Boletín de la Facultad de Derecho, núm. 18, 2001

EMPRESAS Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

José Malpartida Morano y Ricardo Pradas Montilla*

RESUMEN: *Trascendencia en el ámbito laboral de la Ley Orgánica 15/1999, de 13 de diciembre. Comentario a la STCONS 202/1999, de 8 de noviembre, que declaró contraria al derecho de la intimidad una base de datos sobre absentismo del Banco Central Hispanoamericano.*

LA LEY DE PROTECCIÓN DE DATOS Y LAS EMPRESAS

1. La reciente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal (en adelante LOPD), se aplica, sin duda alguna, a los ficheros en que las empresas puedan almacenar datos personales relativos a los trabajadores, como se deduce de las normas legales que describen su ámbito de aplicación en forma «positiva» (art. 2.1 LOPD) y los supuestos que quedan fuera de ese ámbito [ficheros establecidos para la investigación del terrorismo, ficheros regulados por legislación especial, etc. (art. 2.2 y 3 LOPD)] y de las normas que regulan los ficheros de titularidad privada (ver art. 25 LOPD].

Todo lo más, cabría pensar que el único empleador que queda excluido de la referida Ley Orgánica es el titular del hogar fami-

* Profesores Asociados de Derecho del Trabajo y Seguridad Social. UNED.

liar, pues en ella se declara que «el régimen de protección de datos de carácter personal (tal como se establece en la LOPD) no será de aplicación a los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas» [art. 2.2 a) LOPD], aunque, sin duda, pueden idearse argumentos que también acaben con esta, a nuestro juicio, justificadísima excepción.

Por lo dicho, claro está que el examen de la nueva Ley Orgánica requiere que le dediquemos las páginas de esta Presentación, aunque ya advierto que con ella no pretendo –sería ilusorio– agotar un tema que califico de excesivamente complejo, complejidad que se deriva de dos motivos diferentes: a) la dificultad de interpretar lo dispuesto en la LOPD y b) la falta de concordancia entre la citada Ley y algunas leyes laborales, concretamente el Estatuto de los Trabajadores (ET), la Ley Orgánica de Libertad Sindical (LOLS) y la Ley de Prevención de Riesgos Laborales (LPRL).

2. Por «fichero» se entiende, en sentido muy amplio, «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) LOPD] y como «datos de carácter personal» se califica a «cualquier información concerniente a personas físicas identificadas o identificables» [art. 3,a) LOPD].

Las empresas, para poder garantizar una mínima organización del factor trabajo y con el fin de reconocer a los trabajadores sus derechos, es obvio que tienen que abrir «ficheros» y recoger «datos de carácter personal» de sus trabajadores, pues con base en ellos podrán conocer y oponerse al absentismo injustificado (arts. 20.4 y 52 ET), proceder a los descuentos de los salarios por huelga (art. 6.2 RDLRT de 1977), deberán reconocer el derecho de los afiliados a un sindicato a constituir secciones sindicales (art. 8.1 LOLS) o, por poner un último ejemplo, tendrán que realizar la correspondiente resta en las nóminas de determinados trabajadores en cumplimiento de la cláusula de descuento de la cuota sindical (art. 11.2 LOLS).

Los «ficheros» pueden constar en cualquier «soporte», pues el carácter de tales no se desvirtúa por el medio en que constan, y la recopilación de los «datos» es posible llevarla a cabo acudiendo a

cualquier vía lícita en Derecho, desde la consulta de archivos públicos hasta la solicitud al interesado, bien sea verbal o a través de escritos.

Sin embargo, una duda que se puede plantear en este punto es si todo «dato personal» que obre en poder de la empresa exige su almacenamiento en un «fichero» y el seguimiento de los trámites previstos en la LOPD (comunicación a la Agencia de Protección de Datos, etc.). Por ejemplo, si la empresa tiene conocimiento del incumplimiento laboral de uno de sus trabajadores, y toma nota de ello, ¿tal actividad de «archivo» es la un fichero de la LOPD? Pensamos que no, porque la propia palabra «fichero» demanda la existencia de un instrumento organizado –ésta es la palabra que emplea la propia Ley– de almacenamiento de datos, circunstancia que no concurre en el caso señalado.

3. La elaboración de un «fichero» está sometida a varios requisitos, pero, ante todo, aparece condicionada por el principio de proporcionalidad, que utiliza con frecuencia el Tribunal Constitucional, y, según el cual, los derechos fundamentales, como el derecho a la intimidad que se vincula al tema aquí tratado, sólo podrán ser limitados por medios «idóneos», cuando sea «indispensable» y con respeto del conjunto del estatuto jurídico de ciudadanía que la Constitución reconoce a todas las personas.

De acuerdo con lo dicho, en la LOPD (art. 4.1), se establece que «los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido».

Del párrafo transcrito se derivan consecuencias importantes, pues es la vía para determinar cuáles son los datos personales que es posible almacenar –sólo los «adecuados y pertinentes», para el cumplimiento de las leyes laborales en nuestro caso, se entiende– en qué medida se pueden almacenar –cuando no sean «excesivos»– e incluso durante cuánto tiempo es factible mantenerlos almacenados: no olvidemos, con respecto a este último punto, que los datos personales sólo son tratables mientras sean útiles para cumplir con la normativa vigente [lo que puede exigir en bastantes supuestos que se

conserven algunos –como el estado civil o formación– incluso después de extinguida la relación laboral que unía al trabajador con la empresa, y mientras puedan serle exigidas a ésta responsabilidades laborales, de Seguridad Social o fiscales, etc. (ver, también, art. 15.5 LOPD)].

Tales datos, además, están sometidos al fin para el que fueron recogidos (art. 4.2 LOPD), y deberán ser permanentemente actualizados, lo que significa que, todo aquello que haya quedado obsoleto o sea innecesario tiene que ser cancelado de manera inmediata, para evitar sanciones administrativas y la condena al abono de indemnizaciones a los perjudicados por la desidia del responsable del fichero (ver art. 4.3.4 y 5 LOPD).

Es interesante que paremos por un momento en el precepto que declara: «los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados» (art. 4.5 LOPD), pues su lectura puede hacer pensar en la necesidad de «borrar» de los ficheros aquellas infracciones laborales claramente prescritas –aunque en este punto la existencia de la falta continuada pueda hacer algo dificultoso el cumplimiento de la Ley–.

4. Como antes dijimos, la elaboración de un «fichero» está sometida al principio de proporcionalidad y, además, a algunos requisitos, que se refieren: a) a los datos almacenables, b) al procedimiento a seguir para almacenarlos y c) a los derechos de información de los sujetos cuyos datos personales aparezcan almacenados.

Por lo que a nosotros interesa, parece lógico pensar que son siempre datos «almacenables» los que se refieren al trabajador y a la relación laboral de la que es parte.

Entre los primeros, encontramos el nombre, DNI, domicilio, etc., o sea, todos los precisos para la identificación del empleado y su localización, e incluso el estado civil, cuando el empresario se vea en la necesidad de cumplir ciertas obligaciones laborales (pago de complementos por hijos a cargo o por existencia de cónyuge).

Por cierto, que aunque el ET [art. 8.3 a)] establece que algunos de estos datos (DNI, domicilio) no son comunicables a los represen-

tantes de los trabajadores que, como sabemos, tienen derecho a recibir copia básica de todos los contratos de trabajo que deban celebrarse por escrito, tal prohibición se agota en su ámbito específico, y no afecta, como es lógico, al empleador, que tiene necesariamente que saber dónde encontrar al trabajador (por eso necesita saber su dirección) o rellenar determinados formularios oficiales en su favor (por eso necesita saber el DNI).

Además de los datos estrictamente personales del trabajador, son almacenables los datos personales cuyo necesario conocimiento por el empresario se derive de la índole del contrato formalizado: por ejemplo, si se concierta un contrato en prácticas, es obvio que el empleador debe conocer la titulación que ostenta el trabajador y dejar constancia de ella en sus archivos mientras dura la relación laboral e, incluso, después de extinguida, en tanto puedan exigírsele responsabilidades por su concertación.

En general, los datos anteriormente referidos (sin duda los que se refieren a su identificación) cabe almacenarlos sin obtener el consentimiento del interesado, porque así se deduce de lo dispuesto en la LOPD (art. 6.1.2 y 4), en la cual se inserta la regla del consentimiento, pero se admite su excepción cuando los datos de carácter personal «se refieran a las partes de un contrato o precontrato de una relación... laboral... y sean necesarios para su mantenimiento o cumplimiento», aunque el empleado podrá oponerse a su tratamiento por muy tasadas razones: «cuando existan motivos fundados y legítimos relativos a una concreta situación personal».

5. Los datos relativos a la salud de los trabajadores pueden almacenarse, por supuesto (aunque luego nos referiremos a la STCONS 202/1999, de 8 de noviembre, que precisa el modo de hacerlo), pero la LOPD establece al respecto alguna precisión interesante.

Por lo pronto, «los datos de carácter personal que hagan referencia... a la salud... sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente» (art. 7,3 LOPD). Además, «las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos de acuerdo con

lo dispuesto en la legislación estatal o autonómica sobre sanidad» (art. 8 LOPD).

Es importante recalar en el primero de los preceptos transcritos, porque tiene trascendencia laboral: según lo en él dispuesto, es factible almacenar los datos relativos a la salud de los trabajadores siempre que tal almacenamiento se justifique como cumplimiento estricto de lo dispuesto en la normativa sobre prevención de riesgos laborales.

En este punto, debemos recordar lo dispuesto en los arts. 22 y 23 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, que llevan por título, respectivamente, «vigilancia de la salud» y «documentación», y cuyos textos pueden plantear problemas si no se interpretan debidamente.

El primero de los preceptos referidos ordena al empresario garantizar a los trabajadores a su servicio la vigilancia periódica de su estado de salud (incluso, en determinados supuestos, una vez extinguida la relación laboral), pero sólo –naturalmente– «en función de los riesgos inherentes al trabajo» (que realicen, se entiende), aunque tal vigilancia queda condicionada por el consentimiento del interesado.

No obstante, el consentimiento no será necesario en varios casos: a) en aquellos en los que «la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores», o b) «para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa» y c) «cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad». Es importante advertir que en los supuestos a) y b) anteriores la vigilancia médica del trabajador sin su consentimiento se podrá llevar a cabo «previo informe de los representantes de los trabajadores».

Ordena la Ley que la práctica de los reconocimientos se ajuste al principio de proporcionalidad y a las exigencias de los derechos a la intimidad y a la dignidad de los trabajadores. La referencia a la intimidad significa –entre otras cosas– que el acceso a la información

médica de carácter personal se limite al personal médico y a las autoridades sanitarias a los que se encomiende la vigilancia de la salud.

El empresario, en este punto, no tiene derecho a acceder, sin consentimiento del trabajador, a «la información médica de carácter personal», pero sí a conocer «las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que pueda desarrollar correctamente sus funciones en materia preventiva».

Todos los datos que se extraigan del cumplimiento del deber empresarial de garantía de la salud, deben ser almacenados en «ficheros» de empresa, y su mantenimiento en ellos se condiciona a su utilidad –según ley– y, consecuentemente, a su periódica actualización. De acuerdo con el segundo de los preceptos que antes citaba, el art. 23 de la LPRL, el empresario debe elaborar y conservar a disposición de la autoridad la documentación por la que acredite que cumple con el deber de control de la salud de los trabajadores –a la que tiene acceso, como antes vimos, el personal médico y las autoridades sanitarias, y el empleador previo consentimiento del trabajador– y las «conclusiones que se deriven de los reconocimientos médicos» practicados, en los términos anteriormente referidos, que el empleador sin más trámite puede conocer.

En fin, es importante advertir que el citado art. 23 de la LPRL establece que el deber empresarial de elaborar y conservar a disposición de la autoridad laboral cierta documentación sobre la salud de los trabajadores se extiende a las «enfermedades profesionales que hayan causado al trabajador una incapacidad laboral superior a un día de trabajo».

Como puede comprobarse, el cumplimiento de lo previsto en la LPRL demanda al empresario realizar un acopio documental que, en ciertos casos, dependiendo de la índole de la actividad empresarial, puede resultar ingente, y para cuya «organización» será de todo punto necesaria su acumulación en «ficheros». No obstante, hay que tener en cuenta que, de acuerdo con la LPRL, el empleador no ve garantizado su libre acceso a la totalidad de los «ficheros» referidos, aunque sea responsable del mantenimiento de todos ellos.

6. La LOPD se refiere a los datos personales sobre ideología, religión o creencias en general y, en particular, al dato de la «afiliación sindical», que puede ser encuadrado en el primero de los géneros mencionados. En concreto, se establece: a) que «sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la... afiliación sindical...» (art. 7,2 LOPD) y b) que «quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la... afiliación sindical...» (art. 7.4 LOPD).

Hay que concluir, entonces, que la acumulación de datos referentes a la afiliación sindical de los trabajadores presentes o pasados sin un fin legítimo y sin proceder a su periódica actualización no está permitida por el ordenamiento español. Distinta es la acumulación de esos datos con un fin concreto y legítimo, como puede ser, se nos ocurre, volviendo a ejemplos citados antes, para facilitar los derechos sindicales de las personas o para proceder al descuento, por el empresario, de las cuotas sindicales con el fin de remitirlas a las asociaciones obreras.

No obstante, en este último caso, es siempre necesario que el trabajador preste su consentimiento de forma expresa y por escrito, y aquí, al contrario de lo que sucede en casos vistos anteriormente, no caben excepciones, lo que es lógico dado que del desconocimiento de estos datos por el empresario no tendría que derivarse inicialmente grave perjuicio para la empresa o los ciudadanos, aunque sí pudiera originársele este perjuicio al trabajador [pensemos, por poner un ejemplo, en el derecho de audiencia que tienen los delegados sindicales de los afiliados a los sindicatos en el supuesto de que éstos sean despedidos (art. 10.3.3.° LOLS)].

7. No nos resistimos, para terminar esta breve aproximación a los potenciales contenidos de los «ficheros» de empresa, a hacer una breve reflexión sobre la norma que dispone: «los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras» (art. 7.5 LOPD).

Como decimos, no nos resistimos a reflexionar sobre esta norma poniéndola en relación con el precepto del ET [art. 45,1,g)] que con-

templa entre las causas de suspensión del contrato de trabajo la «privación de libertad del trabajador, mientras no exista sentencia condenatoria», ya que este precepto parece que obliga al empresario –bien es verdad que en casos aisladísimos– a hacer acopio de documentos relativos a la comisión de infracciones penales de sus empleados, con el fin de cumplir con los derechos que le otorga la norma laboral y respetar los deberes que la misma le impone. Quizá, en este punto, hubiera sido precisa una coordinación mayor entre la LOPD y el ET, o quizá habría que entender derogada, en este punto, la Ley laboral, aunque de ello pudieran, tal vez, derivarse perjudiciales consecuencias para los trabajadores.s.

8. Como ya anunciabamos, la elaboración de ficheros por las empresas está sometida a requisitos que se relacionan con los datos personales almacenables (tema éste que acabamos de estudiar) y la forma de hacerlo y con el derecho de información de los afectados por ese almacenamiento, tema en el que vamos a profundizar ahora.

La Ley que examinanos contempla en buen número de preceptos el derecho de los afectados a examinar los datos relacionados con ellos que figuren en los «ficheros», lo que prueba que, como es lógico, el derecho de información en el caso que nos ocupa forma parte de la garantía del derecho a la intimidad. El TCONS ha recordado que «la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona» (STCONS 202/1999, de 8 de noviembre).

Según la Ley, «los interesados a los que se soliciten datos personales», además de ser informados sobre la existencia de «ficheros» y de su finalidad, de quiénes sean sus responsables, del carácter obligatorio o facultativo de las respuestas que puedan dar cuando se les requieran los datos, además de ostentar tales derechos, tienen como muy específicos el de acceder a aquéllos, y el de pedir la rectificación o cancelación de lo que en ellos obre (art. 5.1 LOPD).

Concretamente, se ha dispuesto que «el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos» (art. 15.1 LOPD), aunque tal derecho está sometido a un

límite temporal, pues sólo puede ser ejercitado «a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes» (art. 15,3 LOPD).

Más comprometido es pronunciarse sobre el tema espinoso de si el mismo derecho de acceso que tienen los trabajadores, individualmente considerados, de acceder a los «ficheros» del empresario sobre datos personales, tiene una «dimensión colectiva», que favorece a los representantes de tales trabajadores. Ya adelantamos que es difícil hablar, en este punto, de una «nueva» competencia de los comités de empresa, delegados de personal y delegados sindicales.

La Ley que examinamos dispone inicialmente que «los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero (distinto del afectado) para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado» (art. 11.1 LOPD).

En conformidad con dicho precepto, los representantes de los trabajadores tendrán derecho a acceder a los datos de carácter personal que obren en un fichero cuando se cumplan dos condiciones: a) en primer lugar, que sus representados les autoricen a ello (en cualquier modo válido en derecho: es obvio que un formalismo excesivo no puede utilizarse en contra de las manifestaciones laborales colectivas) y b) en segundo lugar –y es muy importante– cuando mediante la cesión se trate de cumplir con un fin relacionado con «funciones legítimas del cedente y del cesionario», lo que significa, por lo que aquí interesa, con funciones legítimas de los representantes de los trabajadores que, no lo olvidemos, tienen entre sus competencias ejercer acciones administrativas y judiciales (art. 65.1 ET) y vigilar el cumplimiento de las normas laborales por el empresario (art. 64.1.9.° ET), «normas laborales» entre las que hay que incluir –por la trascendencia que en nuestro ámbito tiene– la LOPD.

No obstante, a lo anterior se añade que la cesión de datos de carácter personal sin consentimiento del interesado es posible en determinados supuestos; por lo que en esta presentación interesa, en los siguientes: a) cuando la cesión está autorizada en una ley y b) «cuando el tratamiento responda a la libre y legítima aceptación de

una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente concesión de dicho tratamiento con ficheros de terceros», y en este caso «la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique» (art. 11.2 LOPD).

Creemos que la aplicación de la segunda de las anteriores excepciones al tema que ahora nos ocupa no es acertada, dado que no parece que del hecho de concertar un contrato de trabajo se derive la necesidad de trasmitir datos personales de los trabajadores a sus representantes, con el fin de hacer posible su desarrollo, cumplimiento y control. De hecho, la opinión contraria encontraría obstáculos importantes para imponerse, como el ya citado art. 8.3 ET, en el que se configura el deber de remitir a los representantes de los trabajadores todos los contratos de trabajo que deban celebrarse por escrito, pero tachando en ella el DNI, el domicilio, el estado civil del trabajador, y cualquier otro dato «que, de acuerdo con la Ley Orgánica 1/1982, de 5 de mayo, pudiera afectar a la intimidad personal».

En resolución, sólo podría sostenerse que los representantes de los trabajadores tienen derecho a acceder a los datos personales de sus representados sin consentimiento de ellos cuando así lo disponga la ley y, en particular, la Ley laboral, lo que significa encontrarse con un problema grave, pues la ley laboral, anterior a la LOPD y muy ajena a la problemática que ésta plantea, dada la fecha de que datan los preceptos que dedica a las competencias de los comités y delegados de personal, más complica que aclara el problema.

En fin, aunque el ET admite entre las citadas competencias las de «ser informado de todas las sanciones impuestas por faltas muy graves» (art. 64.1.7.º) y «conocer, trimestralmente al menos, las estadísticas sobre el índice de absentismo y sus causas, los accidentes y enfermedades profesionales y sus consecuencias, los índices de siniestralidad... y los mecanismos de prevención que se utilizan» (art. 64.1.8.º), en fin, aunque el ET contiene tales previsiones, la existencia en la LOPD (art. 43 y ss) de una batería de sanciones laborales tendentes a garantizar el secreto de los «ficheros» obliga a la prudencia, y más aún cuando del ET lo que más bien se deduce es que el derecho de información de los representantes se refiere a aspectos laborales colectivos (estadísticas de absentismo y enfermedades, por ejemplo) que a «datos personales de los trabajadores».

Únicamente la LPRL (art. 36) contempla entre las facultades de los delegados de prevención –sólo entre las facultades de estos representantes laborales– la de «tener acceso, con las limitaciones previstas en el apartado 4 del art. 22 de esta Ley, a la información y documentación relativa a las condiciones de trabajo que sean necesarias para el ejercicio de sus funciones y, en particular, a la prevista en los arts. 18 y 23 de esta Ley», a lo cual se añade que «cuando la información esté sujeta a las limitaciones reseñadas, sólo podrá ser suministrada de manera que se garantice el respeto de la confidencialidad».

De ello se deduce que los delegados de prevención no pueden acceder, sin consentimiento de los interesados, a la información médica de carácter personal de los trabajadores, aunque sí tienen derecho a conocer, en igualdad con el empresario, las «conclusiones» que se deriven de los reconocimientos médicos efectuados a aquéllos en relación con la aptitud para el desempeño de sus actividades, y en particular la documentación en que tales «conclusiones» obren, así como la documentación sobre accidentes y enfermedades profesionales que hayan causado al trabajador que los padeció una incapacidad laboral superior a un día de trabajo y, en general, cualquier otra que sea necesaria para facilitar la actuación de sus competencias en materia de garantía de la salud laboral.

LA SENTENCIA DEL TRIBUNAL CONSTITUCIONAL 202/1999, DE 8 DE NOVIEMBRE

9. La sentencia referida, por medio de la que se ordena la destrucción de determinados datos de un «fichero» del antiguo Banco Hispanoamericano, ha causado cierta alarma en medios empresariales, pero ya adelantamos que ello es debido más a su lectura apresurada que a su trascendencia real.

Para aclarar algo las cosas, comencemos por ofrecer un relato sintético de los hechos que provocaron el conflicto:

a) el Banco Hispanoamericano S.A. tenía una base de datos que se denominaba «absentismo con baja médica»; b) en tal base figuraban los partes de baja de los trabajadores en los cuales se

consignaban las fechas de alta y baja laboral, el motivo de la baja (enfermedad común o accidente laboral), los días durante los cuales se prolongó la incapacidad temporal y el diagnóstico médico; c) tales partes de baja se retrotraían bastante en el tiempo (los había, por ejemplo, de 1988); d) para almacenarlos, nunca se solicitó el consentimiento de los trabajadores (ni individual ni colectivamente); e) en el «fichero», por el contrario, no figuraban los historiales clínico-sanitarios de los empleados, esto es, «las reseñas circunstanciadas de los datos y antecedentes relativos a la salud de los afectados»; f) la base de datos no estaba dada de alta en la Agencia de Protección de Datos; g) a ella podían acceder cuatro médicos y un empleado de la empresa (ver Antecedentes de Hecho y Fundamentos de Derecho 1 y 4).

Como se deduce de los hechos relatados, la «base de datos» referida no estaba actualizada ni cuidadosamente custodiada, y, aunque su verdadero fin (relacionado con el control del absentismo) era lícito, el «medio» que se utilizaba para cumplirlo (acumular todo tipo de datos sobre las patologías padecidas por los trabajadores, sin límite temporal alguno) tal vez no se ajustaba a todos los requerimientos del principio de proporcionalidad. El comité de empresa de la entidad, entonces, tenía el camino allanado para plantear demanda por vulneración de derechos fundamentales.

Hay que pensar, tras la lectura de los antecedentes de hecho de la sentencia que comento, que la defensa que el Banco hizo del fichero, alegando que, en realidad, tenía por fin garantizar la salud de los trabajadores y se justificaba con base en normas de cita no excesivamente acertada (arts. 10,11 y 61 de la Ley 14/1986, de 25 de abril, General de Sanidad; arts. 22 y 23 de la LPRL...), quizá enconó más el debate sobre la licitud del archivo, y empujó al TCONS a elaborar un pronunciamiento que entiendo excesivo.

10. El TCONS, en efecto, ha declarado (Fundamentos de Derecho 4 y 5 de la sentencia comentada):

«... el fichero automatizado de que trae causa el presente proceso constitucional no es un compendio de historiales clínico-sanitarios, esto es, de reseñas circunstanciadas de los datos y antecedentes relativos a la salud de los afectados, sino, sencillamente, una relación de partes de baja... En ellos se consignan las correspondientes fechas de

baja y alta laboral, el motivo de la baja..., los días durante los que se prolongó la situación de incapacidad temporal y el diagnóstico médico.

«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... Consecuentemente, la creación y actualización del fichero... no puede ampararse... en la existencia de un interés general... ni tampoco en lo dispuesto en los arts. 22 y 23 de la LPRL, 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».

«... mediante la creación de la base de datos ahora discutida 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 éstos. 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 solución de consideración idónea, necesaria y proporcionada para la consecución del fin, en este caso, el control del absentismo laboral..., pues no se trata de medida de suyo 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...»

«Consiguientemente, debemos concluir que el tratamiento y conservación del diagnóstico médico en la mencionada base de datos, sin mediar consentimiento expreso del afectado, incumple la garantía que para la protección de los derechos fundamentales se contiene en el art. 53 de la Constitución Española».

En coherencia con tales argumentos, la STCONS declara «que la existencia de diagnósticos médicos en la base de datos 'Absentismo con baja médica', cuya titularidad corresponde al Banco Central Hispano (en la actualidad), vulnera el derecho... a la intimidad (art. 18.1 y 4 CE)».

11. Es importante advertir que, aunque el TCONS en su sentencia parece criticar el almacenamiento de datos para controlar el absentismo laboral, en realidad no sucede tal, porque el control del absentismo es uno de los derechos-deberes del empresario, como se deduce de lo dispuesto en los arts. 20.4 y 52 del ET, que se refieren al control de las ausencias del trabajador por enfermedad y al despido por absentismo. Además, hay que tener presente que el último de los preceptos mencionados no sólo franquea al empleador el control del absentismo individual, sino también el del absentismo colectivo, ya que el despido mencionado será procedente si las ausencias de la plantilla del centro de trabajo superan el cinco por ciento en determinados lapsos temporales.

La sentencia, en realidad, lo que declara contrario a Derecho y, en particular, contrario al derecho a la intimidad, es el almacenamiento en un fichero de los «diagnósticos médicos» de los trabajadores, y aquí reside la clave para entender correctamente su doctrina. De ella hay que deducir que no es ilícito controlar las ausencias por enfermedad (como cualquier lector de lo dispuesto en el art. 52 del ET deducirá sin mayor problema), sino que lo ilícito es incorporar al fichero los diagnósticos de que fueron objeto los trabajadores, más aún cuando no se adivina ninguna finalidad «legal» para proceder a tal almacenamiento de datos. En este caso, la restricción del derecho a la intimidad no se justifica, y ya no sólo porque sea una restricción inadecuada e innecesaria y contraria a los derechos fundamentales, sino porque con ella pueden llegarse a causar perjuicios antijurídicos a los ciudadanos.