Expediente Nº: E/01137/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el Hospital Quirón de Madrid, en virtud de denuncia presentada por Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 10 de enero de 2013, tuvo entrada en esta Agencia un escrito remitido por Don ***A.A.A.,***, en el que denuncia que, con fecha 4 de enero de 2013, ha recibido en su teléfono 21 SMS del Hospital Quirón de Madrid, recordándole una supuesta cita. Puesto en contacto con el Hospital le comunican, primero que la cita era para su esposa y que se trataba de un Prueba Piloto.

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 23 de mayo de 2013, se realizó inspección en el Hospital Quirón de Madrid, sito en la localidad de Pozuelo de Alarcón (Madrid), poniéndose de manifiesto los siguientes hechos durante la inspección:

   1.1. En el mes de mayo de 2012, Hospital Quirón Madrid pone en marcha un servicio de envío de sms recordatorio para las consultas de Endocrinología y nutrición y Dermatología, ya que son dos consultas con largas listas de esperas y en las que los pacientes fallan mucho. Hasta este momento solo se sigue utilizando dicho servicio para estas dos consultas.

   1.2. Con fecha 4 de enero de 2013, tienen constancia de que ese día ocurrió un error con la aplicación que gestiona el envío de sms, motivo por el cual se paró la aplicación hasta encontrar la causa que motiva el error.

   1.3. Una vez analizado, se verificó que efectivamente la aplicación estaba dando un error, motivado por el retardo excesivo de respuesta desde el proveedor de servicios para cada sms, confirmando el envío correcto y su recepción por el usuario; esto provocó que no se actualizaran los sms enviados, generando un bucle de 20 sms en la remesa siguiente. Una vez detectado el problema y tomado las medidas necesarias para que no volviera a ocurrir, se reanudó el servicio con fecha 8 de febrero de 2013.

   1.4. Con fecha 8 de enero de 2013, reciben un correo electrónico remitido por el denunciante, donde pone en conocimiento del Hospital los mismos hechos denunciados ante la Agencia Española de Protección de Datos. Con fecha 15 de enero de 2013 se dio contestación a dicho correo. Se le informa que el servicio de sms lleva aproximadamente un año en funcionamiento, a pesar de

que la persona del Call Center lo desconocía porque es de reciente incorporación, y que se trataba de un fallo puntual del Sistema.

1.5. A pesar de que el denunciante fue informado de que se trataba de una prueba, esto fue debido al desconocimiento de la persona que atendió el teléfono. El Hospital nunca realiza pruebas con datos reales y además el servicio de envío de sms llevaba en funcionamiento desde el mes de mayo de 2012.

1.6. El Hospital entregó durante la inspección copia de la Hoja de incidencias que ha sido incluida en el Registro de incidencias del Documento de Seguridad al que hace referencia el artículo 88 del Real Decreto 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, y cuyo contenido se encuentra adjunto a estas actuaciones.

1.7. Con relación a estas incidencias el Hospital ha tomado las siguientes acciones: Informar a todo el personal nuevo del Call Center y recordar al resto del personal, la existencia del recordatorio de citas mediante sms en las consultas de Dermatología y Endocrinología y, con objeto de evitar el envío de sms duplicados, se han puesto dos filtros de seguridad.

1.8. Se verifica mediante acceso a la información existente en sus sistemas relativa a la destinataria de los sms recordatorio, recibidos en el teléfono del denunciante, que dichos sms iban dirigidos a nombre de una paciente**,** que según manifiestan los representantes de la entidad es la esposa del reclamante, la cual tenía una cita registrada con fecha 9 de enero de 2012 a las 09:42 horas en el servicio de Endocrinología y Nutrición, constando dicha consulta como “NO REALIZADA”.

1.9. Así mismo, se accede a los datos de la paciente, comprobándose que el número de teléfono principal que consta en su ficha coincide con el aportado por el denunciante como teléfono receptor de los sms.

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 se refiere al envío de 21 SMS, por parte del Hospital Quirón de Madrid, recordándole una cita, que no era para él, y al hecho de que se realizaran pruebas piloto con datos reales.

Los hechos denunciados podrían constituir una infracción del artículo 9 de la LOPD, que 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 citado 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.

En el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, en sus tres primeros apartados, se determina lo siguiente:

"1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

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."

Las incidencias de seguridad deben quedar reflejadas en dicho documento. Durante la visita de inspección al Hospital Quirón, se constató que en el documento de seguridad estaba anotada la incidencia ocurrida el día 4 de enero de 2013 y que propició que se enviaran mensajes de forma reiterada.

En cuanto a la realización de pruebas con datos reales, el artículo 94.4 del citado Reglamento determina lo siguiente: *"4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.*

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad".

El Centro hospitalario ha manifestado que nunca realizan pruebas con datos reales y que los SMS respondían a un sistema de recordatorio de citas médicas que llevaba implantado durante algunos meses y que dio un error, que se subsanó y quedó reflejado en el Registro de Incidencias.

En consecuencia, no se han vulnerado las medidas de seguridad por parte del Hospital denunciado.

III

En cuanto a la utilización de sus datos para recordarle una cita que él no tenía, el artículo 6 de la LOPD, cuyo apartado 1 y 2 dispone: *"El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa".*

2. 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".

A este respecto, debe señalarse que el artículo 3.c) de la LOPD define el tratamiento de datos como *"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".*

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 proporciona 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.

En este sentido, la esposa del denunciante facilitó el teléfono móvil de su marido para las comunicaciones que tuvieran que hacerle desde el Hospital, como fue el caso de recordarle una cita en la consulta de Endocrinología y Nutrición el día 9 de enero a las 9,42 horas, contando con su consentimiento para el tratamiento efectuado.

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 Hospital Quirón Madrid 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.

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