



Expediente N°: E/05420/2015

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante las entidades CLINSA, S.A., y VITHAS SANIDAD, S.L., en virtud de denuncia presentada por Don **A.A.A.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 28 de julio de 2015, tuvo entrada en esta Agencia un escrito remitido por Don **A.A.A.** en el que declara lo siguiente:

Con motivo de la hospitalización de su padre, en el hospital VITHAS NUESTRA SEÑORA DE AMÉRICA, sito en (C/...1) Madrid, se le hizo entrega, entre la documentación del alta, del documento adjunto, en el cual figuran datos personales de una tercera persona, a la que desconoce y donde figura, entre otros, la especialidad médica en la que dicha persona fue tratada.

Junto a su denuncia aporta los siguientes documentos:

Documento con membrete del HOSPITAL NUESTRA SEÑORA DE AMÉRICA en el que figura una etiqueta con los siguientes datos:

HOSPITALIZACION:

*Nombre: **B.B.B.***

*N asistencia: *****NÚM.1***

*Cama: **********

*NHC: *****NHC.1***

*Edad: **AA***

*Fecha de nacimiento: **DD/M***

*Teléfono: *****TEL.1***

*Fecha de admisión *****FECHA.1***

*Servicio Profesional: **XXXX, Doctor C.C.C.***

Domicilio: (C/...1), MADRID

*DNI: *****DNI.1***

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 fecha de 1/4/2016, se solicitó información VITHAS SANIDAD, S.L., quien remite escrito en el que informa que la sociedad encargada de la explotación del Hospital Nuestra señora de América es la entidad CLINSA, S.A.
2. Con fecha de 5/4/2016 se solicita información a CLINSA, S.A., quien, tras solicitar ampliación de plazo, remite escrito de respuesta en el que informa de lo siguiente:
 - 2.1. Señala CLINSA, S.A., que, en general, el Hospital no entrega a sus pacientes

- documentos que contengan datos de carácter personal relativos a terceros pacientes.
- 2.2. Detalla a continuación la entidad el procedimiento implantado para la gestión de la documentación relativa los pacientes y que, básicamente, es almacenada en carpeta individuales por paciente custodiada en un armario con llave y al que únicamente tienen acceso el personal médico y de enfermería del centro, custodiando la llave del citado armario el personal de enfermería. Añade la entidad que cuando se da de alta al paciente se le hace entrega de una copia de dicha documentación junto con el informe de alta. La entidad ha aportado fotografías del armario utilizado para el almacenaje y custodia de la mencionada documentación.
 - 2.3. En relación con los vales de farmacia, la entidad describe el procedimiento implantado, y que sigue uno de los procedimientos indicados a continuación:
 - 2.3.1. Vale de farmacia que se realiza de forma electrónica y que se realiza en el ordenador del despacho común de enfermería y que se comunica telemáticamente a la farmacia del Hospital.
 - 2.3.2. Vale de farmacia realizado de forma manual durante una visita a un paciente en su habitación, en cuyo caso al terminar la visita es llevado personalmente a la farmacia del Hospital
 - 2.4. Según CLINSA, no le consta que el personal de enfermería del Hospital facilitase al progenitor del Sr. **A.A.A.** junto con la documentación relativa a su alta un vale de farmacia realizado a mano correspondiente a otro paciente. En todo caso, señala la entidad, se trataría de un hecho aislado, puntual y sin precedentes.
 - 2.5. Finalmente señala la entidad que cumple con lo previsto en la normativa de protección de datos y en este sentido señala lo siguiente:
 - 2.5.1. Ha aportado copia del documento de seguridad manifestando que realiza las correspondientes auditorías bienales de las medidas de seguridad.
 - 2.5.2. Todos los empleados han firmado una cláusula de confidencialidad, de la adjunta copia, sobre los datos de los pacientes y sobre el cumplimiento de las obligaciones en materia de seguridad.-
 - 2.5.3. La entidad realiza comunicaciones periódicas a sus empleados acerca del cumplimiento de las obligaciones de la normativa de protección de datos, adjuntando copia de una de dichas comunicaciones.
 - 2.5.4. Desde mediados de 2015 los empleados de la entidad han de realizar un curso on-line en materia de protección de datos.
 - 2.6. Finalmente, señala la entidad que al tener conocimiento de los hechos a través del requerimiento efectuado desde la Agencia ha procedido a realizar una investigación interna al objeto de descartar anomalías en el funcionamiento interno de la entidad así como, en su caso, a tomar las medidas oportunas para su regularización.

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

El artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal 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 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 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.

III

Un supuesto similar al denunciado, fue revisado por la Audiencia Nacional que estimó el Recurso interpuesto, en Sentencia de fecha 23 de diciembre de 2013 (Recurso C-A 341/2012), indicando lo siguiente:

“Los hechos por los que fue impuesta la multa aquí recurrida se contraen a que, en fecha 5 de enero de 2011, una persona (que luego formuló denuncia ante la Agencia de Protección de Datos), había recibido en su cuenta de correo electrónico una póliza de seguro, acompañada de las condiciones particulares, a nombre de un tercero y expedida por MAPFRE.



Y así, por ello, la Agencia de Protección de Datos consideró infringido el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por contravención del deber del secreto y de adecuada custodia de los datos de carácter personal, dado que los datos de aquel tercero llegaron a conocimiento del denunciante.

En impugnación de la resolución antedicha, la parte recurrente indica que el envío de una póliza de seguros referente a tercero, en el correo electrónico del denunciante, se debió un error involuntario en el proceso de mecanización del dato de la dirección de aquél en el momento de dar cumplimiento a su solicitud de remisión de un duplicado de su póliza de seguro.

En concreto indica que se produjo una mera equivocación puntual y aislada por parte de la tramitadora que gestionó aquella solicitud de duplicado de póliza. Y dice que dicho error no produjo perjuicio alguno ni al denunciante ni al tomador de la póliza ni tampoco beneficio a MAPFRE." (...)

Añadiendo, a su vez, en su Fundamento de Derecho Cuarto lo siguiente:

"En un caso similar al suscitado en el presente recurso, en el que hemos de poner en relación la concurrencia de un error humano, concreto y aislado, y el principio de culpabilidad (aun a título de "simple inobservancia") se ha pronunciado esta Sala en su Sentencia de 14 de diciembre de 2006 (autos de recurso 136/2005).

En dicha Sentencia decíamos que:

«La resolución del presente recurso pasa por recordar, en primer lugar, que la culpabilidad es un elemento indispensable para la sanción que se le ha impuesto a la actora, tal como lo prescribe el artículo 1301.1 de la Ley 30/1.992 de 26 de noviembre, que establece que sólo pueden ser sancionados por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia.

Se ha de hacer hincapié en que esa simple inobservancia no puede ser entendida que en el derecho administrativo sancionador rijan la responsabilidad objetiva. Efectivamente, en materia sancionadora rige el principio de culpabilidad (SSTC 15/1999, de 4 de julio; 76/1990, de 26 de abril; y 246/1991, de 19 de diciembre), lo que significa que ha de concurrir alguna clase de dolo o culpa. Como dice la sentencia del Tribunal Supremo de 23 de enero de 1998, "...puede hablarse de una decidida línea jurisprudencial que rechaza en el ámbito sancionador de la Administración la responsabilidad objetiva, exigiéndose la concurrencia de dolo o culpa, en línea con la interpretación de la STC 76/1990, de 26 de abril, al señalar que el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (artículo 25 de la Constitución) o de las exigencias inherentes al Estado de Derecho".

En esta misma línea, el Tribunal Supremo considera que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el sujeto infractor no se comporta con la diligencia exigible. Y el grado de diligencia exigible habrá de determinarse en cada caso en atención a las circunstancias concurrentes, tales como



el especial valor del bien jurídico protegido, la profesionalidad exigible al infractor, etc.

Pues bien, la aplicación de la citada Doctrina al específico y singular caso enjuiciado en este procedimiento ha llevado a esta Sala a concluir que en la referida conducta de la actora reseñada en los hechos probados de la resolución originaria impugnada no concurre el citado elemento de culpabilidad a la hora de determinar si la misma ha incurrido en una falta del deber de secreto del artículo 10 de la Ley Orgánica 15/1999 que se le imputa, pues así se ha de entender cuando dicha recurrente incurre en el mero error de enviar al domicilio de un cliente el contrato suscrito con otro cliente, sin que se aprecie culpa, incluso en ese grado mínimo previsto en la referida Ley 30/1992, en lo que se refiere al dato esencial de revelar a un tercero los datos personales que la misma trata en sus ficheros de ese cliente titular de dicho contrato que ni siquiera fue quien la denunció, sino aquel otro, y, como arriba se ha expuesto, por otras razones. En consecuencia, no se aprecia falta de diligencia en la recurrente en lo que respecta a la conducta imputada de incumplimiento del deber de secreto, dado que sólo incurrió en ese error de enviar el contrato de un cliente a un domicilio que no era el suyo».

La cuestión, pues, ha de resolverse conforme a los principios propios del derecho punitivo dado que el mero error humano no puede dar lugar, por sí mismo (y sobre todo cuando se produce con carácter aislado), a la atribución de consecuencias sancionadoras; pues, de hacerse así, se incurriría en un sistema de responsabilidad objetiva vedado por nuestro orden constitucional.(...)

Esta conclusión resulta, a juicio de la Sala, contraria al principio de presunción de inocencia...y del principio de culpabilidad, lo que nos lleva a la estimación del presente recurso y a la anulación del acto impugnado.”

Así las cosas, no se aprecia, en este caso, incumplimiento del deber de secreto. No obstante, se recuerda a la entidad denunciada que extreme las precauciones al objeto de evitar conductas como las descritas en su denuncia.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

- 1. PROCEDER AL ARCHIVO** de las presentes actuaciones.
- 2. NOTIFICAR** la presente Resolución a CLINSA, S.A., a VITHAS SANIDAD, S.L., 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 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