El tratamiento y protección de los datos de salud de los trabajadores en el ordenamiento español

Javier Fernández-Costales Muñiz[1]

Resumen: La vigilancia de la salud es uno de los principios básicos de la salud y la seguridad en el trabajo. La legislación ha venido a construir un sistema amplio y complejo de vigilancia de la salud dotado de no pocos y variados fundamentos y cuestiones de evidente interés, tanto a nivel doctrinal como práctico, entre los cuales, y por lo que aquí interesa, cabe destacar las importantes connotaciones del respeto a la intimidad, la dignidad de la persona y la confidencialidad de los datos de salud obtenidos en el marco de los reconocimientos médicos efectuados a los trabajadores.

Las informaciones relativas a la salud son datos especialmente sensibles a los cuales el legislador ha proporcionado una especial protección en distintas y diversas normas, salvaguardia que surge del hecho de encontrarse ante datos estrechamente vinculados a la dignidad y personalidad humanas.

Palabras clave*: salud, protección de datos, digitalización, nuevas tecnologías.*

Abstract: Monitoring health is one of the basic principles of Occupational Health and Safety. The legislation has built up a broad and complex system of health surveillance with many and varied foundations and questions of obvious interest, both doctrinal and practical, among which,

[1] Catedrático de Derecho del Trabajo y de la Seguridad Social, Universidad de León. E-mail: javier.costales@unileon.es

and as far as we are concerned here, the important connotations of respect for privacy, personal dignity and the confidentiality of health data obtained in the framework of medical examinations carried out on workers should be highlighted.

Health-related information is particularly sensitive data to which the legislator has afforded special protection in different and diverse rules, a safeguard that arises from the fact that the data in question are closely linked to human dignity and personality.

***Key words**: health, data protection, digitalisation, new technologies.*

1. Introducción

El imparable y continuo avance de las nuevas tecnologías y la transformación digital constituye, a día de hoy, uno de los aspectos más destacados, característicos y definitorios de nuestro actual entorno. La que ya se ha calificado como nueva revolución tecnológica o Cuarta Revolución Industrial ha introducido a la sociedad en una nueva dimensión de avances y desarrollos técnicos aplicables a todos los ámbitos a nivel social, productivo o económico, además de estar condicionando y haciendo evolucionar nuestros sistemas conceptuales, así como las formas de organización y gestión de nuestra vida personal y cotidiana.

El sistema productivo está transformándose desde hace mucho tiempo merced a esa cuarta revolución industrial y la industria 4.0 o "industria inteligente" supone "un salto cualitativo en la organización y gestión de la cadena de valor del sector"[2], implicando la incorporación de las nuevas tecnologías a la considerada "tradicional", permitiendo que dispositivos y sistemas colaboren entre ellos y con otros para crear

[2] ÁLVAREZ CUESTA, H.: *El futuro del trabajo vs. el trabajo del futuro*, A Coruña (Colex), 2017, pág. 15.

una industria inteligente[3]. La industria transforma, al tiempo, la economía tradicional en digital, y adquiere cuatro características específicas: "la irrelevancia de la ubicación geográfica, el papel clave de las plataformas, la importancia de los efectos de red y el uso de grandes datos"[4].

Cabe destacar cómo, respecto a esta utilización masiva de datos, se está ante una nueva forma de creación de valor que, como lo hicieran la agricultura o la revolución industrial en su momento, permitirá una transformación no solo cuantitativa, sino cualitativa de la sociedad, pues los datos masivos tienen la capacidad de "revolucionarlo todo, desde las empresas y las ciencias hasta la atención médica, la administración, la educación, la economía, las humanidades y todos los demás aspectos de la sociedad"[5]. Así, los anclajes de la cuarta revolución industrial redimensionan, en su conjunto, los procesos de automatización y digitalización, vuelven a profundizar en las consecuencias del cambio tecnológico, y complejizan aún más las dimensiones del mismo[6] hasta llegar a la esfera laboral, en cuyo ámbito, y por lo que aquí interesa, la protección d ellos datos de salud de los trabajadores cobra una especial dimensión, dadas las múltiples implicaciones existentes y las posibles vulneraciones de derechos que se pueden producir en este campo.

---

[3] AA.VV.: *Industria conectada* 4.0. *La transformación digital de la industria española*, Madrid (Ministerio de Industria), 2015, pág. 5 y ss., señalando cómo "la industria está abocada a una transformación digital que afectará a todas las empresas y todas tendrán la necesidad de adaptarse a esa transformación".

[4] ÁLVAREZ CUESTA, H.: *El futuro del trabajo vs. el trabajo del futuro*, cit., pág. 16.

[5] Un análisis exhaustivo general de la materia en MAYER-SCHÖENBERG, V. y CUKIER, K.: *Big Data. A revolution that will transform how we live, work and think*, Boston/Nueva York (Eamon Dolan Book/Mariner Books/Houghton Mifflin Harcourt), 2013, (en version traducida: *Big Data. La revolución de los datos masivos*, Madrid (Turner), 2013), pág. 3 y ss., quienes señalan cómo la salud pública es solo un área en la cual el big data marca una gran diferencia y destacan el hecho de que no existe ninguna definición rigurosa de los datos masivos, o *big data*, que deben ser entendidos en un contexto en el que el volumen de información ha aumentado de manera exponencial, lo que ha favorecido nuevas tecnologías de procesamiento que permiten recopilar y analizar cientos de miles de millones de puntos de datos.

[6] ALEMÁN PÁEZ, F.: "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi Travail n.º 2016-1088", *Trabajo y Derecho. Nueva revista de actualidad y relaciones laborales*, núm. 30, 2017, pág. 12 y ss.

En este sentido, lógicamente, el mundo del trabajo y de la prevención de riesgos laborales no ha sido ni mucho menos ajeno a esta realidad, sino más bien al contrario, se ha erigido como uno de sus grandes protagonistas, habida cuenta de que en el marco del indudable impacto del tan inexorable como forzoso avance de las nuevas tecnologías en todos los órdenes de nuestra vida, las relaciones laborales son, obviamente, uno de los aspectos en los cuales más se va a ver su influencia. La irrupción de la digitalización en el ámbito laboral, tanto desde una perspectiva individual como colectiva, ha provocado "un profundo impacto transversal sobre el conjunto de las instituciones reguladoras de las relaciones laborales"[7].

La transformación digital ha traído de la mano múltiples nuevas formas de trabajo, tipo de organizaciones y perfiles profesionales que requieren la adopción de una estrategia de seguridad y Prevención de Riesgos Laborales adecuada, avanzada, moderna y adaptada a cada uno de ellos y, por otra parte, respetuosa con la protección de datos del trabajador, un derecho en riesgo permanente por sus propias características, pues la amenaza y la inseguridad del afectado pueden provenir no solo de la empresa para la que se prestan servicios, sino también del exterior por diferentes medios como los miles de ciberataques diarios que se producen a distintos niveles, riesgos ante los cuales el Derecho está reaccionando para proteger la privacidad y la intimidad de las personas, pero necesitado de pasos más profundos en el día a día de la empresa en cuanto a la protección de datos y cuestiones relativas a los datos de salud de los trabajadores.

La introducción de nuevas tecnologías en las actividades humanas provoca la aparición de supuestos de hecho hasta ahora inéditos[8], habida cuenta de que en muchas ocasiones no se encuentran regulados en la normativa y constituyen auténticas lagunas, de forma tal que un

[7] CRUZ VILLALÓN, J. "El impacto de la digitalización sobre los derechos fundamentales laborales", en AA.VV. (RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A., Dirs.): *Vigilancia y control en el Derecho del Trabajo digital*, Pamplona (Aranzadi), 2020, pág. 35.

[8] FERNÁNDEZ COSTALES, J.: "La aplicación y la incidencia de la informática en el ámbito del Derecho Civil", *Revista General de Legislación y Jurisprudencia*, núm.4, 1985, pág. 508.

cambio tecnológico en su incidencia en el ordenamiento jurídico provoca la aparición de un supuesto de hecho enteramente nuevo respecto a la cual falta la normativa concreta y genera una laguna legal[9]. Además, la reiteración típica de una serie de hechos nuevos constituye o crea una nueva problemática social que, a su vez, exige un tratamiento jurídico nuevo, distinto en sus principios rectores y en sus directrices.

2. El tratamiento y protección de datos de salud

Un aspecto que guarda evidente relación con algunas de las cuestiones anteriormente tratadas y acrecienta las dificultades es la voluntariedad y el respeto a la intimidad y confidencialidad de datos del trabajador en los reconocimientos médicos, no en vano la protección de los datos e informaciones relativas a la salud y, en especial, la historia clínica[10], "es uno de los aspectos del derecho a la intimidad que presenta mayor relevancia desde el punto de vista de su titularidad por parte del usuario de los servicios sanitarios"[11].

La nueva realidad digital y conectada viene a añadir relevancia a ciertos aspectos preventivos que hasta ahora podían pasar desapercibidos o no tener apenas importancia en la mayoría de las empresas. En este punto, entraría en juego la protección de datos como un elemento a tener muy en cuenta, también en materia preventiva. La utilización y manipulación de datos personales integrados en ficheros informáticos hace necesaria una protección jurídica de la persona y de tales datos, en tanto se ve afectado un derecho fundamental, como es la intimidad personal, tal y como ya se destacó, sin olvidar tampoco cómo el propio artículo 18

[9] DÍEZ-PICAZO, L.: *Experiencias jurídicas y teoría del Derecho*, 3.ª ed., Barcelona (Ariel), 1993, págs. 314-315.

[10] Sobre la materia, RODRÍGUIEZ ESCANCIANO, S.: "La intimidad del trabajador en el uso de diagnósticos médicos informatizados", *Revista Española de Derecho del Trabajo*, núm. 101, 2000, pág. 176 y ss.

[11] TARODO SORIA, S.: *Libertad de conciencia y derechos del usuario de los servicios sanitarios*, Bilbao (Universidad del País Vasco), 2005, pág. 353.

CE que lo regula, en su apartado 4 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".

Aun cuando en un primer momento el derecho a la intimidad se configuraba como un derecho del titular a exigir la no inferencia de terceros en su vida privada, al apreciarse la necesidad de su protección frente al creciente desarrollo de los medios y procedimientos de captación, divulgación y difusión de la misma y de datos y circunstancias pertenecientes a ella, pasó a concebirse en virtud de la doctrina del Tribunal Constitucional[12] como un bien jurídico que se relaciona con la libertad de acción del sujeto, las facultades positivas de actuación para controlar la información relativa a su persona y su familia en el ámbito público, dando forma a lo que se ha dado en llamar segunda dimensión de la intimidad, conocida como libertad informática o habeas data que encuentra su apoyo en el artículo 18.4 CE.

Las continuas innovaciones tecnológicas encuentran "pilar y exponente fundamental" en la cada vez más extensa e intensa utilización de la informática en la actividad productiva[13]. Tal circunstancia no solo ha venido a afectar de forma determinante a los instrumentos de trabajo y al desarrollo de las relaciones en la empresa, sino que también ha generado nuevos problemas que, lógicamente, cuestionan la validez de determinadas soluciones dadas por el ordenamiento ante una realidad empresarial que día a día se ve superada[14] por una realidad social en continuo avance, de forma tal que el ordenamiento en su conjunto, y la disciplina laboral por lo que aquí interesa, deben afrontar una necesaria y permanente adaptación a los nuevos tiempos y a los cambios tecnológicos en curso[15].

---

[12] Así, STCo 144/99 de 22 de julio.

[13] RODRÍGUEZ ESCANCIANO, S.: "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", en *Revista Española de Protección de Datos*, núm. 2, 2007, pág. 97.

[14] LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, T. II, 2005, pág. 55.

[15] GOÑI SEIN, J. L.: "Flexibilidad y revisión del ámbito del Derecho del Trabajo", en AA.VV. (RIVERO LAMAS, J., Coord.): *La flexibilidad laboral en España*, Zaragoza (Instituto de Relaciones Laborales), 1993, pág. 71.

La gestión informatizada del personal facilita que todos los datos concernientes al desarrollo del contrato de trabajo, desde el momento de la selección de personal, pasando por la constitución del vínculo contractual hasta su resolución, sean incluidos en los soportes informáticos de la empresa. Además, no se puede obviar cómo la incorporación del trabajador a la organización productiva empresarial favorece tanto una continua adquisición de información sobre extremos personales de diversa naturaleza como su minuciosa puesta al día. Al aumentar los medios técnicos, el poder del empresario sobre la prestación laboral y sobre el propio trabajador también crece, hecho que constituye una amenaza real para los derechos del empleado. La protección de tales derechos frente al uso ilegítimo de la informática es una necesidad "que se deja sentir con la mayor crudeza en el ámbito objetivo de las relaciones laborales"[16] en tanto en cuanto el tratamiento de datos constituye una práctica cada día más extendida, incluso imprescindible en ya numerosísimos supuestos, hasta el punto de poder afirmar que "gestión de personal e informática son, hoy en día, términos parejos"[17].

Desde tales premisas, cobra especial relevancia la necesidad de proteger el interés legítimo del trabajador de controlar sus datos personales insertos en los sistemas de comunicación empresariales, habida cuenta de que únicamente de tal forma se podrá evitar una afectación negativa durante la relación laboral, máxime si se trata de datos especialmente sensibles, obtenidos en el cumplimiento de las obligaciones relacionadas con la Prevención de Riesgos Laborales principalmente a través de la realización de los pertinentes reconocimientos médicos.

El Tribunal Constitucional ha mantenido en algunos pronunciamientos la idea de que la práctica totalidad de los derechos de la persona pueden verse afectados por un indebido tratamiento de datos,

[16] RODRÍGUEZ ESCANCIANO, S.: "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", cit., pág. 115.

[17] BORRAJO DACRUZ, E.: "El impacto de tecnologías y medios de información en el Derecho del Trabajo", en AA.VV.: *Implicaciones socio-jurídicas de las tecnologías de la información: encuentros 1980-1990: los juristas ante la revolución informática*, Madrid (CITEMA), 1991, pág. 71.

considerando la protección de los mismos como un derecho fundamental que "amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona"[18].

Los reconocimientos médicos permiten, mediante la realización de pruebas clínicas, averiguaciones biológicas o biométricas, la evaluación del estado de salud del trabajador, el conocimiento de sus posibles patologías y su origen así como la aplicación de los oportunos remedios en orden a un eventual restablecimiento del bienestar, tratamientos en los cuales las nuevas tecnologías pueden estar muy presentes a través de mecanismos como la vigilancia del paciente en sus patrones de ingesta y seguimiento de estos, por lo que habría que abordar los riesgos que conllevaría un control invasivo de la persona utilizando tecnologías embebidas dentro del medicamento y adheridas al cuerpo del individuo, con la finalidad de facilitar a los facultativos un control de los patrones de correcto o incorrecto seguimiento de su tratamiento, con lo que ello puede afectar a la autonomía del paciente/trabajador, tecnologías que, en definitiva, facilitan un control exhaustivo de la conducta de la persona sometida a un tratamiento y el acceso por parte de terceros a una importante cantidad de datos de salud[19].

---

[18] "Sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o a cualquier otro bien constitucionalmente amparado… [de forma tal que] el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el artículo 18.1 de la CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos", SSTCo 292/2000, de 30 de noviembre o 70/2009, de 23 de marzo.

[19] Sobre la materia, de interés, DE MIGUEL BERIAIN, I. y MORLA GONZÁLEZ, M.: "Digital pills for mental diseases: an ethical and social analysis of the issues behind the concept", *Journal of Law and the Biosciences*, agosto 2020, pág. 3 y ss. quienes señalan que, además, podría ser un medio esencial para el sostenimiento y mejora del sistema sanitario, dado que habitualmente la información que el paciente proporciona a su profesional no siempre resulta plenamente fiable y los métodos de control del paciente son ineficientes.

En este sentido, los riesgos fundamentales que el uso de la informática entrañan para los derechos de quien presta servicios por cuenta ajena aparecen fundamentalmente derivados de su capacidad para recopilar y transmitir datos sobre la persona del trabajador, así como la capacidad de tratamiento o elaboración de la información obtenida, permitiendo un ilimitado e indiscriminado manejo de informaciones sobre los empleados, lo que facilita a la empresa el acceso al conocimiento de circunstancias personales con su total desconocimiento[20].

Resulta fácil, por tanto, observar el potencial peligro que derivaría de un inadecuado uso de tales informaciones, que adecuadamente tratadas y cruzadas llegarían a permitir a la unidad productiva elaborar perfiles extremadamente precisos sobre sus empleados que incluyan datos de su más estricta intimidad (estado de salud, tendencias sexuales, afiliación sindical o política, aficiones…), circunstancia que podría dar lugar al inicio de actuaciones discriminatorias camufladas bajo otras formas y basadas en tales conocimientos, momento en el cual la información como poder deja atrás "su carácter de tópico para convertirse en una muy tangible realidad"[21].

Así, vista la agresividad que la informática puede poseer frente a los derechos del individuo en el marco de una prestación de servicios, lo importante será, por tanto, establecer un punto de equilibrio entre el derecho del empresario a utilizar de la forma más óptima las posibilidades que las nuevas tecnologías ponen a su alcance y la correcta preservación y respeto de los derechos y libertades fundamentales del trabajador[22].

---

[20] GOÑI SEIN, J. L.: "Vulneración de derechos fundamentales en el trabajo mediante instrumentos informáticos, de comunicación y archivo de datos", en AA.VV. (ALARCÓN CARACUEL, M. R. y ESTEBAN LEGARRETA, R., Coords.): *Nuevas tecnologías de la información y la comunicación y Derecho del Trabajo*, Albacete (Bomarzo), 2004, pág. 51.

[21] TASCÓN LÓPEZ, R.: "Sobre la ejecución procesal de las obligaciones derivadas de la legislación sobre protección de datos personales; en este caso, eliminar los datos relativos a los diagnósticos médicos de los trabajadores de un archivo empresarial sobre absentismo con baja médica (Comentario a la STCo 153/2004, de 20 de septiembre)", *Revista Española de Protección de Datos*, núm. 2, 2007, pág. 223.

[22] Al respecto, LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, cit., pág. 55.

El ordenamiento social permanece, no obstante, ayuno de una regulación específica, de forma tal que, en este intento, como suele ser habitual, la normativa laboral debe iniciar su regulación desde reglas jurídicas que ordenan con carácter general el tratamiento automatizado de datos personales para, a partir de las mismas, y como un plus a través del cual atender a las circunstancias específicas presentes en la relación de trabajo, proceder a la construcción de principios y reglas especiales[23].

En cualquier caso, la elaboración de un concepto de dato relativo a la salud constituye una de esas cuestiones pendientes de culminación[24], en tanto a día de hoy no existe texto legal interno alguno que aporte una definición vinculante, aun cuando afortunadamente sí cabe destacar la existencia de una categoría de datos sensibles o especialmente protegidos[25] en la cual aparecen incardinados aquellos relativos a la salud.

Se está, por tanto, ante un derecho en riesgo permanente por sus propias características, pues la amenaza y la inseguridad del trabajador pueden provenir no solo de la empresa para la que se prestan servicios, sino también del exterior por diferentes medios como los miles de ciberataques diarios que se producen a distintos niveles, riesgos ante los cuales el Derecho está reaccionando para proteger la privacidad y la intimidad de las personas, pero necesitado de pasos más profundos en el día a día de la empresa en cuanto a la protección de datos y cuestiones relativas a los datos de salud de los trabajadores.

En esta línea, el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección

---

[23] FERNÁNDEZ DOMÍNGUEZ, J. J. y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Madrid (Agencia de Protección de Datos), 1997, pág. 101.

[24] Al respecto, DE MIGUEL SÁNCHEZ, N.: "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *Revista Española de Protección de Datos*, núm. 1, 2006, págs. 146-147.

[25] Sobre la materia, y en torno al concepto de los datos de salud, FERNÁNDEZ LÓPEZ, J. M.: "El derecho fundamental a la protección de datos personales. Obligaciones que derivan para el personal sanitario", *Derecho y Salud*, Número extraordinario del XI Congreso de Derecho y Salud, 2003, págs. 42 y ss.

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[26], ha venido a destacar, en su considerando 35, cómo "entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro", incluyendo la información sobre la persona física recogida con ocasión de su inscripción "a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia…; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro".

En este sentido, algún autor ha venido a entender que este concepto abarcaría los datos de carácter médico, pero también los que mantengan conexión con fines relacionados con la salud, ya sean tratados en el ámbito de la salud pública, en seguros de enfermedad o en actividades científicas o estadísticas, incorporando todo lo relativo al cuerpo humano y afectando, por tanto, a la sexualidad, raza y código genético[27] e incluyendo antecedentes familiares, hábitos de vida y consumo y

[26] Un amplio estudio sobre la norma en PRECIADO DOMÈNECH, C. H.: *El Derecho a la Protección de Datos en el contrato de trabajo. Adaptado al nuevo Reglamento 679/2016, de 27 de abril*, Pamplona, (Aranzadi), 2017, pág. 29 y ss. o BLÁZQUEZ AGUDO, E. M.ª.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid (CISS), 2018, pág 21 y ss.

[27] HEREDERO HIGUERAS, M.: "La protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de octubre", *Derecho y Salud*, Vol. 2, 1994, pág. 19.

enfermedades presentes, pasada o previsibles en un futuro[28], así como los datos psicológicos y referentes a la salud mental[29].

Destacar cómo, y aun cuando la primera parte del concepto señalado resulta válida en tanto efectivamente se trata de datos de carácter personal, no puede obviarse que jurídicamente la inclusión en el expediente médico-laboral de datos como los señalados supondría, salvo consentimiento expreso del afectado, una clara y flagrante vulneración del derecho a la intimidad de la persona. Más aún si a datos médicos en el marco de la relación laboral se está haciendo referencia, en tanto el personal médico no podrá realizar más pruebas que las estrictamente necesarias e imprescindibles, dado que, de otra forma, constituiría una intromisión ilegítima en la intimidad del trabajador.

En todo caso, y por mor de la propia actividad médica, la información de carácter personal en torno a esta cuestión incluirá tanto datos sobre salud que tengan que ver con el puesto de trabajo como otros que no tienen tal relación pero han surgido inevitablemente de la práctica del examen médico, por lo que cabe colegir que será necesaria una acepción amplia del concepto de información médica de carácter personal, aun cuando no cabe olvidar en ningún momento que las conclusiones extraídas de dicha información deben aparecer relacionadas exclusivamente con la aptitud del trabajador para desempeñar sus obligaciones profesionales o con la necesidad de mejorar o introducir nuevas medidas preventivas y protectoras frente a determinados riesgos, pues no puede obviarse el hecho de que los reconocimientos realizados tienen

[28] LUCAS MURILLO DE LA CUEVA, P.: "El tratamiento jurídico de los documentos y registros sanitarios informatizados y no informatizados", en AA.VV.: ***Información y documentación clínica (Actas del Seminario Conjunto sobre Información y Documentación Clínica celebrado en Madrid los días 22 y 23 de septiembre de 1997), Vol. II*, Madrid (CGPJ/ MSC), 1997, págs. 586-587.**

[29] SÁNCHEZ-CARO, J. y ABELLÁN, F.: *Telemedicina y protección de datos sanitarios. Aspectos legales y éticos*, Granada (Comares), 2002, pág. 45, quienes incluyen los datos de salud mental y psíquicos en el concepto de salud "bien deriven expresamente de historiales médicos (de un determinado tratamiento psicológico o psiquiátrico), bien provengan de encuestas, y en este último supuesto por considerar que, en cualquier caso, se trata de datos referentes a la salud de las personas, que concierne directamente a su salud mental o se encuentran estrechamente relacionados con esta última".

en todo momento una finalidad preventiva y no terapéutica, que se enmarcaría en otro estadio.

Así, partiendo del principio de la pertinencia y proporcionalidad de las pruebas y los resultados a los supuestos que justifican la vigilancia de la salud, no ha faltado algún autor para quien cabría plantearse la legitimidad de incluir en el historial clínico de un trabajador las noticias o datos sobre su estado de salud que no resulten relevantes dentro de la política de Prevención de Riesgos Laborales[30].

Desde la óptica del cumplimiento de la obligación empresarial de proporcionar seguridad en el trabajo, los resultados de los reconocimientos médicos "permitirán planificar y, en su caso, reorientar la actividad preventiva en la empresa. Ahora bien, ocurre que el reconocimiento médico implica, en sí mismo, una intromisión en la esfera privativa del trabajador. Tal contraposición de intereses exige la búsqueda de un punto de equilibrio"[31]. Así, vista la agresividad que la informática puede poseer frente a los derechos del individuo en el marco de una prestación de servicios, lo importante será, por tanto, establecer ese punto de equidad entre el derecho del empresario a utilizar de la forma más óptima las posibilidades que las nuevas tecnologías ponen a su alcance y la correcta preservación y respeto de los derechos y libertades fundamentales del trabajador[32].

Cuestión distinta la constituye la facultad otorgada al empresario ya mencionada en epígrafes anteriores que le permite verificar el estado de salud alegado por el trabajador para justificar su falta de asistencia al trabajo mediante la realización de un reconocimiento a cargo del personal médico, pudiendo significar una negativa del empleado la

[30] Principio que "parece ser el adoptado en el artículo 37 RSP", MARTÍNEZ FONS, D.: *La vigilancia de la salud de los trabajadores en la Ley de Prevención de Riesgos Laborales*, Valencia (Tirant lo Blanch), 2002, págs. 97-98.

[31] RODRÍGUEZ ESCANCIANO, S.: "El tratamiento de datos sensibles vinculados a la Prevención de Riesgos Laborales", *Revista Jurídica de la Universidad de León*, núm. 5, 2018, pág. 168.

[32] Al respecto, LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, cit., pág. 55.

suspensión de los derechos económicos que pudieran existir a cargo de quien proporciona empleo por dichas situaciones (art. 20.4 ET)[33].

Dicho control ni es equiparable ni sigue las mismas reglas que la vigilancia de la salud en materia de Prevención de Riesgos Laborales, pues sus objetivos se centran básicamente en un control del absentismo. En cualquier caso, afecta a la materia ahora tratada en tanto en cuanto implica la verificación de la existencia de enfermedad, circunstancia que va a significar un tratamiento de datos de salud, y por tanto de una categoría especial de datos, teniendo como base jurídica para el tratamiento de estos el propio contrato de trabajo (art. 6.2.b del RGPD) en relación con las facultades concedidas por el artículo 20.4 ET, de forma tal que no se requiere el consentimiento del afectado.

En cualquier caso, la empresa tampoco se encuentra legitimada en este supuesto para conocer los detalles concretos del reconocimiento médico, sino únicamente su conclusión, que no puede ser otra que determinar si la persona está o no en condiciones psicofísicas de reincorporarse a su puesto de trabajo.

En este sentido, la incorporación de datos de salud a un fichero con la única finalidad de realizar controles del absentismo resulta desproporcionada, habida cuenta de que mediante la creación de tal base de datos "parece perseguirse un control más eficaz del absentismo laboral, según las facultades que al efecto reconoce al empresario la legislación vigente. En este sentido, lo primero que conviene advertir es que entre dichas facultades no figura la de proceder al almacenamiento en soporte informático de los datos atinentes a la salud de los trabajadores -y en concreto del diagnóstico médico- prescindiendo del consentimiento de estos. Por otra parte, y con independencia de ello, lo verdaderamente relevante es que la medida adoptada por la empresa, sometida a los cánones establecidos para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, no reviste la

[33] Sobre la cuestión, AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *La protección de datos en las relaciones laborales*, Madrid (Agencia Española de Protección de Datos), 2021, pág. 57.

consideración de solución idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral", en tanto en cuanto no constituye una medida "ponderada y equilibrada, ya que de ella no se derivan más beneficios o ventajas para el interés general o para el interés empresarial que perjuicios sobre el invocado derecho a la intimidad"[34].

Así, y atendiendo al contenido del fichero cabe destacar 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 (art. 7.3 L.O.R.T.A.D. y, por remisión, arts. 10.11 y 61 L.G.S.), que justificaría la autorización por ley, sin necesidad del consentimiento del trabajador, para el tratamiento Control de la actividad laboral… [como no puede serlo en la protección de datos automatizados] en las relaciones laborales de los datos atinentes a su salud, ni tampoco en lo dispuesto en los arts. 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"[35].

Por otra parte, este control del absentismo adquiere una relevancia particular cuando su desarrollo corre a cargo de un prestador de servicios externo ya que, además de cumplir con las obligaciones propias de un encargado del tratamiento, debe atenerse a ciertas condiciones: en primer término, la información a la persona trabajadora debe ser muy precisa e indicar que se trata de un control laboral, debiendo tal

[34] STC 202/1999, de 8 de noviembre. Sobre la materia, también, SSTC 207/1996, de 16 de diciembre o 69/1999, de 26 de abril.

[35] STSJ Madrid 8 marzo 2019 (JUR 118324).

información referirse a que se están verificando sus condiciones de aptitud por cuenta de la empresa y que el tratamiento de datos se ampara en el art. 20.4 del ET; de otro lado, la incorporación de los datos de salud de la persona trabajadora por parte del prestador de ese servicio a una historia clínica le convertirá en responsable del tratamiento[36].

Será también válido en estos supuestos que la empresa subcontrate los servicios médicos de una sociedad externa para reconocer a los trabajadores que se ausentan por motivos de salud, siempre y cuando esta se realice dentro de los límites de la buena fe y sea proporcional con los objetivos buscados[37], encontrándose legitimadas para elaborar estadísticas sobre el índice de absentismo y sus causas, aunque, eso sí, estas no pueden contener datos personales, sino únicamente datos disociados al objeto de impedir la identificación de las personas concretas que constan en fichero.

2.1. La Ley de Protección de Datos y los daños a la salud de los trabajadores

Tras la aprobación de la nueva Ley de Protección de Datos se hace necesario analizar sus contenidos y los principios y garantías recogidos en el Reglamento UE 2016/679 del Parlamento europeo y del Consejo de 27 de abril de 2016, de Protección de Datos Personales[38], sin olvidar tampoco las pautas introducidas al respecto en la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, que acoge como postulado básico la autonomía de la persona del trabajador para someterse o no a los reconocimientos médicos, propuestos por la empresa, permitiendo, en su caso, exploraciones y analíticas sobre datos corporales, o impidiendo pruebas clínicas ajenas a la finalidad de la vigilancia de la

[36] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *La protección de datos en las relaciones laborales*, cit., pág. 58.

[37] STS 25 enero 2018 (RJ 725).

[38] Al respecto, GARCÍA MURCIA, J. y RODRÍGUEZ CARDO, I. A.: "La protección de datos personales en el ámbito del trabajo: una aproximación desde el nuevo marco normativo", *Nueva Revista Española de Derecho del Trabajo*, núm. 216, 2019, pág. 20 y ss.

salud en relación con los riegos inherentes al trabajo. Este criterio se conecta directamente con la obligación de información previa, de forma que el trabajador debe ser expresamente alertado sobre los exámenes médicos especialmente invasores de su intimidad al tiempo de otorgar su consentimiento[39].

La redacción utilizada por la Ley de Prevención de Riesgos al señalar la confidencialidad de estos datos y la imposibilidad de su uso con fines discriminatorios o en perjuicio del trabajador está aludiendo a las normas sobre protección de datos de carácter personal[40], en particular, al artículo 5 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, de acuerdo con el cual "los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1 f) del Reglamento (UE) 2016/679"[41], destacando que "la obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable".

Quedan, en definitiva, proscritas las vigilancias médicas indiscriminadas, injustificadas o generalizadas para cualquier caso o actividad[42], aun cuando, funcionando como una especie de excepción a la

[39] Sobre estas cuestiones, entre otros, PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, Madrid (CES), 2005, pág. 120 y ss.; ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F.: *El derecho de los trabajadores a su intimidad*, Pamplona (Thomson/Aranzadi), 2006, pág. 123 y ss. o FERNÁNDEZ-COSTALES MUÑIZ, J.: *La vigilancia de la salud de los trabajadores*, León (Junta de Castilla y León/Eolas), 2009, pág. 95 y ss.

[40] FERNÁNDEZ-COSTALES MUÑIZ, J.: *Prevención de Riesgos Laborales y empresa: obligaciones y responsabilidades*, Pamplona (Aranzadi), 2019, págs 143-144.

[41] Sobre esta cuestión en el Reglamento europeo, PEDROSA ALQUÉZAR, S. I.: "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Empleo y Seguridad Social*, núm. 137, 2018, pág. 166 y ss.

[42] SÁNCHEZ CUBEL, M. D.: *Todo sobre la nueva Ley de Prevención de Riesgos Laborales*, Barcelona (Praxis), 1996, pág. 89.

excepción, no cabe olvidar la necesidad del consentimiento[43] expreso del trabajador o que una Ley, por razones de interés general, permita el tratamiento de estos datos especialmente sensibles, tal y como establece el artículo 9.2 del RGPD y su trasposición en España a través del artículo 9.2 LOPDP, que destaca cómo "los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad… En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte".

Además, el artículo 9.2.h) del Reglamento admite la recogida y tratamiento de datos con fines de "medicina preventiva o laboral" y "evaluación de la capacidad laboral del trabajador", sin perjuicio de que hayan de respetarse las garantías y límites pertinentes en relación con los datos que se pretenden obtener y su posible uso posterior.

La determinación del sujeto responsable del fichero que integre las obligaciones relativas a la salud "requiere la previa determinación del sujeto de quién deba predicarse la obligación de mantener la información relativa a la salud, así como la extensión de la misma", siendo posible diferenciar al menos tres hipótesis distintas: "el personal médico que practica las medidas de vigilancia, el empresario sobre el que recae la obligación legal de mantener la información derivada de la vigilancia de la salud y, en fin, la existencia de servicios de prevención internos o externos encargados de la vigilancia de la salud"[44].

---

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

[44] MARTÍNEZ FONS, D.: *La vigilancia de la salud de los trabajadores en la Ley de Prevención de Riesgos Laborales*, cit., págs. 110 y ss.

En este sentido, cabe destacar cómo la nueva normativa obliga a que los responsables y encargados determinen "las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa" (arts. 24 y 25 RGPD y 28 LOPDP).

Todos los datos extraídos del cumplimiento del deber empresarial de garantizar la salud deben ser almacenados en ficheros de la empresa, quedando condicionado su mantenimiento en ellos a su utilidad y, consecuentemente, a su periódica actualización. Es más, el empresario debe elaborar y conservar a disposición de la autoridad competente la documentación por la que acredite que efectivamente cumple con el deber de control de la salud de los trabajadores y las conclusiones que se deriven de los reconocimientos médicos practicados.

Así, el cumplimiento de lo previsto demanda al titular de la organización empresarial realizar un acopio documental que, en ciertos casos, dependiendo de la índole de la actividad empresarial, puede resultar ingente, y para su organización resultará de todo punto necesaria su acumulación en ficheros, de los cuales es responsable precisamente el empresario, aunque, paradójicamente, no tiene derecho al acceso a la totalidad del contenido de los mismos[45]. No cabe olvidar, en definitiva, que uno de los principios fundamentales de un adecuado sistema de tratamiento de datos viene dado por conseguir un "escrupuloso respeto a la confidencialidad de los mismos"[46] en tanto en cuanto esta forma parte fundamental e inescindible del derecho a la intimidad de la persona.

Cabe señalar también la importancia del principio de veracidad, el cual viene a exigir que los datos de carácter personal almacenados sean

---

[45] PRADAS MONTILLA, R.: "Empresas y protección de datos de carácter personal", *Actualidad Laboral*, T. I, 2003, pág. 73.

[46] PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, cit., pág. 119.

exactos y estén actualizados, de forma tal que el trabajador no se vea lesionado en su posición jurídica en tanto la empresa pueda tomar decisiones partiendo de datos inexactos o desactualizados que, incluso, puedan ir en detrimento de la propia salud. Ello permitirá hacer uso de los derechos de rectificación o cancelación regulados en los artículos 14 y 15 LOPDP.

No obstante, si los datos resultaren pertinentes para otro fin compatible (art. 6.4 LOPDP) y resulten útiles al empresario para la organización y dirección de la prestación laboral en la unidad productiva, deberá permitirse su mantenimiento[47], previa notificación o petición de consentimiento respecto a esta nueva finalidad a cual serán destinados, habida cuenta de que obstaculizar con garantías "excesivamente formalistas" una actividad empresarial cada vez más irremediablemente obligada al uso de sistemas informáticos no ofrece a día de hoy una lógica clara, pues resultaría absurdo la exigencia de cancelación de una serie de datos que ya se poseen y se necesitan para un nuevo fin en tanto significaría obligar a una segunda recogida de los mismos, sin que tal circunstancia redunde en una mayor garantía de los derechos del trabajador[48].

Estos principios y derechos implican que los datos no podrán ser mantenidos por tiempo ilimitado[49], siendo el principio de conservación limitada otro de los aplicables a la protección de datos y a la vigilancia de la salud, de acuerdo con el cual los pormenores referentes al control médico únicamente permanecerán en los ficheros por el tiempo

[47] Sobre la conservación y custodia de la historia clínica, con carácter general, AYERRA LAZCANO, J. M.ª.: "Regulación general de la historia clínica", *Derecho y Salud*, Vol. 11, 2003, págs. 29 y ss.

[48] En tal sentido, aunque no en el ámbito estricto de los datos de salud, FERNÁNDEZ VILLAZÓN, L. A.: "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores", *Relaciones Laborales*, T. I, 1994, pág. 537.

[49] En torno a la materia, destacando las distintas legislaciones autonómicas a este respecto, o haciendo notar cuestiones como los plazos de una posible reclamación en vía civil o penal por actuaciones médicas, ÁLVAREZ CIVANTOS, O. J.: *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada (Comares), 2002, págs. 261 y ss.

necesario para el cumplimiento de los fines para los cuales fueron en su momento recabados. Así, ante los resultados de un nuevo examen habrá de determinarse cuáles mantienen su validez respecto a los anteriores para contribuir a una eficaz protección, de forma tal que si algún dato carece ya de utilidad deberá ser cancelado[50].

De tal manera, parece evidente que ante determinados supuestos, como que el trabajador cambie de empresa o cuando tras un proceso de selección no haya sido aceptado para formar parte de la misma, el fin para el cual las informaciones fueron recogidas desaparece, careciendo de sentido su mantenimiento en poder de la unidad productiva, resultando lo contrario en todo caso una intolerable apropiación perpetua e indebida de amplios aspectos y facetas de la vida personal del sujeto[51].

El artículo 18.1 CE impide las injerencias "arbitrarias o ilegales" en la intimidad. De tal premisa cabe deducir cómo el derecho a la intimidad personal será vulnerado cuando la intromisión en el ámbito propio y reservado del sujeto no sea acorde con la Ley, no sea eficazmente consentida o, aún autorizada, subvierta los términos y el alcance para el que se otorgó el consentimiento, quebrando la conexión entre la información personal que se recaba y el objetivo tolerado para el que fue recogida. La ley impone, por tanto, no solo la confidencialidad de los datos recabados y análisis realizados en los reconocimientos médicos, sino también su realización en la forma y con los medios que no lleguen a suponer una intrusión fuera de contexto en la vida privada e íntima del trabajador.

En cualquier caso, y con todo, al tener que entregar las conclusiones que tengan que ver con el correcto desarrollo de las funciones en materia preventiva, la confidencialidad de la información puede correr riesgos que resultan difícilmente evitables. Que un dato tenga el

[50] PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, cit., págs. 168-169.

[51] MURILLO DE LA CUEVA, P. L.: "Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)", *Cuadernos y Debates*, núm. 43, 1993, pág. 69.

carácter de confidencial significa su "reservabilidad", su mantenimiento en secreto frente a personas que no tienen interés legítimo alguno en su conocimiento, de forma tal que dicha privacidad debe ser interpretada de forma restrictiva y siempre funcionarizada directa e imprescindiblemente a la prevención.

El artículo 22 LPRL, al margen de establecer el principio de confidencialidad, lo modula también tomando en consideración la articulación de la documentación como resultados o como conclusiones de las pruebas practicadas, dando a los primeros una máxima confidencialidad, mientras las segundas ven mermado ese blindaje en virtud del tipo de datos que incorporan y la mayor cantidad de sujetos a los cuales se les comunican, aun cuando no deben en caso alguno trascender más allá de la Administración sanitaria, la empresa o los sujetos con responsabilidades en materia preventiva.

La información médica de carácter personal plasmada en los resultados de la vigilancia de la salud incluye (destacando así la amplia acepción que el término posee, aun cuando no todos los autores lo hayan considerado de tal manera), además de información sobre la salud que tiene que ver con el puesto de trabajo, datos que no poseen relación directa con la prestación de servicios pero que han surgido en la práctica del examen de salud. Referencia terminológica, en definitiva, orientada a unos resultados que, al pertenecer a la esfera íntima del trabajador, resultarán únicamente accesibles al personal médico o autoridades sanitarias que han desarrollado las distintas pruebas enmarcadas en el proceso de vigilancia de la salud, quienes deberán guardar secreto[52] respecto al contenido de los resultados frente al resto de personas con alguna relación con las tareas preventivas de vigilancia de la salud y, por supuesto, frente a terceros, excepción hecha del supuesto de que la no revelación de esos datos pudiera suponer un perjuicio para la salud de otros trabajadores o terceras personas relacionadas con la empresa o que por imperativo legal se establezca lo contrario.

[52] Al respecto, TOLOSA TRIBIÑO, C.: "El secreto profesional de los médicos en la Ley de Prevención de Riesgos Laborales", *Relaciones Laborales*, núm. 20, 1997, pág. 125 y ss.

Cuestión distinta es que, partiendo de tal información, resulte necesario extraer unas conclusiones relativas exclusivamente a la aptitud (o no) del empleado en relación con el desempeño de las obligaciones que su puesto de trabajo implica o con la posible necesidad de introducir cambios o mejoras preventivas y protectoras. Estas conclusiones se elaborarán utilizando, pero no incorporando, lo más destacado de la información médica, evitando facilitar información de índole médica o clínica o reflejar el problema de salud concreto padecido por un trabajador.

Respecto a las mismas el deber de confidencialidad aparece algo más relajado, en tanto que serán comunicadas al empresario y a ellas tendrán acceso las personas y órganos con responsabilidad en materia de prevención con objeto de que puedan desarrollar correctamente sus funciones, o lo que es lo mismo, delegados de prevención, comité de Seguridad y Salud y la representación unitaria y sindical de los trabajadores, quienes aparecen igualmente sometidos al deber de confidencialidad.

Esta obligación no solo atañe a estos y a los profesionales médicos, sino también al resto de profesionales y trabajadores del ámbito sanitario que participan en la asistencia del paciente. Así, bajo el paraguas de la confidencialidad se obliga también a sujetos tales como administrativos, documentalistas, informáticos, etc. que pueden tener acceso a datos de salud de los pacientes[53].

El acceso de los representantes de los trabajadores a datos sanitarios, debido a la sensibilidad y naturaleza de los mismos, parece hacer conveniente que los datos sean oportunamente disociados. Respecto a esta facultad de la que disfrutan los delegados de prevención de conocer y analizar los daños producidos en la salud e integridad física de los trabajadores del artículo 39.2 LPRL, al venir situados los objetivos en analizar las causas y proponer medidas preventivas oportunas, y aun

[53] SÁNCHEZ CARO, JAVIER Y ABELLÁN-GARCÍA SÁNCHEZ, FERNANDO: *Derechos y deberes de los pacientes (Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas)*, Granada (Comares), 2003, pág. 41 y ss.

cuando no faltan autores que opinan que tal disposición legal habilita en todo caso al tratamiento de datos personales de los trabajadores afectados, cabe destacar que no siempre será necesario conocer los datos personales del operario, aun cuando es posible que, en ocasiones, sea relevante identificar las condiciones particulares del sujeto para llevar a cabo de la manera más adecuada la tarea preventiva.

2.2. La anonimización de datos personales

En cualquier caso, y dada la excesiva implicación de una amplia pluralidad de sujetos con legitimidad en materia preventiva lo más razonable resulta mantener en el anonimato la identidad concreta del trabajador respecto al cual trascienden determinados datos médicos, de forma tal que únicamente se ofrezca el conocimiento de aspectos que permitan localizar el riesgo en el sistema organizativo de la empresa, utilizando para ello datos cifrados mediante claves codificadas o el envío de manera separada de los datos personales y de salud de los trabajadores impidiendo así la asociación de ambos.

En esta línea, el recurso que permite aminorar los riesgos y garantiza la seguridad en la utilización masiva de datos es la anonimización[54], que no es otra cosa, tal y como señala el Considerando 26 Reglamento 2016/679, que el vaciado de contenido personal de los datos denominados personales. Para anonimizar un dato debe vaciarse a este de todo aquel contenido que lo conecte con el individuo al cual pertenece, de forma tal que no pueda utilizarse para identificar a una persona física a través del conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento de datos o por terceros. Así, entendiendo que el estado anónimo ha de garantizarse de manera tan permanentemente como el borrado, la anonimización implicará una desidentificación sólida e irreversible.

[54] COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", *Health Affairs*, vol. 33, núm. 7, 2014, pág. 1139 y ss.

La anonimización consistía tradicionalmente en un proceso de dos fases principales. La primera despojaba a los conjuntos de datos de todos los rasgos identificadores personales (nombre, dirección, número de Seguridad Social,…). La segunda modificaba o eliminaba otras categorías de datos que podían actuar como identificadores en un contexto concreto. En este punto existe una dicotomía entre los datos de carácter personal, sujetos a las normas de protección de datos, y los datos ya anonimizados, habida cuenta de que una vez esto ha ocurrido "y los individuos ya no son identificables, la normativa de protección de datos no se aplica"[55].

Así, en un principio, la anonimización aseguraba la privacidad. Sin embargo, las fisuras que presenta esta técnica han alertado a la comunidad científica y a los juristas de las amenazas que sufre la información privada de los sujetos que han cedido sus datos a determinadas plataformas tecnológicas, pues, no en vano, de la mano del big data la creciente cantidad de información almacenada de millones de usuarios de internet facilita la reidentificación de las personas a las que pertenecen los datos en cuestión, aun cuando estos han sido anonimizados[56], lo que evidencia el peligro de que se produzcan accesos indeseados y no consentidos, así como usos diferentes, incluso fraudulentos, de aquellos para los cuales tales datos se han cedido o almacenado, con la consiguiente pérdida de la intimidad del afectado.

Por ello, este proceso de anonimización es un proceso crítico para las autoridades de protección de datos y las agencias creadas en la materia, en tanto en cuanto existen evidencias suficientes "que demuestran que los avances tecnológicos y la posibilidad de combinar diferentes

[55] GIL GONZÁLEZ, E.: *Big data, privacidad y protección de datos*, Madrid (Agencia Española de Protección de Datos/Boletín Oficial del Estado), 2016, pág. 83, quien señala cómo "de este modo, el resultado anulaba lo mejor de ambos lados: los datos continuaban siendo útiles, y podían ser analizados, compartidos o puestos a disposición del público al tiempo que los individuos no podían ser identificados, y por lo tanto se protegía su privacidad".

[56] Sobre esta cuestión, analizando los riesgos y el control de los datos MAYER-SCHÖENBERG, V. y CUKIER, K.: *Big Data. A revolution that will transform how we live, work and think*, cit., pág. 150 y ss.

datos puede conllevar la identificación de un consumidor, ordenador o dispositivo, incluso si estos datos por sí mismo no constituyen datos de identificación personal. Es más, no solo es posible reidentificar datos que no son identificadores personales a través de medios diversos, sino que las empresas tienen fuertes incentivos para hacerlo"[57].

La densidad del aspecto de protección de datos y ciberseguridad en la medicina digital impide que se pueda desarrollar en este trabajo un análisis en profundidad de la cuestión. Sin embargo, conviene hacer una breve reflexión respecto de un eventual acceso por parte de terceros especialmente interesados en estos datos del paciente, que, en un primer momento anonimizados, permitan ser desanonimizados, pudiendo reconectarlos con el sujeto al que pertenecen, y es que tal y como algún autor ha alertado es un hecho que "lo que el médico sabe también lo pueden saber –o intentar saber– terceros"[58].

A pesar de que el avance de las nuevas tecnologías permitiría, siempre y cuando fueran adoptadas las medidas precisas para garantizar la integridad y confidencialidad de los datos, la comunicación de los resultados a través del correo electrónico o de una página de internet facilitando al trabajador su acceso a través de una clave, el sobre cerrado y sellado por el servicio de prevención con la referencia expresa de confidencial parece el mejor sistema para garantizar dicha confidencialidad, siendo los mismos remitidos directamente al interesado y no a la empresa, circunstancia que generaría el riesgo de la filtración o el conocimiento de los datos por terceros no autorizados o no deseados.

---

[57] FEDERAL TRADE COMMISION: *Protecting consumer privacy in an era of rapid change. Recommendations for bussinesses and policymakers*, Washington (FEDERAL TRADE COMMISION), 2012, pág. 20.

[58] MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", *Revista Internacional de Éticas aplicadas*, núm. 29, 2019, pág. 129, pág. 129.

2.3. El tratamiento de datos y el acceso a los ficheros y documentación

Los avances tecnológicos y las labores de gestión y administración han obligado a que personal no sanitario pueda acceder y acceda a documentación clínica, ya sea para desarrollar sus tareas administrativas, ya para el mantenimiento de bases de datos en las que se alberga información de carácter médico. Ello ha dado lugar al denominado secreto médico derivado, configurado como un deber de sigilo a respetar por el personal no sanitario, que surge motivado por la complejidad administrativa y técnica existente en la actualidad en relación con la Medicina. Dicho personal posee la capacidad de acceso a información confidencial, quedando así obligado al secreto correspondiente, y, desde luego, siempre justificado dicho acceso por el ejercicio de sus legítimas funciones.

En este sentido, la labor del personal informático se debe centrar en asegurar una garantía sobre la correcta utilización de la información clínica. El informático tiene el deber de no acceder a datos que no requieren su conocimiento, puesto que "pese a tener la posibilidad de acceso en la medida que controla los propios sistemas informáticos no debe de hacer uso de esta prerrogativa"[59].

Las compañías informáticas y tecnológicas han venido desarrollado y desarrollan múltiples, variadas y diferentes aplicaciones y dispositivos en el ámbito de la salud con igualmente distintos usos y fines, lo que les obliga a "procurar que su servicio sea efectivo y óptimo. Para ello, el acceso a información sensible del paciente, usuario de sus servicios, se convierte entonces en un factor esencial para fines tales

[59] "La labor del personal informático se enmarca dentro del desarrollo de la actividad dirigida a garantizar que los datos contenidos en los sistemas de tratamiento de la información clínica de los pacientes sean utilizados de forma correcta. En ocasiones pueden producirse pérdidas de información accidentales, debiendo el informático proceder a la recuperación de dicha información, es en este momento, donde pueden darse casos en que tenga conocimiento de datos sobre la salud de determinadas personas". DE LORENZO Y MONTERO, RICARDO: "El secreto médico derivado", *Redacción Médica*, Núm. 1848, 2013, https://www.delorenzoabogados.es/blog/?p=52&idioma=eng.

como identificar eventuales fallos en sus dispositivos, desarrollar mejoras y llevar a cabo un control de calidad sobre sus servicios"[60]. En el eventual caso de que las empresas desarrolladoras de aplicaciones y dispositivos tuvieran acceso a datos de salud del paciente "se verán entonces sometidas a los deberes de confidencialidad que el secreto médico derivado descarga sobre ellas en aras de garantizar esa protección a la intimidad… cuya configuración… ha ido evolucionando en paralelo al avance de las nuevas tecnologías"[61].

Además, resulta preciso tener en cuenta, en términos de seguridad, que la tecnología no constituye un medio infalible, es más, la realidad nos muestra continuamente que puede fallar y lo hace, de forma tal que depositar elevados índices de confianza y dependencia en los productos médico-tecnológicos utilizados por los profesionales, conlleva riesgos y una serie de dilemas éticos y jurídicos de no poca importancia[62], y no solo en relación a la eventual responsabilidad en la que incurriría el médico ante el fallo del dispositivo que esté utilizando para tratar a su paciente[63], sino también en relación al acceso por parte de terceros a sus datos de salud, que tienen la categoría de especialmente protegidos (art. 9.1 reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016) o ante eventuales amenazas de ciberseguridad[64].

La Comisión Europea ha destacado los beneficios sociales que proporcionan estas aplicaciones, pero al mismo tiempo ha sido consciente de sus particularidades y de la tipología de datos que tratan y, en

---

[60] COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", cit., pág. 1139 y ss.

[61] MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", cit., pág. 128.

[62] GIOTA, K. y KLEFTARAS, G.: "Mental health apps: innovations, risks and ethical considerations", *E-Health Telecommunications Systems and Networks*, núm. 3, 2014, págs. 19-23.

[63] COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", *Health Affairs*, vol. 33, núm. 7, 2014, pág. 1139 y ss.

[64] MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", cit., pág. 128.

consecuencia, de la protección que debe otorgárseles, por lo que, sobre estas bases, ha estado elaborando un código de conducta europeo sobre privacidad en aplicaciones móviles de salud, en aras de proteger el debido cumplimiento de la protección de datos y de promover las buenas prácticas tanto de desarrolladores de aplicaciones como de los usuarios de Apps de salud.

Los principios en los que se basa el código de conducta no son más que un reflejo de aquellos incluidos explícitamente en el Reglamento 2016/679 de protección de datos dirigido especialmente a los desarrolladores de aplicaciones, habida cuenta de que son estos quienes en el diseño de las mismas deben garantizar el pleno respeto a los principios de privacidad desde el primer momento, pues la constante necesidad de mejora y mantenimiento de los dispositivos médico-tecnológicos necesita de al menos la información anonimizada como parte de la investigación en el ámbito de la medicina digital, y que para una mejora más cualificada de los dispositivos, sea posible el acceso a una información identificable[65].

En fin, la realidad es que quien posee la información será quien pueda suministrarla y, en tal sentido, el personal sanitario deberá integrar y delimitar el contenido de las conclusiones de los reconocimientos en cada caso concreto en función de los límites y condicionantes expuestos, de forma que será su conciencia en los términos de la deontología de su disciplina profesional la que deberá asegurar que los informes finales aparezcan delimitados en los estrictos términos impuestos legalmente.

La Recomendación 171 de la OIT, sobre los servicios de salud en el trabajo, constituye un buen ejemplo en cuanto a la fijación de este elemento interpretativo a utilizar en las conclusiones, habida cuenta de que en su artículo 16 destaca como "al término de un examen médico prescrito para determinar la aptitud de un trabajador para un puesto de

[65] Sobre la materia, KLUGMAN, C.; DUNN, L.; SCHWARTZ, J. y COHEN, I.: "The ethics of smart pills and sefl-acting devices: autonomy, truth-telling, and trust at the dawn of digital medicine", *American Journal of Bioethics*, vol. 18, núm. 9, 2017, pág. 1 y ss.

trabajo que entraña exposición a un riesgo determinado, el médico que lo haya realizado debería comunicar sus conclusiones por escrito al trabajador y al empleador. Por otra parte, esta comunicación no debería contener indicación alguna de índole médica; según los casos, podría indicar que el trabajador es apto para el puesto de trabajo previsto o bien especificar los tipos de trabajo y las condiciones de trabajo que le estén contraindicados, temporal o permanentemente, desde el punto de vista médico".

Por otra parte, y del mismo modo, el personal administrativo de un centro sanitario, puede, siempre en el ejercicio de sus funciones inherentes a su cargo, acceder a otro tipo de información confidencial relacionada con los pacientes, como puede ser la facturación por los servicios prestados, la gestión del sistema de citas para especialistas, etc, datos de los cuales podría llegar a deducirse con un mínimo conocimiento el tipo de enfermedad padecida, o si se está siguiendo un tratamiento en virtud del número de visitas o revisiones realizadas. Debe destacarse claramente que también en tales supuestos se mantiene el deber de secreto frente a tales informaciones y datos para el personal no sanitario, circunstancia evidentemente igual protegida por la regulación en materia de protección de datos[66].

[66] DE LORENZO Y MONTERO, RICARDO: "El secreto médico derivado", *Redacción Médica*, Núm. 1848, 2013, https://www.delorenzoabogados.es/blog/?p=52&idioma=eng.

BIBLIOGRAFÍA

AA.VV.: *Industria conectada* 4.0. *La transformación digital de la industria española*, Madrid (Ministerio de Industria), 2015.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS: *La protección de datos en las relaciones laborales*, Madrid (Agencia Española de Protección de Datos), 2021.

ALEMÁN PÁEZ, F.: "El derecho de desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi Travail n.º 2016-1088", *Trabajo y Derecho. Nueva revista de actualidad y relaciones laborales*, núm. 30, 2017.

ÁLVAREZ CIVANTOS, O. J.: *Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades*, Granada (Comares), 2002.

ÁLVAREZ CUESTA, H.: *El futuro del trabajo vs. el trabajo del futuro*, A Coruña (Colex), 2017.

ARIAS DOMÍNGUEZ, A. y RUBIO SÁNCHEZ, F.: *El derecho de los trabajadores a su intimidad*, Pamplona (Thomson/Aranzadi), 2006.

AYERRA LAZCANO, J. M.ª.: "Regulación general de la historia clínica", *Derecho y Salud*, Vol. 11, 2003.

BORRAJO DACRUZ, E.: "El impacto de tecnologías y medios de información en el Derecho del Trabajo", en AA.VV.: *Implicaciones socio-jurídicas de las tecnologías de la información: encuentros 1980-1990: los juristas ante la revolución informática*, Madrid (CITEMA), 1991.

COHEN, I.; AMARASINGAHM, R.; SHAH, A.; XIE, B. y LO, B.: "The legal and ethical concerns that arise from using complex predictive analytics in health care", *Health Affairs*, vol. 33, núm. 7, 2014.

CRUZ VILLALÓN, J. "El impacto de la digitalización sobre los derechos fundamentales laborales", en AA.VV. (RODRÍGUEZ-PIÑERO ROYO, M. y TODOLÍ SIGNES, A., Dirs.): *Vigilancia y control en el Derecho del Trabajo digital*, Pamplona (Aranzadi), 2020.

DE LORENZO Y MONTERO, RICARDO: "El secreto médico derivado", *Redacción Médica*, Núm. 1848, 2013, https://www.delorenzoabogados.es/blog/?p=52&idioma=eng.

DE MIGUEL SÁNCHEZ, N.: "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *Revista Española de Protección de Datos*, núm. 1, 2006.

DE MIGUEL BERIAIN, I. y MORLA GONZÁLEZ, M.: "Digital pills for mental diseases: an ethical and social analysis of the issues behind the concept", *Journal of Law and the Biosciences*, agosto 2020.

DÍEZ-PICAZO, L.: *Experiencias jurídicas y teoría del Derecho*, 3.ª ed., Barcelona (Ariel), 1993.

FEDERAL TRADE COMMISION: *Protecting consumer privacy in an era of rapid change. Recommendations for bussinesses and policymakers*, Washington (FEDERAL TRADE COMMISION), 2012.

FERNÁNDEZ COSTALES, J.: "La aplicación y la incidencia de la informática en el ámbito del Derecho Civil", *Revista General de Legislación y Jurisprudencia*, núm.4, 1985.

FERNÁNDEZ DOMÍNGUEZ, J. J. y RODRÍGUEZ ESCANCIANO, S.: *Utilización y control de datos laborales automatizados*, Madrid (Agencia de Protección de Datos), 1997.

FERNÁNDEZ LÓPEZ, J. M.: "El derecho fundamental a la protección de datos personales. Obligaciones que derivan para el personal sanitario", *Derecho y Salud*, Número extraordinario del XI Congreso de Derecho y Salud, 2003.

FERNÁNDEZ VILLAZÓN, L. A.: "Tratamiento automatizado de datos personales en los procesos de selección de trabajadores", *Relaciones Laborales*, T. I, 1994.

FERNÁNDEZ-COSTALES MUÑIZ, J.: *La vigilancia de la salud de los trabajadores*, León (Junta de Castilla y León/Eolas), 2009.

– *Prevención de Riesgos Laborales y empresa: obligaciones y responsabilidades*, Pamplona (Aranzadi), 2019.

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

GIL GONZÁLEZ, E.: *Big data, privacidad y protección de datos*, Madrid (Agencia Española de Protección de Datos/Boletín Oficial del Estado), 2016.

GIOTA, K. y KLEFTARAS, G.: "Mental health apps: innovations, risks and ethical considerations", *E-Health Telecommunications Systems and Networks*, núm. 3, 2014.

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

GOÑI SEIN, J. L.: "Flexibilidad y revisión del ámbito del Derecho del Trabajo", en AA.VV. (RIVERO LAMAS, J., Coord.): *La flexibilidad laboral en España*, Zaragoza (Instituto de Relaciones Laborales), 1993.

HEREDERO HIGUERAS, M.: "La protección de datos de salud informatizados en la Ley Orgánica 5/1992, de 29 de octubre", *Derecho y Salud*, Vol. 2, 1994.

KLUGMAN, C.; DUNN, L.; SCHWARTZ, J. y COHEN, I.: "The ethics of smart pills and sefl-acting devices: autonomy, truth-telling, and trust at the dawn of digital medicine", *American Journal of Bioethics*, vol. 18, núm. 9, 2017.

LUCAS MURILLO DE LA CUEVA, P.: "El tratamiento jurídico de los documentos y registros sanitarios informatizados y no informatizados", en AA.VV.: *Información y documentación clínica (Actas del Seminario Conjunto sobre Información y Documentación Clínica celebrado en Madrid los días 22 y 23 de septiembre de 1997), Vol. II*, Madrid (CGPJ/MSC), 1997.

LUJÁN ALCARAZ, J.: "Uso y control en la empresa de los medios informáticos de comunicación", *Aranzadi Social*, T. II, 2005.

MARTÍNEZ FONS, D.: *La vigilancia de la salud de los trabajadores en la Ley de Prevención de Riesgos Laborales*, Valencia (Tirant lo Blanch), 2002.

MAYER-SCHÖENBERG, V. y CUKIER, K.: *Big Data. A revolution that will transform how we live, work and think*, Boston/Nueva York (Eamon Dolan Book/Mariner Books/Houghton Mifflin Harcourt), 2013, (en version traducida: *Big Data. La revolución de los datos masivos*, Madrid (Turner), 2013).

MORLA GONZÁLEZ, M.: "Medicamentos digitales. La autonomía del paciente a debate", *Revista Internacional de Éticas aplicadas*, núm. 29, 2019.

MURILLO DE LA CUEVA, P. L.: "Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)", *Cuadernos y Debates*, núm. 43, 1993.

PEDROSA ALQUÉZAR, S. I.: *La vigilancia de la salud en el ámbito laboral. Regulación legal, límites y cuestiones problemáticas*, Madrid (CES), 2005.

– "Vigilancia de la salud laboral y protección de datos", *Revista del Ministerio de Empleo y Seguridad Social*, núm. 137, 2018.

PRADAS MONTILLA, R.: "Empresas y protección de datos de carácter personal", *Actualidad Laboral*, T. I, 2003.

PRECIADO DOMÈNECH, C. H.: *El Derecho a la Protección de Datos en el contrato de trabajo. Adaptado al nuevo Reglamento 679/2016, de 27 de abril*, Pamplona, (Aranzadi), 2017, pág. 29 y ss. o BLÁZQUEZ AGUDO, E. M.ª.: *Aplicación práctica de la protección de datos en las relaciones laborales*, Madrid (CISS), 2018.

RODRÍGUEZ ESCANCIANO, S.: "La intimidad del trabajador en el uso de diagnósticos médicos informatizados", *Revista Española de Derecho del Trabajo*, núm. 101, 2000.

– "La potencialidad lesiva de la informática sobre los derechos de los trabajadores", en *Revista Española de Protección de Datos*, núm. 2, 2007.

– "El tratamiento de datos sensibles vinculados a la Prevención de Riesgos Laborales", *Revista Jurídica de la Universidad de León*, núm. 5, 2018.

SÁNCHEZ CARO, JAVIER Y ABELLÁN-GARCÍA SÁNCHEZ, FERNANDO: *Derechos y deberes de los pacientes (Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas)*, Granada (Comares), 2003.

SÁNCHEZ CUBEL, M. D.: *Todo sobre la nueva Ley de Prevención de Riesgos Laborales*, Barcelona (Praxis), 1996.

SÁNCHEZ-CARO, J. y ABELLÁN, F.: *Telemedicina y protección de datos sanitarios. Aspectos legales y éticos*, Granada (Comares), 2002.

TARODO SORIA, S.: *Libertad de conciencia y derechos del usuario de los servicios sanitarios*, Bilbao (Universidad del País Vasco), 2005.

TASCÓN LÓPEZ, R.: "Sobre la ejecución procesal de las obligaciones derivadas de la legislación sobre protección de datos personales; en este caso, eliminar los datos relativos a los diagnósticos médicos de los trabajadores de un archivo empresarial sobre absentismo con baja médica (Comentario a la STCo 153/2004, de 20 de septiembre)", *Revista Española de Protección de Datos*, núm. 2, 2007.

TOLOSA TRIBIÑO, C.: "El secreto profesional de los médicos en la Ley de Prevención de Riesgos Laborales", *Relaciones Laborales*, núm. 20, 1997.