Revista de Bioética y Derecho
Perspectivas Bioéticas
www.bioeticayderecho.ub.edu - ISSN 1886-5887

ARTÍCULO

Infracciones de la Ley Orgánica de Protección de Datos en el ámbito sanitario. Descripción estadística de las infracciones

Infringements of the Organic Data Protection Law in the health area. Statistical description of the infringements

Infraccions de la Llei orgànica de Protecció de Dades en l'àmbit sanitari. Descripció estadística de les infraccions

MANUEL PALOMO NAVARRO *

* Manuel Palomo Navarro. Médico intensivista, Hospital de Sagunto, Valencia (España). E-mail mapana80@gmail.com.

Resumen

La Ley Orgánica de Protección de Datos (LOPD) es necesaria para garantizar el derecho a la intimidad reconocido en la Constitución Española. La gestión de los datos personales debe ser especialmente sensible en el ámbito sanitario por las características de los protegidos. Este trabajo revisa las resoluciones dictadas desde el 28 de octubre de 2005 hasta el 29 de octubre de 2018 por la Agencia Española de Protección de Datos (AEPD), agrupando las infracciones por frecuencia de infracción y describiendo las peculiaridades de algunas resoluciones. En la medida de la información aportada por la denuncia, se trata de valorar la intención de la misma.

Palabras clave: protección de datos; ámbito sanitario; infracciones LOPD.

Abstract

The Organic Law on Data Protection (LOPD) is necessary to guarantee the right to privacy recognized in the Spanish Constitution. The management of personal data must be especially sensitive in the health field due to the characteristics of the protected persons. This paper reviews the resolutions issued from October 28 2005 to October 29 2018 by the Spanish Agency for Data Protection (AEPD), grouping the infractions by frequency of infringement and describing the peculiarities of some resolutions. To the extent of the information provided by the complaint, the aim is to assess its intention.

Keywords: data protection; health area; infringement data protection law.

Resum

La Llei Orgànica de Protecció de Dades (LOPD) és necessària per a garantir el dret a la intimitat reconegut en la Constitució Espanyola. La gestió de les dades personals ha de ser especialment sensible en l'àmbit sanitari per les característiques dels protegits. Aquest treball revisa les resolucions dictades des del 28 d'octubre de 2005 fins al 29 d'octubre de 2018 per l'Agència Espanyola de Protecció de Dades (AEPD), agrupant les infraccions per freqüència d'infracció i descrivint les peculiaritats d'algunes resolucions. En la mesura de la informació aportada per la denúncia, es tracta de valorar la intenció d'aquesta.

Paraules claus: protecció de dades; àmbit sanitari; infraccions LOPD.

1. Introducción

En 1992 fue aprobada la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) Ley Orgánica 5/1992. Esta fue la primera ley que, basándose en el artículo 18.4 de la Constitución Española, desarrolla las herramientas para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos y definió, por primera vez en España, los datos de carácter personal y la identificación del afectado.

La Ley Orgánica de Protección de Datos (LOPD), también conocida como Ley 15/1999, fue aprobada el 13 de diciembre de 1999 por las Cortes españolas, derogando la LORTAD. La LOPD se ampara en:

- Constitución Española: en su artículo 10 reconoce el derecho a la dignidad de la persona. Por su parte, el artículo 18.4 dispone que la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno de sus derechos.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995: relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos.

La LOPD se desarrolla en:

- Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (RLOPD).
- Reglamento(UE) 2016/679 (RGPD) del Parlamento Europeo y del Consejo de 27 de abril de 2016, que entró en vigor en España el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018.

En esta revisión, la AEPD no aplica la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. En el título II de dicha ley se desarrollan los principios de protección de datos, siguiendo la línea de la LOPD. En el título III, IV y V se desarrollan otros derechos y deberes que podrían afectar en la dirección de las resoluciones emitidas y revisadas en este artículo.

2. Justificación

El ámbito sanitario es el lugar real o virtual donde desempeña su trabajo el personal sanitario. La Organización Mundial de la Salud (OMS) define como personal sanitario a: "todas las personas que llevan a cabo tareas que tienen como principal finalidad promover la salud".

Al desarrollar su trabajo con los pacientes, la información generada por los trabajadores de la salud se caracteriza por su sensibilidad y es un derecho fundamental de los ciudadanos tanto su salud o enfermedad, así como la privacidad de sus datos y la información que se genere de su procesamiento.

Por esto, el manejo de la información generada en el ámbito sanitario es complejo. La ingente cantidad de datos debe fluir entre los profesionales de un modo eficiente para garantizar una atención óptima del paciente. El flujo y custodia de información son responsabilidad de todo el personal sanitario.

La LOPD y el RGPD se aplican al ámbito sanitario para proteger la información que se pueda generar derivada de la actividad sanitaria, ya sea privada o pública.

3. Metodología

Se revisarán las 201 resoluciones administrativas dictadas por la AEPD en el ámbito sanitario desde el 28 de octubre de 2005 hasta el 29 de octubre de 2018. Se analizarán algunas de las resoluciones, los artículos infringidos, la dirección de las resoluciones y las infracciones más frecuentes. En la medida de la accesibilidad a la información, se analizará quién las comete y la intencionalidad de las mismas.

Para realizar esta valoración estadística se ha consultado la página web de la AEPD (www.aepd.es) y se han extraído las 201 resoluciones dictadas en el campo de la sanidad sobre la LOPD (Ley Orgánica 15/1999). Se ha acotado a las resoluciones dictadas desde el 28 de octubre de 2005 hasta el 29 de octubre de 2018, del ámbito sanitario y que hayan infringido la LOPD. Se han elegido estas fechas porque es este periodo el máximo rango de fechas que permite el buscador de la página web de la AEPD.

4. Resultados

Se han encontrado un total de 201 resoluciones. En algunas se demuestra la infracción de diferentes artículos o de párrafos específicos de los mismos. En las 201 resoluciones se han infringido un total de 20 artículos (o algún párrafo específico del mismo). Como en algunas resoluciones se ha infringido más de un artículo, la incidencia acumulada es de 221, distribuidos de la siguiente manera:

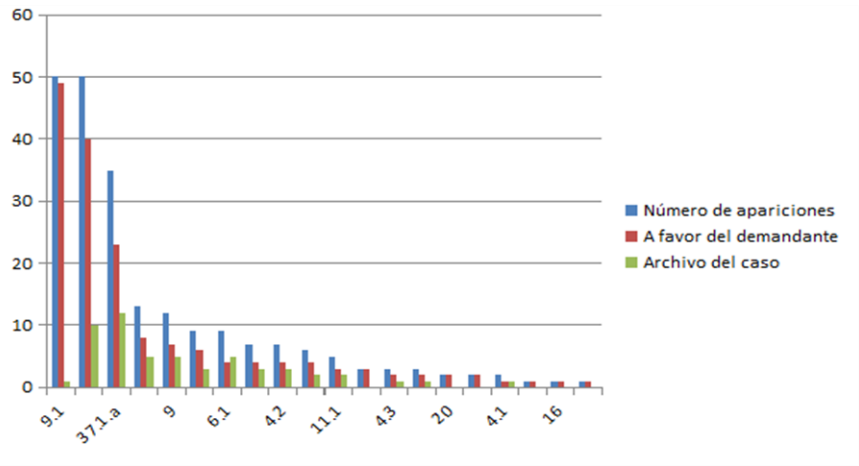

Ilustración 1: Distribución de las infracciones a la LOPD

A continuación, se revisan las infracciones agrupadas:

Infracciones agrupadas

Artículo	Nº de apariciones	A favor del demandante	Archivo del caso
9.1	50	49	1
10	50	40	10
37.1.a	35	23	12
6.1	13	8	5
9	12	7	5
7.3	9	6	3
6.1	9	4	5
6	7	4	3
4.2	7	4	3
5	6	4	2
11.1	5	3	2
37.1.f	3	3	0

4.3	3	2	1
5.1	3	2	1
20	2	2	0
15	2	2	0
4.1	2	1	1
26	1	1	0
16	1	1	0
4	1	1	0

Artículo 9. Seguridad de los datos

Este artículo desarrolla el principio básico de la LOPD de seguridad de los datos.

> *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.*

La infracción del artículo 9 es la más frecuente, especialmente por las infracciones de su primer párrafo.

Hay un total de 62 resoluciones y el fallo ha ido a favor del demandante en un 90,3% de las veces.

Estos datos nos dan una idea sobre la preocupación de la población en general sobre la protección de sus datos y sobre la sensibilidad de la agencia en su fallo a favor del demandante.

La infracción de las mismas se han considerado prácticamente en su totalidad como faltas graves.

Un ejemplo de infracción de este artículo se da en esta resolución. Una mujer (la demandante) presentó en una oficina Caixabank (la denunciada) la documentación que le fue requerida para gestionar la tramitación del rescate de un plan de pensiones, entre la cual se incluían informes médicos, historial clínico y tratamientos seguidos. La situación de salud de la paciente cumplía los criterios para el rescate. Posteriormente, la denunciante tuvo conocimiento tanto del extravío de dicha documentación como de que debía volver a presentar la información aportada. Fue la propia entidad bancaria la que le comunicó por carta que la documentación aportada en la oficina no había llegado al departamento correspondiente. Para realizar el trámite bancario en cuestión, Caixabank tiene un procedimiento establecido que la denunciante cumplió: cumplimentar y enviar el formulario correspondiente, imprimir el formulario enviado y junto a la documentación del expediente incluirlo en sobre blanco, indicar en el frontal del sobre blanco el producto y tipo de contingencia y enviar inmediatamente el sobre blanco cerrado a través del sobre de valija al Departamento de Operaciones - Planes de Pensiones (042 -5504). Hasta que se hace este envío por valija, el sobre con la documentación se custodia en la oficina bajo llave, según determina la LOPD. Los empleados no tienen acceso a esta documentación y son los propios clientes los que introducen la documentación en los sobres. La entidad bancaria aceptó que hubo algún error en el envío del sobre blanco mediante valija y no llegó a su destino en el tiempo previsto, pero alegan que ello no significa que el sobre haya sido extraviado y que no se haya garantizado la seguridad de los datos, sino que ha habido una incidencia en el envío normal del sobre y el mismo llegará con retraso a su destino. Los hechos probados de esta resolución muestran que la entidad no garantizó la seguridad de los datos pues hubo un extravío de la documentación. La resolución fue a favor de la demandante.

Artículo 10. Deber de secreto

Este artículo desarrolla el principio básico de la LOPD del deber de secreto.

> *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.*

No hay que confundir el deber de secreto de los intervinientes en el manejo de ficheros y datos con los medios técnicos y organizativos que se hacen referencia en el artículo 9 de la LOPD que garantizan la seguridad del soporte de la información y de sus circuitos.

De las 50 veces que se hace referencia en la búsqueda del artículo 10, el 80% de las veces el fallo va a favor del demandante. La condición para esto es la demostración en hechos probados de

la revelación de información, ya sea de forma accidental como de forma intencional. Estas son tipificadas como faltas graves.

Un ejemplo de violación del deber de secreto es cuando una mujer (la demandante) se realizó una revisión médica en un centro privado de Madrid. Al día siguiente, en el fax del trabajo de la demandante (un colegio de Ciudad Real), se recibió el justificante de asistencia a dicha prueba y el servicio que la atendió. No hubo petición de la demandante de tal documentación. Tras investigación por la AEPD, se concluyó que había habido una tercera persona que, actuando de mala fe, solicitó la documentación. La agencia que se encargaba de la gestión de las llamadas (Call Center) entendió que la persona que actuaba de mala fe era la demandante, confusión que se aprovechó para solicitar dicha documentación. Se apercibió a la empresa médica por no garantizar el deber de secreto y se le instó a desarrollar un protocolo para la solicitud de datos e informes, de modo que no pudiesen ser solicitados por terceras personas sin autorización de la persona interesada.

Artículo 37. Funciones: Artículo 37.1.a y f

Este artículo rige las funciones de la AEPD. 38 resoluciones fueron emitidas en 2010, a expensas de las infracciones del apartado 1.a y 1.f.

> *1. Son funciones de la Agencia de Protección de Datos:*
>
> *a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.*
>
> *b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.*
>
> *c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.*
>
> *d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.*
>
> *e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.*
>
> *f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.*

g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

k) Redactar una memoria anual y remitirla al Ministerio de Justicia.

l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.

n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

2. Las resoluciones de la Agencia Española de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos. Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones. Lo establecido en los párrafos anteriores no será aplicable a las resoluciones referentes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos ni a aquéllas por las que se resuelva la inscripción en el mismo de los Códigos tipo, regulados por el artículo 32 de esta ley orgánica.

Este artículo es el que permite requerir a los diferentes entes, ya sean públicos o privados, la toma de medidas para salvaguardar la información de la que son responsables. Es la propia AEPD la que actúa como demandante a raíz de la no comunicación de los diferentes entes a la propia Agencia de las medidas que han tomado para ajustarse a la Ley.

En este caso, el fallo fue a favor del demandante en un 68,4% de las resoluciones, esto es, en 2010 los entes denunciados no se había adecuado a las exigencias de esta Ley. Respecto a las

causas archivadas (31,6%), lo fueron porque sí que se habían adecuado pero no lo habían comunicado.

Artículo 6. Consentimiento del afectado

El artículo 6 desarrolla un principio básico de la LOPD, el principio de consentimiento. El afectado tiene el control de sus datos.

> *1. 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.*
>
> *3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.*
>
> *4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable de fichero excluirá del tratamiento los datos relativos al afectado.*

Los supuestos que se dan en la infracción de este artículo (16 resoluciones que incluyen al artículo 6 en su totalidad o específicamente al 6.1) tienen su origen en el uso de los datos del paciente para un fin por el que no fueron dados. Un ejemplo común es el uso por parte de un facultativo (público o privado) de datos de contacto para continuar con la asistencia en otro centro o consulta.

Otro ejemplo de la infracción de este artículo se explica a continuación: Una mujer (la demandante) denuncia ante la AEPD que hay entradas reiteradas en su historial médico de atención primaria por parte de un médico que no es su médico de cabecera. Las entradas a su

historia de salud las está realizando su exmarido. No había registro del consentimiento a estas actuaciones.

De las 16 resoluciones, el 50% fueron a favor del demandante. El 50% fue archivado porque el uso de los datos estaba en relación con el apartado 2 del artículo 6: "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".

Artículo 4. Calidad de los datos

El artículo 4 desarrolla el principio básico de la calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Ha habido 13 resoluciones sobre posibles infracciones de este artículo, de las cuales el 61,5% han sido a favor de la parte demandante y un 38,5% archivadas.

Las infracciones vienen dadas tanto por la constancia en la historia clínica de diagnósticos obsoletos que siguen en vigor, o incluso erróneos que no se han corregido y siguen apareciendo en registros sucesivos del paciente. También se ha dado la infracción de este artículo en su párrafo 1, por el hecho de aparecer en un justificante de ingreso la causa del mismo, como el que se refleja en la resolución contra el hospital Virgen de la Macarena, en la que la cuñada de la demandante solicitó un justificante de hospitalización a su entrada por Urgencias y constaba como causa de ingreso "parto".

Artículo 7. Datos especialmente protegidos

Este artículo desarrolla el principio básico de los datos especialmente protegidos. En el caso de los datos relacionados con la salud, sólo pueden ser recabados, tratados y cedidos con el consentimiento expreso del paciente.

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Las nueve resoluciones emitidas se han dado por infracción del párrafo 3. En seis de ellas, se ha fallado a favor del denunciante por cesión de datos a otras entidades sin consentimiento del afectado. Las tres causas archivadas obedecían a la excepción contemplada en el párrafo 6.

Fuera del ámbito sanitario, también se producen infracciones de la LOPD relacionadas con materias de salud. Un ejemplo de esto es la resolución a favor de la demandante por el incorrecto tratamiento de la información dada en sobre cerrado por una incapacidad temporal. Una empleada de la limpieza de un ayuntamiento presentó en sobre cerrado en el que constaba "Servicio Médico Exclusivamente, contiene Información Clínica" el parte de baja con el diagnóstico que va dirigido al servicio médico (según el modelo: "Parte médico de baja de incapacidad temporal por contingencias comunes" dirigido al Servicio Aragonés de Salud, Atención Primaria Huesca). El correcto protocolo consiste en enviar el parte de baja que se adjunta al sobre, por fax, a la asesoría laboral que gestiona el personal de servicios del ayuntamiento. Posteriormente, se envía por correo ordinario el sobre cerrado. En este caso, la persona que se encarga de estos trámites en el ayuntamiento estaba de vacaciones y la persona sustituta en sus funciones abrió el

sobre y envió su contenido por fax a la asesoría, generando un documento que se adjuntó a los archivos del ayuntamiento.

Los datos sobre la salud son datos especialmente protegidos. Todas las entidades o personas deben manipular estos datos con el consentimiento expreso. En este ejemplo, hubo manipulación física de la información (apertura del sobre) y almacenamiento de las copias generadas al enviarlas por fax.

Artículo 5. Derecho de información en la recogida de datos

Este artículo desarrolla el principio básico de información de recogida de datos. Todos los ciudadanos tienen derecho a saber la información que se ha recabado sobre ellos, el uso que se da a esa información y de quién se ha recabado esa información.

> *1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:*
>
> *a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.*
>
> *b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.*
>
> *c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.*
>
> *d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.*
>
> *e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.*
>
> *Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.*
>
> *2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.*

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

De las seis resoluciones, cuatro fallaron a favor del demandante. Estas se debieron a los impedimentos que pusieron diferentes empresas de prestaciones de servicios sanitarios al control de los datos sanitarios por parte de los demandantes. Tipificadas como leves, las empresas fueron sancionadas con multas desde 2000€.

En las dos resoluciones archivadas, se advertía que no existía una cláusula clara en la que se incluyera la identificación del responsable del fichero ni el domicilio para el ejercicio de los derechos de acceso, rectificación y cancelación. La modificación durante el proceso archivó las causas.

Un ejemplo de infracción de este artículo se ve en esta resolución. Una paciente precisa de los servicios de Urgencias de la entidad Hospital USP Costa Adeje. En el servicio de admisión le informan que debe firmar una cláusula de protección de datos, donde al parecer, se contemplaba la posibilidad de ceder sus datos a terceros, motivo por el cual la denunciante se niega a firmar, puesto que no se da la opción de firmar la cláusula de protección de datos negándose a ceder los datos a terceros. En la inspección del caso por la AEPD, la entidad denunciada explicó que hay un

documento de oposición a la cesión de datos, que se adjunta si se solicita. Tras la exposición de los hechos, en los que la entidad denunciada explica que se ha optado por esta fórmula para agilizar los procesos administrativos, la AEPD aclara que: "resulta mucho más rápido la inclusión de una casilla que permita manifestar expresamente al afectado su negativa al tratamiento ya mencionada en el documento que se le entregue para la celebración del contrato."

Artículo 11. Comunicación de datos

Este artículo no regula un principio básico, sino la gestión de la transmisión de datos y los consentimientos necesarios para la misma. Las resoluciones dictadas están en relación con el párrafo 1.

> *1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*
>
> *2. El consentimiento exigido en el apartado anterior no será preciso:*
>
> *a) Cuando la cesión está autorizada en una ley.*
>
> *b) Cuando se trate de datos recogidos de fuentes accesibles al público.*
>
> *c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.*
>
> *En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.*
>
> *d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.*
>
> *e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.*
>
> *f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.*

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

De las cinco resoluciones, tres fallaron a favor del denunciante por ceder datos a terceros sin consentimiento del usuario ni conocimiento del mismo. Las tres se relacionaron con transferencia de información de mutua a empresa sin expreso consentimiento del usuario/paciente. A pesar de ser una práctica habitual, no eximen a mutua y empresa de solicitar el consentimiento para la comunicación de los datos de los usuarios, no pueden compartir los datos libremente. En las dos que fueron archivadas, la comunicación de datos, a pesar de no ser deseada por el usuario se realizaban conforme a la ley.

Un ejemplo de infracción se expone a continuación. La entidad MMC (Mutua de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social) suministró datos personales de un ex trabajador de la mutua a la entidad SANITAS tras agotar la póliza de seguro médico suscrita con ADESLAS. Hubo una negociación en la que se incluyó unas mejores condiciones para los ex empleados y por un error en la confección de la lista de personas protegidas en el anterior seguro que deseaban acogerse al nuevo. Se califica como error, por cuanto no se tenía constancia de la voluntad inequívoca del propio denunciante de consentir en la comunicación de sus datos a la nueva entidad.

Artículo 15. Derecho de acceso

Este artículo regula acceso a la información del usuario de sus datos, como una extensión del artículo 5 (derecho a la información recogida).

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

En las dos resoluciones sobre este artículo se falló a favor del demandante.

Artículo 20. Creación, modificación o supresión

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

En dos ocasiones las Administraciones Públicas fueron denunciadas y condenadas por la AEPD por modificar ficheros sin cumplimentar los requisitos de la ley. Fueron instruidos por la propia AEPD y en sus resoluciones se dicta también la infracción del artículo 5: se vulnera el derecho a la recogida de datos por la modificación de los ficheros.

Artículo 16. Derecho de rectificación y cancelación

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

En la resolución dictada por la AEPD a raíz de una denuncia de un usuario, se condenó al Centro de Hemoterapia y Hemodonación de Castilla y León por no respetar el derecho de cancelación que el usuario quiso hacer efectivo. No hubo sanción económica pero se deja abierta la vía contencioso-administrativa.

Artículo 26. Notificación e inscripción registral

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Este caso fue instruido por la propia AEPD, por personal del equipo provincial de Cádiz de Inspección de Prestaciones y Servicios Sanitarios contra un centro médico privado por no haber dado de alta sus ficheros en el Registro General de Protección de Datos. Se le sanciona con una multa y se le insta a la regulación de sus ficheros conforme a la LOPD.

5. Conclusiones

La LOPD es efectivamente una herramienta útil en la protección de los datos de los usuarios y especialmente en el ámbito sanitario.

De las 201 resoluciones, el 78,1% de ellas están relacionadas con infracciones de los principios básicos.

La protección de los principios básicos (seguridad de los datos, deber de secreto, consentimiento, calidad de los datos, datos especialmente protegidos, información de la recogida de datos) de esta ley parece estar asegurada en el ámbito sanitario, a nivel administrativo, por la Agencia Española de Protección de Datos pues corresponde al grueso de sus resoluciones en sanidad.

En aquellos casos en los que ha habido mínimo conflicto por la revelación de información a terceros, la AEPD ha sido categórica fallando a favor del demandante, independientemente de la intención del demandante.

Es la intencionalidad del demandante donde se ha podido ver un uso poco convencional de la LOPD.

En lo referente a la intencionalidad, se exponen dos ejemplos:

- En una sentencia relacionada con el artículo 10, un pediatra fue denunciado por su expareja por enviar algunos mensajes vía *WhatsApp* a la demandante (cuando aún mantenían una relación) con fotografías de su dietario explicando que aún tenía trabajo por acabar. Al poderse distinguir en las fotos los nombres y otros datos administrativos de los pacientes, el pediatra fue multado por la AEPD. Efectivamente, se infringe la LOPD pero la intención de la demandante no es la protección de los afectados.
- En otra sentencia relacionada con el artículo 9, un cirujano fue demandado por una paciente, que firmó un consentimiento para que se grabara su operación con fines docentes y de investigación. Dos años más tarde, la paciente le requirió al cirujano una copia de su intervención. El cirujano respondió, vía correo electrónico, que no podía darle una copia pues el video se había añadido de forma fragmentada una base de datos del hospital y, al estar anonimizada, no podría encontrar su operación. Añadió en el mismo correo que el no sabía donde podría estar el archivo original porque cree que sus hijos estropearon el soporte del mismo (*pendrive*). El cirujano fue multado y en su reclamación sólo disminuyó el importe de la multa, pues consiguió demostrar que aunque no dispusiera del archivo original no había forma alguna de relacionar las imágenes con la paciente.

Podemos concluir que la LOPD y su brazo ejecutor, la AEPD, son extremadamente sensibles a la protección de los principios básicos. Es de esperar que la aplicación del Reglamento UE 2016/679 de 27 de abril de 2016 le permita mayor sensibilidad. Puede ser que el punto pendiente de la LOPD es la valoración de la intencionalidad del demandante.

Bibliografía

- Resoluciones de la Agencia Española de Protección de Datos, 2018 https://www.aepd.es/es/informes-y-resoluciones/resoluciones.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Publicada en: Boletin Oficial del Estado número 298, de 14/12/1999. España.
- Ley Orgánica 5/1992, de 31 de octubre de 1992, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD). Boletin Oficial del Estado número 262, de 31/10/1992. España.
- Real Decreto 1720/2007, de 21 de diciembre, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal (RLOPD). Publicada en: Boletín Oficial del Estado número 17, de 19/01/2008. España.
- Reglamento General de Protección de Datos (UE) 2016/679 (RGPD) Del Parlamento Europeo y del Consejo de 27 de abril de 2016. Publicada en: Diario Oficial de la Unión Europea número 119, de 4/5/2016. Europa.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos. Publicada en: Diario Oficial de las Comunidades Europeas número 281, de 23/11/1995. Europa.
- Constitución Española de 1978. Publicada en: Boletín Oficial del Estado número 311, de 29/12/1978.

Fecha de recepción: 14 de octubre de 2019

Fecha de aceptación: 12 de diciembre de 2019