Expediente Nº: E/05930/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad ABIL UROLOGÍA, S.L.P., Don ***A.A.A.,*** y el HOSPITAL MONCLOA, S.A., en virtud de denuncia presentada por Don ***B.B.B.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 27 de agosto de 2015, tuvo entrada en esta Agencia un escrito remitido por Don ***B.B.B.,*** en el que denuncia

1 El Dr. ***A.A.A.*** presta sus servicios por la mañana en el Hospital de la Paz y algunas tardes en el Hospital Moncloa.

2 El denunciante, tras realizar varias visitas en consultas externas del Hospital Moncloa al Dr. ***A.A.A.***, es ingresado e intervenido, el 29 de octubre de 2014, en el Hospital Moncloa.

3 La intervención es iniciada por un doctor que desconoce y que posteriormente es identificado como el Dr. ***C.C.C.***. Surgen problemas durante la operación que es finalizada por la Dra. ***D.D.D.***.

4 En el momento de la intervención el Dr. ***C.C.C.*** era residente de 5º año del Hospital de la Paz, quien en base a dicha condición de residente tenía dedicación exclusiva y no podía colaborar en dichas tareas.

5 El denunciante entiende que el acceso del Dr. ***C.C.C.*** a sus datos vulnera la normativa vigente y que tanto el hospital como ABIL UROLOGIA no han garantizado debidamente la privacidad de sus datos.

El denunciante presenta los siguientes documentos junto con el escrito de denuncia:

a) Respuesta de 15 de abril de 2015 a la reclamación interpuesta por el denunciante ante el Servicio Madrileño de Salud.

b) Acuerdo de 11 de mayo de 2015 del pleno de la Junta Directiva del Ilustre Colegio de Médicos de Madrid en relación con la denuncia interpuesta por el denunciante ante el citado órgano.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Sobre las relaciones entre los intervinientes

1. El Hospital Moncloa es gestionado por HOSPITAL MONCLOA GRUPO HLA, S.A., en adelante HOMONSA.

2. ABIL UROLOGÍA SLP, es una sociedad limitada profesional constituida por dos socios, el Dr. ***A.A.A.*** y el Dr. ***E.E.E.***.

3. El 1 de marzo de 2010, ABIL UROLOGIA SLP, firmó contrato con la sociedad CLINICA MONCLOA, S.A., (anterior denominación social de HOMONSA) para contratar la prestación los servicios de un médico especialista en Urología. El contrato tiene vigencia hasta el 31 de diciembre de 2018.

   El contrato prevé en su estipulación primera que los servicios serán prestados dentro de las dependencias del hospital, en el área de urología.

   La estipulación tercera del contrato constan los compromisos asumidos por la sociedad, entre los que se encuentra "*Guardar el secreto profesional, considerándose como confidencial cuanta información reciba o se facilite en orden al cumplimiento de este contrato….*"

4. El Dr. ***C.C.C.***, residente de 5º año en el momento de la intervención quirúrgica, término su especialidad y es actualmente uno de los médicos que presta sus servicios en el HOMONSA.

   En el momento de los hechos denunciados la relación del Dr. ***C.C.C.*** no se articulaba mediante un convenio con el Hospital de La Paz o mediante contrato laboral con HOSPITAL MONCLOA.

   HOMONSA aporta copia de una autorización emitida por la entidad a la solicitud realizada por el Dr. ***A.A.A.*** para que el Dr. ***C.C.C.*** pueda acudir al centro como observador del equipo de urología y pide a dicho equipo que transmita al Dr. ***C.C.C.*** que sólo podrá actuar como observador y que deberá seguir las instrucciones directas del equipo de urología y las internas del hospital.

   ABIL UROLOGIA SLP, aporta copia de un documento firmado a nombre del Dr. ***C.C.C.*** mediante el que éste "*Se compromete expresamente a respetar el secreto médico profesional confirme obliga el código de Deontología Médica y Estatuto del Colegiado en todos los actos médicos a los que asista para completar su formación.* "

<u>Respecto de los datos del denunciante</u>

5. ABIL UROLOGIA y HOMONSA manifiestan que:

   a. La historia clínica utilizada en Hospital Moncloa es almacenada únicamente en formato electrónico en un sistema de información que gestiona una historia clínica única para el conjunto de los 15 hospitales que forman el grupo al que pertenece HOMONSA.

   b. ABIL UROLOGIA SLP, no dispone de consulta propia fuera del Hospital Moncloa ni de sistemas de información propios sino que utiliza aquellos que HOMONSA pone a su disposición.

   La inscripción realizada en el Registro General de Protección de Datos del fichero "HISTORIAL CLINICO" se realizó cuando aún no se había establecido la forma en que ABIL UROLOGIA SLP, colaboraría con HOMONSA.

   c. Cuando un paciente pide cita en el hospital por primera vez, sus datos son recogidos en el sistema de información del HOSPITAL MONCLOA y antes de pasar a la consulta, debe de pasar por el departamento de

admisiones donde sus datos personales son recogidos (filiación). En ese momento es cuando se crea la historia clínica del paciente que posteriormente podrá ser utilizada por los médicos.

d. Es práctica habitual que los médicos en formación asistan a operaciones como observadores. Durante esas operaciones a los médicos observadores no se les proporcionan datos identificativos de los pacientes ni se les da acceso a la historia clínica sino que se les informa de los datos relevantes de la intervención como pueden ser la patología del paciente, el tipo y objeto de la intervención, la técnica a utilizar y cualquier antecedente médico relevante al caso.

e. En el momento de la intervención que cita el denunciante, el Dr. ***C.C.C.*** no tenía usuario ni clave para acceder a la historia clínica de ningún paciente. Actualmente, como parte del cuadro médico del Hospital Moncloa, sí que dispone de usuario y clave propios.

6. A pesar de que el representante de ABIL UROLOGIA describe las funciones del Dr. ***C.C.C.*** en la intervención como de "observador", en el expediente 216/14 del Ilustre Colegio de Médicos de Madrid figura que el Dr. ***A.A.A.*** manifiesta que "…el D. ***C.C.C.*** (MIR 5º) comienza a preparar al paciente e inicia de forma incipiente la intervención continuando la misma hasta el final la Dra. ***D.D.D.***".

7. Se comprueba mediante acceso a los sistemas de información de HOMONSA que en éstos consta una historia clínica asociada al denunciante y que uno de los registros de dicha historia es la intervención descrita en los antecedentes.

8. HOMONSA manifiesta que el sistema de información que gestiona la historia clínica de los pacientes no se gestiona desde las instalaciones de cada hospital del grupo sino que está centralizada y debido a ello la consulta a los registros de acceso o a los datos de los usuarios autorizados en los sistemas no se pueden realizar en el momento de la inspección, sino que debe de ser solicitada por el hospital quien lo aportará lo antes posible.

   HOMONSA remite por correo electrónico el 4 de agosto de 2016 la información solicitada de la que se desprende lo siguiente:

   El alta del usuario del Dr. ***C.C.C.*** se produce el 14 de julio de 2015, fecha posterior a la intervención citada en los antecedentes.

   En el registro de accesos de la historia clínica del denunciante aparecen un total de 38 registros de accesos efectuados entre el 24 de julio y el 29 de octubre de 2014, ambas fechas incluidas.

   En el registro consta el código de usuario de Windows (que coincide con la inicial del nombre y el apellido de la persona física), el código de usuario de la aplicación de historia clínica (que coincide con el NIF de la persona física) y, a petición de los inspectores actuantes, el nombre y apellidos del usuario. Ninguno de los registro está asociado al Dr. ***C.C.C.***.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36,

ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La denuncia se concreta, en lo referido a protección de datos, en el acceso indebido por parte del Dr. Don C.C.C. a la historia clínica del denunciante.

La Ley 41/2002, de 14 de noviembre, reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, en su artículo 16 dedicado a los usos de la historia clínica, dispone:

"1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten. (…)

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso."

Por otra parte, el artículo 17 de la misma Ley, dedicado por completo a la conservación de la documentación clínica, establece en su punto primero que *"Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial" y* en su apartado 6 determina lo siguiente: *"Son de aplicación a la documentación clínica las medidas técnicas de seguridad establecidas por la legislación reguladora de la conservación de los ficheros que contienen datos de carácter personal y, en general, por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal".*

III

El artículo 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"*Seguridad de los datos:*

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El artículo 17.1 de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

IV

La LOPD traspuso al ordenamiento interno el contenido de la Directiva 95/46, y en su artículo 1 dispone que *"la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

El artículo 2.1 de la misma Ley Orgánica establece: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".*

El artículo 9 de la LOPD dispone lo siguiente:

"1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

El art. 9 de la LOPD *establece* el principio de *"seguridad de los datos"*

imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado".*

Para poder delimitar cuáles sean los accesos que la Ley pretende evitar exigiendo las pertinentes medidas de seguridad es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD.

En lo que respecta a los ficheros el art. 3.b) los define como *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

Por su parte la letra c) del mismo artículo permite considerar tratamiento de datos a las "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*."

Para completar el sistema de protección en lo que a la seguridad afecta, el art. 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".*

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

V

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en su artículo 81.1 señala que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*". Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104. El artículo 88, en su punto 3, se refiere al documento de seguridad.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma. En el caso que nos ocupa como establece el artículo 81.3.a) del Reglamento de desarrollo de la LOPD, además de las medidas de nivel básico y medio, deberán adoptarse las medidas de nivel alto a los ficheros o tratamientos de datos de carácter personal que se refieran a datos de salud.

El artículo 88, en sus puntos 3 y 4, referido al documento de seguridad,

establece lo siguiente:

"3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento."

Con relación al "Registro de accesos", el Reglamento de desarrollo de la LOPD aprobado por Real Decreto 1720/2007, en su artículo 103 establece:

"*1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.*

2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.

4. El período mínimo de conservación de los datos registrados será de dos años.

5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.

6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.

b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

Esta es la concreta medida de seguridad de las legalmente previstas que permite detectar el problema de los accesos injustificados a las historias clínicas y así poder corregir las posibles anomalías que se produzcan.

VI

En los hechos de este procedimiento, consta probado que el denunciante fue intervenido quirúrgicamente en el Hospital Moncloa y denuncia el acceso a su historia clínica por parte de un profesional que no tenía encomendada su asistencia sanitaria ni estaba ligado profesionalmente con el Centro hospitalario citado.

El denunciante ha aportado con su denuncia, documentación acreditativa de que el Dr. ***C.C.C.*** era Residente en el Hospital La Paz en el momento de la intervención y, expone, que inició la cirugía pero que la continuó la Dra. ***D.D.D.***, de lo que deduce que el médico residente había accedido indebidamente a su historia clínica.

Tras las actuaciones previas de investigación efectuadas, no se ha podido constatar el acceso del Dr. ***C.C.C.*** a la historia clínica del denunciante, ya que el Hospital Moncloa tiene las historias clínicas automatizadas y tiene incorporado el control de accesos a las mismas, habiendo verificado que no se habían producido accesos del mencionado facultativo a la historia clínica del Sr. ***B.B.B.***

Al Derecho Administrativo Sancionador, por su especialidad, le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad del principio de presunción de inocencia.

En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera 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".*

De acuerdo con este planteamiento, el artículo 130.1 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), establece que *"Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aun a título de simple inobservancia."*

Asimismo, se debe tener en cuenta, en relación con el principio de presunción de inocencia lo que establece el art. 137 de LRJPAC: *"1. Los procedimientos sancionadores respetarán la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario."*

En definitiva, la aplicación del principio de presunción de inocencia impide imputar una infracción administrativa cuando no se haya obtenido y comprobado la existencia de elementos indiciarios que permitan acreditar los hechos que motivan esta imputación, circunstancia que no se produce en el presente caso, ya que no se ha constatado que el Dr. ***C.C.C.*** hubiese accedido a la historia clínica del denunciante, de ahí que no se den las condiciones para iniciar un procedimiento sancionador por infracción de la LOPD.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

c) **PROCEDER AL ARCHIVO** de las presentes actuaciones.

d) **NOTIFICAR** la presente Resolución a ABIL UROLOGÍA, S.L.P., a Don ***A.A.A.,*** al HOSPITAL MONCLOA, S.A., y a Don ***B.B.B..***

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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido 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, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente 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 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, 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 del referido texto legal.

Mar España Martí
Directora de la Agencia Española de Protección de Datos