmente protegidos cuya obtención, tratamiento y cesión sólo podrá realizarse cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente (art. 7.3). En este caso, es la propia LPRL desde la interpretación conjunta de, fundamentalmente, sus artículos 22 y 23 junto al artículo 12.4 del TRLISOS –que considera falta grave no registrar ni archivar la información referida a la vigilancia de la salud– la que autoriza esa obtención, tratamiento y cesión, sin necesidad de que exista un consentimiento específico del trabajador. Es así que el consentimiento en la vigilancia de la salud restringe su campo de actuación al sometimiento o no a determinadas pruebas y a la decisión de conocer o no la información sobre la salud de uno mismo. No alcanza el posible tratamiento de datos –con las actividades que pueden derivarse del mismo, como la cesión– sobre la salud que podrá efectuarse sin el consentimiento del afectado [57]. Si bien, el hecho de tratar los datos derivados de la vigilancia de la salud sin ese consentimiento no excluye el derecho a la información sobre los extremos de ese tratamiento, que se recogen en el artículo 5 de la LOPD [58], y que deben ser puestos en conocimiento del trabajador de modo expreso, preciso e inequívoco, lo que implica su comunicación por escrito y de forma entendible para sus destinatarios.

Esta inclusión en el ámbito de actuación de la normativa sobre protección de datos de aquellos recogidos en ficheros relacionados con la vigilancia de la salud requiere, no obstante, delimitar qué se entiende por datos sobre salud a esos efectos con el fin de conocer si pudiera excluirse algún dato de los incorporados en los resultados o en las conclusiones.

Para ello, debe acudirse a la definición de la Agencia Española de Protección de Datos (AEPD) [59] que recurrió al concepto del apartado 45 de la Memoria explicativa del Convenio núm. 108 y concluyó que los datos sobre salud hacen referencia a las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo, pudiendo tratarse de informaciones concernientes a un individuo que goce de buena salud, enfermo o fallecido, incluyendo las que se refie-

57 Así lo pone de manifiesto también la Jurisprudencia Constitucional que justifica la creación de ficheros con datos derivados de la vigilancia de la salud para fines preventivos sin necesidad de consentimiento por exigencia de los artículos 22 y 23 de la LPRL (*vid.*, FJ 3.º y 4.º de la STC 202/1999, de 8 de noviembre).

58 No sirve, así, solamente comunicar al afectado de forma genérica que se aplica la normativa vigente (en este sentido, ÁLVAREZ CIVANTOS, O.J.: *Normas para la implantación de una eficaz protección de datos…*, *op. cit.*, pág. 31).

59 Agencia de Protección de Datos: *Memoria 1999*, Madrid, 1999, págs. 433-434. Se siguen también las explicaciones a partir de esta Memoria de ÁLVAREZ CIVANTOS, O.J.: *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada, Comares, 2001, págs. 116-117 y de VIZCAÍNO CALDERÓN, M.: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid, Civitas, 2001, págs. 128-129. Téngase en cuenta que, conforme al artículo 79 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social (BOE de 31 de diciembre) las referencias a la Agencia de Protección de Datos deberán entenderse realizadas a la Agencia Española de Protección de Datos.

ren al abuso de alcohol o al consumo de drogas, datos psicológicos, incluidos en historiales clínico-psiquiátricos o los que se deriven de las propias manifestaciones de los interesados en formularios o encuestas [60], y datos genéticos.

Esta definición parece hacer referencia directamente a lo que se ha entendido en este estudio por resultados, si bien, en la medida en que las conclusiones hacen referencia también a la salud del trabajador en cuanto a su aptitud exenta de riesgos para desempeñar un determinado puesto de trabajo –aunque no reflejen la concreta enfermedad o problema de salud que tiene por imposición del principio de confidencialidad–, por datos de salud a efectos de tratamiento de esos datos habrá que entender también los que se reflejan en las conclusiones, a los que serán de aplicación las disposiciones que la LOPD reserva para aquéllos.

Así parece, además, deducirse de la definición dada por la Recomendación sobre protección de datos médicos que incluye en estos términos los que tengan una clara y estrecha relación con la salud, y de las declaraciones de algunos autores que consideran que en el concepto de datos sobre salud hay que incluir aquellos datos administrativos, contables o fiscales que puedan tener relación con la salud [61], para evitar conductas y actuaciones que, «aludiendo aspectos tangenciales, vulneren de manera flagrante la intimidad de las personas» [62].

2.2.2. Las medidas de seguridad.

2.2.2.1. Concepto y finalidad.

Las medidas de seguridad constituyen un instrumento de especial importancia en el tratamiento de datos derivados de la práctica de la vigilancia de la salud en la medida en que cualquier filtración de los mismos no sólo puede vulnerar la intimidad, sino llegar a atentar, más directamente que en otros ámbitos, contra la dignidad y la igualdad pues esa filtración de datos puede llegar a crear empresas con «trabajadores a la carta».

---

60 La Agencia justifica esa incorporación de las propias manifestaciones sobre salud psíquica –entiendo, así, que también las propias manifestaciones subjetivas sobre salud física e incorporadas a una historia clínica o documento– en evitar que se proceda al tratamiento de estos datos «con base en meras sospechas o apreciaciones subjetivas que no presentasen una constatación fáctica real, generando una situación de riesgo que pudiera, con base en dichas sospechas, crear una situación social de prejuicio hacia las personas cuyos datos psicológicos negativos hubieran sido incorporados a un fichero automatizado» ÁLVAREZ CIVANTOS, O.J.: *Normas para la implantación de una eficaz protección de datos…*, *op. cit.*, pág. 117, advirtiendo, además, de la trascendencia que esto puede tener en situaciones en las que las empresas obtienen datos o realicen valoraciones psicológicas, con base en preguntas formuladas con finalidades no relacionadas directamente con la salud.

61 ALONSO MARTÍNEZ, C.: «Aproximación a determinados conceptos del RD 994/1999, de 11 de junio, sobre medidas de seguridad», *Actualidad Administrativa Aranzadi*, núm. 35, 2000, pág. 11. Considera que en la definición sobre datos relativos a la salud se encontrarían los relativos a minusvalías a efectos del cálculo de IRPF, los datos relativos a las bajas por causas de enfermedad, los diagnósticos médicos realizados en empresas mediante concierto con entidades médicas, etc.

62 FREIXAS GUTIÉRREZ, G.: *La protección de los datos de carácter personal en el derecho español*, Barcelona, Bosch, 2001, pág. 146.

Su regulación se encuentra en el artículo 9 de la LOPD y, hasta nuevo desarrollo reglamentario, en el RMSFA, declarado vigente, como se señaló, por la LOPD [63]. Pueden definirse como «las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal» (art. 1 del RMSFA) en aras de la protección de la intimidad, el honor y el pleno ejercicio de los derechos personales –en este caso de los trabajadores– frente a su alteración, pérdida, tratamiento o acceso no autorizado [64].

En su establecimiento, debe tenerse en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que están expuestos ya provengan de la acción humana o del medio físico o natural, prestando especial atención a los ficheros que contengan datos sobre salud u otros datos sensibles del artículo 7 de la LOPD, como ideología o religión (art. 9.1 en relación con el art. 9.3 de la LOPD).

El RMSFA estructura las medidas a aplicar en tres niveles: básico, medio y alto, en aras de garantizar determinados grados de confidencialidad e integridad de la información según el tipo de datos (art. 3 RMSFA). Se aplican a cada uno de los concretos ficheros que la empresa haya creado. Los que contengan datos de salud deberán estar protegidos con los tres niveles.

Estas medidas van a reflejarse en el denominado documento de seguridad en el que se reflejarán más o menos aspectos destinados a cubrir esa seguridad en función de si a los datos que se van a tratar les corresponde un nivel de seguridad básico, medio o alto, teniendo en cuenta las pautas que se recogen en los artículos 9 a 26 de ese RMSFA [65]. Este documento deberá mantenerse actualizado en todo momento y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo (art. 8.3). En esta actualización, conforme al artículo 9 de la LOPD, debe tenerse en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos los mismos. Es de obligado cumplimiento para el personal con acceso a los datos, en nuestro caso, relacionados con la vigilancia de la salud (art. 8.1 RMSFA) lo que implica que la empresa o el servicio de prevención, como se verá, responsables del fichero o tratamiento, deberán entregarlo a cualquier persona que tenga acceso a los datos derivados de la vigilancia de la salud y podrá establecer, a propósito de su entrega –aunque también antes o después–, claúsulas de confidencialidad [66] en el propio contrato labo-

63 Debe ponerse de relieve que, si la LOPD se aplica también a los ficheros no automatizados, este Reglamento debe aplicarse por analogía también a los mismos en la medida en que la aplicación del contenido de sus normas tenga algún sentido para los ficheros no automatizados.

64 *Vid.* Exposición de Motivos del RMSFA.

65 Pautas sobre los siguientes aspectos: funciones y obligaciones del personal; registro de incidencias; identificación y autentificación; control de acceso físico e informático y registro de accesos; copias de respaldo y recuperación; auditorías; pruebas; distribución de soportes y telecomunicaciones.

66 Recomendadas por ÁLVAREZ CIVANTOS, O.J.: *Normas para la implantación de una eficaz protección de datos…*, *op. cit*, págs. 193-194.

ral para todo empleado al que se asignen funciones de tratamiento de datos cuyo incumplimiento daría lugar a una vulneración de la buena fe contractual con la posibilidad de despido conforme al artículo 54.2.d) del ET, teniendo en cuenta, además, que cualquier sujeto que tenga que ver con el tratamiento de datos debe guardar secreto sobre los mismos con fundamento en el artículo 10 de la LOPD [67] que viene a reforzar la exigencia de confidencialidad de la LPRL. Entrega de documento y cláusula de confidencialidad constituyen, así, una forma de frenar o aminorar la responsabilidad de empresarios y servicios de prevención por incumplimientos derivados de la protección de datos, además de una garantía para los trabajadores cuyos datos van a ser objeto de tratamiento.

Este documento cuando se refiere a los datos sobre salud debe contener los siguientes extremos: qué datos son los protegidos; las medidas, procedimientos o reglas encaminadas a garantizar el nivel de seguridad exigido (entre ellas medidas de identificación, de control de acceso o de manejo de los soportes informáticos); las funciones y obligaciones del personal que tenga que ver con la utilización de ese fichero; estructura del fichero y descripción de los sistemas de información que tratan los datos incluidos en el mismo; procedimiento de notificación, gestión y respuesta ante los problemas que pueda haber con el manejo de ese fichero; procedimiento de realización de copias de respaldo y de recuperación de datos (art. 8.2 RMSFA); identificación del responsable o responsables de seguridad; controles periódicos para verificar el cumplimiento de lo establecido en el documento; y medidas a adoptar en caso de reutilización o desecho de soportes (art. 15 RMSFA).

De alguna manera se pretende que ese documento contenga las garantías precisas para –en virtud de lo dispuesto en el artículo 9 de la Recomendación sobre datos médicos y conforme a una interpretación integrada de la LOPD y del RMSFA– impedir, en primer lugar, que cualquier persona no autorizada tenga acceso a las instalaciones de procesamiento de datos personales [68]. En segundo lugar, que el soporte de los datos sea leído, copiado, alterado o retirado por personas no autorizadas. En tercer lugar, la introducción no autorizada de datos en el sistema de información, y cualquier consulta, modificación o borrado no autorizados de datos procesados –controlar la memoria del fichero–. En cuarto lugar, que los sistemas de procesamiento automatizado de datos sean usados por personas no autorizadas a través de equipos de transmisión de datos y, por último, impedir, a su vez, la lectura, copia, alteración o borrado no autorizados de datos personales durante la comunicación y el traslado de soportes de los mismos.

Una vez establecida la finalidad de estas medidas, se hace preciso determinar qué sujetos intervienen en la articulación de las mismas e identificar estos sujetos con aquellos que tienen que ver con la obligación de vigilancia de la salud.

---

67 «El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo».

68 Que en nuestro caso sería controlar qué personas tienen llave de acceso a la oficina donde se encuentra el ordenador o el fichero manual donde se recopilan y procesan los datos de vigilancia de la salud.

2.2.2.2. Sujetos.

El sujeto más importante a efectos de tratamiento de datos es, sin duda, el responsable del fichero, término que, en vigilancia de la salud, remite inmediatamente a servicios de prevención o a empresa por lo explicado en relación con los resultados o las conclusiones, pero que también puede llevar a pensar en una multiplicidad de sujetos que intervienen en todo el tratamiento de datos, como son grabadores, analistas, programadores, etc. Si bien, interesa una identificación concreta desde el punto de vista jurídico para lo que hay que acudir a la definición dada por la LOPD en su artículo 3.d) donde señala que el responsable del fichero es «la persona física o jurídica, pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento». Es, así, aquella persona que tiene la capacidad de tomar decisiones sobre el objeto, utilización y fin del tratamiento o sobre el uso que se va a dar a los datos de carácter personal resultantes del tratamiento independientemente de si ha sido o no quien ha creado el fichero o lo gestiona [69]. Lo que caracteriza al responsable del fichero es el poder de decisión sobre el tratamiento de datos, distinguiéndose, así, del encargado del tratamiento como la concreta persona jurídica, física, autoridad pública, servicio o cualquier otro órgano que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento [art. 3.g) LOPD], es decir, siguiendo las instrucciones de ese responsable, pero, en virtud del artículo 12 de la LOPD, no bajo la dependencia o autoridad del mismo desde el punto de vista laboral, sino a través de un contrato de *outsourcing* y con responsabilidad equivalente al responsable del fichero conforme al artículo 43 de la LOPD [70].

En el ámbito de la vigilancia la definición de «responsable de fichero» conduce a la siguiente determinación de los sujetos: conforme a lo explicado *supra*, podría concluirse que en los ficheros de resultados el responsable del fichero sería el servicio de prevención, pues es quien decide sobre la finalidad, contenido y uso del tratamiento, aunque estas funciones vengan justificadas por el mandato de la empresa ante la obligación de vigilancia de la salud que tiene que ejecutar, obligación que, en principio, no justificaría constituir como responsable del fichero de resultados a la empresa, pues no puede tener acceso a los mismos.

---

69 La LORTAD, sin embargo, sí que distinguía entre el titular del fichero y el responsable del mismo, creando, en ocasiones, consecuencias perturbadoras, sobre todo en los procedimientos sancionadores (VIZCAÍNO CALDERÓN, M.: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal, op. cit.*, pág. 79).

70 Si se quieren poner a disposición los datos a través de Internet con claves para que los distintos interesados y sólo ellos puedan consultarlos, los modelos de *outsourcing* más utilizados, siguiendo a TÉLLEZ, son, por un lado, el contrato *hosting* y por otro el llamado contrato *housing*. El *hosting* es aquel en el que el encargado del tratamiento se limita a facilitar al responsable del fichero o tratamiento el emplazamiento, el hardware y las líneas de comunicación necesarios para poder realizar el tratamiento de los datos. Su responsabilidad es por la seguridad física de las máquinas, ya que es él quien puede disponer del emplazamiento y, por tanto, de la seguridad física que precise, salvo que se haya estipulado expresamente lo contrario, y el responsable del tratamiento deberá aplicar las medidas de seguridad lógicas. En el *housing*, el proveedor o encargado del tratamiento presta toda la infraestructura para que el cliente introduzca sus datos y contenidos; además, explota el sistema. En este caso la responsabilidad en cuanto a la seguridad de evitar los accesos no autorizados es imputable a la empresa de *housing*, por lo que responderá de la efectiva aplicación de las medidas que se hayan determinado en el contrato y el documento de seguridad (TÉLLEZ AGUILERA, A.: *Nuevas Tecnologías. Intimidad y protección de datos*, Madrid, Edisofer, 2001, págs. 119-121).

En los ficheros de conclusiones, sin embargo, el responsable sería el servicio de prevención o el empresario si ya ha elaborado su propio fichero con este contenido. Sobre este particular, debe insistirse en la conveniencia de que el empresario elabore su propio fichero de conclusiones cuando contrata la obligación de vigilancia con un servicio de prevención mancomunado o externo para evitar el acceso masivo de las empresas a las conclusiones custodiadas por los mismos. Se pueden dar claves de acceso para entrar al concreto archivo donde se recojan los datos de las conclusiones correspondientes a la vigilancia de la salud de una concreta empresa, pero en aras de conseguir la máxima seguridad en el acceso a los datos es preferible su comunicación directa a las empresas implicadas y que éstas sean las que creen sus propios ficheros. En realidad, más que conveniente casi se hace obligatoria esa creación de fichero de conclusiones propio de la empresa, pues va a decidir las medidas a adoptar en vigilancia de la salud con base en esas conclusiones y lógico es que pase a ser responsable del fichero al que van a tener acceso, también, como se señaló, otros órganos o personas físicas con responsabilidad preventiva. Otra cosa es que para la imputación de responsabilidades derivadas de una manipulación inadecuada de datos de esas conclusiones haya que averiguar si ha venido del «responsable del fichero servicio de prevención» o del «responsable del fichero empresa». Cosa distinta es el fichero de conclusiones en los servicios de prevención propios. En este caso no haría falta la creación de un nuevo fichero en la empresa puesto que se entiende ya creado en la medida en que este servicio es considerado parte de la misma. El responsable sería el empresario, aunque la gestión correspondería al servicio de prevención propio.

Ahora bien, estas afirmaciones, si bien pueden sostenerse para los ficheros de conclusiones porque conducen a constituir al empresario como responsable del fichero, arrojan ciertas dudas en el caso de los ficheros de resultados porque de la Doctrina [71] y la Jurisprudencia [72] se extrae, en general, la idea de que a quien se denomina responsable del fichero es a la empresa englobando también en este término a los servicios de prevención externos como empresas dedicadas a ofrecer a otras actividades preventivas, pero debiendo excluir a los servicios de prevención propios o mancomunados porque tal y como los configura la LPRL no son entes independientes, forman parte de la propia empresa. Esto, en principio, no ofrece ningún problema si no se tratara de unos datos tan íntimos como los de salud incorporados a los resultados de la vigilancia y del gran poder –aunque también asume responsabilidades– que en cuanto al tratamiento tiene el responsable del fichero en la LOPD –entre cuyas funciones se encuentra la de la elaboración del documento de seguridad–, poder que podría llegar a desvirtuar la confidencialidad de los resultados.

Para articular, así, mecanismos de respeto hacia esos resultados la empresa debe optar por una delegación de sus funciones de responsable del fichero, concreta y determinada por escrito, en una

71 Por todos, APARICIO SALOM, J.: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Pamplona, Aranzadi, 2000, pág. 33; ÁLVAREZ CIVANTOS, O.J.: *Normas para la implantación de una eficaz protección de datos…*, *op. cit.*, pág. 169; VIZCAÍNO CALDERÓN, M.: *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, págs. 78-81.

72 Por todas, STC 202/1999, de 8 de noviembre.

persona integrante del servicio de prevención propio o mancomunado [73] –de éste una o un grupo de personas por cada una de las empresas constituyentes del mismo– para abstenerse de posibles injerencias en esos resultados [74].

No obstante, en aras del control del cumplimiento por la entidad de las exigencias establecidas en la LOPD y, en particular, del respeto de los derechos afectados por el tratamiento, el RMSFA, en sus artículos 2.11 y 16, regula la figura del responsable de seguridad. Es exigida para toda entidad que realice tratamiento de datos que exijan la aplicación de medidas de seguridad de nivel medio o alto. Son las personas físicas o jurídicas [75] a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables, pero que no eximen de responsabilidad al responsable del fichero. Debería ser una persona que tuviera conocimientos de informática suficientes para introducir –u orientar sobre su introducción– las medidas que corresponden a todos los ficheros de conclusiones o resultados sobre datos de salud para garantizar los principios y derechos derivados del tratamiento de datos a los que se hará referencia posteriormente. Además, debería tener conocimientos jurídicos para la coordinación de aspectos legales u organizativos que requieran esas medidas (procedimientos de acceso, rectificación, oposición y cancelación, cesiones de datos y encargos de tratamiento, etc.). Para la coordinación de medidas de seguridad que tuvieran que ver con los ficheros de vigilancia de la salud debería formar parte del servicio de prevención, independientemente de que la empresa tuviera otros responsables de seguridad para otros ficheros. Si esto no es posible, deberá actuar con la mayor confidencialidad posible frente a la empresa en toda la gestión de esas medidas de seguridad aplicadas a la vigilancia de la salud.

Además, es importante señalar el concepto de usuario como todo sujeto o proceso autorizado para acceder a datos o recursos (art. 2.2 del RMSFA) que en el supuesto tratado serían todos aquellos sujetos relacionados con la posiblilidad de conocer resultados o conclusiones (delegados de prevención, psicólogos, médicos, representantes de los trabajadores, etc.). Este concepto viene, en parte, a identificarse con el de tercero –regulado por la Directiva de protección de datos en su artículo 2.f) que la LOPD no incorporó [76] – y debe distinguirse del de afectado o interesado que, en el caso tra-

---

73 En el País Vasco, por ej., el Decreto núm. 78/2000, de 16 de mayo de 2000, por el que se regula la Organización y Funcionamiento del Servicio de Prevención Propio de la Administración y sus Organismos Autónomos (BOPV de 19 de junio) establece en su artículo 5 que «el personal sanitario del Servicio de Prevención o cualquier otra persona que por su cargo u ocupación tuviera conocimiento de datos médico-personales garantizará el respeto a la dignidad e intimidad de la persona y la confidencialidad de dichos datos. Para ello, dispondrán de los equipos y material de archivo con los sistemas de custodia que garanticen la confidencialidad de los datos, de acuerdo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal», apostando, así, por una delegación de funciones.

74 Sin perjuicio de que la empresa asuma responsabilidades analizadas *infra*.

75 El tenor literal del artículo 16 del RMSF, «uno o varios responsables de seguridad» puede hacer pensar en la exclusión de las personas jurídicas ya que parece referirse a personas individuales, pero también podría interpretarse que «uno» o «varios» se refiere a grupos, como otras empresas, dedicados a articular medidas de seguridad en las empresas, aunque entonces podría considerarse quizá encargado de tratamiento.

76 Aunque sí que se tuvo en cuenta en el proceso de tramitación parlamentaria de esta Ley. Así, *vid.* Enmienda núm. 47 del Grupo Parlamentario Socialista (BOCG-CD, serie A, núm. 135-7, de 4 de noviembre de 1998) que lo definía, en términos prácticamente idénticos a la Directiva, como aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo distinta del afectado, del responsable del fichero, del encargado del tratamiento o de personas autorizadas para tratar los datos bajo la autoridad directa del responsable del fichero o del encargado del tratamiento.

tado, sería el trabajador, pues es la persona física titular de los datos que sean objeto del tratamiento [art. 3.e)] de la LOPD, a pesar de que se comportaría como usuario si tiene que acceder a determinada página de Internet de la empresa o servicio de prevención para conocer sus datos.

Una vez concluido quiénes son los sujetos intervinientes en la aplicación y creación de las medidas de seguridad, hay que seguir concretando las mismas en relación con la vigilancia de la salud haciendo especial hincapié en los sistemas de identificación y autenticación.

2.2.2.3. Sistemas de identificación y autenticación [77].

Las medidas de seguridad deben garantizar la posibilidad de comprobar y establecer *a posteriori* quién ha tenido acceso al sistema y qué datos personales han sido introducidos en el sistema de información, cuándo y por quién. Para su consecución, el RMSFA exige al responsable del fichero unas medidas muy severas en cuanto al acceso a estos datos relacionados con la salud y la identificación de quien accede. Así, debe llevar una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y establecer procedimientos de identificación y autenticación para dicho acceso tales como contraseñas que deben asignarse, distribuirse y almacenarse de forma que se garantice su confidencialidad e integridad y cambiarse periódicamente para cumplir con ese fin (art. 11 RMSFA). Esas contraseñas deberán permitir la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado, limitándose la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información (art. 18 RMSFA). Estas contraseñas deben servir también para que el personal de la empresa o de los servicios de prevención tenga tan sólo acceso a los datos que le conciernen (art. 12 RMSFA) [78], de ahí la importancia de establecer en el documento la estructura de los ficheros. El personal médico tendrá acceso a los datos de los exámenes de salud físicos, y los psicólogos y sociólogos a los datos sobre los exámenes de salud psico-sociales. Cuestión distinta es que se haga una comunicación conjunta de los mismos para llegar a las oportunas conclusiones y que el acceso a los datos de las mismas sea común. Es importante que exista una separación de datos referidos a la salud del trabajador para evitar la obtención de una completa información destinada a posibles fines ilícitos que pudieran atentar contra sus derechos fundamentales. Debe garantizarse al trabajador que el acceso a sus datos se hace de forma selectiva, que el acceso se restringe a determinadas personas y para aquellos datos que precisen para el correcto desarrollo de sus funciones. Además, el artículo 24 del RMSFA exige, como medida de seguridad de nivel alto, la necesidad de que se registren en cada acceso la identificación de cada usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado, y que este registro se guarde, al menos, durante dos años. Esta información registrada debe revisarse periódicamente y elaborar un informe de esas revisiones y problemas detectados al menos una vez al mes.

77 No sólo constituyen una garantía para los trabajadores de la empresa, sino también para la propia empresa que puede sufrir las consecuencias de no disponer de sistemas de seguridad en los accesos a determinadas informaciones (*vid.* STSJ de Cataluña, de 10 de octubre de 2000 –RJ 2000/47830–).

78 Para evitar conductas fraudulentas de aquellos que teniendo medios a su alcance para desempeñar determinadas funciones los utilizan para obtener información ajena a la que no deberían acceder (*vid.* STSJ de Madrid, de 28 de marzo de 2000).

A propósito de estos sistemas de identificación y autenticación para el acceso, debe señalarse que, si bien el establecimiento de códigos de usuario y contraseñas son los métodos más utilizados hasta el momento que deben reunir las características señaladas, su carácter personal y transferible –por el mero olvido en lugar accesible por otros, por ejemplo– hace conveniente que, al menos, en lo que a datos sobre salud se refiere, las empresas se acostumbraran a incorporar sistemas de identificación biométrica.

Los datos biométricos son aquellos aspectos físicos, específicos y únicos de cada individuo que, sometidos a un análisis técnico, permiten su identificación inequívoca. Se incluirían las huellas digitales, la palma de la mano, la huella plantar, el aspecto del iris del ojo, la modulación de la voz, el ADN, etc. [79]. Todos ellos garantizan que quien se identifica frente a un medio electrónico de control que es capaz de emplear tales medios es la persona que dice ser, de modo que otorgan una efectividad y seguridad prácticamente absoluta a los sistemas de control de acceso a dependencias o sistemas informáticos, frente a los problemas que acarrea la memorización de las contraseñas. Su utilización es perfectamente lícita para esta finalidad de acceso a ficheros relacionados con la vigilancia de la salud salvo el recurso al ADN, que sería un medio desproporcionado, pues revela datos sobre la salud o personalidad del individuo.

Por otra parte debe señalarse que, unido a estos sistemas, hay que garantizar la posibilidad de comprobar y verificar a qué personas u órganos se pueden comunicar los datos a través de los correspondientes equipos de transmisión. Debe hacerse, en el caso de la vigilancia de la salud, un control exhaustivo de la comunicación de los datos a través del correo electrónico, por ejemplo, para evitar posibles filtraciones a los responsables de la empresa que no deban enterarse de los resultados de los exámenes de salud. Debería introducirse, en el sistema informático utilizado, los datos de las personas físicas o jurídicas a las que puede ir dirigida la transmisión de los datos relacionados con la vigilancia de la salud y un mecanismo de bloqueo de la transmisión si no van dirigidos a ninguna de esas personas. No obstante, para evitar una posible enervación de los mecanismos informáticos por personas afines a la empresa, sería conveniente plantearse, en algunos casos, una comunicación directa en soporte papel –propuesta que ya se apuntó *supra*–.

2.2.2.4. Otras medidas.

El RMSFA recoge también normas sobre gestión de soportes informáticos que contienen esos datos (arts. 13 y 20), pues la seguridad de los datos personales objeto de tratamiento comporta no sólo una obligación de controlarlos mientras se encuentran dentro de los sistemas informáticos, sino también la de controlar sus salidas y el uso que de ellos se haga mientras estén fuera de las instalaciones de la empresa, control especialmente importante si estos datos son de los considerados sensibles. Estas normas sobre gestión de soportes obligan a adoptar medidas para evitar que en los supuestos de eliminación, reutilización o mantenimiento del soporte se consiga una recuperación de

[79] Por todos, para el concepto y ejemplo, APARICIO SALOM, J.: *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, *op. cit.*, pág. 54.

la información almacenada que pueda ser utilizada con fines inadecuados, y, a su vez, en el caso de que sea necesaria la transmisión de esos datos a través de redes de telecomunicaciones, para cifrarlos o utilizar cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros (art. 26 RMSFA).

Por otro lado, en el documento de seguridad debe hacerse referencia al procedimiento de notificación, gestión y respuesta ante las incidencias, debiendo contener un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la misma (art. 10 RMSFA). Como son datos relativos a la salud deberán consignarse, además, los procedimientos de recuperación de datos realizados –actividad para la que se requiere autorización del responsable del fichero– indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación (art. 21 RMSFA).

Además, los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría, que conforme al artículo 17 del RMSFA puede ser interna o externa. Estimo que en el supuesto de tratamiento de datos derivados de la práctica de la vigilancia, en aras de una objetividad especialmente necesaria en este caso, debería ser externa para garantizar con más contundencia el respeto a la intimidad de los trabajadores que puede verse afectada por una auditoría interna en la que se puedan filtrar los datos de sus exámenes médicos.

Esta auditoría debe realizarse, como mínimo, cada dos años y debe dictaminar sobre la adecuación a las medidas y controles del RMSFA, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias debiendo justificar estas decisiones (art. 17.2 RMSFA). Quedará a disposición de la AEPD (art. 17.3). Nada obsta para que la auditoría practicada a las empresas que organizan su sistema de prevención con recursos propios (art. 29 y ss. del RSP) pueda aprovecharse, también, para aplicarla a este tratamiento de datos.

2.2.2.5. Creación, modificación o supresión de ficheros.

Como medidas de seguridad pueden considerarse también los requisitos exigidos a la Administración pública [80] y empresas privadas para la creación, modificación o supresión de estos ficheros en aras de la protección del derecho a la intimidad del trabajador y que se recogen no sólo en la LOPD –arts. 20 a 26–, sino también en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal [81] –que sigue en vigor conforme a la Disposición Transitoria Tercera de la LOPD–.

80 Tanto Administración central, autonómica o local (*Vid.* art. 41 y ss. de la LOPD).

81 BOE de 21 de junio de 1994.

De estos artículos se deduce que el carácter público del fichero atiende a un dato puramente subjetivo: la naturaleza administrativa de los órganos a los que pertenecen. Si éstos no tienen naturaleza pública, el fichero debe reputarse privado, aun cuando coadyuve, en todo o en parte, al ejercicio de funciones públicas.

Los ficheros de los servicios de prevención propios o mancomunados que pertenezcan a las Administraciones Públicas, de acuerdo con el dato subjetivo de la naturaleza pública del órgano al que atiende la LOPD, serán también públicos, si bien, creo que esto requeriría alguna reforma *de lege ferenda* exceptuando algún requisito de constitución como el hecho de la disposición general publicada en el BOE o Diario Oficial correspondiente [82]. Las Administraciones Públicas, conforme al artículo 103 de la CE, deben servir con objetividad los intereses generales para los que sin duda se hacen necesarios los ficheros «que han de tener una regulación privilegiada con relación a los ciudadanos, limitando sus derechos cuando puedan llegar a colisionar con el interés público» [83]. Es así que en cuanto con ellos se consigue un mejor servicio para los ciudadanos es importante que existan ficheros de gestión de procedimientos administrativos, gestión de estadísticas internas, gestión tributaria y de recaudación, gestión económica con terceros, gestión de función estadística pública, gestión del Padrón e, incluso, gestión de personal, pero considero que un fichero de los servicios de prevención de la Administración no contribuye, al menos directamente, a un mejor servicio al ciudadano [84] y, por tanto, aun considerándose ficheros públicos porque su titular tiene este carácter, deberían tener otro tipo de regulación más asimilable quizá a los de titularidad privada.

2.2.3. Principios y derechos de la LOPD de aplicación a la vigilancia de la salud.

Resulta de gran interés analizar y exponer qué principios debe cumplir cualquier tratamiento de datos obtenidos tras la práctica de la vigilancia de la salud, principios que suponen una garantía de respeto a los derechos de los trabajadores y que demuestran que un fichero manual o informatizado no es algo arbitrario o una simple recogida de datos en un determinado ordenador, sino un almacén al que hay que dotar de todas las garantías precisas para realizar una vigilancia de calidad. A estos principios se añaden los derechos derivados del tratamiento para la persona afectada por el mismo que vienen a aumentar el elenco de derechos que deben respetarse en la práctica de esa vigilancia de la salud.

---

82 Requisito, no obstante, que podría obviarse si en la normativa por la que se constituyen servicios de prevención propios o mancomunados, se hace referencia también a esta creación de ficheros.

83 FREIXAS GUTIÉRREZ, G.: *La protección de los datos de carácter personal en el derecho español, op. cit.*, pág. 221, haciendo referencia a la STC 110/1984, de 26 de noviembre.

84 Cosa distinta es la de aquellos ficheros que inciden sobre aspectos preventivos pero se establecen como control y garantía respecto a los que pueden tener un interés en los mismos. Así, el Decreto núm. 36/1999, de 4 de marzo, de la Comunidad de Madrid, por el que se crea el Registro, el fichero manual y el fichero automatizado de datos de carácter personal de profesionales que ostentan certificación para ejercer las funciones establecidas en el RSP (BOCM, de 31 de marzo).

Los principios se encuentran regulados en el artículo 4 de la LOPD y se aplican tanto a la recogida y almacenamiento de los datos, como a la utilización de los mismos contenidos en los ficheros de la empresa o de los servicios de prevención.

2.2.3.1. Los principios de finalidad, pertinencia y licitud.

Relacionado con la propia creación del fichero, se encuentra el principio de finalidad. Un fichero debe tener un fin concreto y lícito. En este caso es la recogida de datos relacionados con la salud física, psíquica o social del trabajador para cumplir con la obligación de practicar una adecuada vigilancia de la salud en relación con los concretos riesgos del puesto de trabajo que esté desempeñando el trabajador. Los datos incorporados en el fichero no deben convertirse en base de discriminaciones ni deben ser utilizados para fines incompatibles –como literalmente dispone el artículo 4.2 de la LOPD– con la prevención. Así, la finalidad debe ser, prioritariamente, la prevención y, conforme a ese tenor literal del artículo 4.2 de la LOPD, también son posibles fines compatibles con la misma [85], compatibilidad que debe interpretarse, en el ámbito tratado, de forma extremadamente restrictiva, teniendo muy en cuenta el principio de proporcionalidad, para evitar perjuicios al trabajador.

Además, hay que tener en cuenta que para cumplir con ese principio de finalidad, será necesario que los datos sean «adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido» (art. 4.1 de la LOPD). Adecuación, pertinencia y no excesividad que recuerdan el principio de proporcionalidad que supone que a la hora de seleccionar los datos que deben incorporarse a un fichero para su posterior tratamiento deba determinarse si éstos son aptos para conseguir el fin propuesto y si se encuentran en una relación razonable o proporcionada con la importancia del interés que se trata de proteger para no vulnerar la intimidad informática del trabajador, proporcionalidad que deberá ser valorada, a su vez, en los supuestos de compatibilidad.

Así, como ha puesto de manifiesto el TC, no pueden incorporarse datos derivados de la vigilancia de la salud a un fichero de control del absentismo con baja médica porque éste no tiene una finalidad preventiva y, por tanto, esa inclusión se consideraría desproporcionada [86].

---

85 Entre los que se encuentran los fines históricos, estadísticos o científicos siempre que se establezcan las garantías oportunas [art. 4.2 *in fine* de la LOPD y art. 6.1.b) Directiva 95/46/CE].

86 *Vid.* STC 202/1999, de 8 de noviembre –BOE de 16 de diciembre–, manifestando lo siguiente: «A la vista del contenido del fichero, forzoso resulta convenir que su mantenimiento no se dirige a la preservación de la salud de los trabajadores, sino al control del absentismo laboral, lo que, por otra parte, resulta plenamente acorde con la denominación "absentismo con baja médica" que recibe el fichero. Consecuentemente, la creación y actualización del fichero, en los términos en que se ha llevado a efecto, no puede ampararse, frente a lo sostenido por la empresa en la existencia de un interés general…. que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento automatizado de los datos atinentes a su salud, ni tampoco en lo dispuesto en los artículos 22 y 23 de la Ley de Prevención de Riesgos Laborales, habida cuenta de que en el fichero en cuestión no se reflejan los resultados arrojados por la vigilancia periódica –y consentida por los afectados del estado de salud de los trabajadores en función de los riesgos inherentes a su actividad laboral–, sino tan sólo la relación de períodos de suspensión de la relación jurídico-laboral dimanantes de una situación de incapacidad del trabajador» (FJ 4.º). «… el expresado tratamiento informático –con vistas a su conservación– de los datos referidos a la salud de los trabajadores de que tenga conocimiento la empresa quiebra la aludida exigencia de nítida conexión entre la información personal que se recaba y el legítimo objetivo para el que fue solicitada» (FJ 5.º).

Otro de los principios con relevancia en el ámbito de la vigilancia de la salud es el de licitud o legalidad recogido en el artículo 4.7 de la LOPD que supone la prohibición de la recogida de datos por medios fraudulentos, desleales o ilícitos, como pueden ser los datos obtenidos con dolo [87] o coacciones o a través de una investigación privada realizada por el propio empresario o un tercero encargado por éste sobre los hábitos de vida del trabajador que pueden influir en su salud.

2.2.3.2. El principio de veracidad y los derechos de rectificación y cancelación.

También es importante señalar el principio de veracidad que exige que los datos de carácter personal almacenados sean exactos y estén actualizados para que el trabajador no se vea lesionado en su posición jurídica, en la medida en que la empresa puede tomar decisiones erróneas sobre la base de unos datos inexactos o que han cambiado con el paso del tiempo e ir en detrimento de la propia protección de su salud.

Este principio de veracidad supondrá que si los datos son inexactos o incompletos para el fin de la vigilancia de la salud deberán ser cancelados y sustituidos de oficio o a petición del trabajador por los correspondientes datos rectificados o completados (art. 4.4 de la LOPD) y trae como consecuencia el derecho de ese trabajador, precisamente, a esa cancelación o rectificación regulado en el artículo 16 de la LOPD. Así, el derecho a la rectificación permite completar o corregir los datos de carácter personal, en este caso sobre salud, incluidas en un fichero. En el ámbito estudiado puede darse, por ejemplo, en supuestos en los que una persona tras un determinado examen de salud se encuentra apta para el desempeño del trabajo y pasado un tiempo antes de realizar otro examen nota algún síntoma de malestar que puede estar relacionado con las circunstancias del puesto de trabajo, lo comunica y tras el oportuno examen se rectifican los datos; o cuando le remiten los resultados y no está de acuerdo con sus datos de anamnesis. Si se comprueba que, efectivamente, los datos son inexactos o incompletos, el responsable del tratamiento procederá a su rectificación o cancelación dentro del plazo de diez días –se entiende que serán hábiles, aunque nada dice la LOPD–.

Por su parte, el derecho a la cancelación se dirige a eliminar físicamente del fichero los datos relacionados con la salud que resulten inservibles para la finalidad preventiva de vigilancia [88], si bien, como señala el artículo 16.3 de la LOPD, antes de producirse esa eliminación física se llevará a cabo un bloqueo de datos –entendiendo por tal la identificación y reserva de datos con el fin de impedir su tratamiento (art. 1.1 del RD 1332/1994)– para conservarlos a disposición de las Administraciones Públicas, Jueces o Tribunales «para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas». Cumplido el citado plazo deberá procederse a la supresión. Este bloqueo de datos también se producirá en los supuestos en los que,

87 Por ejemplo, con falsedad sobre el tipo de tratamiento de los datos, no comunicando, por ejemplo, que se va a transmitir inmediatamente a una tercera empresa.

88 No obstante, si los datos son pertinentes para otro fin compatible con el de vigilancia, conforme al tenor literal del artículo 4.2 de la LOPD, no habría que proceder a su cancelación, sino a comunicar o pedir el consentimiento sobre esta otra finalidad a la que van a ser destinados (en este sentido, FERNÁNDEZ DOMÍNGUEZ, J.J.; RODRÍGUEZ ESCANCIANO, S.: *Utilización* y *control de datos laborales...*, *op. cit.*, págs. 214 y 215).

siendo ya definitivamente procedente la cancelación de los datos, no sea posible su extinción física por razones técnicas y/o por causa del procedimiento o soporte utilizado, aunque si los datos son recogidos o registrados por medios fraudulentos, desleales o ilícitos, no se bloquearán, se destruirá directamente ese soporte utilizado (art. 16 del RD 1332/1994). Además, también debe advertirse que, conforme ha señalado la AEPD [89], la cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros, aunque en este caso parece que sí que debería procederse, al menos, al bloqueo de datos.

Esa eliminación física de los datos debe entenderse en la literalidad de sus términos, es decir, debe realizarse una destrucción total de esos datos, sin que sea suficiente, por tanto, una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas [90].

Este derecho de rectificación y cancelación implicará, también, la comunicación a aquellas empresas, servicios o autoridades a quienes se les haya cedido datos relacionados con la vigilancia de la salud para que procedan, a su vez, a ejecutar esos derechos (art. 16.4 LOPD).

2.2.3.3. El derecho de acceso a los datos contenidos en los ficheros.

Estos derechos están íntimamente unidos al derecho de acceso, regulado en el artículo 15 de la LOPD, en la medida en que sin éste difícilmente podrán ejercerse aquéllos si no se conoce qué datos se recogen en el fichero. En la vigilancia de la salud este derecho de acceso se materializa en la comunicación de los resultados y conclusiones de los exámenes practicados que es, junto a las anotaciones subjetivas del personal del servicio de prevención, lo que va a insertarse en el fichero. No obstante, este derecho permite ir más allá de estos extremos. Si el trabajador lo solicita, debe darse constancia de los datos que han sido cedidos o entregarle otra copia de datos específicos dentro de sus resultados como un análisis de orina, por ejemplo.

No será de aplicación a este derecho de acceso en el ámbito de la vigilancia de la salud el apartado 3 del artículo 15 de la LOPD, en la medida en que señala que sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo, pues este derecho se activará siempre que se practique la vigilancia de la salud en la empresa o se realice alguna prueba relacionada con la misma, aunque sí que podría ser de aplicación para otros supuestos, como la solicitud para conocer a quiénes se han cedido sus datos de salud. Además, habrá que tener en cuenta que para los trabajadores con un contrato temporal el plazo, necesariamente, habrá de ser menor [91]. La solicitud de copias puede realizarse también sin sometimiento a ese intervalo de tiempo, pero parece que deberían estar justificadas: para información urgente del propio trabajador, por ejemplo.

89 *Vid.* Norma 3.ª de la Instrucción 1/1998, de 19 de enero, de la AEPD, relativa al ejercicio de los derechos de acceso, rectificación y cancelación (BOE de 29 de enero).

90 Ibídem.

91 En este sentido, DEL REY GUANTER, S.: «Tratamiento automatizado de datos de carácter personal y contrato de trabajo», *Relaciones Laborales*, núm. 15, 1993, pág. 154.

Este derecho de acceso tiene su fundamento en el derecho a la información que, en el ámbito de la vigilancia de la salud, por su especial incidencia en la intimidad y la dignidad de las personas, se manifiesta en un derecho a conocer qué tipo de pruebas van a ser practicadas, los resultados de esas pruebas y, además, de un modo expreso, preciso e inequívoco que sus datos son recopilados en un fichero manual o informático, del que estará a cargo el servicio de prevención o la empresa en función del tipo de datos incorporados, al que tendrán acceso unas personas físicas o jurídicas determinadas –debe concretarse exactamente dichos sujetos e informar si hay algún cambio, con referencia explícita a la función que desempeñan (representante de los trabajadores, delegado de prevención, encargado del tratamiento, responsable de seguridad, psicólogo de la empresa, etc.)–. Además, también deberán indicarse las finalidades para las que van a ser utilizados; a quiénes van a ser cedidos; las formas de ejercicio de los derechos de acceso, rectificación, cancelación e, incluso, oposición [92] y cualquier otra información que resulte relevante para garantizar los derechos fundamentales del trabajador en el ámbito de la vigilancia de la salud.

2.2.3.4. La conservación limitada de los datos.

Otro principio de aplicación a la vigilancia de la salud, unido al de cancelación, es el de conservación limitada. Es decir, los datos referidos a la vigilancia de la salud sólo estarán en los ficheros durante el tiempo necesario para el cumplimiento de los fines para los que fueron recogidos. Ante los resultados de un nuevo examen de salud, habrá que determinar qué datos del anterior examen pueden mantener su validez para contribuir a una eficaz protección de la salud de los trabajadores según los últimos datos obtenidos, de modo que, si algún dato carece ya de utilidad, habrá que proceder a su cancelación.

Casi todos los Reglamentos sobre riesgos especiales anteriores y posteriores a la LPRL recogen plazos específicos de conservación –a veces de períodos de hasta cuarenta o cincuenta años debido a la lenta aparición de una enfermedad derivada de la exposición a un concreto riesgo en el trabajo [93]–.

92 El derecho de oposición es el derecho de los interesados en determinadas circunstancias –motivos fundados– a oponerse al tratamiento de los datos que les conciernen (por todos, MARTÍN-CASALLO LÓPEZ, J.J.: «Derechos de acceso, rectificación y cancelación de los datos sanitarios en la LOPD», VV.AA.: *VII Congreso Nacional de Derecho Sanitario*, Madrid, octubre de 2000, http://www.aeds.org/congreso7/). La LOPD no lo regula expresamente, si bien, hace referencia al reglamento de procedimiento del mismo, con lo que, implícitamente, se entiende regulado, aunque ese reglamento todavía no se ha elaborado (art. 17 LOPD). Sí que se recoge en el artículo 14 de la Directiva 95/46/CE para determinados supuestos que pueden ampliarse. A la luz de uno de los supuestos recogidos en la misma –oposición incluso cuando un tratamiento de datos sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a quienes se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo a esa Directiva– puede decirse que en el ámbito laboral se manifiesta en un *ius-resistentiae* ante un tratamiento de datos que el trabajador pudiera considerar abusivo, pero también en la posibilidad de oponerse al tratamiento de sus datos con otros fines diferentes a los exclusivos de la vigilancia.

93 *Vid*., por ej., el artículo 9.3 del Real Decreto 664/1997, sobre exposición a agentes biológicos, en el que se obliga a conservar los historiales médicos durante un plazo mínimo de diez años después de finalizada la exposición, siendo, por tanto, dispositivo por el Convenio Colectivo de aplicación un plazo mayor que debe ser en todo caso de cua-

2.2.3.5. La Negociación Colectiva en la legislación de protección de datos.

Como colofón de este apartado resulta de especial importancia señalar el papel relevante que puede alcanzar la Negociación Colectiva –estatutaria, extraestatutaria y pactos de empresa– en la aplicación de los principios y medidas de seguridad recogidos en la LOPD al tratamiento de datos relacionados con la salud en el medio laboral por la fuerza que le ofrece el artículo 32 de la LOPD, ya que «mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo».

III. LAS RESPONSABILIDADES DERIVADAS DE LA VIGILANCIA DE LA SALUD EN RELACIÓN CON EL TRATAMIENTO DE DATOS

La tutela protectora de los derechos de los trabajadores en vigilancia de la salud se lleva a cabo, al igual que en otros supuestos, no sólo para poner en marcha un mecanismo de compensación por la vulneración de esos derechos, sino también para exigir responsabilidades de tipo administrativo, civil, penal, laboral o de Seguridad Social con recargo de prestaciones para la empresa –a veces incluso conjuntamente– a los intervinientes en esta medida preventiva. A ellas hay que unir la responsabilidad en la que incurran los propios trabajadores si no cumplen con las obligaciones adecuadas para que la vigilancia se lleve a cabo de forma que pueda cumplir su objetivo final de conseguir el más alto grado de salud física, psíquica y social.

En el ámbito del tratamiento de datos en relación con esta medida preventiva debe prestarse atención a la responsabilidad civil, a la responsabilidad administrativa y a la penal respecto del incumplimiento del deber de secreto. Este estudio se centrará en las dos primeras.

renta años en caso de exposiciones que pudieran dar lugar a una infección en la que concurran alguna de las siguientes características: «A) Debida a agentes biológicos con capacidad conocida de provocar infecciones persistentes o latentes. B) Que no sea diagnosticable con los conocimientos actuales, hasta la manifestación de la enfermedad muchos años después. C) Cuyo período de incubación, previo a la manifestación de la enfermedad, sea especialmente prolongado. D) Que dé lugar a una enfermedad con fases de recurrencia durante un tiempo prolongado a pesar del tratamiento. E) Que pueda tener secuelas importantes a largo plazo». Anterior a la LPRL puede citarse el artículo 9 del Real Decreto 1316/1989, de 27 de octubre, sobre medidas de protección de los trabajadores frente a los riesgos derivados de su exposición al ruido, con un período de conservación de treinta años.

1. La responsabilidad civil *ex* artículo 19 de la LOPD.

Conforme al artículo 19 de la LOPD «los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley, por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados». Además, «cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas» y en el caso de los ficheros de titularidad privada, «la acción se ejercitará ante los órganos de la jurisdicción ordinaria».

De este tenor literal puede deducirse que este artículo tiene como función recordar que también en el ámbito de la protección de datos puede exigirse responsabilidad civil y que los dos sujetos principales, aunque no los únicos, a los que se imputará la misma son el responsable del fichero y el encargado del tratamiento. La mención expresa a este encargado del tratamiento puede hacer pensar si no excluiría la responsabilidad del empresario en el caso de que aquél fuera el verdadero causante del daño. Habría que ver lo que está estipulado en el contrato de *outsourcing* pero parece que una interpretación conjunta de este artículo 19 de la LOPD con el artículo 12.4 de la misma norma cuyo tenor literal establece que «en el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente» indica que la *mens-legislatoris* quería imputar tanto responsabilidad administrativa como responsabilidad civil directa al encargado del tratamiento pudiendo excluir la responsabilidad del empresario si existe acción contra él y demuestra la diligencia debida en las obligaciones que le competen.

2. La responsabilidad administrativa.

2.1. Tipos infractores y sujetos responsables por infracción de la normativa preventiva en relación con el tratamiento de datos.

2.1.1. Ideas generales sobre la responsabilidad administrativa en el ámbito preventivo.

En materia de prevención de riesgos laborales, la responsabilidad administrativa se menciona en el artículo 42.1 de la LPRL pero su regulación se encuentra, fundamentalmente, en los artículos 2, 5.2, 11, 12, 13, 39.3, 40.2, 42 y 48.2 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el TRLISOS. Con ella la Administración laboral cumple una función de tutela en el reconocimiento del derecho del trabajador a su seguridad y salud en el desa-

rrollo de sus funciones imponiendo las sanciones que legalmente procedan en el ejercicio de su potestad sancionadora [94]. Esas sanciones tienen un fin disuasorio: se pretende evitar la realización de nuevas infracciones que afecten a la seguridad y salud en el trabajo [95].

El artículo 5.2 del TRLISOS va a considerar infracciones laborales en materia de prevención de riesgos las acciones u omisiones no sólo de la empresa en sí, sino también, y a efectos de incumplimientos de vigilancia de la salud, las entidades que actúen como servicios de prevención ajenos a las empresas, así como promotores y propietarios de obra u otros sujetos considerados responsables [96] que incumplan las normas legales, reglamentarias y cláusulas normativas de los convenios colectivos en materia de seguridad y salud laboral sujetas a responsabilidad conforme al TRLISOS. Así, las infracciones reguladas en esta Ley y que afecten a la vigilancia de la salud van a poder ser cometidas no sólo por la empresa, sino, a su vez, por los servicios de prevención externos –mención que excluye la responsabilidad de otras modalidades de organización de la prevención–. De este modo, las infracciones que cometan los servicios de prevención mancomunados o los servicios de prevención propios no serán imputadas a ellos sino a la empresa en sí por ser considerados aquéllos parte de ésta, pues para la modalidad de organización preventiva propia el legislador ha sopesado más la condición de trabajadores de la empresa en la misma que las tareas especializadas asumidas para exigir responsabilidad por ellas [97] y, para la modalidad mancomunada, ha querido equipararla a la propia aunque con un régimen que no acaba de entenderse bien, pues si puede ser lógico que responda la empresa en supuestos en los que esta modalidad se crea, por ejemplo, por distintas empresas de diferentes sectores ubicadas en un mismo centro comercial o área geográfica limitada porque es cada una de ellas la que tiene que estar pendiente de que el servicio cumpla las tareas preventivas asumidas respecto a las mismas, no lo es tanto en los supuestos en los que este servicio se crea por un grupo de empresas, con actividades afines, donde parece que es más común la gestión de la prevención y las empresas pueden despreocuparse más de las tareas preventivas, ni en supuestos en los que el servicio mancomunado tiene personalidad jurídica propia en los que el legislador podía haberle imputado responsabilidad sin ninguna tacha jurídica. Quizá el diferente tratamiento respecto de los servicios de prevención ajenos pueda estar en el hecho de que, mientras éstos se contratan, aquéllos se gestionan y las empresas deben ser consecuentes con las obligaciones de gestión. No obstante, *de lege ferenda*, creo que es necesaria una regulación más próxima a los servicios de prevención externos para exigirles mayor grado de responsabilidad y evitar, así, el peligro de que relajen sus compromisos preventivos y esto repercuta en la eficacia de la prevención y en los intereses económicos de las empresas constituyentes de esos servicios de prevención.

Esta imputación de responsabilidad a la empresa por actos de los servicios de prevención propios y mancomunados podría justificarse en la «teoría del órgano», en la que, si la persona jurídica se beneficia de todos los actos provechosos realizados por sus órganos, igualmente debe responder

94 SEMPERE NAVARRO, A.; GARCÍA BLASCO, J. *et al.*: *Derecho de la seguridad… op. cit.*, pág. 307.

95 Por todos, GARCÍA MURCIA, J.: *Responsabilidades y sanciones en materia de Seguridad y Salud en el trabajo*, Pamplona, Aranzadi Editorial, 2003, pág. 68.

96 La nueva redacción dada al artículo 5.2 del TRLISOS por la Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la prevención de riesgos laborales (BOE de 13 de diciembre), no acota a los sujetos responsables, sino que parece remitirse a los que lo son conforme al artículo 2 del mismo Texto Refundido.

97 IGARTUA MIRÓ, M.T.: *Manual del Servicio de Prevención*, Madrid, Tecnos, 2002.

de sus actos perjudiciales [98]; o en «la reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona que está sometida al cumplimiento de dicha norma» [99]; o en los artículos 14.4 y 15.4 de la LPRL que establecen, por un lado, que «la atribución de funciones en materia de protección y prevención a trabajadores o servicios de empresa y el recurso al concierto con entidades especializadas para el desarrollo de actividades de prevención complementarán las acciones del empresario, sin que por ello le eximan del cumplimiento de su deber en esta materia, sin perjuicio de las acciones que pueda ejercitar, en su caso, contra cualquier otra persona» y, por otro, que el empresario debe prever las distracciones o imprudencias no temerarias del trabajador [100].

Si bien, la responsabilidad del empresario no es objetiva, debe concurrir en su conducta cierto grado de culpabilidad –pues no hay que olvidar que éste es uno de los principios de la potestad sancionadora– aunque sólo se exija a título de simple inobservancia (art. 130.1 LRJPAC), por la más pequeña falta de diligencia, por culpa levísima [101], sin que ello implique necesariamente una efectiva lesión del bien jurídico protegido [102]. Es así que, en el ámbito preventivo, esta exigencia de culpa hay que ponerla en relación con la previsibilidad y evitabilidad de la propia acción u omisión que ha supuesto el incumplimiento de la norma y no tanto con el resultado antijurídico [103]. En cualquier caso, el caso fortuito, la fuerza mayor o el error serán factores que podrán justificar su actuación o incumplimiento de la norma.

La comisión de infracciones administrativas dará lugar, tras el oportuno procedimiento (arts. 51 a 54 del TRLISOS y RIS), a las correspondientes sanciones que se impondrán en su grado mínimo, medio o máximo teniendo en cuenta los criterios de graduación recogidos en el artículo 39.3 del TRLISOS –peligrosidad de las actividades, número de trabajadores afectados, incumplimiento de las advertencias o requerimientos previos de la Inspección de Trabajo y Seguridad Social, conducta seguida por el empresario para evitar incurrir en esas infracciones…– con las cuantías recogidas en el artículo 40.2 del TRLISOS y competencia para sancionar atribuida, según la cuantía de las sanciones, en el artículo 48.2 del TRLISOS y en distintas normas autonómicas [104].

---

98 NIETO GARCÍA, A.: *Derecho administrativo sancionador*, Madrid, Tecnos, 2002, pág. 360.

99 STC 246/1991, de 19 de diciembre.

100 «La deuda de seguridad de la empresa con los trabajadores no se agota con la facilitación de los medios de protección, sino que debe vigilar su utilización, como contrapartida a la potestad organizativa, no quedando enervada su responsabilidad por la posible imprudencia de los trabajadores al no utilizarlos» (STSJ–Contencioso–Administrativa de Asturias, de 12 de febrero de 1999 –Ar. 628–). «El empresario está obligado a vigilar el cumplimiento efectivo de dicha normativa por parte del trabajador y, si cumple ese deber y comprueba que el trabajador también lo hace con sus propios deberes, en caso de que se produjera en alguna ocasión excepcional un accidente debido a que el trabajador no observó las obligaciones que pesaban sobre él, no habría reproche hacia el empresario; por el contrario, si el empresario constata un incumplimiento sistemático o frecuente de las obligaciones a cargo de los trabajadores y se muestra permisivo o pasivo, incurrirá en responsabilidad en caso de que se produzca el accidente» (STSJ del País Vasco de 9 de abril de 2002, http://www.laley.net).

101 DE PALMA DEL TESO, A.: *El principio de culpabilidad en el derecho administrativo sancionador*, Madrid, Tecnos, 1996, pág. 137.

102 Ibídem, pág. 138.

103 *Vid*. CAMÁS RODA, F.: *Las obligaciones del empresario en la normativa de prevención de riesgos laborales*, Madrid, La-Ley, 2002, págs. 372-373.

104 Como el Decreto 27/1999, de 16 de febrero, de la Comunidad Autónoma de Valencia, por el que se atribuyen competencias en materia de infracciones en el orden social y prevención de riesgos laborales (BOGV de 22 de febrero).

Además de las oportunas sanciones pecuniarias, esta responsabilidad puede implicar suspensión de actividades o cierre del centro de trabajo (art. 53 LPRL) y limitación a la facultad para contratar con la Administración Pública (art. 54 LPRL). Por otro lado, para los servicios de prevención externos, el artículo 40.2 del TRLISOS prevé la posibilidad de cancelación de la acreditación otorgada por la Autoridad Laboral para actuar como tales.

2.1.2. Falta de comunicación de resultados.

La responsabilidad administrativa a que puede dar lugar el incumplimiento del deber de vigilancia de la salud en relación con el tratamiento de datos obtenidos con su puesta en práctica se articula, en primer lugar, a través de la infracción regulada en el artículo 12.2 del TRLISOS como grave: la no comunicación a los trabajadores que se han sometido a la vigilancia de la salud del resultado de la misma.

Ya se afirmó la conveniencia de que fuera el propio servicio de prevención el que comunicara los resultados. Es así que si la vigilancia de la salud está concertada con un servicio de prevención ajeno, generalmente será éste quien cometa la infracción. Ahora bien, si la comunicación, con garantías de confidencialidad, se hace a través de la empresa y no llega a sus destinatarios podrá ser ésta la responsable que, por los argumentos dados *supra*, lo será en cualquier caso por incumplimientos de las modalidades de organización mancomunada o propia.

2.1.3. Falta de registro y archivo de datos.

Otra infracción grave que dará lugar a responsabilidad administrativa es la recogida en el artículo 12.4 del TRLISOS que imputa responsabilidad si no se registran o archivan los datos obtenidos en las evaluaciones, controles, reconocimientos, investigaciones o informes a los que se refieren los artículos 16, 22 y 23 de la LPRL.

Podría decirse que, con base en lo argumentado en epígrafes anteriores, si la obligación de registro y archivo de las conclusiones de los exámenes de salud corresponde, una vez entregadas, al empresario, será éste quien cometa esta infracción respecto a su no registro o archivo. Además, por aplicación de la teoría del órgano que le atribuye el carácter de garante de la eficiencia del cumplimiento de las normas preventivas, por no estar pendiente de las imprudencias de sus trabajadores o por lo dispuesto en el artículo 14.4 explicado *supra*, responderá también si los servicios de prevención propios o mancomunados incumplen esta obligación respecto de los resultados.

En cuanto a los servicios de prevención externos, está claro que si la empresa contrata la práctica de la vigilancia, va a contratar también el archivo y registro de los datos derivados de la misma. Por tanto, puede llegarse a la conclusión de que esos servicios serán los responsables por no registrar los datos de los resultados como consecuencia de su práctica. Deben conservar esa información porque contribuye a orientar a la empresa sobre las medidas más adecuadas para lograr el más alto grado de salud física y psico-social del trabajador, si bien, esa conservación debe hacerse coordinando las reglas preventivas con aquellas sobre cancelación y conservación limitada que impone la LOPD.

Si esa falta de registro implica riesgo grave para la integridad física o la salud de los trabajadores en relación con el registro de los niveles de exposición a agentes físicos, químicos y biológicos, listas de trabajadores expuestos y expedientes médicos, se cometerá la infracción del artículo 16.6.i) del TRLISOS.

2.1.4. El incumplimiento del deber de confidencialidad: interferencias entre la normativa preventiva y de protección de datos.

Otra infracción administrativa que afecta a la vigilancia de la salud, calificada por el artículo 13.5 como muy grave, es incumplir el deber de confidencialidad en el uso de los datos relativos a la vigilancia de la salud de los trabajadores, en los términos previstos en el apartado 4 del artículo 22 de la LPRL. Es decir, en los términos establecidos según sean conclusiones o resultados. Como se afirmó, unos tienen un deber de confidencialidad respecto a los resultados y otros respecto a las conclusiones pues, salvo autorización del trabajador, algunos implicados en tareas preventivas sólo tienen acceso a las conclusiones. De este modo, podría llegar a pensarse que, en este caso, la responsabilidad debería individualizarse e imputarse al concreto infractor de la confidencialidad. Si bien, las propias características de la responsabilidad administrativa en el ámbito preventivo hacen que, como en los supuestos señalados anteriormente, se impute directamente a la empresa o al servicio de prevención externo, pudiendo luego dirigirse contra el verdadero causante del daño con una acción de responsabilidad civil.

Esta infracción dará lugar, seguramente, a concurrencia con el artículo 199 del Código Penal en el que se castiga la vulneración del secreto con lo que habrá que activar el principio de *non bis in idem*. En este caso concreto resulta más eficaz la tutela penal porque permite extender la responsabilidad a todos los que hayan intervenido en la comisión del delito, superando las limitaciones subjetivas de la responsabilidad administrativa [105].

Respecto de este incumplimiento del deber de confidencialidad debe analizarse, además, qué interferencias existen entre la normativa preventiva y de protección de datos, puesto que en este supuesto puede haber concurrencia de infracciones cometidas por el mismo sujeto y sobre la base de unos mismos hechos y fundamento, de tal forma que deba acudirse a la aplicación del principio *non bis in idem* para conocer cuál es la regla aplicable.

Efectivamente, la infracción por el deber de confidencialidad tiene su análogo en la infracción por el deber de guardar secreto sobre los datos de salud recogido en el artículo 44.4 de la LOPD, también calificada de muy grave. Un mismo hecho cometido por un mismo sujeto da lugar a dos infracciones idénticas, reguladas en dos normas diferentes, cuyo fundamento es evitar la lesión del derecho a la intimidad o a la protección de datos relacionados con la salud y frente a las que no puede existir doble sanción. Es así que hay que elegir qué sanción imponer o, en este caso, qué procedi-

105 Observación que ya fue puesta de manifiesto en GOÑI SEIN, J.L.; GONZÁLEZ LABRADA, M.; APILLUELO MARTÍN, M.; SIERRA HERNÁIZ, E.: «Infracciones en materia de prevención de riesgos laborales: artículos 11 a 13 del TRLISOS», *Justicia Laboral*, 2001, pág. 111.

miento seguir para sancionar: si el de la LOPD o el del TRLISOS. La respuesta, a falta de mecanismos de solución que podían haber articulado esas normas, podría estar en afirmar que resolverá aquel órgano ante quien se haya presentado la denuncia o aquel que primero haya inspeccionado la posible infracción.

Cosa distinta es que la Inspección de Trabajo se encuentre en su actividad de control de cumplimiento de las normas preventivas con infracciones relacionadas con la vigilancia de la salud pero relacionadas directamente con el tratamiento de datos como la infracción de normas de seguridad, la vulneración del derecho de rectificación o incumplir los requisitos de creación del fichero. Entonces, conforme al artículo 9 del Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el ejercicio de la Potestad Sancionadora (RPPOS), deberá comunicar a la AEPD u Órgano autonómico correspondiente el indicio de infracción, porque, aunque con su incumplimiento se esté vulnerando el derecho a la vigilancia de la salud, no hay duda de que son aspectos que pertenecen al ámbito especial de la protección de datos.

2.2. Tipos infractores y sujetos responsables por infracción a la normativa de protección de datos.

Como se ha venido comentando también pueden cometerse infracciones en relación con la vigilancia de la salud que tengan que ver con el tratamiento de datos derivados de la misma. Se recogen en el artículo 44 de la LOPD y se clasifican, al igual que en el TRLISOS, como leves, graves o muy graves. Así, entre otras, como leves: no atender, por motivos formales, la solicitud del interesado-trabajador de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda; o no solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave. Como graves: tratar los datos de carácter personal o usarlos posteriormente conculcando los principios y garantías establecidos en la LOPD o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave; o mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la LOPD ampara. Como muy graves: la recogida de datos de forma engañosa y fraudulenta; la comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas; la vulneración del deber de guardar secreto sobre los datos de carácter personal referidos a la salud, ya citado; o tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

El procedimiento se encuentra regulado en el artículo 48 de la LOPD y, a falta de desarrollo reglamentario en este aspecto, por los artículos 18 y 19 del Real Decreto 1332/1994 –declarado vigente, como ya se comentó, por la disposición transitoria tercera de la LOPD–. Viene a ser similar a otros procedimientos sancionadores, en los que se incluyen las fases de incoación, período probatorio, propuesta de resolución y resolución. Existe un único órgano sancionador, el Director de la AEPD

u Órgano correspondiente de la Comunidad Autónoma que, en principio, conforme al tenor literal del artículo 48 de la LOPD agotan la vía administrativa, pero que, a través del instrumento de la delegación autorizada en materia sancionadora por la modificación de la LRJPAC realizada por Ley 4/1999, de 4 de enero [106], podría darse la oportunidad a los afectados de revisar en vía administrativa acudiendo posteriormente al recurso contencioso-administrativo.

Respecto de los sujetos infractores, debe señalarse que el artículo 43 imputa responsabilidad administrativa por infracción de normas relacionadas con la protección de datos a los responsables del fichero y a los encargados del tratamiento. Respecto a estos últimos que actúan como empresa *outsourcing* en protección de datos, la claridad de ese artículo 43 no ofrece duda de su imputabilidad. Ahora bien, ¿quién es el responsable del fichero a efectos de responsabilidad en este ámbito de protección de datos? Respecto a los ficheros de conclusiones, no hay duda de que será el empresario, y del de resultados, el servicio de prevención ajeno si la vigilancia de la salud se externaliza o la empresa, aunque el efectivo responsable del tratamiento de datos sea el servicio de prevención propio o mancomunado. Si la legislación preventiva ha querido considerar a los componentes del servicio de prevención propio trabajadores de la propia empresa y las responsabilidades administrativas se imputan directamente a la misma por los argumentos dados *supra*, parece no haber duda en que como tales deben considerarse también en responsabilidades recogidas en otras normas que afecten a sus tareas propias.

IV. CONCLUSIONES

PRIMERA:

Los órganos encargados de la vigilancia de la salud deben tener en cuenta el principio de confidencialidad en relación con los datos derivados de su práctica, como manifestación del derecho a la intimidad y especialmente importante para que cualquier sistema de tratamiento de datos en relación con esa vigilancia no vulnere los derechos fundamentales del trabajador.

Para los resultados, entendidos como los documentos que contienen los datos personales referidos a la salud del trabajador derivados de la práctica de las diferentes pruebas a las que ha sido sometido para detectar el efecto que los riesgos de su puesto de trabajo provocan en su salud, la confidencialidad es máxima y sólo pueden tener acceso a ellos el concreto personal médico o psico-social que la hayan llevado a cabo, salvo que el trabajador dé su consentimiento para que sean entregados a otras personas o que exista un interés legítimo que haya que preservar como el daño para terceros si no se comunican. Respecto de las conclusiones, como documentos extraídos de los resultados única y exclusivamente en relación con la aptitud del trabajador en relación con el desempeño del puesto de trabajo o con la necesidad de mejorar o introducir medidas de prevención o protección, la confidencialidad es mínima puesto que pueden tener acceso a las mismas

106 La supresión de la delegación del ejercicio de la potestad sancionadora se justifica en favorecer la descentralización en aras del principio de eficacia (*vid.* exposición de motivos de la Ley 4/1999 –BOE de 14 de enero–).

el empresario y otros sujetos relacionados con la vigilancia si así lo disponen las normas preventivas, como los delegados de prevención o el comité de seguridad y salud, o si a juicio de los concretos sujetos que la realizan es necesario para el correcto desempeño de sus funciones, como los auxiliares de clínica. Considero que esa decisión sobre la aptitud que contienen las conclusiones no debe darse en términos generales. Debe proyectarse sobre una determinada tarea y tener en cuenta que puede ser temporal.

SEGUNDA:

Estas conclusiones, los resultados y el seguimiento continuado del estado de salud del trabajador suministran una serie de datos que se documentan y están sujetos a una elaboración y, posteriormente, a un proceso de archivación y puesta a disposición para su custodia y tutela. Fases, estas, del tratamiento de datos sobre vigilancia de la salud en las que rige, igualmente, el principio de confidencialidad.

Ese tratamiento se realizará, normalmente, en soporte informático, lo que supone la aplicación a la vigilancia de la salud de las normas sobre protección de datos, aplicación que considero especialmente importante en el ámbito empresarial en aras del respeto a los derechos fundamentales de los trabajadores en cuanto la informática otorga un gran poder de control de la prestación laboral a la empresa y, por tanto, exige unas normas de actuación que limiten ese control que puede llegar a convertir al trabajador en un individuo especialmente vulnerable, sobre todo si la empresa combina datos erróneos, inexactos y utilizados con finalidades ilícitas o diferentes a las que fueron obtenidas, o se transmiten arbitrariamente por el empresario.

De la fase de elaboración de los datos se van a hacer cargo, en todo caso, sean resultados o conclusiones, los servicios de prevención. En la de archivación y custodia se harán cargo, por un lado, estos servicios de prevención respecto a los resultados –frente a los que el empresario tiene, salvo excepciones, prohibido el acceso– y, respecto a las conclusiones, una vez ya entregadas al empresario, y aunque consten en los ficheros de los servicios de prevención como consecuencia de los resultados, la empresa. Así, podrían identificarse dos bases de datos: una de resultados a cargo de los servicios de prevención, aunque con alguna responsabilidad de la empresa, y otra más de conclusiones a cargo directo de la empresa.

TERCERA:

A todas estas bases de datos se aplicará, como se ha afirmado, la legislación de protección de datos y, además, se crearán sin necesidad de que el trabajador dé su consentimiento, al ser un supuesto de datos sensibles permitido por las propias normas preventivas (art. 7 de la LOPD en relación con los arts. 22 y 23 de la LPRL y 12.4 del TRLISOS). No obstante, esta posibilidad de prescindir de consentimiento no debe excluir, conforme al artículo 5 de la LOPD, la información detallada al trabajador afectado por el tratamiento sobre la existencia del fichero o la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, entre otros extremos.

CUARTA:

Los ficheros que contienen datos relacionados con la vigilancia de la salud deben contener medidas de seguridad catalogadas de nivel alto por la normativa de protección de datos en aras de la protección a la intimidad, el honor y el pleno ejercicio de los derechos personales –en este caso de los trabajadores– frente a su alteración, pérdida, tratamiento o acceso no autorizado. Su regulación se encuentra en el artículo 9 de la LOPD y el RMSFA. Este último las define como aquellas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

Además, las bases de datos relacionadas con la vigilancia de la salud deben cumplir con los principios de finalidad, respecto del cual la utilización de datos para otros fines compatibles debe interpretarse de forma extremadamente restrictiva por las implicaciones de la vigilancia con los derechos fundamentales; pertinencia, en cuanto a la adecuación de los datos al fin pretendido; veracidad, en cuanto a la exactitud de los datos, de especial interés para un diagnóstico adecuado sobre la aptitud del trabajador; y licitud, en cuanto prohibición de toma de datos por medios fraudulentos, como espiar los hábitos de vida de un trabajador que pueden influir en su salud.

Por otro lado, el empresario debe tener en cuenta que esos ficheros de vigilancia de la salud generan unos derechos para el trabajador que deben ser respetados. Así, el de acceso a los datos, articulado a través de la comunicación de resultados y conclusiones, pero, también, a través de la posibilidad de pedir información sobre los datos que han podido ser cedidos o solicitar copia de datos específicos de los resultados, por ejemplo: el derecho de rectificación y cancelación, inherentes al principio de veracidad; y el derecho de conservación limitada, en cuanto que los datos derivados de la práctica de la vigilancia de la salud sólo podrán estar en los ficheros durante el tiempo estrictamente necesario para el cumplimiento de sus fines; es así que si tras un nuevo examen de salud carecen de utilidad los datos del anterior, deberán ser cancelados. Principios y derechos que suponen, en definitiva, una garantía de respeto a los derechos de los trabajadores y que demuestran que un fichero no es algo arbitrario o una simple recogida de datos, sino un almacén al que hay que dotar de todas las garantías precisas para realizar una vigilancia de calidad.

QUINTA:

En relación con la protección de datos en la vigilancia de la salud, el empresario y el servicio de prevención ajeno incurrirán en responsabilidad administrativa por la falta de la comunicación de sus resultados, falta de registro y archivo de datos, vulneración del deber de confidencialidad, recogidas en el TRLISOS, y por las infracciones específicas recogidas en la LOPD.

La infracción por el deber de confidencialidad tiene su análogo en la infracción por el deber de guardar secreto sobre los datos de salud recogido en el artículo 44.4 de la LOPD, también como infracción muy grave. Un mismo hecho cometido por un mismo sujeto da lugar a dos infracciones

idénticas, reguladas en dos normas diferentes, cuyo fundamento es evitar la lesión del derecho a la intimidad o a la protección de datos relacionados con la salud y frente a las que no puede sancionarse doblemente. Es así que hay que elegir qué sanción imponer o, en este caso, qué procedimiento seguir para sancionar: si el de la LOPD o el del TRLISOS. La respuesta, a falta de mecanismos de solución que podían haber articulado esas normas, podría estar en afirmar que resolverá aquel órgano ante quien se haya presentado la denuncia o aquel que primero haya inspeccionado la posible infracción.

Cosa distinta es que la Inspección de Trabajo se encuentre en su actividad de control de cumplimiento de las normas preventivas con infracciones que afectan a la vigilancia de la salud pero relacionadas directamente con el tratamiento de datos como la infracción de normas de seguridad, la vulneración del derecho de rectificación o incumplir los requisitos de creación del fichero, recogidas, también, en el artículo 44 de la LOPD. Entonces, conforme al artículo 9 del Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora, deberá comunicar a la AEPD u Órgano autonómico correspondiente el indicio de infracción, porque, aunque con su incumplimiento se esté vulnerando el derecho a la vigilancia de la salud, no hay duda de que son aspectos que pertenecen al ámbito especial de la protección de datos.

SEXTA:

Todo ello refleja, a la postre, que una eficaz vigilancia de la salud no es una mera recopilación de datos físicos o psíquicos sobre el estado de salud de los trabajadores. Es una obligación preventiva para la empresa que conlleva la activación de todo un mecanismo de derechos y deberes que deben compenetrarse.