Expediente Nº: E/04385/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el COMPLEJO HOSPITALARIO UNIVERSITARIO DE ALBACETE (CHUA), y el SERVICIO DE SALUD DE CASTILLA-LA MANCHA (SESCAM) en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 13 de junio de 2014, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.***, en el que expone que lo siguiente:

Es médico del Complejo Hospitalario de Albacete y que con esa misma fecha, ha accedido a su lugar de trabajo, comprobando que el ordenador se encontraba abierto en la aplicación de gestión de historias clínicas MAMBRINO, y con acceso a su historia clínica, a nombre de su Jefe de Sección, Don ***B.B.B.***.

El citado doctor le manifestó en ese momento, que estaba él accediendo a su propia historia clínica con su usuario, desde la sesión que él se había dejado abierta por descuido.

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:

1. Con 7 de abril de 2015, se recibe en esta Agencia escrito del Servicio de Salud de Castilla La Mancha (Gerencia de Atención Integrada de Albacete), poniendo de manifiesto que:
    1.1. El denunciante es facultativo Especialista del Área de Oncología con plaza en la Gerencia de Atención Integrada, siendo uno de los ocho médicos de esta especialidad.
    1.2. Como consecuencia de un Informe emitido por el Jefe de Sección de Oncología (denunciado), durante el primer trimestre del año 2012, se pusieron de manifiesto graves irregularidades llevadas a cabo por el denunciante, lo que dio lugar a la apertura de un expediente disciplinario.
    1.3. Al hilo de los hechos descritos, se abre un conflicto entre varios facultativos del Servicio, básicamente entre el denunciante y el denunciado.
    1.4. Estos mismos hechos fueron denunciados ante la Gerencia de Coordinación e Inspección del SESCAM, siendo investigados en el marco del expediente 6/2014, el cual no ha concluido en la actualidad.
    1.5. Se remite el listado de accesos a la historia clínica del denunciante, durante el periodo comprendido entre el 18/06/2013 y el 20/06/2014 comprobándose que entre ellos se encuentran varios acceso a la historia clínica del denunciante

por parte del denunciado, el cual no ha sido médico del denunciante en ningún momento, aunque no figura ningún acceso del denunciado el día 13/06/2014, según manifiesta el denunciante en su escrito de denuncia, ni en días anteriores o posteriores. Desde la Gerencia de Atención Integrada no pueden justificar dichos accesos.

1.6. No obstante, remiten un carta enviada por el denunciado al Inspector de Servicios Sanitario de Albacete con fecha 26 de junio de 2014, la cual había sido enviada con fecha 13 de junio de 2014 al Gerente de Atención Integrada) en el que pone de manifiesto que:

1.6.1. Con fecha 13 de junio de 2014, (según consta en el documento remitido al Gerente de Atención Integrada) accedió al ordenador situado en la consulta 81 de Oncología, para consultar el historial de una paciente que llamaban desde Urgencias.

1.6.2. Se ausentó de dicho consulta sin cerrar la sesión, a las 9.35 horas encontró al denunciante, en el citado ordenador, dentro de la sesión abierta, accediendo a su historia clínica.

1.6.3. Inmediatamente avisó a otra doctora para que estuviera presente en los hechos ocurridos, así como la auxiliar de la consulta, las cuales suscribieron un documento, que se adjunta, dando fe de lo ocurrido.

TERCERO: Con fecha de 15 de diciembre de 2014, tuvo entrada en esta Agencia un nuevo escrito remitido por Don ***A.A.A.*** en el que declara que es paciente del Complejo Hospitalario Universitario de Albacete donde es atendido por el servicio de Oncología Médica, entre otros con NHC ***D.D.D.***. La única persona del servicio autorizada para acceder a sus datos de salud es la Dra. ***C.C.C.***; sin embargo, tres facultativos de ese servicio sin autorización para acceder a su historia clínica, han accedido de forma indebida. Esta información consta en el documento "rastrero de acceso NHC ***D.D.D.***" que forma parte del sumario del procedimiento abreviado contencioso administrativo *****/2014 del que adjunta copia.

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

Con fecha 11/3/2015 se solicita información al Complejo Hospitalario Universitario de Albacete en relación a que acrediten documentalmente los accesos realizados adjuntando copia de la documentación aportada por el Complejo en el procedimiento abreviado contencioso administrativo *****/2014. De la respuesta facilitada se desprende lo siguiente:

1. El denunciante es Facultativo Especialista de Área en Oncología con plaza en la Gerencia de Atención Integrada de Albacete, siendo uno de los ocho médicos de esta especialidad que componen la plantilla orgánica. Dicho médico a su vez es paciente tratado, entre otros, por el Servicio de Oncología de esa Gerencia.
2. Como consecuencia de informe emitido por el Jefe de Sección de Oncología durante el primer semestre del año 2012, se pusieron de manifiesto graves

irregularidades llevadas a cabo por el denunciante en el ejercicio de sus funciones, lo que dio lugar a la apertura de expediente disciplinario con la imposición de sanción de suspensión de empleo y sueldo durante dos años, la cual ha sido confirmada por sentencia del Juzgado de lo Contencioso-Administrativo nº 2 de Albacete. Adjunta copia de la Sentencia.

3. A raíz de los hechos descritos, en el servicio de oncología se abre un conflicto básicamente entre el denunciante y el Jefe de Sección que, en cumplimiento de sus obligaciones, desveló la actuación llevada por el denunciante y que supuso la sanción disciplinaria por falta grave. De dicho conflicto se derivan las siguientes actuaciones:

   - Incoación de expediente de mediación en conflictos denominado PERSEO, con la finalidad de que la comisión constituida medie en el conflicto y proponga una solución que fuera aceptada por las partes en conflicto. Con fecha 1/12/2014 se reúne la comisión formada al efecto y se da por finalizada su función pues a la vista de las posiciones de los contendientes, se agotan las posibilidades de mediación sin resultado.

   - Presentación de denuncia del denunciante al Jefe de Sección por supuesto acceso indebido a los datos de su historia clínica por parte del Jefe de Sección. Dicho expediente es tramitado como "información previa" en la Gerencia de Coordinación e Inspección del SESCAM, desconociendo el resultado del mismo pues al parecer no ha concluido.

4. Por su interés y la posibilidad de que fuera el propio denunciante el que acceda a su historia clínica con las claves de otros médicos para poder imputarles responsabilidad, adjuntan los siguientes documentos facilitados por los interesados:

   - Informe de 23/3/2015, suscrito por seis de los ocho facultativos del servicio de oncología indicando que las sesiones iniciadas por un facultativo pueden quedar abiertas aun no estando presente el médico en la consulta y por ello pueden ser utilizadas por otros médicos del servicio.

   - Informe 23/3/2015, del Jefe de Servicio de Informática de la GAI de Albacete, en el que expresa que los ordenadores de los servicios médicos están dotados de un sistema de bloqueo de seguridad por el que tras el transcurso de 90 minutos sin ser usado queda bloqueado y es preciso introducir de nuevo la clave de acceso, lapsus temporal más dilatado del habitual para facilitar el trabajo médico y en la medida que están instalados en las consultas médicas y solo pueden ser utilizados por el personal médico y sanitario de la propia consulta.

   - Acta de 22/5/2014, de declaración del Jefe de Sección en la que declara que no ha accedido a la historia clínica del denunciante, que las sesiones de los ordenadores se pueden quedar abiertas y que comparte su contraseña con los auxiliares de su consulta. Además, los ordenadores son compartidos. Incluso pudo haber accedido el propio denunciante a su historia utilizando la clave del Jefe de Sección.

   - Escrito de 26/6/2014 del Jefe de Sección dirigido al Inspector médico que tiene a cargo la información previa citada, poniendo de manifiesto que el día 13/6/2014 sorprendió al denunciante utilizando la sesión informática abierta por el propio Jefe de Sección.

- Escrito de 13/6/2014 del Jefe de Sección dirigido al Gerente de la GAI de Albacete haciendo alusión al mismo incidente referido en el punto anterior.
- Declaración de 19/3/2015 de las testigos presenciales del incidente referido en los puntos anteriores, manifestando la existencia del mismo. Consta que el día 13/6/2014 oyeron como el Jefe de Sección preguntaba al denunciante por la razón de que estuviera utilizando su sesión de ordenador y consultado su propia historia clínica, a lo que responde que no se había dado cuenta.

5. Finalmente manifiestan que la Gerencia, respecto de los accesos realizados por médicos oncólogos que en principio no tratan al denunciante, no puede afirmar o negar la existencia de justificación asistencial, pero si cabe afirmar que cabe la posibilidad de accesos por parte del propio denunciante desde la consulta de oncología pero con una sesión abierta por otros médicos.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director 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 planteada por el Dr. Don ***A.A.A.*** se concreta en el acceso indebido a su historia clínica por parte del Jefe de Sección de Oncología y dos compañeros más.

El artículo 6.1 de la LOPD dispone lo siguiente: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa"*.

Por su parte, el apartado 2 del mencionado artículo contiene una serie de excepciones a la regla general contenida en aquel apartado 1, estableciendo que: *"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 292/2000, de 30 de noviembre (F.J. 7 primer párrafo) *"… 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, pues, 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.

El artículo 91 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establece lo siguiente:

"1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Esto significa que cuando un usuario de un fichero accede a una información, ese acceso tiene que ser necesario para desarrollar las funciones que tiene encomendadas y que dicho acceso este justificado.

En las dos denuncias presentadas, el Dr. ***A.A.A.*** señala que tanto el Jefe de Sección como dos compañeros del Servicio han accedido a su historia clínica de forma indebida. Tras las actuaciones de investigación practicadas se ha acreditado que el denunciante ha sido sorprendido por compañeros accediendo a su historia clínica desde la sesión abierta por el Jefe de Sección. Se trata de un ordenador compartido por varios médicos y las sesiones quedan abiertas durante 90 minutos hasta que se bloquean cuando dejan de utilizarse. Este periodo tan dilatado se debe al trabajo específico que realizan los oncólogos, ya que salen del despacho para visitar al paciente hospitalizado o para acompañarle a alguna prueba. Manifiestan que forman parte de un equipo entre los que comentan los casos que trata cada uno, guardando la debida confidencialidad y nunca se había actuado con mala fe. Acompaña el SESCAM un documento en el que el Dr. ***B.B.B.*** contesta a la Inspección sobre los presuntos accesos indebidos a la historia clínica del denunciante, habiendo acreditado que en dos de las tres ocasiones ni siquiera estaba en el Centro.

En síntesis, no se ha podido acreditar que los accesos denunciados hayan sido realizados por los compañeros del Servicio de Oncología.

Se ha de tener en cuenta que 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 137.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece que "*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 hayan obtenido evidencias o indicios de los que se derive la existencia de infracción.

En resumen y para este caso, se ha de señalar que no se han obtenido indicios razonables que permitan establecer que se han producido los hechos denunciados.

III

A pesar de no ser un hecho denunciado, durante las Actuaciones de Investigación, se ha tenido acceso a un informe del Jefe de Servicio de la GAI de Albacete, en el que justifica la necesidad de que las sesiones permanezcan abiertas durante 90 minutos antes de bloquearse. Aun admitiendo que puede estar justificado por lo específico del trabajo que se realiza en Oncología, se hace preciso recordar en qué consisten las medidas de seguridad.

El artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, con la finalidad de evitar, entre otros aspectos, el acceso no autorizado por parte de ningún tercero.

Sintetizando las previsiones legales citadas puede afirmarse que:

- 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.

- 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.

- La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se establecen en normas reglamentarias, de modo que se eviten accesos no autorizados.

- 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 del artículo 9 de la LOPD tipificada como grave en el artículo 44.3.h) de la citada Ley.

El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establece de manera pormenorizada las medidas de seguridad que han de tener incorporadas en sus ficheros los responsables del tratamiento de datos personales. Los ficheros que contengan datos de salud han de tener implantadas las medidas de seguridad de nivel alto.

El artículo 103 de dicho Reglamento regula el registro de accesos en los ficheros con nivel de seguridad alto, como es el caso del que contiene historias clínicas, indicando lo siguiente:

"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."

El Hospital de Albacete tiene incorporadas tales medidas de seguridad, como se constata en la entrega al denunciante de los accesos a su historia clínica. No obstante, las medidas de seguridad es fundamental que sean conocidas por todas las personas que acceden a los ficheros. Si bien puede ser necesaria que, tras identificarse el personal sanitario con su clave y contraseña, la sesión permanezca sin bloquearse durante 90 minutos, es indispensable que se recuerde a todo el personal que al salir del despacho donde se encuentra ubicado el ordenador común bloqueen la sesión inicada, para evitar que se produzcan hechos como los denunciados en el supuesto presente.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.

2. **NOTIFICAR** la presente Resolución al COMPLEJO HOSPITALARIO UNIVERSITARIO DE ALBACETE (CHUA), al SERVICIO DE SALUD DE CASTILLA-LA MANCHA (SESCAM), y a Don ***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 (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 el Director 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos