La protección de datos sanitarios

PID_00248572

Unai Aberasturi Gorriño

Tiempo mínimo de dedicación recomendado: 4 horas

Universitat Oberta de Catalunya

Índice

1. Introducción. E-salud y derecho

1.1. La e-salud como fenómeno consolidado en la realidad actual

Es una idea conocida y reiterada que la incorporación ya generalizada de las tecnologías de la información y la comunicación (TIC) a todos los ámbitos de la vida ha supuesto un cambio radical en la manera de relacionarse de las personas. El valor principal de las TIC lo constituye la creación de una nueva forma de utilizar información. Esta nueva posibilidad afecta irremediablemente a diversos derechos fundamentales, entre los que debe destacar el derecho a la protección de datos de carácter personal o derecho a la autodeterminación informativa. La necesidad de salvaguardar este derecho es una realidad cada vez más evidente tanto para la ciudadanía como para el legislador. Por un lado, conceptos como el *scoring*, el *big data*, el *data mining*, etc. son cada vez más conocidos, y las denuncias ante las diferentes agencias de protección de datos son también cada vez más. Por otro lado, la actividad del legislador, autonómico, estatal o europeo, ha sido prolija en los últimos veinticinco años.

La preocupación por que el derecho a la autodeterminación informativa se proteja de manera eficiente ha sido especialmente alta en determinados sectores que, por las características de la información que se utiliza, son verdaderamente sensibles. Así ha sido en el ámbito sanitario. Es evidente que las personas otorgan especial relevancia a los datos relativos a su salud, sobre todo cuando se refieren a enfermedades especialmente estigmatizadas. Esta situación se ha ido acentuando en la medida en que han sido constantes los adelantos en materias como la genética, la reutilización de la información sobre la salud, el internet de las cosas médicas (caso de la monitorización a distancia de pacientes crónicos o de dispositivos que se pueden vestir y que remiten información sobre la salud de las personas a plataformas que pueden estar en la nube) o el *big data* sanitario[1] (Comisión Europea, 2016; Serrano, 2015). En este contexto, poder controlar lo que sucede con los datos de salud de cada uno constituye un objetivo de primer orden. Más en la actualidad, cuando los ciudadanos reclaman cada vez mayor autonomía y poder de disposición de su salud.

[(1)]Véase, por ejemplo, el Programa Público de Analítica de Datos para la Investigación y la Innovación en Salud-PADRIS en Cataluña, o el proyecto MIDAS en el que participa el Servicio Vasco de Salud.

Referencias bibliográficas

Comisión Europea (2016). «Informe de la Comisión Europea, Study on Big Data in Public Health». *Telemedicine and Healthcare*.

M.ª Mercedes Serrano Pérez (2015). «*Big data* o la acumulación de datos sanitarios: derechos en riesgo en el marco de la sociedad digital». *Derecho y Salud* (núm. 25).

En la práctica sanitaria el tratamiento de datos resulta una actividad esencial. La protección de la salud de las personas exige del tratamiento constante de datos, desde que se nace, incluso antes de nacer, hasta que se muere, incluso después de haber muerto (High Level Committe on Health, 2003). La práctica totalidad de las tareas que se desarrollan en este ámbito requieren de información veraz, completa y actual sobre los usuarios del sistema sanitario. Pues bien, el tratamiento de estos datos es en este sector una tarea cada vez más compleja por diferentes motivos, a saber: la población cada vez envejece más, la movilidad de la ciudadanía es cada vez mayor, cada vez aparecen más fuentes de datos (caso de la genética), la especialización es también cada vez mayor, etc. La gestión de toda esta información sanitaria reclama de instrumentos que hagan posible un flujo ágil y eficiente de la misma, y que pongan a disposición de los profesionales que lo requieran, cuándo, cómo y dónde lo requieran, los datos que precisan para desarrollar sus tareas. La conocida como «salud electrónica» o «e-salud» ha evolucionado sobremanera (Pérez, 2017). El impulso de las nuevas tecnologías en el ámbito de la sanidad ha llevado a que hoy día se hable de la «telemedicina» de una manera más o menos normalizada. La telemedicina, en sentido estricto, se refiere a la práctica de la medicina a distancia. Sin embargo, en un sentido amplio lo relevante no es tanto la distancia entre el paciente o usuario y el profesional de la sanidad, sino el que se empleen las nuevas tecnologías en la práctica de la medicina. Se trataría de una nueva manera de ejercer la medicina en la que lo característico es la aplicación de las TIC en el proceso asistencial, de gestión, de investigación, de fomento, etc. como sinónimo de la e-salud (Sánchez y Abellán, 2002).

Referencias bibliográficas

High Level Committe on Health (2003, 1 de abril). *Health Telematics Working Group of the High Level Committe on Health: Final Report*.

Juan Francisco Pérez Gálvez (dir.) (2017). *Salud Electrónica. Perspectiva y Realidad*. Valencia: Tirant Lo Blanch.

Javier Sánchez Caro; Fernando Abellán (2002). *Telemedicina y protección de datos sanitarios*. Granada: Comares.

Conscientes de las oportunidades que presenta esta nueva manera de gestionar la salud, son muchas las iniciativas que se han adoptado desde diferentes instancias a este respecto. En el ámbito de la UE, el Plan Estratégico Europa 2020[2] incluye distintas iniciativas siguiendo lo establecido en el Plan de acción a favor de un Espacio Europeo de la Salud Electrónica[3], que tiene como uno de los principales objetivos la interoperabilidad de los diferentes sistemas de

(2)Comunicación de la Comisión, de 3 de marzo de 2010, denominada «Europa 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador» [COM(2010) 2020 final.

información sanitaria de los distintos Estados miembros[4]. En el ámbito estatal, en el marco del plan Agenda Digital para España, el plan de Servicios Públicos Digitales, se incluye el objetivo de avanzar en un programa de salud electrónica que posibilite un intercambio de datos sanitarios eficaz entre los diferentes sistemas sanitarios de las diferentes comunidades autónomas.

(4)Recomendación de la Comisión, 2 de julio de 2008, sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos.

La evolución de la telemedicina puede observarse si se atiende al desarrollo que han experimentado herramientas concretas como la historia clínica electrónica, la tarjeta sanitaria electrónica y la receta electrónica.

1) La historia clínica es la herramienta más importante en la prestación del servicio sanitario al ser un conjunto de datos cuyo empleo es esencial para la consecución de fines asistenciales, de investigación, estadísticos, de docencia, administrativos, de gestión económica, etc. Para que los profesionales puedan acceder a esta información de manera sencilla y ágil, el desarrollo de la HC electrónica ha constituido un adelanto esencial. Se trata de una infraestructura para introducir, procesar, almacenar y tratar información a través de vías electrónicas, integrándose con aplicaciones y bases de datos interrelacionadas. Se caracteriza por que la inclusión de la información deja de ser pasiva para el usuario e incluso para terceros, constituyendo un sistema interoperable y permitiendo la incorporación de datos de salud que no haya sido generada en un centro sanitario. Además, la apuesta por la historia de salud electrónica corre paralela con la configuración de una historia clínica única que se cita en las propias normas[5].

2) La tarjeta sanitaria electrónica es otra herramienta de gran relevancia práctica por cuanto es el instrumento por el que los usuarios se identifican frente al sistema sanitario[6]. Si la e-salud pretende que la información sanitaria fluya por las redes a fin de que los usuarios puedan obtener el servicio sanitario en cualquier momento y lugar, la tarjeta deberá permitir esa identificación en diferentes sistemas de información[8]. Hay distintos tipos de tarjetas: las que simplemente se dirigen a identificar al paciente, las magnéticas (que además de identificar constituyen la llave de acceso a la información del paciente), las tarjetas electrónicas de memoria (almacenan datos pero no contienen microprocesador), y las tarjetas electrónicas inteligentes o *smartcards* (además de almacenar datos, contienen un microprocesador). La incorporación de las tarjetas inteligentes al ámbito de la sanidad se está produciendo en la actualidad[7]. Las posibilidades que ofrecen estas tarjetas pueden ser útiles para el caso, por ejemplo, en el que el acceso a la historia de salud en red es más difícil. Esta

(3)Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, «La salud electrónica-hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica, 30 de abril de 2004 y Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI». Ver también el Informe 5 de diciembre de 2013, sobre el Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI. Resolución del Parlamento Europeo, de 14 de enero de 2014, sobre el Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI.

(5)Por ejemplo, artículo 4 Decreto 38/2012, 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

(6)Art. 57 Ley 16/2003, 28 de mayo de 2003, de cohesión y calidad del Sistema Nacional de Salud. Art. 2 RD 183/2004, 30 de enero de 2004, por el que se regula la tarjeta sanitaria individual. Las leyes vigentes fijan la necesidad de crear tarjetas sanitarias que posibiliten la asistencia sanitaria en cualquier punto del Estado. De esta manera, se obliga a crear tarjetas compatibles con los sistemas del Sistema Nacional de Salud y de las comunidades autónomas, y también con los criterios marcados desde la UE.

(7)COM (2003) 73 final. DA Única RD 183/2004 30 de enero, regula la tarjeta sanitaria individual.

opción afecta al derecho a la protección de datos, lo que ha llevado a que en algún momento las agencias de protección de datos hayan cuestionado su virtualidad (*Jano on-line*, 2003).

(8)Decisión núm. 189 de la Comisión Administrativa para la Seguridad Social de los Trabajadores Migrantes (CASSTM), de 18 de junio de 2003, dirigida a sustituir por una tarjeta sanitaria europea los formularios necesarios para la aplicación de los Reglamentos (CEE) núm. 1408/71 y (CEE) núm. 574/72 del Consejo en lo que respecta al acceso a la asistencia sanitaria durante una estancia temporal en un Estado miembro distinto del Estado competente o de residencia; Decisión núm. 190 de la CASSTM, de 18 de junio de 2003, relativa a las características técnicas de la tarjeta sanitaria europea; Decisión núm. 191 de la CASSTIM, de 18 de junio de 2003, relativa a la sustitución de los formularios E 111 y E 111B por la tarjeta sanitaria europea.

3) La receta electrónica es otro proyecto de gran alcance. La receta médica incluye la información necesaria, no solo datos de salud[9], para que un paciente pueda hacerse con un medicamento concreto prescrito por un profesional sanitario[10]. La receta electrónica implica que ese proceso se llevará a cabo a través de medios electrónicos. Se supone que con este sistema el médico prescribe la receta a través del ordenador, esta va a una base de datos a la que está conectado el farmacéutico, quien tiene acceso a la misma a través de la tarjeta sanitaria electrónica o magnética del paciente. La receta electrónica se ha venido incorporando por el legislador tanto estatal como autonómico[11].

(11)Art. 33.2 Ley, 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud; Art. 77.8 Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios. RD 1718/2010, de 27 de diciembre de 2010, sobre receta médica y órdenes de dispensación; Decreto 181/2007, de 19 de junio, por el que se regula la receta médica electrónica, de la comunidad autónoma de Andalucía; Decreto 159/2007, de 24 de julio, por el que se regula la receta electrónica y la tramitación telemática de la prestación farmacéutica a cargo del Servicio Catalán de Salud, reformado por el Decreto 91/2009, de 9 de junio, por el que se modifica la letra h) del artículo 2 del Decreto 159/2007, de 24 de julio, y desarrollado por la Orden SLT/72/2008, de 12 de febrero; Decreto 93/2009, de 24 de abril, por el que se regula la implantación de la receta electrónica en el ámbito del Sistema Sanitario Público de Extremadura; Decreto 206/2008, de 28 de agosto, sobre receta electrónica, Galicia.

La aplicación de las TIC en el ámbito sanitario conlleva innumerables ventajas que son de sobra conocidas: sistemas de comunicación que posibilitan una relación más ágil, continua y directa entre profesionales y entre estos y los usuarios; una mayor integración de la información de los usuarios, lo que evita su aislamiento y las duplicidades, posibilitando una mejor y más eficiente organización de los datos; un fácil acceso a la información desde cualquier lugar y en cualquier momento; un más fácil control de los accesos y tratamiento de los datos, etc. (Wilson, Leitner y Mousalli, 2004). Sin embargo, frente a estas ventajas también se plantean inconvenientes o retos (Méjica, 2002), a saber: las dificultades técnicas para implantar sistemas de información interoperables; la necesidad de garantizar la seguridad de la información a fin de salvaguardar la confidencialidad de los datos; la dificultad de configurar un marco normativo suficientemente claro y preciso que otorgue cobertura jurídica a los diferentes flujos de datos que se plantean, etc. (AEPD, 2010).

Referencias bibliográficas

Jano on-line (2003). «La Agencia de Protección de Datos detecta problemas en la seguridad de la futura Tarjeta Sanitaria». [Fecha de consulta: 10 de febrero].
<http://www.doyma.es/>

Jano on-line (2003). «La semFYC pide garantías para que el paciente controle el acceso a su historial con la tarjeta sanitaria». [Fecha de consulta: 16 de enero].
<http://www.doyma.es/>

(9)RDL 16/2012, de 20 de abril, de medidas urgentes para garantizar la sostenibilidad del Sistema Nacional de Salud y mejorar la calidad y seguridad de sus prestaciones, reforma el sistema de dispensación de medicamentos obligando a que, en las nuevas recetas, se recoja información sobre el nivel de renta de los pacientes.

(10)Art. 1.a) RD 1718/2010, de 27 de diciembre de 2010, sobre receta médica y órdenes de dispensación.

Referencias bibliográficas

Petra Wilson; Christine Leitner; Antoinette Mousalli (2004). «Mapping the Potential og eHealth: empowering the citizen through eHealth Tools and services». Presentado en la eHealth Conference, Cork, Irlanda.

Juan Méjica García (2002). *El enfermo transparente. Futuro jurídico de la Historia Clínica Electrónica* (pág. 21). Madrid: Edisofer.

AEPD (2010, octubre). «Informe de cumplimiento de la LOPD en hospitales».

1.2. La importancia del derecho como instrumento para regular la e-salud

De lo dicho puede fácilmente deducirse que uno de los principales retos que plantea la salud electrónica es la necesidad de proteger el derecho a la autodeterminación informativa de los usuarios. Son conocidos, por ejemplo, supuestos en que datos sanitarios de los usuarios han acabado en internet[12]. El derecho cuenta, para alcanzar ese objetivo, con un papel esencial. Sin embargo, lo cierto es que en la actualidad el marco jurídico a aplicar muestra carencias significativas. Primero, porque las bases jurídicas que configuran las todavía vigentes Ley orgánica de protección de datos (LOPD) y Directiva europea de protección de datos, pero también el nuevo Reglamento general de protección de datos, disponen un marco demasiado abstracto, poco preciso, y emplean conceptos jurídicos muy ambiguos y vagos, lo que dificulta en la práctica la aplicación de las normas en el ámbito sanitario. Segundo, porque esas normas no han encontrado un desarrollo suficiente en lo que afecta al sector sanitario. Y, tercero, porque sigue sin resolverse el problema que plantea el carácter internacional o global de varias de las nuevas herramientas que se quieren aplicar, caso del *big data* sanitario. La preocupación del legislador por proteger la confidencialidad de los datos sanitarios parece evidente si se atiende a la letra de las normas. Las leyes que regulan el sector sanitario expresamente recogen, como reto de primer orden, el respeto a la intimidad y a la autodeterminación informativa de los usuarios[13]. Así lo hacen también las normas que regulan la protección de datos de carácter personal cuando se refieren a los datos de salud. No obstante, lo cierto es que, como se ha comentado, el entramado normativo presenta serias deficiencias. Y esto se debe, principalmente, a que no hay una norma que entre a regular de manera directa y específica esta cuestión. La Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (LBAP) vino a aportar, en el ámbito estatal, cierta claridad al respecto, pero no puede entenderse que esa Ley regula todas las particularidades que presenta el tratamiento de datos sanitarios. Es indicativo de ello el que la LBAP realice remisiones a la normativa de protección de datos[14] (De Miguel, 2004).

Las normas a aplicar son múltiples, provenientes de diferentes instancias, a saber:

(12)SAN 11 de febrero de 2010.

(13)Art. 10.3 LGS; art. 2.1); LBAP; art. 5.1.c); Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

(14)Art. 16.3 LBAP.

Referencia bibliográfica

Noelia de Miguel Sánchez (2004). *Tratamiento de datos personales en el ámbito sanitario: intimidad versus interés público* (pág. 24). Valencia: Tirant Lo Blanch.

1) En el ámbito supranacional, debe observarse el texto del nuevo Reglamento general de protección de datos de la UE (RGPD), aunque todavía siga vigente la Directiva 95/46/CE. De la misma manera deberán tomarse en consideración los informes y documentos emitidos por el Grupo de Expertos del artículo 29 de la Directiva, así como directivas que afectan al concreto sector sanitario, como la Directiva 2011/24/UE, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. Habrá que estar también a lo que en el ámbito del Consejo de Europa se ha aprobado a este respecto, fundamentalmente la Recomendación (97) 5, de 17 de febrero de 1997, sobre la protección de datos médicos[15], que, aunque constituye una suerte de *soft law*, es de gran utilidad a efectos de interpretar el contenido de las normas jurídicas tanto internas como internacionales.

[15]Cabe tener en cuenta a este respecto el «Introductory report updating recommendation R(97) 5», de 15 de junio de 2015, que viene a revisar algunos de los contenidos de la Recomendación de 1997, así como los diferentes textos aprobados en este mismo sentido durante 2014: «Medical technologies and data protections issues», de 2 de junio de 2014; «Opinion on the draft recommendation on the use for insurance purposes of personal health-related information, in particular information of a genetic and predictive nature», de 27 de marzo de 2014.

2) En el ámbito estatal son varias las normas a tener en cuenta.

Primero, las que afectan a la materia de protección de datos, caso de la LOPD y el Reglamento que la desarrolla (RDLOPD), poniéndolas en relación con las recomendaciones, informes jurídicos, memorias, resoluciones e instrucciones de la AEPD, que concretan diversos aspectos de la citada normativa básica.

Segundo, las que regulan la materia sanitaria, entre las que hay que destacar la Ley general de sanidad 14/1986, la Ley 16/2003 (LGS), de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, la Ley orgánica 3/1986, de 14 de abril, de medidas especiales en materia de salud pública, la Ley 33/2011, de 4 de octubre, general de salud pública, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, la Ley 14/2007, de 3 de julio, de investigación biomédica, el RD legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, la Ley 10/2013, de 24 de julio, por el que se incorporan las directivas de la UE sobre farmacovigilancia y prevención de la entrada de medicamentos falsificados en la cadena de suministro legal, el RD 1091/2015, de 4 de diciembre, por el que se crea y regula el Registro Estatal de Enfermedades Raras, el RD 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, el RD 183/2004, de 30 de enero de 2004, por el que se regula la tarjeta sanitaria individual, el RD 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación, o el RD 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza y por el que se modifica el RD 1718/2010.

En el ámbito autonómico también pueden encontrarse normas de gran interés, tanto las que regulan la materia de protección de datos como la sanitaria: la Ley catalana 32/2010, de 1 de octubre, de la autoridad catalana de protección de datos; la Ley vasca 2/2004, de 25 de febrero, de ficheros de datos de carácter personal y de titularidad pública y de creación de la Agencia Vasca de Protección de Datos (AVPD); y los informes y las recomendaciones de las agencias o autoridades de protección de datos autonómicas; la

Ley foral 17/2010, de 8 de noviembre, de derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra, la Ley catalana 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y a la autonomía del paciente, y la Documentación clínica, o el Decreto del País Vasco 38/2012, de 13 de marzo, sobre la historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica, el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica de Galicia, la Resolución de 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la historia clínica en el ámbito del Sescam (Servicio de Salud de Castilla-La Mancha), o el Decreto 181/2007, de 19 de junio, por el que se regula la receta médica electrónica en Andalucía.

Además de las normas, deberá estarse a lo que disponen otros textos que, desde el sector sanitario, se han aprobado con el objetivo de regular esta materia en el ámbito interno. Se trata de códigos de autorregulación o protocolos que, a pesar de aplicarse exclusivamente *ad intra* y de que la exigibilidad de su cumplimiento puede ser cuestionada, cada vez están adquiriendo mayor relevancia práctica[16] (Rubí, 2009).

[16]Art. 31.2 Ley foral 17/2010, de 8 de noviembre, de derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra.

Referencia bibliográfica

Jesús Rubí Navarrete (2009). «Códigos Tipo». En: Ricard Martínez Martínez (coord.). *Protección de datos. Comentarios al Reglamento de Desarrollo de la LOPD* (pág. 167). Valencia: Tirant Lo Blanch.

3) El RGPD muestra una especial preocupación por los datos de salud si se tiene en cuenta, por ejemplo, el alto número de referencias al concepto de «salud». De la misma manera, y como se verá más adelante, es subrayable el importante esfuerzo que realiza el regulador europeo por otorgar una importancia reforzada a la investigación. Sin embargo, dejando a un lado estos detalles, lo cierto es que el Reglamento no aporta grandes novedades al respecto de la protección de los datos de salud, más allá de los nuevos principios, derechos y obligaciones que con carácter general recoge para todos los tratamientos. Lógicamente, esos contenidos serán igualmente aplicables en este sector. Mención especial merecen las obligaciones de crear un Registro de Actividades (art. 30), de nombrar a un delegado de protección de datos (art. 37), de realizar evaluaciones de impacto de protección de datos (art. 35), de aplicar sistemas de privacidad desde el diseño (art. 25) y de consultar previamente a la autoridad de control pertinente, que en el sector público de la salud deberán respetarse en la gran mayoría de ocasiones. Lo mismo sucede con la desaparición de obligaciones ya consolidadas como la de notificar a las autoridades de control la creación de ficheros[17], o la obligación de adoptar medidas de seguridad concretas que ahora se sustituye por la obligación de adoptar medidas que garanticen una «seguridad adecuada»[18]. Más allá de estas previsiones generales, la regulación de los datos de salud de la Directiva de 1995 se mantiene en lo esencial. Es más, se sigue otorgando un amplio margen de actuación a los Estados miembros, por un lado porque en el RGPD se siguen utilizando conceptos jurídicos indeterminados que posibilitan un amplio margen de decisión al legislador interno y, por otro, porque la propia norma europea reconoce que la normativa interna podrá «mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud» a las establecidas en el reglamento[19]. Esta circunstancia hace que se haya de esperar a la futura norma interna que regule el derecho a la protección de datos de carácter personal, para concretar mejor las repercusiones que puede tener el reglamento europeo en el ámbito sanitario. En este sentido, es importante subrayar que la normativa interna,

[17]Considerando 89 RGPD.

[18]Art. 5.1.f) RGPD.

[19]Art. 9.4 RGPD.

tanto la referida a la protección de datos como la concerniente a la materia sanitaria, deberá revisarse y modificarse para acomodarse a lo dispuesto en la regulación europea.

2. La información sanitaria

En la estrecha relación que, a lo largo de la vida, va a mantener una persona con un sistema sanitario, se va a producir un flujo constante de información que englobará datos de diversas características. Esta circunstancia se evidencia fácilmente si se atiende, por ejemplo en el País Vasco, a las normas que crean los ficheros vinculados a los sistemas sanitarios.

Es el caso, por ejemplo, del fichero de Osakidetza denominado Registros de Casos de Sida, que se estructura de la siguiente manera: datos identificativos; datos de características personales; datos de circunstancias sociales, tales como aficiones y estilo de vida; y, datos especialmente protegidos, haciendo referencia en este último apartado a los datos de salud y los relativos a la vida sexual[20]. Se puede observar que se recogen diferentes tipos de datos, entre los que se incluyen los datos de salud y los datos protegidos, pero también otros que, de partida, no se incluirían en esas categorías anteriores.

(20)Anexo II Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud, BOPV núm. 246, 28 de diciembre de 2006.

La consideración de unos datos como datos de salud o no tendrá efectos prácticos relevantes por cuanto que este tipo de información será objeto de una protección reforzada en las normas.

El RGPD dispone que los datos de salud son los «datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud[21]».

(21)Art. 4.15 RGPDUE.

En sus considerandos dispone el Reglamento que

> «entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro»[22].

(22)Considerando 35 RGPD.

Ni la LOPD ni la Directiva UE aportan una definición sobre el concepto de datos de salud. El RDLOPD señala que ese concepto se refiere a «las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética»[23].

(23)Art. 5.1g) RDLOPD

La LBAP recoge que la información clínica es «todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla»[24]. Por su parte la Memoria Explicativa del Convenio de 1981 entiende por dato relativo la salud, la información referida a la salud pasada, presente o futura, física o mental de un individuo. La información puede referirse a una persona enferma, de buena salud o fallecida. Añade que esta categoría cubre también las informaciones relativas al abuso del alcohol o al consumo de drogas[25]. La Recomendación del Consejo de Europa que regula la protección de datos médicos se refiere a estos como los «datos personales relativos a la salud del individuo», incluyendo «los datos que tengan una clara y estrecha relación con la salud y los datos genéticos»[26]. La Memoria Explicativa de esta Recomendación precisa que esa definición abraza la salud pasada, presente y futura, tanto la salud física como mental, y que recoge también cualquier información que tiene una relación directa con la situación sanitaria del individuo: el comportamiento del individuo, la vida sexual, el estilo de vida en general, el abuso de drogas, del alcohol y la nicotina. Se trata de información que tiene relación clara y directa con la salud[27].

(24)Art. 3 LBAP.

(25)Considerando 45 Memoria Explicativa del Convenio 108/1981 del Consejo de Europa.

(26)Art. 1 R (97) 5.

(27)Considerandos 37 y 38 Memoria Explicativa de la Recomendación 5 (1997) del Consejo de Europa.

Se puede observar que las distintas definiciones utilizan conceptos diferentes:

1) En primer lugar, cabe distinguir los conceptos «dato relativo a la salud» y «datos sanitarios». Teniendo en cuenta que los datos de salud pueden emplearse en diferentes sectores, sanitario, laboral, etc., podría considerarse que los datos de salud se refieren, en sentido general, a todos los datos de salud, independientemente del lugar en el que se traten, mientras que los «sanitarios» se referirían a esos datos pero cuando son tratados en el específico sector sanitarios (Serrano, 2003).

Referencia bibliográfica

M.ª Mercedes Serrano Pérez (2003). *El derecho fundamental a la protección de datos: Derecho Español y Comparado* (pág. 414). Madrid: Civitas.

2) En segundo lugar, cabe apuntar que de las definiciones aportadas puede deducirse que el concepto de dato de salud cuenta con una especie de *vis atractiva* en que se incluyen informaciones de diferente índole. Incluso la consideración de una persona como una persona sana se ha considerado como dato de salud[28]. Este concepto amplio lleva a tener que distinguir entre diferentes esferas.

(28)Resolución de la AEPD R/02635/2009, de 9 de diciembre de 2009, que reconoce que el dato de salud de carácter benigno es dato de salud.

a) Los datos que incluyen información que se refieren directa y estrictamente a la salud física y mental[30] de las personas. Estos datos podrían considerarse como «datos médicos»[29];

(29)European Group on Ethics in Science and New Technologies, opinion núm. 13, 30/07/1999, about Ethical Issues of Healthcare on the Information Society.

(30)AEPD, Informe jurídico de la APD sobre la naturaleza de los datos psicológicos a efectos de su tratamiento, incluye la información sobre la salud mental dentro del concepto de datos de salud. La LBAP, todavía hoy, cuando se refiere a la información clínica se refiere exclusivamente al estado físico.

b) Los datos que no son estrictamente médicos, pero que guardan una estrecha relación con el estado de salud de los individuos. Las normas más arriba apuntadas se refieren a los «abusos de alcohol y drogas» o a «los datos que tengan una clara y estrecha relación con la salud» o «el comportamiento del individuo» o «el estilo de vida»[31] (Murillo, 2006).

(31)Informe jurídico AEPD, 0129/2005, entiende que el dato de que una persona es fumadora no puede constituir un dato de salud, si no se asocia con algún indicador del efecto que este uso tiene sobre la salud.

Referencia bibliográfica

Pablo Lucas Murillo de la Cueva (2006). «El derecho fundamental a la protección de los datos relativos a la salud». En: Santiago Ripol Carulla (ed.); Jordi Bacaría Martrus (coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud* (pág. 32). Madrid: APDCat.

c) Cabe preguntarse si también pueden incluirse en el concepto de dato de salud aquellos que tienen un carácter administrativo o económico, de gestión, que en los centros sanitarios resultan del tratamiento médico de las personas (Larios, 2009). Se entiende aquí que esto es posible debido a que muchas veces el estado de salud de una persona puede deducirse de este tipo de datos. Así parece haberse admitido en algún caso por el Consejo de Europa o las autoridades de protección de datos[32]. Piénsese en las referencias que se pueden realizar a números de historias clínicas en ficheros que tienen como fin el control de gastos económicos, en relación, por ejemplo, con la solicitud de material protésico[33]. Esta interpretación parece seguir el nuevo RGPD al señalar que «se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia»[34].

(32)Art. 1.2 Anexo de la Recomendación 1 (81), del Comité de Ministros del Consejo de Europa, de 23 de enero de 1981, que regula las bases de datos médicos automatizadas. Dictamen AVPD CN09-003, de 5 de febrero de 2009.

(33)Informe jurídico AEPD, 0625/2009.

(34)Considerando 35 RGPD.

Referencia bibliográfica

David Larios Risco (2009). «La Historia Clínica como conjunto de datos especialmente protegidos». En: VV. AA. *El derecho a la protección de datos en la historia clínica y la receta electrónica* (pág. 163). Cizur Menor: Aranzadi.

La importancia de determinar qué datos son relativos a la salud deriva del hecho de que son objeto de una protección reforzada[35]. En principio, parece que la naturaleza de estos datos lleva a que estos sean considerados como «sensibles». Se trataría de información que toca el ámbito más interno de las personas[36] (Gómez, 2010). Más allá de que el criterio de la naturaleza de los datos pueda ser cuestionable (Nicolás, 2006), parece lógico pensar que hay datos que, mal empleados, pueden originar en algunos contextos un perjuicio mayor, sobre todo de carácter discriminatorio[37]. Resulta coherente, así, que los datos de salud se incluyan en este grupo de «datos sensibles».

(35)Art. 7.3 LOPD; art. 9 RGPD.

(36)SSTEDH de 26 marzo de 1987, Leander y 5 mayo de 2000, caso Rotaru. STC de 23 marzo de 2009, FJ 2.

(37)Considerando 43 Memoria Explicativa Convenio 108/1981 del Consejo de Europa.

No obstante, quizás tendría sentido establecer una diferenciación entre distintos datos de salud, pues resulta evidente que no es lo mismo que un dato refleje que una persona cuenta con una buena salud a que se refiera a una

(38)Resolución de la AEPD R/00342/2008, de 14 de abril de 2008.

(39)SAN de 16 de enero de 2008, FJ 3.

enfermedad como el VIH[38]. Los propios tribunales suelen atender la mayoría de veces al contenido concreto del dato, a la hora de ponderar si su uso ha sido acorde a derecho o no[39].

Referencias bibliográficas

Yolanda Gómez Sánchez (2010). «Datos de salud como datos especialmente protegidos». En: Antonio Troconso Reigada (dir.). *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (pág. 648). Cizur Menor: Civitas / Thomson Reuters.

Pilar Nicolás Jiménez (2006). *La protección jurídica de los datos genéticos de carácter personal* (pág. 75). Bilbao / Granada: Comares.

3. Los principios de calidad aplicados al ámbito sanitario

Las normas de protección de datos recogen una serie de principios relativos a la «calidad de los datos» que constituyen una especie de principios generales o pautas esenciales que deben guiar todo tratamiento de datos[40]. Los más importantes son el de finalidad, pertinencia y veracidad.

(40)SAN de 24 de marzo de 2004, FJ 2.

3.1. El principio de finalidad

El principio de finalidad exige que todos los datos que un responsable vaya a recoger y utilizar lo sean para cumplir con un objetivo o fin específico[41]. Esta finalidad debe cumplir con unos requisitos. Primero, la finalidad debe estar bien delimitada y tiene que ser legítima y explícita[42]. Se reclama, por tanto, un gran celo a la hora de concretar la finalidad, sin que pueda ser un objetivo ambiguamente definido[43]. Una vez la finalidad se haya cumplido, los datos deberán cancelarse. Segundo, una vez determinada la finalidad, los datos no podrán emplearse para fines incompatibles. El criterio de incompatibilidad debe interpretarse en sentido restrictivo, de manera que los datos no puedan utilizarse para fines distintos a los que justificaron su recogida y tratamiento inicial[44], más allá de los fines que en las normas expresamente tengan reconocida la compatibilidad. Es subrayable que el RGPD, como ya venían haciendo las anteriores normas de protección de datos, reconozca la compatibilidad del uso de los datos con fines de investigación científica, sin bien añade que ese nuevo tratamiento deberá guardar unas garantías específicas[45].

(41)Art. 5.1.b) RGPD; art. 4.2 LOPD.

(42)Memoria de la AEPD de 1999.

(43)STSJ de Asturias de 12 de septiembre de 2005, FFJJ 3 y 14.

(44)SAN de 6 de abril de 2006, FJ 4; STC de 30 de noviembre de 2000, FJ 13. Resolución de la AEPD, R/00485/2004, de 8 de septiembre de 2004, procedimiento AAPP/00011/2004.

(45)Art. 5.1.e) RGPD.

La Administración sanitaria recoge los datos para cumplir finalidades concretas y no podrá utilizarlos, de inicio, para cumplir objetivos distintos. La exigencia de que esa finalidad se concrete al máximo posible lleva a que no sea suficiente con argumentar que se emplearán con el objetivo general de proteger la salud de las personas. Más hoy día, cuando se asume un concepto amplio de «protección de la salud», incluyendo acciones muy variadas (Delgado y Llorca, 2008). Este concepto amplio se recoge en las diferentes normas que concretan las diferentes actividades que completan la protección de la salud: LGS, Ley general de salud pública, Ley de cohesión y calidad del Sistema Nacional de Salud, LBAP, Ley del medicamento o Ley de investigación biomédica, que incluyen actividades incluso dirigidas a la docencia, pasando por la estadística, investigadora, preventiva y asistencial. La concreción de la finalidad deberá realizarse en las normas que crean los ficheros públicos en los que se recogen los datos[46].

(46)Art. 20 LOPD. La obligación de que los ficheros públicos se creen a través de normas concretas no parece que vaya a desaparecer con la aplicación del RGPD.

Referencia bibliográfica

M. Delgado Rodríguez; J. Llorca Díaz (2008). «Concepto de salud. El continuo salud-enfermedad. Historia natural de la enfermedad. Determinantes de la salud». En: VV. AA. *Manual de epidemiología y salud pública* (pág. 3). Madrid: Editorial Médica Panamericana.

Puede ponerse como ejemplo el Registro de Casos de Sida de Euskadi, que tiene por finalidad contabilizar el número de casos de sida en la comunidad autónoma, la vigilancia epidemiológica, el tratamiento estadístico de la información obtenida, la realización de estudios epidemiológicos, la investigación y planificación sanitaria y la entrega de una cartilla sanitaria específica para enfermos de sida[47].

(47)Anexo II, 4.1, Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los ficheros automatizados de datos de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud

El problema de este sistema deriva del hecho de que las finalidades aparezcan descritas de manera genérica, ampliando así las opciones de uso de los datos. Y es que no todas las actividades que completan la salvaguarda de la salud afectan de la misma manera al derecho a la protección de datos de carácter personal. No es lo mismo que una muestra de sangre pueda ser utilizada para hacer unos análisis con fines asistenciales o que los resultados de esos análisis se remitan a una clínica privada que colabora con la Administración con el objetivo de llevar a cabo una investigación de carácter científico. Este problema se acentúa en la actualidad cuando ya hay en marcha tratamientos de *big data* sanitario, justificados inicialmente por tener como finalidad la investigación científica. Se dice que, en estos casos, se acentúa el problema porque muchas veces este tipo de proyectos vienen motivados por finalidades indefinidas o por finalidades que pueden ir variando en la medida en que los proyectos avanzan.

3.2. El principio de pertinencia

El principio de pertinencia o proporcionalidad exige que, cuando se tratan datos de carácter personal, haya coherencia entre la finalidad que se persigue con dicho tratamiento y el uso que se dé a los datos[48]. Esta coherencia se traduce en que los datos que se vayan a tratar para la consecución de la finalidad que el responsable del fichero pretende sean los estrictamente adecuados, necesarios y «no excesivos». Si se tratan más datos de los estrictamente pertinentes, el derecho a la autodeterminación informativa se verá innecesariamente afectado[49].

(48)Art. 5.1.d) RGPD; art. 4.1 LOPD. STC de 20 de julio de 1993, FJ 7.

(49)Resolución de la AEPD, R/01235/2007, de 21 de diciembre de 2007.

La aplicación de este principio en el ámbito sanitario lleva a analizar primero si un tratamiento de datos de carácter personal concreto es adecuado, empíricamente, para conseguir el fin pretendido. Esta finalidad no será, en general, la protección de la salud, sino una actuación concreta como la investigación, un estudio epidemiológico, la asistencia directa frente a unos síntomas específicos, etc.[50]. El tratamiento de cada uno de los datos tiene que ser un medio apto para llevar a cabo el fin pretendido. Piénsese en el caso en que un paciente acude al médico de cabecera con los síntomas de una gripe. En este caso, será adecuado recoger y utilizar diferentes datos que lleven a diagnosticar y tratar la enfermedad: cuándo comenzó a padecer los síntomas, si tiene fiebre, etc., independientemente de que unos datos sean más adecuados que otros. No sería adecuado, sin embargo, recabar para tratar esa enfermedad información sobre la orientación sexual del paciente. La adecuación reclama

(50)Informe jurídico de la AEPD, 0173/2008, de 26 de marzo de 2008: sobre una historia clínica en la que se recogía el dato de si el paciente iba en su automóvil con el cinturón de seguridad puesto en un momento determinado, señala que este dato no es adecuado para tratar al paciente con fines sanitarios.

también que el tratamiento de cada dato encuentre fundamento formalmente en alguna norma. En este caso, las normas que crean los ficheros sanitarios deberán indicar qué datos podrán utilizarse en cada caso para llevar a cabo los diferentes fines sanitarios.

Por ejemplo, la norma que crea el fichero denominado Detección Precoz del Cáncer de Mama de Osakidetza habilita a los profesionales para manipular datos identificativos, DNI, nombre y apellido, dirección, teléfono; datos personales: fecha y lugar de nacimiento, sexo; datos de circunstancias sociales: aficiones y estilo de vida; datos especialmente protegidos: salud, con el fin de coordinar el programa de prevención del cáncer de mama, realizar las citaciones, gestionar los flujos de información y evaluar los resultados del programa[51]. La adecuación, desde el punto de vista formal, quedaría cubierta con esta previsión.

(51)Punto 4.3.d) del anexo II, Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud.

En segundo lugar, deberá observarse si el tratamiento de todos y cada uno de esos datos es necesario para proteger la salud en esa concreta situación[52]. La LBAP dispone en esta línea que la HC recabará los datos necesarios para llevar a cabo el tratamiento sanitario correspondiente[53]. Los problemas comienzan a la hora de concretar qué datos son necesarios y cuáles no.

(52)Informe de la AEPD, 266/2006. Resolución AEPD, R/00977/2008, de 22 de julio de 2008, donde se analiza el supuesto en que un centro sanitario transmitió a una empresa más información de la debida en el justificante de una baja laboral.

(53)Art. 15 LPAB.

Por ejemplo, piénsese en el caso arriba citado en que a un sujeto afectado por la gripe se le solicita información sobre el estilo de vida familiar. La manipulación de estos datos podría resultar adecuada para tratar la enfermedad. No obstante, no parece que sea necesario conocer dicha información para tratar la enfermedad citada, pues el uso de dichos datos afectaría directamente a la autodeterminación informativa, mientras que su efectividad para tratar la enfermedad sería mínima.

En el ámbito sanitario, la aplicación del criterio de necesidad plantea algún problema práctico. ¿Qué sucede si hay alguna duda sobre la necesidad de tratar unos datos concretos? En este sector muchas veces es muy difícil concretar los datos que se van a emplear en cada caso para llevar a cabo los diferentes fines. Es por eso que, en las normas que crean los ficheros, se emplean usualmente conceptos amplios a la hora de definir los datos que se van a tratar para el cumplimiento de fines específicos.

Es el caso, por ejemplo, del fichero relativo al registro de los casos de sida del Sistema Vasco de Salud, en el que los datos a recoger se identifican con conceptos ambiguos como «estilo de vida».

El uso de este tipo de conceptos en el ámbito sanitario puede estar plenamente justificado, en la medida en que el profesional sanitario no puede estar constantemente preguntándose sobre si el uso de unos datos es necesario o no en un caso concreto (Troncoso, 2004). En cualquier caso, este principio debe llevar a plantearse una interrogante importante: ¿es necesario que los datos aparezcan en todo caso asociados al paciente o usuario concreto? Esta pregunta podría plantearse sobre todo cuando los fines que se pretenden son estadísticos o de investigación. En el caso del ya mentado *big data* sanitario, por ejem-

Referencia bibliográfica

Antonio Troncoso Reigada (2004). *Guía de protección de datos personales para Servicios Sanitarios Públicos (Introducción y Presentación)* (pág. 407). Madrid: Thomson Civitas / APDCM.

plo, por definición se considera que se tratará el mayor número posible de datos, lo que está llevando a cuestionarse constantemente si es necesario o no anonimizar o seudonimizar esos datos previamente antes de proceder a su uso.

El tratamiento de datos será excesivo o no en términos estrictamente jurídicos si se entiende que está justificado para proteger la salud. Se trata de analizar el choque entre los diferentes intereses en juego en cada supuesto en que se van a tratar datos sanitarios. En términos generales, establecen las normas de protección de datos que el derecho a la autodeterminación informativa cede cuando la finalidad perseguida es la protección de la salud[54].

(54)STSJ Comunidad de Madrid, de 10 de abril de 2003, FJ 9.

3.3. El principio de veracidad

Este principio reclama que los datos que se vayan a tratar para la consecución de un fin concreto reflejen la realidad actual a la que se refieren, sin que pueda ser inexacta, falsa, incompleta u obsoleta[55]. Los datos falsos, inexactos, desfasados deben ser rectificados o cancelados. La exigencia de que los datos «desfasados», no actuales, sean cancelados merece una puntualización, sobre todo ahora que el RGPD modifica la redacción al respecto exigiendo la actualización «si fuera necesario»: ¿es posible que en algunos casos se permita la conservación de datos que se refieren a la realidad del pasado? Es evidente que en determinados supuestos esta conservación será necesaria.

(55)Art. 5.1.d) RGPD; art. 4.3 LOPD. SAN de 28 de junio de 2002, FJ 3.

En el ámbito sanitario es especialmente relevante el cumplimiento de este principio, por cuanto que el uso de una información sanitaria no veraz podría tener consecuencias nefastas para la salud de las personas (Egusquiza, 2009). Es así que la propia LBAP parece exigir que los datos que se utilicen en el sector sanitario sean veraces y actualizados[56]. En esta línea, uno de los principales objetivos de los nuevos sistemas de información sanitaria que se dirigen a crear historias clínicas únicas electrónicas es la desaparición de bases de datos aisladas y duplicidades o repeticiones, situaciones que inducen al error[57]. En el ámbito sanitario, el cumplimiento de la veracidad reclama de la actuación tanto de la Administración sanitaria como de los propios usuarios, para que no haya errores tanto cuando se incluyen datos nuevos en los ficheros como cuando se tratan una vez han sido recabados. En este entorno son varios los apuntes a realizar. Primero, hay que tener en cuenta que la sanidad es un ámbito en el que colaboran, normalmente, el profesional y el usuario basándose en una relación de confianza. En estas circunstancias el error en la información debería ser mínimo, más aún si con las nuevas tecnologías se permite un seguimiento remoto a los pacientes del contenido de sus historias clínicas. Segundo, el cumplimiento del principio de veracidad en el ámbito sanitario se enfrenta al problema de que se mezclan tanto informaciones objetivas como subjetivas, caso de las anotaciones subjetivas de los profesionales en las historias clínicas. Tercero, hay que tener en cuenta que la información sanitaria cuenta con un alto grado de tecnicismo, con lo que si el paciente impulsa la rectificación o supresión de los datos de salud deberá hacerlo bajo supervisión

(56)Art. 15.1 LBAP.

(57)Art. 15.4 LBAP.

(58)Art. 18.3 LBAP.

Referencia bibliográfica

M.ª Ángeles Egusquiza Balmaseda (2009). *Protección de datos: intimidad y salud* (pág. 140). Cizur Menor: Aranzadi.

de profesional sanitario. Cuarto, para poder aplicar de una manera correcta el principio de veracidad, será necesario que el titular de los datos acceda a la información sanitaria que le concierne, para así conocer si dichos datos son correctos o no. Esta necesidad choca muchas veces con los límites que se han impuesto a este derecho de acceso[58]. Por último, el principio de veracidad no lleva en el ámbito sanitario a que únicamente se contengan en los ficheros datos actuales; es necesario que se conserven datos del pasado de los usuarios a fin de tener una perspectiva histórica de la salud de las personas.

4. El consentimiento informado en la protección de datos sanitarios

4.1. Cuestiones generales

Es conocido que uno de los contenidos fundamentales del derecho a la protección de datos es el denominado consentimiento informado. Podría definirse como una institución a través de la cual un sujeto capaz, o, en su caso, su representante, autoriza, consciente y voluntariamente, de una manera clara, el tratamiento de los datos que le conciernen, después de haber sido informado nítida y suficientemente sobre los distintos aspectos que van a rodear a dicha utilización[59].

(59)SAN de 17 de abril de 2007, FJ 3.

La aplicación de la regulación sobre el consentimiento informado al ámbito sanitario tiene que partir de algunos matices, a saber: en el ámbito sanitario, el consentimiento informado reconocido en la normativa de protección de datos debe conjugarse con el consentimiento informado al que se hace referencia en la normativa sanitaria[60], dirigido a autorizar un tratamiento médico concreto, y al que la jurisprudencia le ha dado una relevancia especial como vehículo para ejercer la autonomía individual sobre la salud de cada uno[61] (González y Lizarraga, 2004). Ambos consentimientos informados contribuyen a crear una relación de confianza entre profesionales e interesados o usuarios y a reforzar la autonomía de los pacientes. En segundo lugar, el alcance del consentimiento informado en este entorno deberá ajustarse a las necesidades prácticas que los profesionales sanitarios tienen para desarrollar su trabajo. Este estudio pasa por distinguir entre dos contenidos: por un lado, el derecho de los afectados a «ser informados» de las características del tratamiento de datos que va a llevar a cabo el responsable del fichero. Por otro, el derecho de los afectados a autorizar cualquier tratamiento que alguien quiera realizar de sus datos.

(60)Arts. 3, 4.3 y 8.1 LBAP.

(61)SSTS de 23 de mayo de 2007, FJ 3; 4 de abril de 2000, FJ 3; 15 de noviembre de 2006, FJ 2.

Referencia bibliográfica

Pedro González Salinas; Emilio Lizarraga Bonelli (coords.) (2004). *Autonomía del paciente, información e Historia Clínica*. Madrid: Thomson Civitas.

4.2. El derecho a ser informado en el ámbito sanitario

El derecho a ser informado es la facultad de los afectados a conocer las características de los tratamientos de datos que le conciernen. Esta información debe guardar unas características, a saber: primero, la información debe darse normalmente en el momento de la recogida de datos. Únicamente si los datos son recabados de fuente distinta al titular, y no se requiere del consentimiento de este último para su tratamiento, la información puede retrasarse más allá del momento en que se recogieron. Segundo, la información debe ser expresa,

precisa, inequívoca y completa, de manera que no puede haber duda de que la persona afectada ha tenido conocimiento de las características principales del tratamiento de datos que se pretende.

No cabe el recurso a la letra pequeña, ni a formas indirectas de informar, ni a informaciones ambiguas, y a pesar de lo afirmado en su día por el TS[62], se entiende, siguiendo el RGPD, que debe darse preferentemente de manera escrita. Tercero, la información debe referirse a múltiples aspectos, entre los que cabe destacar la finalidad del fichero, los destinatarios de la información, los derechos que el titular de los datos puede ejercer, y la identidad y dirección del responsable del fichero. La información sobre estas cuestiones debe ser, además, lo más concreta posible[63].Todas estas exigencias se refuerzan en el RGPD estableciendo nuevos contenidos sobre los que informar y más garantías para que la información se haga efectiva[64]. Cabe subrayar el que se obligue al responsable a informar sobre los plazos de conservación de los datos o, si eso no es posible, sobre los criterios utilizados para determinar esos plazos, por la incidencia que tiene en el ámbito sanitario. También el que expresamente se indique que si los datos recabados en un momento dado van a ser empleados posteriormente para un fin distinto al que inicialmente motivó la recogida de datos, se deberá informar al interesado sobre ese nuevo tratamiento, por la incidencia que puede tener esta previsión, por ejemplo, en los casos en que se utilizan datos obrantes en las historias clínicas para realizar posteriormente investigaciones.

(62)STS de 15 de julio de 2010, FJ 6.

(63)Resolución AEPD 00288/2006, de 9 de mayo de 2006.

(64)Arts. 12-14 RGPD.

La normativa de protección de datos reconoce una serie de excepciones al derecho a ser informado. Cuando los datos se recaban del propio titular, el RGPD no prevé excepciones concretas. La LOPD, en cambio, ha venido exceptuando este derecho si la información que se debe proporcionar al titular es deducible «de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban»[65]. Si los datos se recaban de fuente distinta al interesado, puede exceptuarse la obligación de informar al afectado si así lo dispone expresamente una ley, si el tratamiento de datos tiene una finalidad histórica, científica o estadística y la información es imposible o implica un esfuerzo desproporcionado para el responsable del fichero, siempre que se adopten las garantías oportunas[66]. El Reglamento UE añade una excepción cuyo alcance está por determinar al poder ser interpretada en un sentido excesivamente amplio: cuando los datos tengan carácter confidencial sobre la base de una obligación de secreto profesional[67]. Por último, según la LOPD también podría plantearse la limitación del derecho a ser informado cuando se pueda poner en riesgo la defensa nacional, la seguridad pública o una investigación penal[68]. Se trata de límites que han planteado numerosos problemas interpretativos y, en la mayoría de casos, de dudosa implementación en la práctica. Estos límites se reconocen también en el RGPD en el catálogo de excepciones generales para todos los derechos que componen la autodeterminación informativa y que se podrán incluir en futuras normas estatales o europeas[69].

(65)Art. 5.3 LOPD.

(66)Art. 14.5 RGPD; art. 5.5 LOPD.

(67)Art. 14.5.d) RGPD.

(68)Art. 24.1 LOPD.

(69)Art. 23 RGPD.

La aplicación de estos parámetros en el sector sanitario plantea problemas prácticos al partir de la idea de que, en el ámbito sanitario, está en juego la protección de la salud de las personas y la obligación de informar no debe constituir un obstáculo para el correcto desarrollo de la actividad sanitaria. Esta circunstancia lleva a una serie de consideraciones.

Primero, el esquema general a la hora de informar en el ámbito sanitario sería el siguiente: la mayoría de veces en este entorno los datos de carácter personal se recaban de los propios usuarios. Siendo así, la información debería darse siempre que fuera posible en el mismo momento en que se recogen los datos. Ello no sería posible en situaciones concretas, de urgencia sobre todo, en que empíricamente no cabría darse la información de esa manera, con lo que deberían buscarse fórmulas alternativas[70]. Si los datos son recabados de terceros, por ejemplo, cuando derivan de una cesión de datos, la información podría prorrogarse en aplicación de la Ley. Este esquema, sin embargo, debe matizarse. Lo más normal será que los usuarios reciban la información pertinente, cuando menos una información básica, general, en el momento en que se inicie su relación con un sistema sanitario. Esta información general estará presente durante el desarrollo de dicha relación y se llevará a cabo a través de medios que permitan la perpetuación de la misma, a través de folletos, boletines, información directa cuando se entrega la tarjeta sanitaria, etc., y será válida para todo usuario, señalando posibles usos de datos, derechos de los interesados, la identidad del responsable y cómo contactar con él (Sánchez y Abellán, 2004). Esta situación llevará a que normalmente no se requiera del cumplimiento de la obligación de informar en cada acto sanitario concreto. Ahora bien, si un acto sanitario concreto va a conllevar un tratamiento especial, distinto al general ahora descrito, sí se requerirá de una información adicional a la básica[71]. Es decir, independientemente de que los datos se hayan recabado directamente del titular o de terceros, lo normal será que la información que reclaman las normas se aporte al interesado en el desarrollo de la relación con el sistema sanitario. Lo contrario llevaría a una excesiva burocratización.

(70)Dictamen AVPD CN09-021, de 24 de septiembre de 2009.

(71)Art. 5.6.a.ii) R (97)5.

Referencia bibliográfica

Javier Sánchez Caro; Fernando Abellán (2004). *Datos de salud y datos genéticos. Su protección de la Unión Europea y en España* (pág. 58). Granada: Comares.

Segundo, la exigencia de que la información sea expresa, precisa, inequívoca y completa deberá cohonestarse con el derecho de los pacientes a tener una asistencia sanitaria efectiva, de calidad. Para que esta premisa se cumpla, habrá de estarse a las características de cada caso concreto que se plantee en la realidad: no es lo mismo informar en una urgencia que en un ensayo clínico, por ejemplo. De partida, será necesario que se cumpla escrupulosamente con lo que las normas dictan, cosa que no siempre sucede[72], pero pueden darse situaciones en las que la necesidad de que la información sea expresa, precisa, inequívoca y completa se convierta en todo lo expresa, precisa, inequívoca y completa que sea posible.

(72)Informe jurídico de la AEPD, «Informe de cumplimiento de la LOPD en hospitales», octubre de 2010.

Si la información se recaba a través de cuestionarios o formularios, la información puede ser escrita, completa, expresa e inequívoca[73]. Si es recabada por otras vías, la situación es más compleja. Como se ha dicho, la obligación de

(73)Resolución de la AEPD, R/00017/2008, de 15 de enero de 2008.

informar podría verse satisfecha con una información general a aportar a todos los usuarios a través de folletos, carteles, pósteres o paneles. Podría darse esta información, por ejemplo, en el momento en que se da y renueva la tarjeta sanitaria. Esta opción tiene la ventaja de que se trata de una información que puede mantenerse a lo largo del tiempo[74]. Más allá de esta información genérica, cuando los datos de una persona vayan a ser tratados en una operación concreta, especial, que exija de una información añadida a la aportada en la genérica, sí se requerirá que se sea más cuidadoso a la hora de individualizar la información. Esta obligación se subrayará, sobre todo, cuando se vaya a producir una cesión que lleve a que los datos de alguien se vayan a incluir en un nuevo fichero, distinto a los ficheros más comunes, o cuando se vayan a producir nuevos tratamientos con fines distintos a los inicialmente previstos o representados en la información genérica antes referida (Martínez, 2004).

(74)Informe jurídico 0304/2005, AEPD. Punto 111 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa

Referencia bibliográfica

Carlos Hernández Martínez Campello (2004). «La Ley 41/2002 y la normativa sobre protección y tratamiento de datos de carácter personal relativos a la salud». En: Pedro González Salinas; Emilio Lizarraga Bonelli (coords.). *Autonomía del paciente, información e Historia Clínica* (pág. 180). Madrid: Thomson-Civitas.

Tercero, la información debe ser lo más completa posible, como reiteradamente ha dispuesto la AEPD[75]. Es subrayable cómo en el ámbito sanitario ha sido práctica común el que, en las normas internas, caso de los protocolos de actuación, instrucciones o circulares, se haya ido más allá de lo dispuesto en las normas a la hora de determinar el contenido de la información que se ha de aportar a los usuarios. Es lo que ha sucedido, por ejemplo, en la conocida Circular del INSALUD[76] o en otros códigos tipo[77]. Es más, hay leyes específicas que también han apuntado en esta dirección[78]. Lo mismo sucede con el RGPD que amplía el contenido de la información. En principio, la fórmula antes descrita en la que se combinan una información previa genérica y otra individualizada debería ser un sistema lo suficientemente eficaz para que el titular de los datos tuviera una perspectiva completa sobre las características del tratamiento que el responsable del fichero va a llevar a cabo. La información genérica vendría a cubrir, en este sentido, gran parte de esta información: descripción de las finalidades, los derechos de los usuarios, dónde y cómo ejercer estos derechos, la importancia de aportar una información correcta, veraz y completa a los profesionales, la identificación del responsable, etc.

(75)Resolución AEPD, R/00711/2005, de 3 de octubre de 2005, procedimiento PS/00018/2005.

(76)Art. 9.1.g) Circular 9/97, de 9 de julio de 1997.

(77)Art. 13.h) Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España, inscrito el 12 de julio de 2004, y modificado en 2006.

(78)Arts. 15, 47 y 59 Ley 14/2007, de 3 de julio, de investigación biomédica.

Cuarto, la aplicación de las excepciones arriba comentadas en el ámbito sanitario puede darse únicamente en supuestos contados en el ámbito sanitario:

1) En caso de que los datos se recaben directamente del propio paciente o usuario, cosa que sucede en la mayoría de casos, no parece que tenga sentido la aplicación de las excepciones arriba comentadas (Gil, 2010, parece reconocer esa aplicabilidad). De hecho, se trata de límites que no se prevén en los protocolos, circulares o instrucciones de aplicación interna, ni siquiera en el RGPD, y que en algún caso los propios tribunales han rechazado[79].

Referencia bibliográfica

Cristina Gil Membrado (2010). *La historia clínica. Deberes del responsable del tratamiento y derechos del paciente* (pág. 156). Granada: Comares.

(79)SAN de 15 de junio de 2001, FJ 3, en la que se niega la aplicabilidad del artículo 5.3 LOPD a un supuesto en que se recaban datos sanitarios para incluirlos en un fichero cuyo responsable es un centro sanitario.

2) En caso de que los datos se recaben de fuentes distintas a los usuarios, la aplicación de las excepciones podría tener, en determinados casos, algún sentido. No se conoce, sin embargo, ley alguna en este ámbito que expresamente limite el derecho a ser informado. Es más, en diferentes normas se refuerza este derecho[80]. Tampoco la finalidad científica justifica un límite general al derecho a ser informado. Las últimas leyes que en el ámbito estatal han entrado a regular esta cuestión siguen reconociendo la vigencia de este derecho[81]. Sí podría plantearse la posibilidad de limitarlo cuando su ejecución implique un gran esfuerzo para la Administración sanitaria, cosa que parece preverse en el nuevo RGPD[82]. Hay que pensar que, en determinados supuestos, la actividad sanitaria se dirige a colectivos muy amplios (niños, mujeres, mayores, etc.), fundamentalmente en proyectos de *big data* sanitario, lo que podría dificultar la tarea de informar. No obstante, también debe tenerse en cuenta que las administraciones sanitarias son organizaciones con grandes recursos tanto económicos como personales y materiales. Además, si se entiende que la e-salud debe acercar a los pacientes y las administraciones sanitarias, no parece que pueda justificarse un límite al derecho a ser informado en este ámbito a no ser que se den circunstancias realmente excepcionales.

(80)Art. 3.2.d) RD 1718/2010, de 27 de diciembre de 2010, sobre receta médica y órdenes de dispensación.

(81)Art. 47 Ley 14/2007, de 3 de julio, de investigación biomédica.

(82)Art. 14.5.b) RGPD.

3) La defensa nacional, la seguridad pública o el desarrollo adecuado de una investigación penal sí pueden constituir un bien jurídico de suficiente entidad para limitar el derecho a ser informado. La lucha contra una epidemia, por ejemplo, puede constituir un argumento suficiente para limitar ese derecho. O el uso de datos de salud, como muestras de ADN, para identificar a presuntos delincuentes.

4) En algún caso se ha planteado la opción de aplicar otras excepciones, más allá de lo que reconocen expresamente las normas. Se ha planteado, por ejemplo, la posibilidad de que no se informe al titular de los datos de las características del tratamiento de los mismos atendiendo a una supuesta finalidad terapéutica. Sin embargo, no se entiende aquí de qué manera puede afectar esta información negativamente a la salud del usuario.

4.3. El consentimiento en la sanidad

4.3.1. El consentimiento en la normativa de protección de datos

Ha sido comúnmente asumido que el consentimiento constituye una de las instituciones más importantes, sino la que más, en materia de protección de datos[83]. Debe cumplir unas características para que sea considerado válido. En primer lugar, el consentimiento tiene que ser libre.

(83)STSJ de Madrid, 15 de enero de 2004, FJ 6.

La libertad debe conllevar tanto la posibilidad de otorgar el consentimiento voluntariamente como la posibilidad de revocarlo cuando se quiera[84]. En segundo lugar, el consentimiento debe ser inequívoco, siendo necesario que sea «incuestionable», sin que quepa duda sobre su otorgamiento[85]. Mucho se ha escrito sobre el significado de este requisito. Baste señalar que hasta ahora se ha venido admitiendo, aunque no sin crítica[86], tanto el consentimiento expreso como el tácito[87]. Esta situación parece modificarse en el nuevo RGPD, que reclama una actuación positiva, de hacer o declarar, del afectado para que se entienda que el consentimiento se ha dado. En tercer lugar, se reclama que el consentimiento sea específico, consciente e informado. La autorización, por lo tanto, deberá ir dirigida a un objeto concreto, a un tratamiento de datos determinado, bien delimitado[88]. Además, será necesario que el afectado comprenda por sí mismo, o a través de un representante, las consecuencias de otorgar el consentimiento. Por último, de las normas puede deducirse que el consentimiento debe ser previo al tratamiento.

(84)Art. 4.11) RGPD; art. 6.3 LOPD.

(85)SAN 9 de mayo de 2007, FJ 4.

(86)SAN, de 20 de octubre de 2006, FJ 6.

(87)SAN de 13 de junio de 2007, FJ 3; Informe jurídico, 49/2007 AEPD.

(88)Documento de Trabajo, Grupo de Trabajo Artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.

4.3.2. El consentimiento en el ámbito de la sanidad

En el ámbito de la sanidad la aplicación de los requisitos que se han comentado no presenta mayores problemas prácticos. Lo realmente relevante en este entorno es el estudio, que se realizará posteriormente, de las excepciones al consentimiento.

En primer lugar, el cumplimiento del requisito de libertad no merece mayor comentario. No se llega a imaginar un supuesto en que el consentimiento puede obtenerse en el ámbito sanitario sin dicha libertad, más allá de que pueda cuestionarse si en situaciones en que la salud de una persona está en juego existe o no una libertad absoluta para tomar una decisión. Se ha dicho que la libertad debe llevar también a la libertad de revocar el consentimiento.

> Esta práctica podría tener sentido, por ejemplo, en casos en que unos datos que inicialmente se recabaron para que los trataran determinados sujetos ahora se pretenda que sean utilizados por otros sujetos o porque se dan circunstancias excepcionales como un cambio en la naturaleza jurídica del responsable. También en el supuesto en que una persona que se somete a un ensayo posteriormente pretende revocar su autorización. El único límite a la posibilidad de revocar debería derivar de los supuestos en que el consentimiento está exceptuado, caso, por ejemplo, de que el tratamiento de datos se esté llevando a cabo en el ámbito de una investigación de interés general.

En segundo lugar, el requisito de que el consentimiento sea inequívoco se refuerza en el caso de los datos sanitarios, en la medida en que las normas reclaman que ese consentimiento sea en estos casos expreso o, en términos del RGPD, explícito. No parece haber problema en la práctica para considerar que en el ámbito sanitario es factible el cumplimiento de esta exigencia. Cuando el usuario acude a una consulta médica para someterse a un diagnóstico y posterior tratamiento y remite al profesional la información que le reclama está consintiendo el uso de sus datos. Cuando se va a someter a una operación concreta y consiente dicha actuación, parece evidente que consiente el uso de sus datos. No cabe pensar que alguien autoriza someterse a un tratamiento

médico concreto y no va a consentir el uso de los datos necesario para llevar a cabo esa operación. En estos casos el consentimiento sería expreso por cuanto hay un comportamiento activo del titular, autorizando una operación, siempre y cuando se haya respetado previamente el derecho a ser informado antes analizado.

Cabe destacar que pueden encontrarse textos en el que el carácter inequívoco de los datos se refuerza, exigiendo que la autorización sea además de expresa escrita. Así ha sido en algún Código Tipo[89] y también en alguna Ley[90]. Tiene sentido esta exigencia reforzada si se tiene en cuenta que en la mayoría de casos el consentimiento informado para autorizar un tratamiento médico se otorga por escrito[91]. Si esto es así, parece sencillo que en el mismo escrito pueda recogerse la referencia a ambas operaciones, tanto al tratamiento médico al que se va a someter a un paciente como al tratamiento de los datos que se pretenden. Y es que no hay duda de que la mejor manera en que se deje constancia de una autorización es la forma escrita[92].

(89)Art. 5.3 Código Tipo de la Asociación Catalana de Recursos Asistenciales, inscrito en el Registro el 27 de diciembre de 2004.

(90)Arts. 5.2 y 48.1 Ley 14/2007, de 3 de julio, de investigación biomédica.

(91)Art. 8.2 LBAP.

(92)SAN de 16 de febrero de 2008, FFJJ 1 y 3.

En tercer lugar, la necesidad de que el consentimiento sea específico, consciente e informado no debería plantear mayores problemas. Más aún si se tiene en cuenta que, en el entorno sanitario, debe imperar una relación cercana y directa entre profesionales y usuarios.

Por último, la necesidad de que el consentimiento sea previo tampoco debería presentar mayores problemas. Es cierto que hay situaciones en las que podría plantearse prorrogar el consentimiento, a saber: situaciones de inconsciencia, enajenación, etc. No obstante, más que una prórroga al consentimiento quizás sería adecuado reconocer una excepción al mismo.

4.3.3. Causas que justifican el tratamiento de datos sanitarios además del consentimiento

El RGPD, al igual que lo hacía la Directiva europea de protección de datos, parte de la prohibición del tratamiento de datos de salud[93]. Para levantar esa prohibición es necesario, más allá del consentimiento del titular de los datos, que el tratamiento de la información se lleve a cabo para proteger un interés de gran relevancia. La protección de la salud puede constituir un objetivo de entidad en este sentido. Esta excepción se recoge en el RGPD, en el artículo 9, como se ha venido haciendo hasta ahora en la LOPD, artículos 7 y 8, y en la Directiva UE en el artículo 8. En cualquier caso, las excepciones al consentimiento en el ámbito sanitario pueden provenir de distintas fuentes.

(93)Art. 9 RGPD; art. 8 Directiva 95/46/CE.

1) Si lo dispone la ley a fin de proteger un interés general

En primer lugar, la excepción puede venir dispuesta en las leyes siempre y cuando sea para salvaguardar un interés general[94]. Se entiende aquí que se trata de una reserva legal, pudiéndose discutir además si se trata de una reserva

(94)Art. 9.2.g) RGPD; art. 7.3 LOPD; art. 8.4 Directiva 95/46/CE.

de ley orgánica. Pueden encontrarse leyes concretas que exceptúan el consentimiento[95]. Es necesario, además de la previsión legal, que el límite se dirija a la protección de un interés general de suficiente entidad. El propio TC ha reconocido que el concepto de «interés general» es un concepto «abierto e indeterminado»[96] (De Miguel, 2002). En la Directiva y la Recomendación del Consejo de Europa que regula el tratamiento de datos médicos se ejemplifica, en algunos apartados, el interés general refiriéndose a la seguridad del Estado, la defensa, la seguridad pública, la prevención de infracciones penales o de deontología, un interés económico o financiero importante o una función de control, de inspección o de reglamentación con el ejercicio de la autoridad pública en los casos anteriores[97]. El RGPD se refiere a «intereses públicos esenciales», lo que parece elevar el nivel de exigencia a la hora de justificar el tratamiento de datos, pues parece que no cualquier fin de «interés colectivo o público» puede legitimar dicho uso de datos. En la misma línea, cabe subrayar que el RGPD exige que si la legislación prevé excepciones al consentimiento para el tratamiento de datos de salud, debe hacerlo con ciertas garantías: el límite tiene que ser proporcional y deben adoptarse las garantías adecuadas para que el derecho a la protección de datos del interesado se vea afectado en la menor medida posible.

(95)Art. 58.2 Ley 14/2007, de 3 de julio, de investigación biomédica; art. 16.3, LBAP.

(96)STC de 11 de junio de 1984, FJ 4.

(97)Art. 13.1 Directiva 95/46/CE.

Referencia bibliográfica

Noelia de Miguel Sánchez (2002). *Secreto médico, Confidencialidad e Información Sanitaria* (pág. 283). Madrid: Marcial Pons.

2) La protección de la salud como finalidad que justifica la excepción

En segundo lugar, la excepción que más interesa es la que se refiere a la protección de la salud de las personas. Tanto la normativa estatal como la europea reconocen la posibilidad de exceptuar el consentimiento cuando esté en juego la salud de los usuarios. El RGPD justifica el tratamiento de estos datos con fines sanitarios, refiriéndose tanto a prácticas asistenciales como preventivas. Menciona, así, como actividades que justifican de una u otra manera el tratamiento de los datos de salud tanto los diagnósticos, la prestación de asistencia y la gestión de los sistemas como intervenciones dirigidas a proteger la salud pública o a la investigación[98]. En la normativa estatal, tanto el artículo 7.6 como el 8 LOPD prevén esta excepción, aunque sea de una manera un tanto críptica, al no quedar claro cuándo se aplica un precepto y cuándo el otro[99]. En la Directiva europea o en la Recomendación del Consejo de Europa la excepción aparece más clara, tanto para tareas de prevención y de asistencia sanitaria como tareas de gestión[100]. En ambas normas la protección de la salud se considera una finalidad que legitima el tratamiento de datos de salud equiparable al consentimiento del titular[101]. Por su parte, la LBAP parece partir también de la idea de que los profesionales tienen que tener acceso a la historia clínica sin necesidad de recabar el consentimiento del afectado con la finalidad asistencial[102].

(98)Arts. 9.2.h), 9.2.i) y 9.3 RGPD.

(99)Informe jurídico AEPD «Tratamiento de datos de salud», 2001.

(100)Art. 8.3 Directiva 95/46/CE; arts. 4.3 y 4.4 de la R (95) 5 Consejo de Europa.

(101)SAN de 12 de abril de 2002, FJ 5.

(102)Art. 16.1 LBAP; Resolución R/00593/2009, de la AEPD, de 25 de mayo de 2009.

Tampoco parece requerirse el consentimiento cuando la finalidad sea de gestión, administración, inspección y control de calidad, por entender que es una actividad fundamental para llevar a cabo el objetivo asistencial[103]. No sucede lo mismo en esta última norma, salvo excepción, cuando el fin sea la investigación, la docencia o la defensa de salud pública[104].

(103)Art. 16.3 LBAP.

(104)Art. 16.4 LBAP.

La interpretación conjunta de la normativa de protección de datos y de la sanitaria no es tarea fácil. La excepción al consentimiento implica partir de la idea de que los profesionales de la sanidad no tienen la obligación de recabar la autorización de los usuarios para recoger y tratar sus datos cuando el bien protegido es la salud de las personas. La excepción afecta tanto a la recogida de datos como a la posterior utilización. En la recogida la excepción opera de la siguiente manera: no se trata de que se puede obligar a nadie, salvo excepción en que esté en juego la salud pública, a aportar información sobre su persona, sino de que sea el usuario el que se responsabilice de las consecuencias de no aportar esos datos. En el caso del posterior tratamiento, la excepción implicará que no se requerirá la autorización del usuario para emplear los datos. Se entiende que la protección de la salud es un bien jurídico que merece una mayor protección en este ámbito que el derecho a la autodeterminación informativa[105].

(105)STC de 11 de abril de 1985, FJ 3.

Cabe preguntarse si todas las actividades que componen la protección de la salud exceptúan de la misma manera el derecho a la protección de datos (Navarrete, 2006). En algunos casos se ha hecho una interpretación limitativa de la excepción[106], considerando que solo es aplicable cuando una disposición expresamente lo establezca, haya una situación de urgencia o el tratamiento de datos sea estrictamente necesario[107]. En otros la interpretación ha sido más laxa, entendiendo que cabe la excepción siempre y cuando el tratamiento de datos se relacione con fines estrictamente asistenciales[108]. Por último, también se ha admitido una interpretación más amplia según la cual cabe la excepción más allá de la actividad asistencial, abrazando también actuaciones dirigidas a la prevención y gestión administrativa. Esta última interpretación encontraría fundamento en el RGPD, al igual que en la LOPD, que se refieren a todas estas actuaciones como legitimadoras del tratamiento de datos de salud (Beltrán, 2017). También en informes de la AEPD[109] y la jurisprudencia[110], y se ha aplicado para gestionar sistemas de información de algunos servicios públicos de salud, como el vasco[111]. Es necesario, sin embargo, realizar unas consideraciones al respecto.

(106)SSAN, de 31 de mayo de 2002, FJ 4; 26 de septiembre de 2002, FJ. 3.

(107)Informe jurídico AEPD, 2001, sobre tratamiento de datos de salud.

(108)Documento de Trabajo, Grupo de Trabajo Artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.

(109)Informe jurídico 005/2006, AEPD.

(110)SAN, de 23 de noviembre de 2006, FJ. 3.

(111)Comparecencia del consejero de Sanidad INCLÁN IRÍBAR, Gabriel ante la Comisión de Sanidad del Parlamento Vasco, para informar sobre el proyecto Osabide. Diario de Comisiones del Parlamento Vasco, 23 de mayo de 2002.

Referencias bibliográficas

Jesús Rubí Navarrete (2006). «Experiencias y criterios de la AEPD sobre los datos personales de la salud». En: Santiago Ripol Carulla (ed.); Jordi Bacaria Martrus (coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud* (pág. 265). Madrid: APDCat / Marcial Pons.

Juan Luis Beltrán Aguirre (2017). «Tratamiento de datos personales de salud: incidencia del Reglamento General de Protección de Datos». En: Juan Francisco Pérez Gálvez (dir.). *Salud electrónica* (pág. 111). Valencia: Tirant Lo Blanch.

En primer lugar, no parece que haya problema alguno para concluir que cabe aplicar la excepción cuando hay una situación de urgencia. Independientemente de que el paciente esté inconsciente o no, en una situación de gravedad en la que la rapidez de actuación de los profesionales puede ser un factor relevante para el tratamiento la protección de la salud, debe prevalecer sobre el derecho al consentimiento. En una situación de urgencia se entiende que tiene sentido que los profesionales tengan acceso a los datos de salud de un paciente, incluso frente a su oposición. Hay que tener en cuenta que, si no hay acceso a esa información, los profesionales serán incapaces de determinar el alcance de la urgencia y el tratamiento que se debe aplicar. Sin la información no cabe diagnóstico y tratamiento posible, con lo que la protección de la salud debe prevalecer en este caso sobre el derecho a la protección de datos.

En segundo lugar, tampoco parece que haya problema para admitir que cabe la excepción cuando el fin del tratamiento sea la asistencia sanitaria, aunque no se trate de una situación de urgencia. La normativa sanitaria reconoce en términos generales la posibilidad de que los profesionales sanitarios accedan a la historia clínica en el ejercicio de sus funciones[112]. Esta disposición podría servir de fundamento para reconocer la excepción, incluso en los casos en que haya oposición del paciente. Sin embargo, en situaciones normales o comunes, no de urgencia, podría plantearse que frente a la oposición del paciente sería necesario realizar un juicio de proporcionalidad, valorando la gravedad de la situación y la sensibilidad de los datos a los que se quisiera acceder. Piénsese, por ejemplo, en el supuesto en que una persona es tratada por un profesional sustituto que no tiene una relación de confianza asentada con el paciente. ¿No podría justificarse que el paciente, en caso de no tratarse de una situación de gravedad evidente, se opusiera a ese tratamiento? Podría admitirse el ejercicio del derecho de oposición.

[112] Art. 16.1 LBAP; art. 11.2, Ley 21/2000, de Cataluña, de 29 de diciembre de 2000, sobre los derechos de información relativos a la salud, la autonomía del paciente y la documentación clínica.

En tercer lugar, si el objetivo es la investigación médica, colisionan diferentes intereses. La CE reconoce la libertad de investigación y reclama de los poderes públicos la promoción de la ciencia y la investigación científica[113]. Sin embargo, la intimidad constituye un límite a esta actividad. La LBAP señala que, de inicio, es necesario el consentimiento del titular para manipular los datos de salud con fines de investigación, cuando estos no puedan disociarse[114]. Esta consideración resulta también de la normativa sobre ensayos clínicos y la investigación biomédica[115]. La aplicación del principio de proporcionalidad reclama que la finalidad investigadora se cumpla disociando los datos. Se entiende que únicamente en los casos en que pudiera estar en juego de una manera directa la salud pública, este objetivo podría justificar la aplicación de la excepción[116]. Esta interpretación, que hasta ahora parecía estar consolidada,

[113] Art. 44.2 CE.

[114] Art. 16.3 LBAP.

[115] Art. 60.4 Ley 29/2006, de 26 de julio de 2006, de garantías y uso racional de medicamentos y productos sanitarios. Art. 4 Ley 14/2007, de 3 de julio de 2007, de investigación biomédica.

[116] Art. 60 Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios; art. 9.2, LBAP; art. 21 Ley 14/2007, de 3 de julio, de investigación biomédica.

pues se desprendía de manera más o menos clara de la LBAP, debe revisarse a la luz del RGPD que, como se verá en el apartado siguiente, parece querer dar un impulso al tratamiento de datos con fines de investigación.

En cuarto lugar, si lo que está en juego es la salud pública, realidad que en muchas ocasiones tiene que ver con las investigaciones, también estará justificado el tratamiento, si bien el RGPD reclama que se adopten las «medidas adecuadas» para proteger los derechos de los interesados.

En términos generales, se puede observar que el RGPD mantiene la tendencia a incluir el fin sanitario como argumento suficiente para legitimar el tratamiento de datos de salud. Lo hace, sin embargo, reclamando que esos tratamientos se realicen con ciertas garantías, imponiéndolas en el caso del secreto profesional[117] y sugiriéndolas en otros casos[118].

(117) Art. 9.3 RGPD.

(118) Art. 9.4 RGPD.

5. La cesión de datos sanitarios

5.1. Requisitos generales para que la cesión sea válida

La necesidad de ceder datos sanitarios se da en múltiples ámbitos: el propio sanitario, el policial, otras administraciones, aseguradoras, etc. Piénsese, por ejemplo, que la propia normativa sanitaria reclama de las cesiones cuando aboga por la historia clínica compartida[119]. Estas cesiones deberán realizarse con ciertas garantías, pues no se puede obviar que esta operación es probablemente la que más riesgos genera para el derecho a la protección de datos. La normativa europea no regula la cesión de manera explícita, con lo que se aplica el régimen jurídico general que se ha descrito en el apartado anterior. La LOPD, en cambio, ha venido regulando de una forma un tanto caótica la cesión de datos sanitario, sin aclarar qué preceptos deben tenerse en cuenta a la hora de determinar cuándo y cómo se pueden ceder los datos sanitarios. La interpretación conjunta de los artículos 7.3, 7.6, 8 y 11 de la Ley no es sencilla. Es así que la jurisprudencia, en algún caso, ha considerado que las cesiones de datos sanitarios sin autorización expresa del paciente solo serán posibles cuando lo establezca una ley[120]. Para concretar las garantías que deben respetar estas cesiones, deberá estarse tanto a la normativa de protección de datos como a la sanitaria[121].

(119)DA Tercera LBAP.

(120)SAN de 31 de enero de 2008, FJ 3.

(121)Informe jurídico de la AEPD «Cesión de datos de salud para fines de investigación», 0509/2009.

Como se ha dicho, el estudio de la cesión de datos sanitarios no es tarea sencilla. Sin ir más lejos, la propia definición de este concepto resulta compleja.

> Por ejemplo, pueden plantearse problemas a la hora de concluir si las transmisiones de datos entre órganos de una misma administración son cesiones o no. Piénsese en el caso en que un sistema de información de un servicio público de salud se centraliza desplazando los ficheros que antes se encontraban bajo el control de diferentes órganos administrativos a la esfera de control de un único responsable que gestionará todos los ficheros y a los que tendrán acceso los diferentes usuarios para llevar a cabo sus fines. ¿Es una cesión de datos? ¿Se trata de meros accesos a partir de un punto único o general de acceso?

Más allá de los problemas que se pueden plantear a la hora de definir ese concepto, es necesario que esta operación cumpla con una serie de requisitos para que sea válida: un nuevo consentimiento del titular de los datos, una previa información sobre esta operación y, según la LOPD, que los fines que legitiman la cesión tengan relación con las funciones legítimas del cedente y del cesionario[122]. Cuando se trata de datos de salud, el consentimiento tendrá que ser expreso. La información deberá ser completa señalando las características del nuevo tratamiento que se va a dar a los datos sanitarios. Ya se dijo más arriba que, normalmente, los códigos de conducta que se han ido aprobando en este ámbito otorgan una especial relevancia a esta información[123].

(122)Art. 11 LOPD.

(123)Art. 10.1b), Código Tipo de la Unió Catalana d'Hospitals, inscrito el 12 de julio de 2002 (modificado en julio de 2004).

Cumplir con los requisitos comentados constituye algo fundamental desde el punto de vista práctico. Hay que tener en cuenta que la transmisión de datos a un tercero sin la debida habilitación puede ser sancionada, e incluso constituir un delito[124].

(124)SAN de 12 de abril de 2002; AAP de Madrid, de 19 de octubre de 2004, FJ 3.

5.2. Excepciones al consentimiento que legitiman la cesión de datos sanitarios

5.2.1. La excepción prevista en la Ley

Cabe exceptuar el consentimiento para ceder datos de salud cuando esté previsto en la Ley por razones de interés general[125]. De la Ley deberá desprenderse de manera clara la excepción. Además, esta deberá fundamentarse en la defensa de un interés legítimo de suficiente entidad[126] (Guichot, 2005). Esta excepción se reconoce también en la normativa sanitaria[127].

(125)Art. 9.2.g) RGPD; art. 7.3 LOPD.

(126)Art. 7.3 R (97) 5.

(127)Art. 7.1 LBAP.

Referencia bibliográfica

Emilio Guichot (2005). *Datos personales y Administraciones Públicas* (pág. 255). Cizur Menor: Thomson-Civitas / APDCM.

Puede ponerse como ejemplo la Ley de cohesión y calidad del Sistema Nacional de Salud, que prevé cesiones de datos sanitarios sin autorización del titular a fin de mejorar el sistema de protección de la salud de las personas[128]. También la Ley de garantías y uso racional de medicamentos y productos sanitarios reconoce excepciones semejantes. Por un lado, excepciones para que las administraciones desarrollen sus funciones de una manera eficaz[129]. Y, por otro, excepciones concretas para desarrollar actividades concretas como la farmacovigilancia[130]. En estos supuestos, se prevé de manera clara la excepción al consentimiento para ceder datos sanitarios con el fin de proteger la salud de las personas.

(128)Artículos 53 y 56 Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud; art. 10.5 RDLOPD.

(129)Art. 5 Ley 29/2006, de 26 de julio, de garantías y uso racional de medicamentos y productos sanitarios.

(130)Art. 53.2 y 3 Ley 29/2006, de 26 de julio, de garantías y uso racional de medicamentos y productos sanitarios y art. 3.3 RD 1344/2007, de 22 de octubre, por el que se regula la farmacovigilancia de medicamentos de uso humano. SAN de 24 de octubre de 2007, FJ 4.

También cabe esta excepción en supuestos en que las leyes legitiman cesiones para llevar a cabo finalidades que no tienen que ver con la protección de la salud. Es el caso en que las leyes habilitan a los funcionarios de la Seguridad Social para que conozcan datos sanitarios a fin de controlar, por ejemplo, las contingencias que una persona haya sufrido en su vida laboral que tienen que ver con su estado de salud[131]. Lo mismo podría decirse de la normativa tributaria, que facilita el acceso por la Administración tributaria a datos sanitarios a fin de controlar la actividad de determinados profesionales sanitarios[132].

(131)Art. 40.6 y 71.2 RDLeg. 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley general de la Seguridad Social. STS de 25 de febrero de 2002, FJ 3, en la que se justifica este tipo de cesiones con el fin de controlar las circunstancias en que se producen bajas laborales.

(132)Arts. 29.2 y 95 Ley 58/2003, de 17 de diciembre de 2003, general tributaria. STSJ de Asturias de 5 de junio de 2000. STS de 2 de julio de 1991.

5.2.2. La cesión entre administraciones

Es sabido que la LOPD recoge un régimen jurídico específico aplicable a la cesión de datos entre administraciones. Se está hablando del polémico artículo 21 de la LO, que no encuentra un precepto equiparable en el RGPD. Se ha discutido sobre la aplicabilidad de este precepto a la cesión de datos sensibles[133]

(Bacaría, 2006), aunque en última instancia parece que es práctica común su aplicación, basándose en las remisiones mutuas que se hacen las normas de protección de datos y las sanitarias. La aplicación de esta excepción en el ámbito sanitario podría suponer la creación de flujos de información ilimitados. No obstante, debe matizarse que una interpretación adecuada de este precepto debería llevar a concluir que estos flujos deben limitarse en aplicación del principio de finalidad. No cabe, por lo tanto, justificar basándose en ese precepto comunicaciones de datos entre administraciones para finalidades que nada tienen que ver con las que inicialmente motivaron la recogida de datos. Es decir, no cabe, como ya han señalado la AEPD y la jurisprudencia, ceder los datos de salud entre administraciones con el único argumento de que es para que el órgano administrativo cesionario lleve a cabo sus funciones[134]. Será necesario que esas funciones tengan que ver con la finalidad que motivó la recogida de los datos, que en este caso estará relacionada con la protección de la salud de las personas. Esta interpretación tiene sentido en la actualidad (Gamero y Martínez, 2008) en la medida en que se fomenta la interconexión de las bases de datos de administraciones diferentes para facilitar sistemas de información como la historia clínica única.

(133)Dictamen APDCat. CNS 11/2007 y Dictamen AVPD CN 10-030, de 14 de enero de 2011.

(134)Resolución AEPD, R/00007/2007, de 10 de enero de 2007. SAN de 27 de febrero de 2008, en la que se decide sobre la pertinencia o no del acceso a datos sanitarios para el control del uso del catalán en los centros sanitarios, señalando la necesidad de adoptar todas las garantías, como la anonimización, para llevar a cabo esta labor; STC de 23 de marzo de 2009, FFJJ 2 y 3, en la que reconoce que el acceso de la Administración a los datos de salud de una persona ha de estar justificada en una ley, sin que baste con que la Administración acceda a dicha información para llevar a cabo sus funciones; STC de 29 de junio de 2009, FFJJ 4 y 5: en este caso, los datos médicos extraídos de un proceso selectivo para acceder al cuerpo de la Ertzaintza son empleados, previa cesión de datos entre las administraciones actuantes, para excluir a dicha persona de otro proceso selectivo en otra Administración. A pesar de que el uso de los datos médicos se lleve a cabo con fines de interés público, la cesión no está legitimada.

Referencias bibliográficas

Jordi Bacaría Martrus (2006). «La aplicación de los principios básicos de la normativa sobre protección de datos a los datos médicos». En: Santiago Ripol Carulla (ed.); Jordi Bacaría Martrus (coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud*. Madrid: APDCat.

Eduardo Gamero Casado; Rubén Martínez Gutiérrez (2008). *Legislación de administración electrónica y protección de datos* (pág. 15). Madrid: Tecnos.

5.2.3. La cesión de datos con fines asistenciales

La cesión de datos sanitarios con fines asistenciales puede tener un mayor o menor alcance dependiendo de la norma que se observe. Atendiendo al RGPD[135], al reglamento que desarrolla la LOPD[136], la Directiva[137] y la Recomendación del Consejo de Europa[138], puede interpretarse que el alcance es amplio, pues esas normas emplean conceptos como «atención sanitaria» o «diagnóstico médico» a la hora de justificar la excepción. Lo mismo sucede si se atiende a la normativa sanitaria, tanto estatal[139] como autonómica[141]. Por el contrario,

(135)Art. 9.2.h) RGPD.

(136)Art. 10.5 RDLOPD.

(137)Art. 8.3 Directiva. 95/46/CE.

(138)Art. 7.3 R (97) 5.

de una interpretación literal del artículo 11 de la LOPD podría entenderse que únicamente cabe la cesión de datos sanitarios con fines asistenciales en situaciones de urgencia o para realizar estudios epidemiológicos[140].

(139)Art. 16 LBAP.

(140)Art. 11.2.f) LOPD.

(141)Art. 5 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica; art. 14 Decreto 38/2012, de 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de los pacientes y profesionales de la salud en materia de documentación clínica.

Se entiende que el criterio de urgencia no es adecuado por diferentes motivos. Primero, porque exige definir lo que se entiende por urgencia. Y segundo, porque pueden darse otras situaciones de no-urgencia en la que también puede entenderse como justificable la aplicación de la excepción. La cada vez mayor especialización de la medicina, la cada vez más compleja organización de las administraciones sanitarias (en las que intervienen cada vez más órganos y administraciones) y las múltiples situaciones que en la práctica pueden darse en el ámbito sanitario y que reclaman de una cesión de datos (un cambio de centro, un cambio en el sistema de organizar la información, etc.) hacen que sea necesario ampliar los supuestos en que se pueden ceder los datos sanitarios sin necesidad de recabar el consentimiento del afectado (De Miguel, 2002). En última instancia, tanto la AEPD[142] como la jurisprudencia[143] han parecido admitir esta interpretación amplia. Y lo mismo podría decirse del legislador que, en algunos casos, ha impuesto la obligación de crear flujos de datos para asegurar una prestación del servicio sanitario más eficiente.

(142)Informe jurídico AEPD, 0600/2009.

(143)SAP de Barcelona, de 23 de diciembre de 2004, FFJJ 4 y 5; SAP de Madrid, de 23 de marzo de 2007, FFJJ 5 y 6, en la que se justifica la revelación de información sanitaria de un paciente por parte de un médico a otro profesional sanitario, con el fin de que este le auxilie en el proceso asistencial del paciente.

Referencia bibliográfica

Noelia de Miguel Sánchez (2002). *Secreto médico, Confidencialidad e Información Sanitaria* (pág. 157). Madrid: Marcial Pons.

Es lo que ha sucedido, por ejemplo, con la obligación impuesta a los centros de las distintas CCAA de incluir un conjunto mínimo de datos en los informes clínicos para fomentar la interoperabilidad entre ellos[144]. Lo mismo podría decirse de las normas que regulan la tarjeta sanitaria[145] y la receta electrónica[146], que vienen a justificar la excepción.

(144)Exposición de motivos RD 1093/2010, de 3 de septiembre de 2010, por el que se aprueba el Conjunto Mínimo de Datos de los informes clínicos en el Sistema Nacional de Salud.

(145)Art. 57 Ley 16/2003, de 28 de mayo de 2003, de cohesión y calidad del Sistema Nacional de Salud.

(146)Art. 77.8 Ley 29/2006, de 26 de julio de 2006, de garantías y uso racional de los medicamentos y productos sanitarios; En el mismo sentido, art. 19.2 RD 1718/2010, de 27 de diciembre de 2010, sobre receta médica y órdenes de dispensación.

5.2.4. La cesión de datos sanitarios a allegados, familiares u otros terceros

Hasta hace bien poco, la LGS parecía reconocer una posibilidad genérica de transmitir a los familiares o allegados información sobre el proceso asistencial de un paciente, sin necesidad de recabar su autorización[147]. Esta previsión carece de base hoy día si se atiende tanto a la LBAP como a la jurisprudencia, que parecen exigir dicho consentimiento[148].

(148)Art. 5.1 LBAP. SAP Alicante, 6 de julio de 2001, FJ 3: «Tampoco es lo mismo la entrega del historial médico al propio paciente que la entrega realizada a un familiar». SAN de 9 de noviembre de 2005, FJ 6.

La excepción a este consentimiento podría justificarse, sin embargo, en algunos supuestos. Se está pensando, primero, en los casos en que esa comunicación puede favorecer la asistencia al paciente (piénsese en el campo de la psiquiatría o de personas que requieren de un cuidado especial[149] (Ramírez, 2009). También en el caso en que el paciente sea un menor de edad no-maduro, impedido o incapacitado. Segundo, en la situación en que la cesión es imprescindible para tratar a la persona allegada o familiar (Verdú, 2005). Tercero, podría ser necesario que se acceda a la información sanitaria de un paciente una vez este ha fallecido por razones familiares o de hecho, salvo que haya una oposición expresa del paciente, o para proteger la salud de terceros[150], supuesto polémico debido a que puede llevar a ampliar la posibilidad de acceso de estos terceros a la HC del paciente fallecido (Atela y Garay, 2004). Por último, parece que la normativa sanitaria posibilita la cesión del «informe de alta» de un paciente a los familiares[151]. Teniendo en cuenta el contenido del informe de alta es criticable esta disposición (Pellejero, 2004). Es por ello por lo que debe interpretarse en un sentido restrictivo, sin que quepa una actuación normalizada y generalizada de cesión del informe de alta a los familiares y allegados, salvo situación o autorización que lo justifique. Se está pensando, por ejemplo, en supuestos en que el paciente muestra dificultades para comprender el tratamiento a seguir después de un alta hospitalaria, o en casos en que el alta ha sido forzosa y resulta imprescindible poner en conocimiento del entorno del paciente determinada información sanitaria.

(149)STEDH de 27 de agosto de 1997, Anne Marie Andersson contra Suecia.

(150)Art. 18.4 LBAP. Dictamen AVPD CN09-044, de 26 de octubre de 2009.

(151)Art. 20 LBAP.

5.2.5. La cesión de datos sanitarios para proteger la salud pública, en especial para fines de investigación

La protección de la salud pública reclama de diferentes tipos de acciones, sobre todo de investigación epidemiológica, que encuentra regulación en diferentes normas[152]. Estas tareas exigen del tratamiento de datos de carácter personal por parte de diferentes administraciones. Hoy día, en la LBAP parece justificarse esta comunicación de datos sanitarios cuando se tenga la finalidad de prevenir a la población de un riesgo «grave» para la salud pública. En los demás casos se debe mantener la disociación de los datos[153]. La LOPD parece contravenir esta regulación al disponer que no se requiere el consentimiento del titular para ceder sus datos cuando la finalidad sea la realización de estudios epidemiológicos[154]. Lo mismo podría desprenderse de cierta jurisprudencia[155].

(147)Art. 10.4 LGS.

Referencias bibliográficas

Nieves Ramírez Neila (2009). «Accesos ilegítimos a las historias clínicas electrónicas». En: VV. AA. *El derecho a la protección de datos en la historia clínica y la receta electrónica* (pág. 296). Cizur Menor: Aranzadi / Thomson Reuters.

Fernando A. Verdú Pascual (2005). *Secreto profesional médico. Normas y usos* (pág. 70). Granada: Comares.

Alfonso Atela Bilbao; Josu Garay Isasi (2004). «Ley 41/2002 de derechos del paciente. Avances, deficiencias y problemática». En: Pedro Pérez González; Emilio Lizarraga Bonelli (coords.). *Autonomía del Paciente, Información e Historia clínica* (pág. 74). Madrid: Thomson-Civitas.

Carlos Pellejero García (2004). «Informes de alta y otra documentación clínica en la Ley 41/2002 de 14 de noviembre». En: Pedro Pérez González; Emilio Lizarraga Bonelli (coords.). *Autonomía del Paciente, Información e Historia clínica* (pág. 297). Madrid: Thomson-Civitas.

(152)RD 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica; art. 6 LBAP; art. 5.g) Real decreto, 577/2013, de 26 de julio, por el que se regula la farmacovigilancia de medicamentos de uso humano.

(153)Art. 16.3 LBAP; DF tercera y art. 41 Ley 33/2011, de 4 de octubre, general de salud pública.

(154)Art. 11.2.f) LOPD.

(155)STSJ de la Comunidad Valenciana, de 27 de noviembre de 2002, FJ 2; SAN, de 24 de marzo de 2004, FJ. 6.

Esta interpretación podría resultar también del RGPD, que parece otorgar una relevancia especial a la protección de la salud pública. Primero, porque reconoce que la protección de la salud pública legitima el tratamiento de datos de salud, cuando así se prevea en las normas, sea por «razones de interés público» y se adopten las garantías «adecuadas»[156]. Y, segundo, porque el Reglamento otorga una definición muy amplia del concepto de salud pública, lo que puede llevar a ampliar las posibilidades de tratamiento de datos con estos fines[157]. Lo cierto es que hoy día pueden encontrarse múltiples preceptos que podrían venir a justificar la cesión de datos sanitarios con esta finalidad[158], creando, por ejemplo, redes de información dirigida a la vigilancia epidemiológica[159].

Como actividad específica dirigida a proteger, aunque sea de manera preventiva, la salud pública, aunque no únicamente, debe subrayarse por su relevancia la investigación médica o científica. Viene de largo el debate entre quienes reclaman de una mayor flexibilización de las normas de protección de datos que favorezca un posible uso de la información con fines de investigación y quienes muestran un mayor celo a la hora de proteger esa información. El RGPD, como ya se ha adelantado anteriormente, otorga una importancia especial a la investigación, idea que se deduce de las múltiples referencias que realiza en su articulado a esa finalidad. Reconoce la importancia de la investigación como mecanismo de prevención[160] y, además, otorga una definición amplia a ese concepto de investigación[161]. Todo ello podría llevar a interpretar, como parece que se está pretendiendo desde algunas instancias, por ejemplo en materia de *big data* sanitario, que la investigación es en sí misma una finalidad que legitima el tratamiento de datos sanitarios. Y esa conclusión podría desprenderse de una lectura rápida de determinados preceptos del Reglamento[162]. Esta idea, sin embargo, debe matizarse. Y es que la propia norma europea, cuando se refiere a la finalidad de la investigación, realiza siempre una remisión al artículo 89, que limita las posibilidades de uso de los datos con dicho fin[163] (Mañas, 2016). Este precepto reclama que los datos empleados con fines de investigación se seudonimicen, siempre que sea posible, y se respeten con especial celo los principios de calidad de los datos. Lo cierto es que esta regulación parece dar un paso adelante en materia de investigación médica en comparación a lo que regula, por ejemplo, la LBAP. Esta Ley obliga a que los datos utilizados con fines de investigación, en general, se refieran a personas anónimas, de manera que los datos que identifiquen a los interesados permanecerán separados de los médicos. Únicamente si está en riesgo grave la salud pública pueden acceder las administraciones competentes a los datos identificados[164]. En cualquier caso, a pesar del paso adelante que parece dar el RGPD, las dudas en este ámbito de actuación son todavía varias. ¿Todas las investigaciones tienen el mismo interés para la sociedad? ¿Cuándo se considerará necesaria la seudonimización para llevar a cabo una investigación con datos sanitarios? ¿No se requerirá en ningún caso la anonimización de los datos? (Gómez, 2009). ¿Cómo se van a cumplir las obligaciones de información a los interesados? ¿Se establecerán límites de plazos para el tratamiento

(156)Art. 9.2.i) RGPD.

(157)Considerando 54 RGPD.

(158)Art. 5 Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.

(159)Art. 9 RD 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica.

(160)Considerando 113 RGPD.

(161)Considerandos 54 y 159 RGPD.

(162)Arts. 5.1.b) y 9.2.j) RGPD.

(163)Art. 9.2.j) RGPD.

(164)Art. 16.3 LBAP.

(165)Art. 12 R(97) 5.

(166)Informe jurídico de la AEPD, de 2 de abril de 2008, sobre las garantías de intimidad y protección de los datos de carácter personal de los usuarios del Sistema Nacional de Salud derivados a centros privados; Documento de Trabajo, Grupo de Trabajo Artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.

Referencias bibliográficas

José Luis Piñar Mañas (dir.) (2016). *Reglamento General de Protección de Datos* (pág. 178). Madrid: Reus.

Cristina Gómez Piqueras (2009). «Anonimización y disociación de datos personales en la investigación: cuestiones a resolver». En: VV. AA. *Protección de datos e investigación médica* (pág. 15). Cizur Menor: Aranzadi.

de datos con fines de investigación? Podría plantearse, como se hace en la Recomendación del Consejo de Europa que regula esta materia[165], que fuera un organismo concreto, por ejemplo un comité ético al que por norma se le atribuyeran las competencias pertinentes, el que determinara cuándo se dan las circunstancias oportunas que justifican este tipo de tratamientos, teniendo en cuenta la sensibilidad de los datos que se van a tratar y el interés general que se pretende proteger[166].

5.2.6. La cesión de datos sanitarios con fines de gestión

Se plantea en este apartado si es posible ceder los datos sanitarios con la finalidad de gestionar los servicios sanitarios, a saber: con fines de inspección, de control económico, disciplinarios, etc. Esta actividad requiere en muchos casos del acceso a información sanitaria de los pacientes (Castellano, 1997). En algunas ocasiones, además, estas tareas se llevan a cabo desde empresas privadas y colegios profesionales. Operaciones de este tipo se justifican en múltiples normas, sin que se requiera el consentimiento de los pacientes[167]. La propia LBAP dispone que los profesionales tendrán acceso a las historias clínicas para el desarrollo de estas funciones[168]. Lo mismo podría desprenderse del RGPD y la LOPD al justificar el tratamiento de datos de salud con la finalidad de «gestionar» los servicios sanitarios[169].

(167)Art. 79 Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

(168)Art. 16.5 LBAP.

Referencia bibliográfica

María Castellano Arroyo (1997). «Problemática de la historia clínica». *Actas del Seminario Conjunto sobre información y documentación clínica* (pág. 63). Madrid: Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo.

(169)Art. 9.2.h) RGPD; 7.6 LOPD. AAP Segovia, núm. 95/2000, Sección única, justifica la potestad del INSALUD para llevar a cabo acciones de inspección, para lo cual es necesario que tenga la posibilidad de acceder a las historias clínicas. Resolución de la APDCM, de 18 de septiembre de 2009, «... la cesión con fines de inspección no requiere del consentimiento al estar habilitada por la LBAP». STS de 13 de mayo de 2009, FJ 8. Dictamen AVPD CN10-004, de 8 de marzo de 2010, justifica el acceso de personal administrativo a determinada información con fines de carácter administrativo, si bien limita esta facultad de acceso a los datos necesarios para realizar esas funciones, negando la posibilidad de acceso a las historias clínicas.

5.2.7. Otras cesiones de datos sanitarios fuera del ámbito sanitario

La salida de los datos de salud fuera del ámbito sanitario ha sido vista con recelo, sobre todo desde la jurisprudencia[170]. Sin embargo, son múltiples los casos en que estas comunicaciones están justificadas.

(170)SAN de 9 de julio de 2008, FJ 4; STEDH de 6 de octubre de 2009, C. C. contra España, FFJJ 26-41.

1) La comunicación puede darse a favor de las compañías aseguradoras con el fin de que estas vean justificado el gasto que deban hacer a favor del paciente. En este caso, se puede entender que la normativa sectorial favorece esta cesión sin necesidad de recabar la autorización de los afectados[172], para que puedan conocer si el desembolso de una cantidad de dinero que van a realizar está justificado o no. Así se ha admitido expresamente en algunas normas[171].

(171)Art. 16.4 Decreto 38/2012, de 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica,

(172)Art. 7.1 RDL 8/2004, de 29 de octubre de 2004, por el que se aprueba el texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor; art. 18 Ley 50/1980, de 8 de octubre, de contrato de seguro; apartado I, Informe jurídico de la AEPD, «Cesión de datos de salud a aseguradoras de asistencia sanitaria por centros sanitarios públicos», 526/2003; Informe jurídico de la AEPD, «Cesión de datos de salud a efectos de facturación», 114/2006. SAN de 22 de septiembre de 2004, FJ 2; 18 de enero de 2007, FJ 5, que señala que a pesar de que las previsiones legales no establecen de forma expresa una excepción al consentimiento, esta se deduce del articulado de las leyes.

2) La comunicación también puede darse con fines policiales. Es evidente que estos fines exigen en ocasiones el tratamiento de datos sanitarios[176]. Las normas de protección de datos disponen que las policías pueden tratar estos datos cuando sean «absolutamente necesarios» para llevar a cabo investigaciones concretas y se adopten las garantías adecuadas[173]. En el mismo sentido se pronuncian las normas que regulan la organización y el funcionamiento de las policías[174]. Así, se ha venido interpretando que, a pesar de que las leyes no lo prevean expresamente, no se requiere del consentimiento de los afectados para la cesión de datos sanitarios con fines policiales[175] (Martínez, 2001). Otra cosa es determinar el alcance de esa excepción, y es que se han venido siguiendo interpretaciones diferentes, más o menos estrictas, de la misma.

(173)Art. 22.3 LOPD; art. 10 Directiva 2016/680, de 27 de abril de 2016.

(174)Art. 11.1.g) y h) LO 2/1986, de 13 de marzo, de fuerzas y cuerpos de seguridad.

(175)STS de 20 de mayo de 2008, FJ 4.

Referencia bibliográfica

Ricard Martínez Martínez (2001). *Tecnologías de la Información, Policía y Constitución*. Valencia: Tirant Lo Blanch.

(176)STS de 4 de octubre de 2006, FJ 1, se autoriza el acceso de la policía a la información resultante del análisis de una muestra de saliva extraída de una colilla. STEDH de 4 de diciembre de 2008, S. y Marper contra Reino Unido, FFJJ 113-126, concluye que si bien el uso de estas herramientas puede ser útil en la lucha contra el terrorismo, deberá hacerse de acuerdo al principio de proporcionalidad.

3) La comunicación también puede producirse a favor de los tribunales. Tanto las normas de protección de datos[177] como la normativa sanitaria[178] reconocen la posibilidad de comunicar datos sanitarios a favor de los tribunales a fin de garantizar el derecho a la tutela judicial efectiva (Domínguez, 2007). Los tribunales también parecen haber admitido esta opción sin mayor reserva, por ejemplo en la conocida STEDH Z. contra Finlandia[179]. Esta interpretación, sin embargo, merecería una profundización mayor que la que realizan las normas. Los problemas se producen cuando una persona distinta al paciente reclama que se aporten al proceso datos sanitarios de este último. Lógicamente, las características de cada proceso llevará a la aplicación de normas concretas (Rodríguez, 2004):

(177)Art. 9.2.f) RGPD; art. 11.2.d) LOPD.

(178)Art. 16.3 LBAP.

Referencias bibliográficas

Andrés Domínguez Luelmo (2007). *Derecho sanitario y responsabilidad médica. Comentarios a la Ley 41/2002, de 14 de noviembre, sobre derechos del paciente, información y documentación clínica* (pág. 545). Valladolid: Lex Nova.

Pedro Rodríguez López (2004). *La autonomía del paciente: información, consentimiento y documentación clínica* (pág. 221). Paracuellos del Jarama: Dilex.

(179)SAP Barcelona 5 de enero de 1998, FJ 1; SAN de 11 de enero de 2010, FJ 4, en el que se decide que los datos de salud han de ser trasladados a sede judicial en la medida en que constituyen elemento relevante de prueba; STC de 2 de marzo de 1989, FJ 4, en la que se justifica la entrada y registro por orden judicial en una clínica para acceder a determinados datos sanitarios de una persona implicada en un proceso judicial; STS de 2 de diciembre de 1996, FJ 1; STEDH de 25 de febrero de 1997, Z. contra Finlandia, FJ 97 y siguientes; STS de 23 de noviembre de 2007, FJ 2.

1) En los procesos civiles, la Ley de enjuiciamiento civil (LEC) abre la puerta a esta posibilidad, tanto cuando regula las diligencias preliminares como los medios de prueba[180]. De inicio, parece que los jueces y tribunales tienen la facultad de determinar qué información es pertinente y cuál no. Sin embargo, en la práctica no parece haber problema para reclamar que la información sanitaria se aporte a los procesos civiles[181], si bien respetando los principios de

(180)Art. 256.1.5.bis) LEC; art. 371.1 LEC.

(181)SAP de Madrid 12 de diciembre de 2005, FJ 2.

finalidad y pertinencia[182]. Esta posición debería matizarse en las normas, si se tiene en cuenta sobre todo que en los procesos civiles no se protegen intereses generales sino particulares. Debería analizarse, en cada caso, hasta qué punto la aportación de una información favorece la salvaguarda de la tutela judicial efectiva de una persona y cuál es la sensibilidad de esta información, para ponderar los intereses en juego.

(182)STS de 25 de febrero de 2002, FJ 3.

2) En el ámbito penal, se podrían analizar situaciones diferentes. Primero, la obligación de acuerdo a la Ley de enjuiciamiento criminal (LECrim) y al Código penal (CP) de denunciar los hechos delictivos de los que se tenga conocimiento[183], a pesar de que en algunos casos se ha pretendido aplicar a los profesionales sanitarios la exclusión de denunciar que protege a abogados o ministros de cultos[184]. La obligación de denunciar, sin embargo, debería encontrar matices, pues no debería ser lo mismo denunciar hechos del pasado o hechos que todavía no han ocurrido pero se han planificado y que se pueden evitar. Tampoco es lo mismo que se trate de delitos menores o de delitos graves. Segundo, la obligación de un profesional sanitario de declarar como testigo. Frente a la obligación genérica de declarar la LECrim, reconoce que los funcionarios obligados por el secreto no podrán ser obligados a declarar[185]. Pero, por otro lado, se viene admitiendo que en los procesos penales se acceda a la información sanitaria, sin que se ponga en cuestión que dicha actuación pueda vulnerar el deber de secreto[186].

(183)Art. 450 CP y 259 LEcrim.

(184)Art. 263 LECrim.

(185)Art. 417 LECrim.

(186)STC de 15 de febrero de 1989, FJ 4; Resolución AEPD, R/00645/2004, de 26 de noviembre de 2004.

3) En el ámbito administrativo pueden distinguirse diferentes situaciones. Primero, en procedimientos administrativos sancionadores o en reclamaciones de responsabilidad patrimonial de la Administración, algunas normas parecen admitir la posibilidad de que se acceda a la información sanitaria[187], lo mismo que ha hecho en algún caso alguna agencia de protección de datos[188]. Segundo, en procesos judiciales a seguir en la jurisdicción contencioso-administrativa, la Ley reconoce también la posibilidad de aportar pruebas y el expediente administrativo correspondiente al proceso[189]. En ambos casos podrían encontrarse, por lo tanto, argumentos para favorecer la cesión de datos[190].

(187)Art. 19 Ley 3/2001, de Galicia, de 28 de mayo de 2001, del consentimiento informado y de la historia clínica de los pacientes. Art. 14 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica.

(188)Resolución APDCM, de 18 de septiembre de 2009, «La potestad sancionadora de una Administración habilita la utilización de datos personales para el esclarecimiento de los hechos».

(189)Arts. 45, 60 y 61 LJCA.

(190)SAN de 18 de febrero de 2009, FJ 3. Informe jurídico AEPD 0400/2008.

6. Los derechos de los pacientes

Es conocido que el derecho a la autodeterminación informativa reconoce, además de los contenidos hasta ahora analizados, una serie de facultades a ejercer positivamente por su titular. Se trata en lo que aquí interesa del derecho de acceso, rectificación y supresión. En el ámbito sanitario, el ejercicio de estos derechos tiene una relevancia especial debido a que a través de ellos se garantiza no únicamente el control activo de los afectados sobre sus datos, sino también la calidad de la información.

6.1. El derecho de acceso

6.1.1. El ejercicio del derecho de acceso en el ámbito sanitario

El derecho de acceso implica el derecho del titular de los datos a conocer lo que sucede con ellos cuando están siendo manipulados por otro sujeto: qué datos se están tratando, cuáles son las fuentes de los datos, las comunicaciones previstas, etc.[191] En el ámbito sanitario este derecho tiene una importancia especial porque no solo constituye un instrumento para controlar el tratamiento de sus datos, sino también un mecanismo para conocer su estado de salud en un momento determinado.

(191)Art. 15 RGPD; art; 15 LOPD; art. 12 Directiva 95/46/CE.

La normativa de protección de datos pasa por encima de esta cuestión, salvo puntuales excepciones[192], teniendo que acudir a la normativa sanitaria para conocer su alcance en este sector. Las normas reconocen tanto el derecho del paciente a acceder a la documentación clínica y a obtener copia de los datos que obran en ella[193] como el derecho a la información asistencial[194]. Se trata de dos instrumentos diferentes que favorecen el conocimiento por el afectado de lo que sucede con sus datos. Por un lado, como paciente, puede conocer puntualmente cuál es su estado de salud. Por otro, como usuario que no está siendo objeto de un tratamiento médico concreto, tiene derecho a acceder a los datos que se están tratando y a conocer lo que se hace con ellos. El ejercicio del derecho de acceso a la historia clínica se regula expresamente en algunas normas sanitarias[195]. Lo mismo sucede con el derecho a recibir información sobre la salud en un proceso asistencial, aunque sin establecer procedimientos rigurosos para ello[196]. Estas previsiones deben cohonestarse con las realizadas en la normativa de protección de datos al respecto.

(192)Considerando 42 Directiva 95/46/CE; art. 8 R (97) 5.

(193)Art. 18.1 LBAP.

(194)Art. 4 LBAP.

(195)Resolución de 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la historia clínica en el ámbito del Sescam (Servicio de Salud de Castilla-La Mancha); art. 12 Decreto 38/2012, de 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

(196)Art. 4.1 LBAP.

El acceso a los ficheros sanitarios por parte del usuario debe tener en cuenta diferentes factores. Primero, se trata de una información técnica, con lo que su comprensión por el usuario requerirá en muchos casos de la colaboración de los profesionales. Segundo, el acceso a la información sanitaria no se limita al acceso a la historia clínica sino que abarca a todo fichero que contenga datos de carácter personal[197]. Tercero, hay que preguntarse hasta qué punto puede el ejercicio del derecho de acceso conllevar un derecho a obtener una copia de la documentación obrante en los ficheros. Este derecho podría encontrar apoyo tanto en las normas como en cierta jurisprudencia[198]. Sin embargo, su alcance debe reinterpretarse en el sentido de que los usuarios tendrán derecho a acceder a los datos que le afectan, no a una copia íntegra de los documentos. Lo contrario sería inoperable desde un punto de vista práctico, debido a lo costoso que puede resultar hacer una copia de todos los documentos y pruebas que se le hayan hecho a cada paciente a lo largo de su vida. Esta opción cabría en situaciones justificadas, como podría ser un cambio de centro. Por último, cabe reconocer también, tal como se prevé expresamente en las normas en términos generales[199], en el ámbito sanitario la posibilidad de limitar el ejercicio del derecho de acceso a intervalos concretos de tiempo, de modo que, salvo causa justificada, los usuarios no puedan abusar de su ejercicio.

(197)Resolución AEPD R/00608/2008, de 2 de junio de 2008: cuando se reconoce el derecho de acceso a la HC se refiere al acceso a la información contenida en el artículo 15 LBAP.

(198)Art. 15.3 RGPD; art. 15.2 LOPD; art. 18.1 LBAP; STSJ de Castilla y León, 29 de mayo de 2007, FJ 8: se analiza el derecho de acceso de un paciente a su historia clínica, apelando a una interpretación amplia de dicho derecho; STEDH de 28 de abril de 2009, K. H. y otros contra Eslovaquia, FFJJ 44-58.

(199)Art. 12.5 RGPD.

6.1.2. Los límites al derecho de acceso en el ámbito sanitario

Los límites al derecho de acceso pueden derivar de la aplicación de la normativa de protección de datos y de la normativa sanitaria. En el primer caso, esos límites deben aplicarse en el ámbito sanitario, si bien puede haber problemas para imaginar cuándo se pueden ejecutar en la práctica[200]. ¿El derecho de acceso cuándo puede entorpecer la protección de la seguridad del Estado, la defensa o la seguridad pública, o la posibilidad de reprimir crímenes? Es en la normativa sanitaria donde se reconocen los principales límites que aquí interesan:

(200)Art. 8.2 R (97) 5; art. 13.1.a), b) y c) Directiva 95/46/CE; art. 23.1 LOPD; art. 23 RGPD.

El primer límite lo constituye la intimidad de terceros[201]. El acceso de un usuario a sus datos sanitarios no puede comprometer la confidencialidad de la información relativa a terceros, salvo que ese acceso sea necesario para proteger la salud del paciente, como ha puesto de manifiesto, por ejemplo, el TEDH en el conocido caso Gaskin contra Reino Unido[202].

(201)Art. 18.3 LBAP; art. 23.1 LOPD; art. 8.2.c) R (97) 5.

(202)STEDH, 7 de julio de 1989. Caso Gaskin contra Gran Bretaña, recoge el problema que puede llegar a plantearse entre el derecho de acceso de una persona a ficheros que contienen datos de carácter personal que le conciernen y el derecho a la intimidad de terceras personas.

El segundo límite lo constituye la protección de la salud del propio paciente o usuario[203], lo que se viene calificando como «motivo terapéutico». Este concepto debe ser interpretado en sentido restrictivo para que no se convierta en un argumento recurrente para limitar el derecho de acceso sobremanera (Murillo, 2006).

(203)Art. 8.2.b) R (97) 5; art. 13.1.g) Directiva 95/46/CE; art. 5.4 LBAP.

Referencia bibliográfica

Pablo Lucas Murillo de la Cueva (2006). «El derecho fundamental a la protección de los datos relativos a la salud». En: Santiago Ripol Carulla (ed.); Jordi Bacaría Martrus (coord.). *Estudios de protección de datos de carácter personal en el ámbito de la salud* (pág. 37). Madrid: APDCat.

El último límite lo constituyen los derechos que los profesionales puedan alegar sobre la información que tratan[204] (Cantero, 2009). Se estaría pensando, sobre todo, en los derechos que pueden tener sobre los comentarios, valoraciones o anotaciones subjetivas que incluyan en la documentación clínica. Son límites que tanto los tribunales como las agencias de protección de datos han aceptado[205], a pesar de que plantean algún problema de interpretación: primero, la necesidad de definir lo que se entiende por «anotación subjetiva», y es que a pesar de que tanto normas[207] como tribunales[206] han tratado de definirlo, no queda claro su alcance. Segundo, tampoco está clara cuál es la fundamentación jurídica del límite. ¿Se basa en un supuesto derecho a la propiedad intelectual del profesional? ¿Se trata de proteger su intimidad? Se entiende aquí que ese concepto debe interpretarse en un sentido restrictivo, limitándose a las apreciaciones subjetivas que el profesional realice sobre aspectos que no tengan que ver directamente con la salud de las personas, sino con su comportamiento, personalidad, entorno, etc.

(204)Art. 18.3 LBAP.

(205)STSJ de Castilla y León, 29 de mayo de 2007, FJ 8; Resolución de la AEPD R/00969/2008, 31 de julio de 2008. En algún caso parece haberse limitado el derecho de acceso a la información sanitaria, por exceder lo previsto en la LOPD y reglamento.

(206)STSJ de Castilla y León, 29 de mayo de 2007, FJ 8.

Referencia bibliográfica

Roberto Cantero Rivas (2009). «La historia clínica: naturaleza y régimen jurídico». En: VV. AA. *El derecho a la protección de datos en la historia clínica y la receta electrónica* (pág. 213). Cizur Menor: Aranzadi.

(207)Art. 4.3.7.b) Resolución de 27/02/2009, de la Dirección Gerencia, que aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la historia clínica en el ámbito del Sescam; art. 64.4 Ley 17/2010, de 8 de noviembre, de derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra; art. 21 Decreto 29/2009, de 5 de febrero, de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica. Art. 7.4 Decreto 38/2012, de 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

6.2. Los derechos de rectificación y supresión en el ámbito sanitario

El correcto ejercicio de estos derechos resulta fundamental para garantizar la calidad de los datos, cosa importante en el ámbito sanitario ya que el empleo de datos cuya calidad no está contrastada puede resultar perjudicial a la hora de llevar a cabo un tratamiento médico. La regulación que en la normativa de protección de datos se hace de estos derechos[208] debe cohonestarse con lo establecido en las normas sectoriales. En estas se subraya la importancia de que la historia clínica responda en todo momento a criterios de veracidad y

(208)Arts. 16 y 17 RGPD; art. 16 LOPD.

(209)Art. 15.1 LBAP.

actualidad[209]. Más allá de esta consideración lógica, sin embargo, no entra a detallar cómo se deben ejercer estos derechos. La principal aportación es el establecimiento de la obligación de conservar los datos durante determinados plazos. A pesar de ello, debe entenderse que estos derechos tienen plena vigencia en el ámbito sanitario.

Primero, debe poder ejercerse el derecho de rectificación si se observan datos erróneos, incompletos o desfasados. Esta posibilidad, sin embargo, se enfrenta a dificultades, a saber[210]: la imposibilidad de cancelar datos del pasado debido al deber legal de conservarlos durante un plazo; la complejidad y el alto grado de tecnicismo de la información que se pretende rectificar; el alto componente subjetivo que la información sanitaria puede tener. No es infrecuente que un paciente y un profesional no converjan a la hora de determinar un diagnóstico o un tratamiento, más ahora que los pacientes acceden en internet a diversas fuentes de información sanitaria.

Segundo, en relación con el derecho de supresión, que sustituye al anteriormente conocido como derecho «de cancelación», a pesar de que las normas reconocen este derecho[211], su ejercicio es especialmente complicado en la práctica debido a la obligación que imponen las leyes de conservar la información sanitaria con diversos fines, tanto asistenciales como otros[212] (Atela y Garay, 2004). La LBAP señala que los centros están obligados a conservar los datos con el fin de otorgar la debida asistencia, durante el tiempo adecuado, mínimo de cinco años a contar desde la fecha del alta de cada proceso asistencial[213]. Otros fines como los judiciales, los estudios epidemiológicos, las investigaciones, la organización y el funcionamiento de los sistemas sanitarios también justifican en la Ley la conservación de los datos de carácter personal, si bien, en la medida de lo posible, la conservación se hará de manera que estos aparezcan disociados[214]. En la normativa autonómica también se recogen estos plazos, y en muchos casos se amplían[215]. La AEPD ha subrayado la obligación de conservar los datos, que persiste incluso cuando un centro va a cesar en su actuación[216]. Estas previsiones plantean la cuestión de si es posible en determinados supuestos una conservación *sine die* de los datos sanitarios. La propia LBAP fija un plazo mínimo de conservación, pero no establece un plazo máximo[217] (Coudert, 2007). Esta regulación debería matizarse atendiendo a las diferentes características que tienen las diversas finalidades que pueden justificar la conservación. Y es que no es lo mismo que los datos se conserven para cumplir fines de investigación, lo que podría llevar a una ampliación de estos plazos[218], que para fines judiciales[219]. Además, una vez los datos hayan cumplido sus finalidades iniciales, principalmente asistenciales, deberá pensarse si

(210)STSJ de la Rioja, de 17 de octubre de 2008, FJ 2: lo único que podría hacer el tribunal es verificar si, ante la petición de rectificación del interesado, el centro sanitario ha dado una respuesta adecuada y fundamentada. Otra cosa sería si el interesado presenta, por ejemplo, informes médicos de una segunda opinión que desmienten lo que el principal profesional sanitario ha apuntado y valorado en la historia clínica. En este caso se debería valorar la posibilidad de rectificar el contenido de la HC.

(211)Art. 27 Decreto 38/2012. 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.

(212)Informe jurídico AEPD, «La cancelación de los datos contenidos en historias clínicas», núm. 189/2003, 2003. Resolución de la AEPD R/01103/2009, de 20 de abril de 2009, donde niega a un interesado el derecho a cancelar los datos contenidos en HC.

(213)Art. 17.1 LBAP.

(214)Art. 17.2 LBAP.

(215)Artículo único puntos 4 a 10 Ley 16/2010, 3 de junio, de modificación de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente y la documentación clínica.

(216)Informe jurídico AEPD 0551/2008.

(217)Resolución AEPD R/00113/2005, 22 de marzo de 2005.

es necesario conservar los datos asociándolos a los usuarios o de forma disociada[220] y si es imprescindible, además, que los ficheros se conserven activos o basta con que la documentación sea pasiva, siendo su uso limitado[221].

Referencias bibliográficas

Alfonso Atela Bilbao; Josu Garay Isasi (2004). «Ley 41/2002 de derechos del paciente. Avances, deficiencias y problemática». En: Pedro Pérez González; Emilio Lizarraga Bonelli (coords.). *Autonomía del Paciente, Información e Historia clínica* (pág. 52). Madrid: Thomson-Civitas.

Fanny Coudert (2007). «Tratamiento de datos especialmente protegidos». En: Cristina Almuzara Almaida (coord.). *Estudio práctico sobre la protección de datos de carácter personal* (pág. 352). Valladolid: Lex Nova.

(218)cuando la finalidad perseguida sea la investigación científica, siempre que se guarden las garantías del artículo 89 de la norma.*sine die*Art. 5.1.e) RGPD, parece abrir la puerta a que los datos se conserven

(219)STS 21 de junio de 2004, FJ 2, donde se pone de manifiesto la necesidad de conservar los datos sanitarios, con el fin de salvaguardar la tutela judicial efectiva en futuros procesos judiciales en que el empleo de la información médica pueda constituir un medio de prueba. Concluye el tribunal que no es necesario, para proteger el derecho a defenderse en futuros procedimientos, conservar indefinidamente toda la historia clínica de todas las personas.

(220)Ley 16/2010 de Cataluña, artículo único 7; Decreto 38/2012. 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica, artículo 21.8.

(221)Recomendación 2/2004, de 30 de julio, de la APDCM, sobre custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas, artículo segundo punto quinto.

Abreviaturas

AAP Auto Audiencia Provincial.

AEPD Agencia Española de Protección de Datos.

APDCat Autoridad Catalana de Protección de Datos.

APDCM Agencia de Protección de Datos de la Comunidad de Madrid.

AVPD Agencia Vasca de Protección de Datos.

CE Constitución española.

CP Código penal.

HC Historia clínica.

LBAP Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

LEC Ley de enjuiciamiento civil.

LECrim Ley de enjuiciamiento criminal.

LGS Ley general de sanidad.

LOPD Ley orgánica de protección de datos.

RDLOPD Reglamento de desarrollo de la Ley orgánica de protección de datos.

RGPD Reglamento general de protección de datos de la UE.

SAP Sentencia Audiencia Provincial.

SAN Sentencia Audiencia Nacional.

STC Sentencia Tribunal Constitucional.

STEDH Sentencia Tribunal Europeo de Derechos Humanos.

STS Sentencia Tribunal Supremo.

STSJ Sentencia Tribunal Superior de Justicia.

TIC Tecnologías de la información y la comunicación.