

Expediente Nº: E/05561/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante Doña **A.A.A.**, en virtud de denuncia presentada por Doña **B.B.B.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 13 de septiembre de 2016, tuvo entrada en esta Agencia un escrito remitido por escrito Doña **B.B.B.**, en el que denuncia a Doña **A.A.A.**, por el acceso a su analítica, sin su consentimiento, haciendo uso de su condición de trabajadora del Hospital General de Alicante; después procedió a la impresión de los mismos, haciéndoselos llegar a la denunciante a través de Facebook.

Y, entre otra, anexa la siguiente documentación:

Impresión de pantalla de la página de Facebook donde aparece su analítica, con fecha 01/09/2016.

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 9 de diciembre de 2016, se recibe escrito de la denunciada, en el que pone de manifiesto que:
 - a. Presta sus servicios como Técnico de Laboratorio en el Hospital General de Alicante.
 - b. Acompaña certificado del Hospital en el que se hace constar que ningún Técnico de Laboratorio tiene acceso a las historias clínicas de los pacientes, pero si acceso a datos por su propia trabajo.
 - c. Tuvo constancia de dicha analítica durante el desarrollo de sus funciones, ya que desconocía que la denunciante, que es su hija, se hubiera realizado la analítica.
 - d. La referida analítica se la remitió a su hija a través de Messenger, que es su correo privado de Facebook, es decir no se hizo público.
 - e. No existe consentimiento de la denunciante para el acceso a dicha información, ya que no existe relación alguna entre ambas.

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 LOPD en sus art. 1 y 2.1) establece:

“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.”

“1. 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 público y privado.”

La LOPD delimita su ámbito de aplicación en el párrafo primero de su artículo 2.1, definiendo el concepto de dato de carácter personal en su artículo 3.a) que define los datos de carácter personal como: *“Cualquier información concerniente a personas físicas identificadas o identificables”*. En similares términos se expresa en su artículo 5.f) el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la LOPD.

Por su parte el artículo 3.d) de la LOPD define al responsable del fichero o tratamiento como la *“persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.”*

A su vez, el artículo 3.c) de la LOPD define el tratamiento de datos personales en los siguientes términos: *“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.”*

III

La denunciante señala dos cuestiones, el acceso a los resultados de su analítica y el envío a través de una red social.

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 Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, 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 el supuesto presente, ha quedado acreditado que Doña **A.A.A.** Presta sus servicios como Técnico de Laboratorio en el Hospital General de Alicante; por su propio

trabajo, tiene acceso a las analíticas que se realizan en el Hospital, para el desarrollo de sus funciones.

En consecuencia, no se ha producido un acceso indebido a la historia clínica de la denunciante, sino que una persona, en el ejercicio de sus funciones, accedió a los resultados analíticos de la denunciante.

IV

Por otro lado, la denunciada al advertir que la analítica era de su hija, remitió el resultado a la persona a la que se referían.

El artículo 10 de la LOPD dispone lo siguiente: *“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 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 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>>.

El Tribunal Supremo viene entendiendo 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.

En el presente caso partimos del hecho constatado de que los resultados de la analítica se han enviado a la propia afectada, por lo que ha de entenderse que no se ha vulnerado el deber de secreto que impone el artículo 10 de la LOPD al no difundirlos a terceras personas.

Por lo tanto, de acuerdo con lo señalado,



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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a Doña **A.A.A.**, y a Doña **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 los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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