Procedimiento Nº: A/00080/2016

RESOLUCIÓN: R/00970/2016

En el procedimiento A/00080/2016, instruido por la Agencia Española de Protección de Datos a la entidad ASISA ASISTENCIA SANITARIA INTERPROVINCIAL DE SEGUROS, SAU, vista la denuncia presentada por Don ***C.C.C.,*** y en virtud de los siguientes

ANTECEDENTES

PRIMERO: Con fecha de 31 de marzo de 2015 tiene entrada en esta Agencia un escrito remitido por Don ***C.C.C.,*** en el que declara lo siguiente:

Que ha recibido por error, en fecha de 30 de marzo de 2015, un correo electrónico remitido por la compañía médica ASISA, que incluye adjunto un fichero en formato Microsoft EXCEL conteniendo un listado de más de 25.000 registros con datos personales: *nombre y apellidos, NIF, fecha de nacimiento, teléfono, correo electrónico, nº de póliza*, etc. de más de 25.000 clientes de esa compañía.

Que dio cuenta del error al remitente por correo electrónico, que le contestó pidiendo disculpas y manifestando que se trataba de un correo interno al departamento de soporte y que por error, su cuenta se incluyó en el autocompletar al escribir el nombre del destinatario.

Junto a la denuncia aporta la siguiente documentación:

Copia del correo electrónico de fecha 30 de marzo de 2015 remitido desde la dirección ***F.F.F.*** a la dirección ***B.B.B.***. El correo lleva por asunto *"HOJA INCIDENCIAS CONTESTA 23-3-2015 RECTIFICADA v149".* El correo va firmado por Don ***A.A.A.***, Secretaría del Consejo, (C/...1), Madrid.

Copia del correo electrónico de fecha 30 de marzo de 2015 remitido desde la misma dirección de correo a la dirección ***B.B.B.*** y firmado por la misma persona. En él se dan explicaciones sobre el envío erróneo del correo anterior.

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. En fecha de 22 de septiembre de 2015 se practica diligencia al objeto de incorporar a las actuaciones los dos correos electrónicos de fecha 1/6/2015 remitidos por el denunciante y en los que se incluyen respectivamente:

   1.1. Fichero PANTALLAZO.DOC: contiene copia de pantalla del correo objeto de la

denuncia.

1.2. Fichero CABECERA.DOC: contiene la cabecera del correo objeto de la denuncia.

1.3. Fichero HOJA_INCIDENCIAS_CONTESTA_23-03-2015_RECTIFICADA _v149: contiene una hoja de cálculo en formato Microsoft EXCEL con más de 25.000 registros de los que se imprimen las cinco primeras hojas al objeto de reflejar su estructura.

1.4. Todos los correos anteriores incluidos los ficheros adjuntos se almacenan en un soporte CD que se incorpora a la presente diligencia.

2. En fecha de 9 de febrero de 2016 se realiza una inspección a la sociedad ASISA ASISTENCIA SANITARIA INTERPROVINCIAL DE SEGUROS, S.A.U. (en adelante referenciada como ASISA) en la que se comprueba lo siguiente:

2.1. Se constata que el fichero aportado por el denunciante efectivamente corresponde a clientes de ASISA y que le llegó, como afirma en su denuncia, a través de un correo electrónico remitido por una persona que en el momento del envío era empleado de ASISA.

2.1.1. Los inspectores seleccionaron un conjunto de 10 registros al azar del fichero HOJA_INCIDIDENCIAS_CONTESTA_23-03-2015_RECTIFICADA _v149 aportado por el denunciante, comprobándose que todas las personas figuraban en la base de datos de clientes de ASISA.

2.1.2. A petición de los inspectores, Don ***D.D.D.***, uno de los destinatarios que figuraba en el correo remitido al denunciante, comprobó que en su buzón de entrada de correo, ***H.H.H.***, figura un correo, de fecha 30 de marzo de 2015, remitido desde la dirección ***F.F.F.*** conteniendo el fichero HOJA_INCIDIDENCIAS_ CONTESTA_23-03-2015_RECTIFICADA_v149. En el citado correo se observa que también como destinatario figura la dirección ***B.B.B.*** correspondiente al denunciante.

2.2. Los representantes de ASISA realizaron las siguientes declaraciones:

2.2.1. Don ***A.A.A.*** fue empleado de ASISA hasta hace unos meses en que dejó la compañía. Mientras estuvo en ella se encargaba de facilitar soporte al usuario perteneciendo a la unidad de SOPORTE WEB.

2.2.2. El fichero objeto de la denuncia recoge un listado de incidencias en el acceso web que Don ***A.A.A.*** envió a sus superiores y en los que por error humano, se añadió la dirección ***B.B.B.*** del denunciante, persona que aunque cliente de ASISA, no debía ser receptor de dicho correo. Su inclusión se produjo ya que el programa OUTLOOK utilizado para la remisión de correo y al objeto de facilitar al usuario, incluye de forma automática destinatarios de correos recientes cuyo nombre correspondan con las iniciales de destinarios que el usuario vaya tecleando. De hecho uno de los destinatarios del correo era Don ***E.E.E.***, superior jerárquico de Don ***A.A.A.*** y con dirección de correo ***G.G.G.***.

2.2.3. Como consecuencia de la inspección ASISA tiene previsto llevar a cabo una investigación interna para verificar la incidencia detectada, adicionalmente se ha convocado, con carácter extraordinario, al Comité de Seguridad LOPD de la compañía a fin de establecer las medidas

necesarias para evitar que en un futuro pueda suceder algún hecho análogo. Las decisiones que se adopten en el Comité de Seguridad serán trasladadas a la Agencia a fin de que tenga en consideración las medidas que se acuerden.

TERCERO: Con fecha 25 de febrero de 2016, la Directora de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00080/2016. Dicho acuerdo fue notificado a los denunciantes y al denunciado.

CUARTO: Con fecha 13 de marzo de 2016, se recibe en esta Agencia escrito del denunciado en el que comunica: que ASISA tiene implantados los estándares de seguridad exigidos para garantizar la confidencialidad de la información tratada en los sistemas. Tienen un Comité de Seguridad LOPD, que trimestralmente revisa los aspectos relevantes y aprueba decisiones para mejorar la seguridad. Se convocó el Comité, con carácter extraordinario, el 18 de febrero de 2016, para evitar errores como el acontecido y que ha dado origen a este procedimiento. ASISA dispone de un sistema que permite el cifrado de todas las comunicaciones internas que se efectúan en la compañía para garantizar la inaccesibilidad del contenido de lo enviado por terceros no autorizados. Si se envían archivos adjuntos a un correo fuera de las redes internas de la compañía va cifrado y con contraseña que se envía en mensajes diferentes. La seguridad está garantizada, salvo un error humano. Para evitar errores, se ha automatizado el envío de la información que fue objeto del error humano, así que desde el área afectada ya no se puede enviar un archivo a un destinatario no autorizado. Además se ha comenzado la implantación de un entorno de intercambio interno de archivos de forma segura, lo que permitirá compartir archivos sin que terceros no autorizados puedan tener acceso a la información, continuando con el cifrado de las Redes de la Compañía. Se está consultando al proveedor de servicio de correo electrónico para conocer la posibilidad de eliminar la memoria caché de los destinatarios de los buzones de correo, con lo que no se completara de forma automática el campo de destinatarios de correo una dirección utilizada con anterioridad. Asimismo, se completará la formación de los usuarios que por su actividad en la compañía sean susceptibles de remitir información conteniendo datos personales.

HECHOS PROBADOS

PRIMERO: El 30 de marzo de 2015, un cliente de ASISA recibió un correo electrónico remitido por la compañía médica que incluye adjunto un fichero en formato Microsoft EXCEL con un listado con datos personales de más de 25.000 clientes de esa compañía: *nombre y apellidos, NIF, fecha de nacimiento, teléfono, correo electrónico, nº de póliza*, etc.

Que dio cuenta del error al remitente por correo electrónico, que le contestó pidiendo disculpas y manifestando que se trataba de un correo interno al departamento de soporte y que por error su cuenta se incluyó en el autocompletar al escribir el nombre del destinatario.

SEGUNDO: El 9 de febrero de 2016 por la AEPD se realiza una inspección a la sociedad ASISA ASISTENCIA SANITARIA INTERPROVINCIAL DE SEGUROS, SAU. en la que se comprueba que el fichero aportado por el denunciante efectivamente corresponde a clientes de ASISA y que le llegó, como afirma en su denuncia, a través de un correo electrónico remitido por una persona que en el momento del envío era empleado de ASISA

TERCERO: Los representantes de ASISA declararon, y los inspectores comprobaron que el fichero objeto de la denuncia recoge un listado de incidencias en el acceso web, que un empleado envió a sus superiores y en los que por error humano, se añadió la dirección de correo electrónico del denunciante, persona que, aunque cliente de ASISA, no debía ser receptor de dicho correo. Su inclusión se produjo porque el programa OUTLOOK incluye de forma automática destinatarios de correos recientes cuyo nombre correspondan con las iniciales de destinarios que el usuario vaya tecleando.

CUARTO: Durante la inspección los representantes de ASISA manifestaron que tienen previsto llevar a cabo una investigación interna para verificar la incidencia detectada, adicionalmente se ha convocado, con carácter extraordinario, al Comité de Seguridad LOPD de la compañía a fin de establecer las medidas necesarias para evitar que en un futuro pueda suceder algún hecho análogo. Las decisiones que se adopten en el Comité de Seguridad serán trasladadas a la Agencia a fin de que tenga en consideración las medidas que se acuerden.

QUINTO: ASISA ha señalado las medidas que ha tomado para evitar que se vuelva a producir el error que ha dado lugar a este procedimiento: Se convocó el Comité de Seguridad LOPD, con carácter extraordinario, el 18 de febrero de 2016, para evitar errores como el acontecido y que ha dado origen a este procedimiento. ASISA dispone de un sistema que permite el cifrado de todas las comunicaciones internas que se efectúan en la compañía para garantizar la inaccesibilidad del contenido de lo enviado por terceros no autorizados. Ahora, si se envían archivos adjuntos a un correo fuera de las redes internas de la compañía va cifrado y con contraseña que se envía en mensajes diferentes. La seguridad está garantizada, salvo un error humano. Para evitar estos errores, se ha automatizado el envío de la información que fue objeto del error humano, así que desde el área afectada ya no se puede enviar un archivo a un destinatario no autorizado. Además se ha comenzado la implantación de un entorno de intercambio interno de archivos de forma segura, lo que permitirá compartir archivos sin que terceros no autorizados puedan tener acceso a la información, continuando con el cifrado de las Redes de la Compañía. Se está consultando al proveedor de servicio de correo electrónico para conocer la posibilidad de eliminar la memoria caché de los destinatarios de los buzones de correo, con lo que no se completara de forma automática el campo de destinatarios de correo una dirección utilizada con anterioridad. Asimismo, se completará la formación de los usuarios que por su actividad en la compañía sean susceptibles de remitir información conteniendo datos personales.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37. g) en relación con el artículo 36 de la LOPD.

II

El artículo 10 de la LOPD, establece: *"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."*

Dado el contenido del precepto, ha de entenderse que el mismo 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.

En este sentido, la Sentencia de la Audiencia Nacional de fecha 18/01/02, recoge en su Fundamento de Derecho Segundo, segundo y tercer párrafo: "El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable … no puede 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 automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, 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 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). Este derecho fundamental a la protección de los datos 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 deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento. El deber de secreto profesional que incumbe a los responsables de los ficheros, recogido en el artículo 10 de la LOPD, comporta que el responsable o quienes intervengan en cualquier fase del tratamiento de los datos almacenados 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 tratados automatizadamente o no, 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.

En este caso concreto, un cliente de ASISA recibió un correo electrónico remitido por la compañía médica con un fichero adjunto en formato Microsoft EXCEL con un listado con datos personales de más de 25.000 clientes de esa compañía.

Que el remitente le contestó pidiendo disculpas y manifestando que se trataba de un correo interno al departamento de soporte y que por error su cuenta se incluyó en el autocompletar al escribir el nombre del destinatario.

La entidad denunciada ha manifestado que el fichero objeto de la denuncia recoge un listado de incidencias en el acceso web, que un empleado envió a sus superiores y en los que por error humano, se añadió la dirección de correo electrónico del denunciante, persona que, aunque cliente de ASISA, no debía ser receptor de dicho correo. Su inclusión se produjo porque el programa OUTLOOK incluye de forma automática destinatarios de correos recientes cuyo nombre correspondan con las iniciales de destinarios que el usuario vaya tecleando.

Durante la inspección los representantes de ASISA manifestaron que tienen previsto llevar a cabo una investigación interna para verificar la incidencia detectada, adicionalmente se ha convocado, con carácter extraordinario, al Comité de Seguridad LOPD de la compañía a fin de establecer las medidas necesarias para evitar que en un futuro pueda suceder algún hecho análogo. Las decisiones que se adopten en el Comité de Seguridad serán trasladadas a la Agencia a fin de que tenga en consideración las medidas que se acuerden.

Exponen también en su escrito que han establecido un procedimiento para evitar que el error en la documentación vuelva a cometerse y relacionan las medidas adoptadas al respecto, tal y como se detalla en el Hecho probado Quinto.

En consecuencia, deben estimarse adoptadas ya las medidas correctoras pertinentes en el caso por lo que debe procederse a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la entidad denunciada, en aplicación de la interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica.

III

El artículo 45.6 de la LOPD, introducido a través de la reforma operada por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, dispone:

"Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento."

Trasladando las consideraciones expuestas al supuesto que nos ocupa, se observa que la infracción de la LOPD de la que se responsabiliza a la denunciada es una infracción "grave"; que la denunciada no ha sido sancionada o apercibida por este organismo en ninguna ocasión anterior; y que concurren de manera significativa varias de las circunstancias descritas en el artículo 45.5 de la LOPD. Todo ello, unido a la naturaleza de los hechos que nos ocupan, justifica que la AEPD no acuerde la apertura de un procedimiento sancionador y que opte por aplicar el artículo 45.6 de la LOPD.

Ahora bien, es obligado hacer mención a la Sentencia de la Audiencia Nacional de 29/11/2013, (Rec. 455/2011), Fundamento de Derecho Sexto, que sobre el apercibimiento regulado en el artículo 45.6 de la LOPD y a propósito de su naturaleza jurídica advierte que "*no constituye una sanción"* y que se trata de "*medidas correctoras de cesación de la actividad constitutiva de la infracción"* que *sustituyen* a la sanción. La Sentencia entiende que el artículo 45.6 de la LOPD confiere a la AEPD una "*potestad"* diferente de la sancionadora cuyo ejercicio se condiciona a la concurrencia de las especiales circunstancias descritas en el precepto.

En congruencia con la naturaleza atribuida al apercibimiento como una alternativa a la sanción cuando, atendidas las circunstancias del caso, el sujeto de la infracción no es merecedor de aquella y cuyo objeto es la imposición de medidas correctoras, la SAN citada concluye que cuando no se requieran medidas correctoras, lo procedente en Derecho es acordar el archivo de las actuaciones.

En este caso concreto, atendida la naturaleza de la infracción consistente en un hecho puntual que no admite corrección ni la adopción de una concreta medida correctora, debe procederse en consecuencia, a resolver el archivo de las actuaciones, sin practicar apercibimiento o requerimiento alguno a la denunciada, en aplicación de la interpretación del artículo 45.6 de la LOPD, atendida su interpretación sistemática y teleológica. Recordando que la reiteración en conductas como la denunciada constituye un supuesto sobre el que concurren las circunstancias previstas para la aplicación del régimen sancionador contemplado en la LOPD.

A la vista del pronunciamiento recogido en la SAN de 29/11/2013 (Rec. 455/2011) de acuerdo con lo señalado se debe proceder al archivo de las actuaciones.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- ARCHIVAR (**A/00080/2016**) las actuaciones practicadas a la entidad ASISA ASISTENCIA SANITARIA INTERPROVINCIAL DE SEGUROS, SAU**,** con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de

Protección de Datos de Carácter Personal, con relación a la denuncia por infracción del artículo 10 de la LOPD, tipificada como grave en el artículo 44.3.d) de la citada Ley Orgánica.

2.- NOTIFICAR el presente Acuerdo a la entidad ASISA ASISTENCIA SANITARIA INTERPROVINCIAL DE SEGUROS, S.A.U.

3.- NOTIFICAR el presente Acuerdo a Don ***C.C.C.***.

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 esta 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