Procedimiento Nº AP/00033/2017

RESOLUCIÓN: R/03316/2017

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00033/2017**, instruido por la Agencia Española de Protección de Datos a la entidad **CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA DE LA GENERALITAT DE VALENCIANA**, y en virtud de los siguientes

ANTECEDENTES

PRIMERO: Con fecha de 13 de diciembre de 2016 la Directora de la Agencia Española de Protección de Datos acuerda iniciar actuaciones previas de investigación en relación a la noticia aparecida en el periódico digital "M.M.M.", referente al abandono en la vía pública de docenas de tarjetas sanitarias individuales (SIP) con datos de carácter personal de sus titulares.

SEGUNDO: En el marco de las actuaciones previas de investigación practicadas, los Servicios de Inspección de esta Agencia han tenido conocimiento de los siguientes hechos:

2.1 Según información aparecida con fechas 12 y 13 de diciembre de 2016 en el periódico digital "M.M.M." (***URL.1), con fecha 27 de noviembre de 2016 un vecino de la zona localizó docenas de tarjetas sanitarias con datos personales de sus titulares tiradas en la acera, concretamente junto a un contenedor de basura situado a la altura del nº 8 de la c/ A.A.A. de Valencia y frente al Centro de Salud "P.P.P." de esa ciudad,

Las citadas tarjetas no habían sido sometidas a ningún proceso de destrucción, motivo por el cual resultaban legibles los datos de carácter personal de los titulares de las mismas, tales como sus nombres y apellidos, número de Documento Nacional de Identidad (DNI), número de identificación SIP y número de la Seguridad Social, además de otra información referida a las prestaciones médicas y farmacéuticas a las que pudieran tener derecho.

2.2 En relación con dichos hechos, la CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA de la GENERALITAT VALENCIANA, ha informado a esta Agencia lo siguiente:

a. La presencia de tarjetas sanitarias en la vía pública que se hallaron con fecha 27 de noviembre de 2016, frente al Centro de Salud "P.P.P.", de Valencia, solo puede ser consecuencia de un fallo puntual en la aplicación de protocolos establecidos para la retirada y destrucción de las tarjetas invalidadas.

b. El Centro de Salud "P.P.P.", pertenece al Departamento de Salud Valencia-L.L.L.. Aportan copia del "Protocolo de recogida y destrucción de documentación con datos de carácter confidencial" vigente en dicho departamento (Hospital "L.L.L.", Centro de Especialidades "S.S.S.", Centro de Especialidades de Catarroja y todos los Centros de Atención Primaria del departamento). En

dicho documento figura la siguiente información:

Tiene como objeto: *"establecer las normas que deberán seguirse de forma obligatoria en la recogida de toda aquella documentación que contenga datos tanto de filiación como clínicos de cualquier paciente atendido o no en cada centro."*

En cuanto al método.-

"Debe ser eliminada por esa vía, toda la documentación en la que puedan aparecer datos de pacientes, tanto referidos a datos administrativos como aquellos que contengan información clínica. Se incluye también cualquier tipo de listado en el que aparezca alguno de esos datos.

Si se considera necesario y atendiendo a criterios de destrucción con respecto al medio ambiente, se establecerá un circuito paralelo para recoger y destruir formatos diferentes a los documentos en papel (cintas ribbon, pulseras identificativos, etc.)

Se establecerá una serie de puntos de recogida en los que se instalará un contenedor habilitado a tal fin. Dicho contenedor debe tener un tamaño adecuado para que se adapte a la periodicidad de su recogida. El contenedor debe estar cerrado con llave e imposibilitar el acceso al papel depositado por cualquier otra vía.

Dichos puntos de recogida deben combinar criterios de eficacia a la hora de la recogida con criterios de accesibilidad al personal que deba desechar la documentación.

El personal encargado de la recogida de los contenedores deberá aceptar los criterios establecidos por esta Institución en lo referente a confidencialidad del material tratado."

La ubicación de los contenedores es la siguiente:

- Edificio Hospital: distribuidos en 10 zonas, contando cada una de ellas con al menos un contendor.
- Edificio de Consultas Externas: Al menos un contenedor por cada una de las alas en que se divide cada planta, uno en planta Baja y dos más en el primer piso. Así como en el área de Archivos.
- Centro de Especialidades S.S.S.: Dos contenedores.
- Centros de Atención Primaria: Al menos un contenedor por Centro.

Existen diferentes normas y circulares en este sentido, de las que desde la Conselleria se ha dado traslado al personal sanitario y administrativo, por diferentes vías, tanto al personal Directivo como acciones formativas dirigidas al personal que atiende al público.

TERCERO: Como resultado de las actuaciones previas de inspección, y de acuerdo a lo dispuesto en el artículo 126.2 del Reglamento de Desarrollo de la LOPD (RLOPD), se apreció la existencia de hechos susceptibles de motivar la incoación de procedimiento de infracción de las Administraciones Públicas.

En consecuencia, con fecha 24 de julio de 2017**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento de declaración de infracción de Administraciones Públicas a la CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA de la GENERALITAT VALENCIANA , en adelante CONSELLERIA, por presunta infracción de los siguientes preceptos:

Artículo 9.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), en relación con lo dispuesto en los artículos 92, 108 y 114 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, (RLOPD en adelante), tipificada como infracción grave en el artículo 44.3.h) de dicha norma.

Artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, tipificada como infracción grave en el artículo 44.3.d) de dicha norma.

CUARTO: Notificado el citado acuerdo de inicio de procedimiento de declaración de infracción de Administraciones Públicas, con fecha 14 de agosto de 2017 el responsable de la Oficina de seguridad de la Información de la mencionada CONSELLERIA presentó escrito de alegaciones en el que, en síntesis, manifestaba:

- Que las tarjetas sanitarias no contienen datos de salud ni ningún otro que exija la aplicación de medidas de seguridad de nivel alto, según el RD 1720/2017. Tampoco constan el domicilio ni datos de contacto. Adjuntan documento del Servicio de Aseguramiento Sanitario denominado “Modelos Tarjetas SIP” Tipología Tarjetas SIP, que detalla el contenido de las mismas.

- Que la Conselleria ha venido adoptando las medidas técnicas y organizativas necesarias para la protección y custodia de las tarjetas sanitarias, conforme se indicaba en el escrito de alegaciones y anexos enviados con anterioridad.

- El hecho denunciado sólo puede interpretarse como un incumplimiento lamentable, pero puntual y extraordinario de los protocolos establecidos, añadiendo que a de la aplicación de controles complementarios para el acceso a los servicios asistencias difícilmente se puede entender que el incidente haya puesto en riesgo los derechos fundamentales de los titulares de las tarjetas.

QUINTO: Con fecha 31 de agosto de 2017 se inicia por la Instructora del procedimiento la apertura de un período de práctica de pruebas, en cuyo marco se acuerda practicar las siguientes pruebas:

5.1 Incorporar al expediente del procedimiento arriba indicado, y por tanto dar por reproducida a efectos probatorios, la documentación recabada en las actuaciones previas de inspección que forman parte del expediente E/06752/2016. Asimismo, se dan por reproducidas a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento AP/00033/2017 presentadas por la CONSELLERIA. Todo ello con su correspondiente documentación adjunta.

5.2 Incorporar al expediente del procedimiento arriba indicado, y por tanto dar por reproducida a efectos probatorios, impresión del resultado de la información

obtenida sobre la Tarjeta Sanitaria Individual en las páginas web:
***URL.2
***URL.3

El acuerdo de inicio de práctica de dichas pruebas fue notificado a la CONSELLERIA con fecha 4 de septiembre de 2017.

SEXTO: Con fecha 30 de noviembre de 2017, la Instructora del procedimiento formuló Propuesta de Resolución del procedimiento AP/00033/2017 en el sentido de que por la Directora de la Agencia Española de Protección de Datos resolviera:

Declarar que la CONSELLERIA ha infringido lo dispuesto en el artículo 9.1 de la LOPD en su relación con lo previsto en los artículos 89.2 92.3 y 4 y 108 del RLOPD, tipificada como grave, en el artículo 44.3.h) de dicha norma, así como lo dispuesto en el artículo 10 de la LOPD, tipificada como grave, en el artículo 44.3.d) de dicha norma.

Requerir a la CONSELLERIA, para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción de los artículos 9.1 y 10 de la Ley Orgánica 15/1999.

Notificar la Resolución que se adopte a la CONSELLERIA

Comunicar la resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD.

Dicha propuesta de resolución se notificó a la CONSELLERIA con fecha 4 de diciembre de 2017, no constando que la misma ejerciera su derecho a formular alegaciones en su defensa.

HECHOS PROBADOS

PRIMERO: Consta a través de las noticias de presa aparecidas con fechas 12 y 13 de diciembre de 2016 en el Diario "M.M.M." que, con fecha 27 de noviembre de 2016, se localizaron docenas de Tarjetas SIP, sin destruir, tiradas a la altura del nº 8 de la C/ A.A.A. de Valencia, en concreto junto a un contenedor de basura y mezcladas con restos de material sanitario. Las citadas noticias incluyen una fotografía del lugar en que se localizaron las tarjetas SIP esparcidas por la vía púbica. (folios 2 y 3)

SEGUNDO: Las mencionadas Tarjetas SIP estaban tiradas en la vía pública a la vista de los viandantes que transitaban por ese lugar, constando en la noticia de prensa publicada el día 12 de diciembre de 2016 en el Diario "M.M.M." que "*Uno de los vecinos que se las encontró, **B.B.B.**, sorprendido por el hallazgo, decidió fotografiar las tarjetas esparcidas."* (folio 2)

TERCERO: Dicha documentación procedía del Centro de Salud "P.P.P.", situado enfrente del lugar en el que se encontraron tiradas las reseñadas Tarjetas SIP (folios 2, 3, 22).

CUARTO: El Centro de Salud "P.P.P.", está adscrito al Departamento de Salud Valencia-L.L.L.de la CONSELLERIA DE SANITAT UNIVERSAL I SALUT PUBLICA DE LA GENERALITAT VALENCIANA. (folio 22)

QUINTO: La Tarjeta Sanitaria Individual (Tarjeta SIP) venía conteniendo hasta la implantación de la actual Tarjeta SIP los siguientes datos de carácter personal referidos a su titular: nombre y apellidos, números del Documento Nacional de Identidad (DNI), Tarjeta Sanitaria Individual (SIP), Seguridad Social (SS). La nueva Tarjeta SIP contiene, además el Código de Identificación Personal del Sistema Nacional de Salud (CIPSNS), identificador único estatal para cada ciudadano. (folios 63 y 64)

SEXTO: La CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA de la GENERALITAT VALENCIANA, ha aportado copia del "Protocolo de Recogida y Destrucción de Documentación con Datos de Carácter Confidencial" vigente en el "Departament de Salut València L.L.L.". En dicho documento figura la siguiente información: (folios 25 y 26)

En cuanto al objeto: *"establecer las normas que deberán seguirse de forma obligatoria en la recogida de toda aquella documentación que contenga datos tanto de filiación como clínicos de cualquier paciente atendido o no en cada centro."*

En cuanto al método:

"Debe ser eliminada por esa vía, toda la documentación en la que puedan aparecer datos de pacientes, tanto referidos a datos administrativos como aquellos que contengan información clínica. Se incluye también cualquier tipo de listado en el que aparezca alguno de esos datos.

Si se considera necesario y atendiendo a criterios de destrucción con respecto al medio ambiente, se establecerá un circuito paralelo para recoger y destruir formatos diferentes a los documentos en papel (cintas ribbon, pulseras identificativos, etc.)

Se establecerá una serie de puntos de recogida en los que se instalará un contenedor habilitado a tal fin. Dicho contenedor debe tener un tamaño adecuado para que se adapte a la periodicidad de su recogida. El contenedor debe estar cerrado con llave e imposibilitar el acceso al papel depositado por cualquier otra vía.

Dichos puntos de recogida deben combinar criterios de eficacia a la hora de la recogida con criterios de accesibilidad al personal que deba desechar la documentación.

El personal encargado de la recogida de los contenedores deberá aceptar los criterios establecidos por esta Institución en lo referente a confidencialidad del material tratado."

En cuanto a la ubicación de los contenedores en los "Centros de Atención Primaria: Al menos un contenedor por Centro".

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 título VII de la LOPD, bajo la rúbrica de *"Infracciones y sanciones"*, establece en el artículo 43.1 de dicha norma que: *"1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley."*

El concepto de responsables de los ficheros debe integrarse con la definición que de los mismos recoge el artículo 3.d). Este precepto incluye en el concepto de responsable tanto al que lo es del fichero como al del tratamiento de datos personales. Conforme al artículo 3.d) de la LOPD, el responsable del fichero o del tratamiento es *"la persona física o jurídica (...) que decida sobre la finalidad, contenido y uso del tratamiento".*

Con arreglo a lo cual, se considera que la CONSELLERIA resulta responsable del tratamiento llevado a cabo con las Tarjetas Sanitarias Individuales (Tarjetas SIP) que fueron localizadas en la vía pública, concretamente, junto a un contenedor de basura situado frente al Centro de Salud "P.P.P." de la ciudad de Valencia, ya que decide sobre la finalidad, contenido y uso de los datos de carácter personal contenidos en ese tipo de documentos.

Precisamente, su condición de responsable del tratamiento y de los ficheros en los que se integra la información contenida en dichos documentos, obliga a la CONSELLERIA a establecer y adoptar las medidas de seguridad técnicas y organizativas que resulten necesarias para garantizar la destrucción de las Tarjetas SIP invalidadas mediante procedimientos que impidan accesos de terceros no autorizados a la información de carácter personal incluida en las mismas, exigencia a la que se suman los deberes de secreto profesional y custodia que también incumben a dicha CONSELLERIA respecto de la información contenida en las mencionadas Tarjetas SIP.

III

El artículo 17.1 de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

La LOPD, que traspuso al ordenamiento interno el contenido de la Directiva 95/46, dispone en su artículo 1 que *"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".*

El artículo 2.1 de la misma Ley Orgánica establece: *"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 públicos y privados".

IV

En primer lugar, procede dilucidar si en el caso analizado, en el que se localizaron a la altura del nº 8 de la c/ del ***A.A.A.*** de Valencia, tiradas junto a un contenedor de basura, docenas de Tarjetas SIP procedentes del Centro de Salud "P.P.P." de Valencia, se ha producido una infracción en materia de "Seguridad de los datos" por parte de la CONSELLERIA.

El artículo 9 de la LOPD dispone, bajo la rúbrica "Seguridad de los datos", 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 transcrito 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, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, la "pérdida" de dichos datos o el "acceso no autorizado" a los mismos por terceros.

El Título VIII, bajo la rúbrica "De las medidas de seguridad en el tratamiento de datos de carácter personal" del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre, (en adelante RLOPD), se refiere a las medidas de seguridad que deben implementarse en los ficheros y tratamientos automatizados o no automatizados.

El artículo 79 del RLOPD, en relación con el *"Alcance*" de las medidas de seguridad en el tratamiento de datos de carácter personal dispone que: "*Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cuál sea su sistema de tratamiento*."

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, estableciéndose en el artículo 80 del RLOPD que "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto"

Mientras que en cuanto a la "Aplicación de los niveles de seguridad", el artículo

81.1 del mismo reglamento establece que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*".

Por su parte, los apartados 1 al 4 del artículo 88 del RLOPD establecen:

"Artículo 88. El documento de seguridad.

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.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento. " (El subrayado es de la AEPD)

En el presente supuesto, la infracción en materia de seguridad de datos recogida en el artículo 9 de la LOPD se vincula al presunto incumplimiento por parte de la CONSELLERIA de lo dispuesto en los artículos 89.2, 92.3 y 4 y 108 del RLOPD, los cuales establecen lo siguiente:

Artículo 89.2 "Funciones y obligaciones del personal".

"2.El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento."

Artículo 92.3 y 4 "Gestión de soportes y documentos".

"3. En el traslado de la documentación se adoptarán las medidas dirigidas a

evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.

4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.".

"Artículo 108. Custodia de los soportes.

Mientras la *documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada".*

Sintetizando las previsiones legales reseñadas en el anterior Fundamento de Derecho puede afirmarse que:

a) 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.

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 remite a normas reglamentarias.

d) El mantenimiento de ficheros,- cualquiera que sea la forma o modalidad de éstos-, programas o equipos carentes de las medidas de seguridad que impidan accesos o tratamientos no autorizados constituye una infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley.

V

Para una mejor comprensión de lo expuesto, resulta necesario acudir a los siguientes conceptos relacionados con los preceptos de la normativa de protección de datos anteriormente citados.

El artículo 3 de la LOPD acuña las siguientes definiciones:

"a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.

b) Fichero: Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: 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.

d) Responsable del fichero o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo."

"g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento."

"i) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado."

A su vez, las letras n), ñ) y o) del artículo 5.1 del RLOPD definen los siguientes conceptos*:*

"n) Fichero no automatizado: todo conjunto de datos de carácterpersonal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica."

"ñ) *Soporte: 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*".

"o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados."

La letra f) del artículo 5.2 del RLOPD define, en relación con lo dispuesto en el título VIII del mismo, como *"f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada."*

Con arreglo a dichas definiciones, las Tarjetas SIP localizadas en la vía pública contenían datos de carácter personal concernientes a sus titulares que permitían su identificación, tales como sus nombres y apellidos y números del Documento Nacional de Identidad (DNI), Tarjeta Sanitaria Individual (SIP) y Seguridad Social (SS).

Asimismo, el uso efectuado por la CONSEJERIA con la información de carácter personal incluida en las Tarjetas SIM supone un tratamiento de datos de carácter personal que cae bajo la órbita de la LOPD.

VI

La localización, el día 27 de noviembre de 2016, de las Tarjetas SIP procedentes del Centro de Salud "P.P.P." de Valencia a la altura del nº 8 de la C/ ***A.A.A.*** de esa misma Ciudad constituye la base de facto para fundamentar la infracción del artículo 9.1 de la LOPD.

Es evidente, y en este sentido se expresa en el Reglamento de Desarrollo de la LOPD, que las medidas de seguridad deben reflejarse en unos protocolos de actuación para el caso concreto que se proceda al desecho o destrucción de documentación, y que los mismos deben figurar en el documento de seguridad o en las instrucciones dictadas por el responsable del fichero y/o tratamiento. Entre tales medidas de seguridad deben contemplarse las dirigidas a impedir el acceso a los datos personales contenidos en los ficheros por parte de terceros,

Se alega por la CONSELLERIA que la presencia de tarjetas sanitarias en la vía pública el 27 de noviembre de 2016, frente al centro de Salud P.P.P., de Valencia, sólo puede interpretarse como un incumplimiento puntual y extraordinario en la aplicación de los protocolos establecidos para la retirada y destrucción de las tarjetas invalidadas.

Sin embargo, la aparición de dichas Tarjetas en la vía pública, junto a un contenedor de basura y sin destruir, pone de manifiesto que por parte del responsable del tratamiento no se prestó la diligencia necesaria en orden a hacer efectivas las medidas de seguridad que la CONSELLERIA había adoptado para garantizar la debida custodia de la documentación con datos de filiación, administrativos o clínicos de los pacientes que tenía que ser destruida, y que en este supuesto se recogían en el "*Protocolo de Recogida y Destrucción de Documentación con datos de carácter confidencial*" aportado por la CONSELLERIA al procedimiento. De hecho, las Tarjetas SIP en cuestión no se depositaron en el contenedor habilitado en el Centro de Salud "P.P.P." de Valencia para su posterior eliminación, sino que, conforme ha quedado acreditado, aparecieron tiradas en la vía pública el día 27 de noviembre de 2016 frente al citado Centro de Salud, junto con restos de material sanitario.

De lo que se colige que tanto las medidas de seguridad implantadas por la CONSELLERIA en el reseñado protocolo como las instrucciones que regulan determinadas actuaciones relacionadas con el uso normalizado de la tarjeta sanitaria SIP en los centros sanitarios, en las que se hace referencia a la destrucción de las Tarjetas Sanitarias Individuales (SIP), no han resultado efectivas para evitar que, en este supuesto concreto, los datos de carácter personal contenidos en las Tarjetas SIP localizadas en la vía pública el día 27 de noviembre de 2016 pudieran resultar accesibles a terceros

En cualquier caso, en esta materia se impone una obligación de resultado, que conlleva la exigencia de que las medidas implantadas deben impedir, de forma efectiva, el acceso a la información por parte de terceros. Esta necesidad de especial diligencia en la custodia de la información por el responsable ha sido puesta de relieve por la Audiencia Nacional, en su Sentencia de 11/12/08 (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 adoptan 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 Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable*." El mismo Tribunal razona que *"no basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa" sino que es preciso "que se ha empleado la diligencia que era exigible por quien aduce su inexistencia."* (STS 23 de enero de 1998).

Por lo que no cabe exonerar de responsabilidad a la CONSELLERIA inculpada.

A mayor abundamiento, con arreglo al criterio establecido por la Audiencia Nacional en diversas sentencias, no basta la adopción de cualquier medida, sino que deben ser las necesarias para garantizar con suficiente grado de eficacia la seguridad de los datos.

VII

El artículo 44.3.h) tipifica como infracción grave la siguiente: "*Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"*

En el presente caso ha quedado acreditado que la CONSELLERIA no adoptó las medidas de seguridad adecuadas para impedir el acceso a las mencionadas Tarjetas SIP por terceros no autorizados, ya que ha quedado probado que dicha documentación era visible para los viandantes que transitaban por la vía pública en la que se localizó por un vecino, conforme se informaba en las noticias de prensa.

Por ello, la citada CONSELLERIA resulta responsable de la vulneración del principio de seguridad en materia de protección de datos, que se encuentra recogido en el artículo 9 de la LOPD en su relación con lo previsto en los artículos 89.2, 92.3 y 108 del RLOPD, incurriendo, por tanto, en la infracción grave descrita.

VIII

En segundo lugar, procede valorar si por parte de la CONSELLERIA se ha producido una vulneración del deber de secreto con motivo de la revelación a terceros de la información de carácter personal contenida en las Tarjetas SIP tiradas en la vía pública, sin destruir, junto a un contenedor de basura situado enfrente del Centro de Salud "P.P.P." de Valencia.

El artículo 10 de la LOPD dispone "*El responsable del fichero y quienes intervengan en cualquier fase de tratamiento de los* datos *de carácter personal están obligados al secreto profesional respecto de los mismos y al 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*".

El deber de secreto tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, automatizados o no, se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así, el Tribunal Superior de Justicia de Madrid declaró: "*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 (...)".*

Este deber de confidencialidad obliga no sólo al responsable del fichero, sino a todo aquel que intervenga en cualquier fase del tratamiento y comporta, por lo que ahora interesa, que los datos personales registrados en soportes que deben ser tratados para su destrucción no puedan llegar a ser revelados o divulgados a ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Así, el artículo 10 de la LOPD contiene una regla que afecta a la confidencialidad y custodia de los datos de carácter personal, tratando de salvaguardar el derecho de las

personas a mantener la privacidad de tales datos y, en definitiva, el poder de control o disposición sobre los mismos. El deber de secreto trata de salvaguardar o tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal y en definitiva el poder de control o disposición sobre sus datos. Este deber de secreto está lógicamente relacionado con el secreto profesional. Según el ATC de 11 de diciembre de 1989 "*el secreto profesional se entiende como la sustracción al conocimiento ajeno, justificada por razón de una actividad, de datos o informaciones obtenidas que conciernen a la vida privada de las personas*". *El deber de secreto en el tratamiento de datos personales, tiene la misma fundamentación jurídica, pero se refiere al ámbito estricto del tratamiento de los datos personales, para que el responsable del fichero y, cualquier persona que intervenga en el tratamiento, esté obligado al mantener la confidencialidad de los datos personales*".

En este sentido, las SSAN, Sec. 1ª, de 14 de septiembre de 2002 (Rec.196/00), 13 de abril de 2005 (Rec. 230/2003), 18 de julio de 2007 (Rec. 377/2005) señalan respecto del deber de sigilo que "*es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000 (...) 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 los derechos fundamentales, como la intimidad o el derecho a la protección de datos que recoge el artículo 18.4 de la CE (...)*".

Analizados los hechos objeto del presente procedimiento y la documentación que lo integra, se concluye que resulta acreditada la concurrencia de culpabilidad en la conducta de la CONSELLERIA respecto de la vulneración del deber de secreto, puesto que no obró con la diligencia que le resultaba exigible al haber quedado acreditado que las medidas de índole técnica y organizativas adoptadas para garantizar la seguridad de los datos de carácter personal obrantes en los documentos o soportes destinados a ser destruidos no han evitado, en el presente caso, el acceso no autorizado a la información contenida en las Tarjetas SIP que estaban a la vista de todos los viandantes que transitaban por el lugar en que fueron localizadas, tiradas y sin destruir, siendo por ello completamente legible su contenido para estos viandantes. De hecho, en la noticia publicada el 12 de diciembre de 2016 en el Diario “M.M.M.” se menciona a “ B.B.B..” cómo uno de los vecinos que se encontró dichos documentos. (folio 2).

En consecuencia, la CONSELLERIA es responsable del tratamiento efectuado con dichos documentos, que aparecieron tirados junto a un contenedor de basura. Atendiendo a los hechos ocurridos, se comprueba la existencia de un incumplimiento del deber de secreto, produciéndose una ausencia de confidencialidad, ya que los datos contenidos en las referidas Tarjetas SIP fueron accesibles a terceros, por lo que se considera que se ha cometido una infracción del transcrito artículo 10 de la LOPD.

IX

La conducta descrita en el anterior Fundamento de Derecho se incardina en el artículo 44.3.d) de dicha norma, que considera como tal: “*La vulneración del deber de guardar secreto acerca del tratamiento de los datos de carácter personal al que se refiere el artículo 10 de la presente Ley*.”

En el procedimiento ha quedado acreditado el acceso de terceros no autorizados a los datos personales de los titulares de las Tarjetas SIP contenidos en las mismas. En relación con lo cual se destaca que el artículo 10 impone una obligación de

resultado, por lo que, conforme al criterio de la Audiencia Nacional, entre otras en la sentencia de 18/06/09, lo relevante es que se llegue a producir la divulgación de un secreto.

En el caso que nos ocupa, la CONSELLERIA es responsable de la custodia de esas Tarjetas SIP, constando que terceras personas han tenido acceso a dicha documentación, por lo que al haberse revelado a terceras personas la información contenida en dichos documentos se ha vulnerado el deber de secreto que incumbe a dicha CONSELLERIA como responsable de su custodia, habiendo ésta incurrido en la infracción grave del artículo 44.3.d) de la LOPD descrita al resultar responsable de la revelación a terceros de esa información sin el consentimiento de los afectados y sin mediar autorización legal para ello.

X

El artículo 46 de la LOPD, *"Infracciones de las Administraciones Públicas"*, dispone:

"1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores".

Sin embargo en el presente caso, no procede instar la adopción de medidas adiciones dadas las circunstancias que concurren, ya que se considera que las infracciones cometidas han tenido su origen en un error puntual y extraordinario acaecido en un determinado Centro de Atención Primaria que no siguió el protocolo de seguridad establecido por la CONSELLERIA para la recogida y destrucción de documentación con datos de carácter personal ni las instrucciones que regulan, entre otras actuaciones, la eliminación de las Tarjetas Sanitarias Individuales (SIP), cuyo cumplimiento hubiera evitado el acceso por terceros a las Tarjetas SIP localizadas el día 27 de noviembre de 2016, sin destruir, en la vía pública junto a un contenedor de basura.

Todo ello, sin perjuicio de la adopción de las medidas de seguridad y control que esa CONSELLERIA pueda adoptar para reforzar el seguimiento de las ya existentes y ampliar las cautelas referidas a la recogida y destrucción de documentación con datos de carácter personal especialmente protegidos.

Vistos los preceptos citados y demás de general aplicación,

La Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: Declarar que la **CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA DE LA GENERALITAT DE VALENCIANA** ha infringido lo dispuesto en el artículo 9.1 de la LOPD en su relación con lo previsto en los artículos 89.2 92.3 y 4 y 108 del RLOPD, tipificada como grave, en el artículo 44.3.h) de dicha norma.

SEGUNDO: Declarar que la **CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA DE LA GENERALITAT DE VALENCIANA** ha infringido lo dispuesto en el artículo 10 de la LOPD, tipificada como grave, en el artículo 44.3.d) de dicha norma.

TERCERO: NOTIFICAR la presente resolución a la **CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA DE LA GENERALITAT DE VALENCIANA**.

CUARTO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 46.4 de la LOPD.

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, se podrá 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 lo sucesivo LJCA), 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la LJCA, sólo podrá interponer 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 LJCA, 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