Expediente Nº: E/03088/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad UNMEQUI UNIVERSAL MEDICO QUIRURGICA S.A., (SANATORIO VALLES)**,** en virtud de denuncia presentada por la Jefatura de Policía Local del Ayuntamiento de Alcalá de Henares (Madrid), y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 12 de abril de 2013, tuvo entrada en esta Agencia un escrito remitido por la Dirección General de Evaluación Ambiental de la Comunidad de Madrid, con el que adjuntan una denuncia de la Jefatura de Policía Local del Ayuntamiento de Alcalá de Henares (Madrid), en la que se pone de manifiesto que:

1. Con fecha 20 de octubre de 2012, dos Agentes de la citada Policía Local se personan en la (C/.....1), donde según ha denunciado un vecino de la localidad, hay residuos clínicos en un contenedor de basura orgánica.

2. Los Agentes verifican que en uno de los tres contenedores existentes hay además de residuos clínicos procedentes del SANATORIO VALLES, documentos que contienen datos de carácter personal como historiales clínicos, datos de citas y hojas de tratamiento.

Según hacen constar en el Acta, se dirigen al domicilio de la clínica situada en la (C/.....2), encontrándose cerrada ya que no abre ni sábados ni domingos.

Adjuntan varias fotografías del contenido del contenedor mencionado.

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:

1º. Dado que en las fotografías que se remiten con el Acta de la Policía Local no se aprecian documentos que contengan datos personales, con fecha 10 de julio de 2013, se solicitó a la citada Policía copia de alguno de los documentos encontrados o, en su lugar, alguna fotografía en la que se pudiera apreciar la existencia de datos personales en algún documento. En la fecha de este informe, no se ha recibido contestación a la solicitud.

2º. Con fecha 11 de noviembre de 2013, UNMEQUI UNIVERSAL MEDICO QUIRURGICA S.A. (propietaria de la CLINICA VALLES), ha remitido a esta Agencia la siguiente información en relación con los hechos puestos de manifiesto en el Acta de la Policía Local de Alcalá de Henares.

1. La Clínica Vallés pertenece a la empresa “UNMEQUI UNIVERSAL MEDICO-QUIRURGICA, S.A.”, con CIF *********.

2. Ignoran la existencia de dicha Acta, razón por la que no se pueden manifestar sobre unos supuestos documentos que, ni les han comunicado su existencia, ni, por supuesto, han visto. En cuanto a la causa por la que estarían en el contenedor, suponiendo que fueran de origen de nuestra Clínica, tendrían que manifestarse en sentido de que, bajo su punto de vista, resultaría imposible, habida cuenta las medidas de seguridad que tienen implantadas y el grado de aceptación y colaboración generalizadas de todo su personal.
3. Si los hechos fueran ciertos y existieran dichos documentos, pertenecieran a nuestra Clínica y contuvieran datos individualizadores de pacientes, solamente podría ser debido a un muy improbable error humano puntual o a un acto malicioso.
4. Aportan con su escrito la siguiente documentación:
    a. Copia del Documento de Seguridad de Mayo de 2011, vigente en la fecha de los hechos, en el que se han impreso en color rojo las partes que pueden hacer referencia directa a las medidas de seguridad implementadas con relación a los hechos que se denuncian.
    b. Copia del Documento de Seguridad de Mayo de 2013, vigente en la actualidad.
    c. Copia del Manual titulado “Funciones y Obligaciones del Personal sin acceso a datos”, entregado a todos los trabajadores cuyo puesto de trabajo no precisa el conocimiento, acceso o manejo de datos de carácter personal, de Mayo de 2011, vigente en el momento de los hechos.
    d. Copia del Manual titulado “Funciones y Obligaciones del Personal Sanitario”, entregado a todos los trabajadores del Área Sanitaria, de Mayo de 2011, vigente en el momento de los hechos.
    e. Copia del Manual titulado “Funciones y Obligaciones del Personal Administrativo”, entregado a todos los trabajadores del Área Administrativa, de Mayo de 2011, vigente en el momento de los hechos.
    f. Fotocopia de las Hojas de Recepción de Información, firmadas por todos los Trabajadores, a la recepción de cualquiera de los tres Manuales aportados, en el momento de su entrega (Mayo de 2011), así como los que se han producido con posterioridad.
    g. Certificados de Formación de los años 2009, 2011 y 2012 de los Cursos realizados por los trabajadores relacionados con la LOPD, Seguridad de la Información, Historia Clínica y Responsabilidad Legal, expedidos por la empresa “Aliad Conocimiento y Servido, S.L
    h. Relación de máquinas destructoras de papel, existentes en la Clínica, y la ubicación de las mismas.
5. En la Clínica existe un sistema de video-vigilancia, por supuesto convenientemente señalizado, cuya finalidad es garantizar la seguridad de las instalaciones, y, por tanto, como consecuencia, proteger también la confidencialidad de las Historias Clínicas y de otra documentación sensible.
6. La Clínica ha pasado dos Auditorías de Protección de Datos en los dos últimos años: Mayo de 2012 y Mayo de 2013.

7. La empresa y sus Centros, pertenecen a la Federación Nacional de Clínicas Privadas (FNCP) y a la Asociación Nacional para la promoción de la Excelencia en las Actividades Sanitarias Privadas (ANEASP); asociaciones que, se encuentran promoviendo ante la Agencia un Código Tipo, dirigido al Sector Sanitario. La Gerente y Responsable de Seguridad de sus Centros, forma parte, tanto de la Junta Directiva de la FNCP, como de la ANEASP, en condición de Vocal, por lo que tiene una especial concienciación en la relevancia de la normativa de protección de datos, como exponente fundamental de la defensa de los derechos de los usuarios y pacientes.

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 aparición de documentación con datos de carácter personal en la vía pública y al que hubieran tenido acceso terceras personas supondría una infracción de las medidas de seguridad que deben tener incorporados todos los ficheros con datos personales y una vulneración del deber de secreto.

El artículo 9 de la LOPD, que establece la seguridad de los datos, dispone:

"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 citado artículo 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 aquella, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, la pérdida de los datos.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan

el acceso –la conservación 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 refiere 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.

Partiendo de tales premisas, deben analizarse a continuación las previsiones que el Real Decreto El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, define en su artículo 5.2 ñ) el *"Soporte"* como el *"objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos".*

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 especialmente protegidos.

La necesidad de especial diligencia en la custodia de la documentación por el responsable del tratamiento ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11 de diciembre de 2008 (recurso 36/08), fundamento cuarto: *"Como ha dicho esta Sala en múltiples sentencias…se impone, en consecuencia, una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros…la recurrente es, por disposición legal una deudora de seguridad en materia de datos, y por tanto debe dar una explicación adecuada y razonable de cómo los datos han ido a parar a un lugar en el que son susceptibles de recuperación por parte de terceros, siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor".*

El mencionado Real Decreto 1720/2007, en su artículo 111, referido a las medidas de seguridad aplicables a los ficheros no automatizados, como serían los radiografías, establece en referencia al almacenamiento de la información, lo siguiente:

"1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el

apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad."

En el supuesto denunciado, sería el centro sanitario de dónde procedían los documentos el obligado a su custodia para evitar el acceso por personas no autorizadas y, en el caso de proceder su destrucción, hacerlo de forma que los haga inaccesibles a terceros.

III

El artículo 10 de la LOPD establece 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 profesional que incumbe a los responsables de los ficheros y a quienes intervienen en cualquier fase del tratamiento, recogido en el artículo 10 de la LOPD, comporta que el responsable de los datos almacenados o tratados no pueda revelar ni dar a conocer su contenido teniendo el *"deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, y, por lo que ahora interesa, comporta que los datos personales no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Este deber de sigilo resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riego 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 Constitución Española. En efecto, este precepto contiene, en palabras del Tribunal Constitucional en la citada Sentencia 292/2000, un *"instituto de garantía 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"*. Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino 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.

En el caso denunciado, la Jefatura de Policía Local del Ayuntamiento de Alcalá de Henares (Madrid), indicó que dos Agentes de la citada Policía Local se personaron en la (C/.....1), donde, según ha denunciado un vecino de la localidad, hay residuos clínicos en un contenedor de basura orgánica. Allí verificaron que en uno de los tres contenedores existentes había además de residuos clínicos procedentes del SANATORIO VALLES, documentos que contenían datos de carácter personal como historiales clínicos, datos de citas y hojas de tratamiento.

En las fotografías enviadas no se apreciaba la existencia de documentos con datos personales, por lo que se solicitó que nos enviaran alguno de los documentos encontrados, no habiendo recibido respuesta a la petición.

Durante la realización de las actuaciones previas de investigación, Clínica Vallés ha aportado copia del documento de seguridad vigente en el momento de producirse los hechos denunciados en el que se incluyen los apartados referidos a las funciones y obligaciones del personal en el tratamiento de la documentación que contiene datos personales; asimismo, acompañan certificados de formación de los trabajadores de los años 2009, 2011 y 2012 relacionados con la LOPD, seguridad de la información y de historia clínica y responsabilidad legal. Relacionan las máquinas destructoras de papel existentes en la Clínica. Por último, informan de que en el año 2012 y 2013 han pasado Auditorias de Protección de Datos.

IV

En el presente supuesto, en el que se denuncia la posible vulneración del deber de secreto y de las medidas de seguridad por parte de Clínica Vallés, al haberse encontrado restos biológicos junto con documentos en un contenedor en la vía pública, no consta acreditado que dichos datos hayan sido revelados, ya que en las fotos enviadas no se aprecia la existencia de ningún documento con datos de carácter personal, ni han sido facilitados por la Policía Local al solicitarlos, de modo que no existe prueba suficiente que permita a esta Agencia imputar una posible vulneración del artículo 10 de la LOPD. En cuanto a las medidas de seguridad, la Clínica ha facilitado documentación acreditativa de su cumplimiento.

No puede obviarse que al Derecho administrativo sancionador le son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad de los principios de presunción de inocencia e *"in dubio pro reo"* en el ámbito de la potestad sancionadora, que desplazan a quien acusa la carga de probar los hechos y su autoría. 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"*, 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 26/04, 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, el mismo Tribunal Constitucional, en Sentencia 44/1989, de 20/02, indica que *"Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque*

ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurrente aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate".

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya practicado una mínima prueba de cargo acreditativa de los hechos que motivan esta imputación o de la intervención en los mismos del presunto infractor, aplicando el principio *"in dubio pro reo"* en caso de duda respecto de un hecho concreto y determinante, que obliga en todo caso a resolver dicha duda del modo más favorable al interesado.

Como conclusión, de las actuaciones realizadas por parte de la Inspección de Datos y del presente procedimiento en relación a los hechos denunciados y, en atención a lo expuesto, no se ha podido acreditar que existieran documentos de la Clínica Vallés en la vía pública que contuvieran datos de carácter personal, por lo que procede acordar en archivo del presente expediente.

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 a UNMEQUI UNIVERSAL MEDICO QUIRURGICA S.A., (SANATORIO VALLES) y a la JEFATURA DE POLICIA LOCAL.

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.

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