Procedimiento nº.: E/02649/2009

ASUNTO: Recurso de Reposición Nº RR/00082/2010

Examinado el recurso de reposición interpuesto por la entidad Dª. A.A.A. contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de investigación, E/02649/2009, y en base a los siguientes:

HECHOS

PRIMERO: Con fecha 17 de diciembre de 2009 se dictó resolución por el Director de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de investigación, E/02649/2009, procediéndose al archivo de actuaciones en aplicación del principio de presunción de inocencia.

Dicha resolución, que fue notificada al recurrente en fecha 4 de enero de 2010, según aviso de recibo que figura en el expediente.

SEGUNDO: Dª. A.A.A. (en lo sucesivo la recurrente) ha presentado en fecha 3 de febrero de 2010 en esta Agencia Española de Protección de Datos, recurso de reposición fundamentándolo, básicamente, en que el colegio de abogados denunciado *"difunde mediante Circular a todos los Colegiados de Alava, datos de salud y datos económicos referidos a mi persona"*, dado que la historia clínica no podía ser tratada en un procedimiento judicial distinto a aquél para la que fue obtenida, estando obligados a cancelar los datos personales.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en lo sucesivo LRJPAC).

II

En relación con las manifestaciones efectuadas por la recurrente, debe señalarse que ya fueron analizadas y desestimadas en los Fundamentos de Derecho II a V de la Resolución recurrida de archivo de actuaciones de 17 de diciembre de 2009; y se advertía suficientemente sobre la doctrina mantenida por la Audiencia Nacional en relación con las reglas que rigen en materia probatoria. En dichos Fundamentos de Derecho se indica lo siguiente:

<<II

El artículo 6 de la LOPD, apartados 1 y 2, dispone lo siguiente:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

El tratamiento de datos sin consentimiento de los afectados constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia NÚM. 292/2000, de 30 de noviembre, "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)."

Son elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos.

Por su parte, de igual modo, el artículo 11 de la LOPD, apartados 1 y 2, establece que:

"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una Ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de

Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica".

III

Así, en la propia LOPD existe una mención concreta a la posibilidad del tratamiento de datos sin consentimiento del titular de los mismos, dentro del ámbito de la tutela judicial efectiva que el artículo 24 de nuestra Constitución consagra, ya que en su punto 2 establece:

"2. Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa,(…)".

La ley 1/2000 de 7 de Enero, de Enjuiciamiento Civil (en adelante LEC) en este sentido viene a establecer en su artículo 265.1:

"A toda demanda o contestación habrán de acompañarse: Los documentos en que las partes funden su derecho a la tutela judicial que pretenden."

De la lectura de los preceptos legales anteriormente indicados, se entiende que la realización de un tratamiento de datos sin consentimiento de sus titulares dentro del marco de un procedimiento jurisdiccional, da lugar a un conflicto entre el derecho a la protección de datos de carácter personal, y el derecho a la tutela judicial efectiva de los jueces y tribunales del artículo 24 de la Constitución. En este sentido el legislador, a partir de las menciones que la propia constitución, la ley de enjuiciamiento civil y la LOPD en su artículo 11.2. realizan al respecto, ha creado un sistema en el que cede el derecho a la protección de datos en favor de la defensa del derecho constitucional de tutela judicial efectiva y a la propia defensa, dado que la exigibilidad del consentimiento del oponente en un procedimiento judicial, para el tratamiento de sus datos, podría dar lugar a una merma en la posibilidad de la contraparte de aportación de elementos que permitan la identificación del mismo, así como en la utilización de "los medios de prueba pertinentes para su defensa", vulnerándose las garantías derivadas del citado derecho a la tutela judicial efectiva y coartándose el derecho a obtener el pleno desenvolvimiento de este derecho.

En este caso, y de acuerdo con las actuaciones de investigación realizadas por la Inspección de Datos de esta Agencia, ha quedado acreditado que Dª. A.A.A. manifestó que los documentos fueron aportados por el citado Colegio en el juicio de despido, sin su autorización y sin la del juez que resolvió el despido, al no haber sido solicitada como prueba, y que el Colegio de Abogados de Álava era parte demandada en este procedimiento de determinación de contingencia n° 897/2008 seguido ante el Juzgado de lo Social n° 3. Este proceso fue promovido por la denunciante figurando como partes demandadas el Instituto Nacional de la Seguridad Social, la Tesorería General de la Seguridad Social, ASEPEYO, Mutua Patronal de Accidentes de Trabajo y el propio Colegio de Abogados de Álava.

También recordar que el historial médico fue aportado por OSAKIDETZA al proceso a petición de la codemandada Asepeyo como consecuencia del requerimiento efectuado por el Juzgado Social N° 3. Asimismo, en la demanda por Despido 766/2008 dirigida contra el Colegio de Abogados de Álava por la trabajadora (la denunciante) se solicitaba la nulidad del despido, invocando la existencia de un acoso moral en el trabajo (mobbing). Subsidiariamente se solicitaba que se declarase improcedente el despido. En dicha demanda, la trabajadora alegaba que había venido sufriendo una persecución contra su persona por parte del Colegio de Abogados.

IV

En otro orden de cosas, de igual modo, en el presente caso, y de acuerdo con las citadas actuaciones de investigación realizadas por la Inspección de Datos de esta Agencia, ha quedado acreditado que Dª. A.A.A. manifestó que los destinatarios de la citada circular fueron todos los colegiados – abogados ejercientes y no ejercientes – superando la cifra de 500 colegiados. Asimismo, no le constaba que los documentos clínicos que aportaba con su denuncia llegaran a ser distribuidos junto con la citada circular o colgados en la extranet del Ilustre Colegio.

La circular 11/08 fue enviada por correo electrónico, a través del sistema DSI (Difusión Selectiva de Información) exclusivamente a los colegiados tanto ejercientes como no ejercientes del Ilustre Colegio de Abogados de Álava, y junto con el mensaje sólo se adjuntó la circular, donde no aparecen datos personales excesivos. Sin embargo, los documentos clínicos no se incluyeron para su distribución con la circular 11/08 ni fueron colgados en el árbol documental. Además en el texto del mensaje se indicaba a los colegiados que podían consultar la sentencia en cuestión accediendo a la extranet con firma digital y consultando en el árbol documental.

El artículo 10 de la LOPD dispone que: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

El deber de secreto tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así, el Tribunal Superior de Justicia de Madrid declaró en su sentencia de 19 de julio de 2001: "El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".

En este sentido, la Audiencia Nacional también ha señalado, entre otras, en sentencias de fechas 14 de septiembre de 2001 y 29 de septiembre de 2004 lo siguiente: "Este deber de sigilo resulta esencial en las sociedades actuales cada vez mas complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE.

En efecto, este precepto contiene un <<instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un

uso ilegítimo del tratamiento mecanizado de datos>> (STC 292/2000). Derecho fundamental a la protección de los datos que <<persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino>> (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, <<es decir, el poder de resguardar su vida privada de una publicidad no querida>>.

También hay tener en consideración lo alegado por el Colegio de Abogados al decir que el artículo 53 del Estatuto General de la Abogacía estable que:

"Son atribuciones de la Junta de gobierno:

o) Informar a los colegiados con prontitud de cuantas cuestiones conozca que puedan afectarles ya sean de índole corporativa, colegial, profesional o cultural.

(…)

s) recaudar, distribuir y administrar los fondos del Colegio; redactar los presupuestos, rendir las cuentas anuales y proponer a la Junta General la inversión o disposición del patrimonio colegial, si se tratare de inmuebles".

Así, el despido de un empleado afecta al colegiado, ya que el Colegio de Abogados en sí se sustenta principalmente por cuotas de colegiados y en menor medida por subvenciones.

Y en el artículo 57 dice a su vez que:

"La Junta General ordinaria a celebrar en el primer trimestre de cada año tendrá el siguiente orden del día:

2º Examen y votación de la cuenta general de gastos e ingresos del ejercicio anterior."

V

No obstante, los artículos 24.2 de la Constitución Española y 137 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, reconocen el derecho a la presunción de inocencia en el ámbito del procedimiento administrativo sancionador. Su contenido esencial implica no sólo la acreditación de los hechos ilícitos, sino también "...la prueba de la responsabilidad del sujeto en la comisión de los mismos" (sentencia del Tribunal Supremo de 2 de julio de 1990).

La presunción de inocencia debe regir, sin excepciones, en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del "ius puniendi" del Estado, en sus diversas manifestaciones, está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional, en su sentencia 76/1990 de 26 de abril de 2004, consideraba que el derecho a la presunción de inocencia comporta: "que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio."

Conforme señalaba, asimismo, el Tribunal Supremo, en su sentencia de 26 de octubre de 1998, el derecho a la presunción de inocencia "no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba

indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo."

Como conclusión de las actuaciones realizadas por parte de la Inspección de Datos y del presente procedimiento en relación a los hechos comunicados por Dª. A.A.A: y, en atención a lo expuesto, no se ha podido acreditar que los datos que dan soporte a la información difundida fuesen excesivos.

Ello frente a la certeza y concreción exigida en estos supuestos para poder calificar la conducta como sancionable, debe concluirse que no existe prueba de cargo suficiente, por lo que procede acordar en archivo del presente expediente.

En todo caso, si se considera lesionado el derecho al honor o a la intimidad personal, la persona afectada podrá acudir a los tribunales de la jurisdicción ordinaria de orden civil, al amparo de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, dado que la Agencia Española de Protección de Datos no es el órgano competente para dirimir estas cuestiones, que deben ser resueltas en sede jurisdiccional.

En consecuencia, no se aprecia infracción de la normativa de protección de datos personales por parte de la entidad investigada, por lo que procede el archivo de las presentes actuaciones>>.

III

En consecuencia, en el presente recurso de reposición, la recurrente no ha aportado nuevos hechos o argumentos jurídicos, aparte de lo ya expuesto, que permitan reconsiderar la validez de la Resolución impugnada.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por **Dª. A.A.A.** contra la Resolución de esta Agencia Española de Protección de Datos dictada con fecha 17 de diciembre de 2009, en el expediente de actuaciones previas de investigación E/02649/2009.

SEGUNDO: NOTIFICAR la presente Resolución a **Dª. A.A.A.**.

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus

Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa, se podrá interponer en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto según lo previsto en el artículo 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta del referido texto legal.

Madrid, 25 de febrero de 2010
EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte