Universitat de Barcelona
Observatori de Bioètica i Dret Universitat de Barcelona
FLACSO ARGENTINA

Revista de Bioética y Derecho
Perspectivas Bioéticas

www.bioeticayderecho.ub.edu - ISSN 1886-5887

ARTÍCULO

La historia clínica compartida y el ejercicio de la autonomía de las personas en sanidad

Shared Electronic Health Record and the exercise of personal autonomy in Health

LIDIA BUISÁN I ESPELETA *

OBSERVATORI DE BIOÈTICA I DRET DE LA UNIVERSITAT DE BARCELONA

La Revista de Bioética y Derecho se creó en 2004 a iniciativa del Observatorio de Bioética y Derecho (OBD), con el soporte del Máster en Bioética y Derecho de la Universidad de Barcelona: www.bioeticayderecho.ub.edu/master. En 2016 la revista Perspectivas Bioéticas del Programa de Bioética de la Facultad Latinoamericana de Ciencias Sociales (FLACSO) se ha incorporado a la Revista de Bioética y Derecho.

* Lídia Buisan i Espeleta. Licenciada en Medicina y Doctora en Derecho. Miembro del Observatori de Bioètica i Dret, Universitat de Barcelona. Correo electrónico: lidia.buisan@sanitatintegral.org

Resumen

En este artículo se exponen los elementos principales que configuran la relación entre los usuarios de la sanidad y la gestión de sus datos personales de salud en el marco de la implementación de la historia clínica compartida, poniendo el énfasis en los riesgos que para la privacidad de las personas y para la debida confidencialidad pueden ocasionar la compartición de estos datos sensibles.

Palabras clave: historia clínica; confidencialidad; protección de datos; secreto médico.

Abstract

This article set out the main elements that structure the relationship between Health Service users and the management of their personal health data, in the frame of implementation of Shared Electronic Health Record, emphasizing the risks that sharing this sensitive data can produce to personal privacy and confidentiality.

Keywords: health record; confidentiality; data protection; medical secrecy.

1. El consentimiento del paciente en el tratamiento de los datos de salud. Excepciones legales

El derecho a la intimidad está reconocido constitucionalmente en toda su dimensión, incluida la informática, según el artículo 18.4 CE, por lo que no es discutible que los ciudadanos tengan derecho a una privacidad informática, si utilizamos la terminología anglosajona, o a la autodeterminación informática, en terminología alemana. Tampoco es motivo de discusión que en el ámbito de la salud es imposible gestionar los servicios sanitarios sin una informatización de los datos sanitarios. Se genera, por tanto, una dialéctica de tensión entre, por un lado, un derecho a la privacidad en su proyección informática y la creciente e imparable utilización de las TIC para el tratamiento informatizado de los datos sanitarios, y por otro, si estos datos se gestionan de manera que sean compartidos por los diferentes agentes de salud. Según Fermín Morales[1], todas las fórmulas jurídicas vienen a significar un pacto entre tecnología y libertad que suponga generar un circuito de confidencialidad de los datos sanitarios y un derecho de control de los mismos por parte de la persona afectada. Este mismo autor se preguntaba, hace ya diez años, si se había establecido este circuito de confidencialidad necesario en el ámbito sanitario, y reconocía que no. Pero, hoy esta misma pregunta sigue siendo del todo procedente e igualmente debemos responder que no, aunque se haya avanzado parcialmente. ¿Por qué motivos?

En especial, por los mismos motivos que este autor remarcaba tras la aprobación de la LOPD: si bien en el artículo 7 se inscriben los datos sanitarios en el núcleo duro de la privacidad de la persona —pues se dice que son datos especialmente protegidos—, después, el legislador, en el mismo artículo 7 y en el artículo 8, levanta las garantías jurídicas porque es consciente de que estos datos deben poder circular dentro del ámbito sanitario público; así, en el artículo 11 se refiere a que se podrá acceder a estos datos especialmente protegidos entre los centros sanitarios del circuito público de salud. El articulado antes referenciado contiene más bien declaraciones retóricas que un estatuto jurídico de confidencialidad de los datos de salud. A todo eso, se debe recordar también que esta especial protección de los datos de salud resulta, además, de las normas internacionales y comunitarias reguladoras del tratamiento automatizado de los datos de carácter personal tal como lo recoge el Informe 0367/2009 de la Agencia Española de Protección de Datos (AEPD).

[1] MORALES F., Ponencia presentada en el IX Congreso Derecho y Salud, noviembre de 2000. Véase en: http://www.ajs.es/revista-derecho-y-salud/volumen-9-num-2-2001 (última consulta: 15 de mayo 2013).

El tratamiento de los datos de carácter personal está recogido en los artículos 6 y 11 de la LOPD con especiales restricciones en lo que se refiere a los datos sanitarios; entre otros, el artículo 7 de la misma Ley, establece en su apartado 3, que como regla general "los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo determine una ley o el afectado consienta expresamente".

Conviene analizar también la Ley 21/2000 del Parlament de Catalunya y la Ley básica 41/2002, de 14 de noviembre. Estas dos leyes regulan, entre otros, los aspectos relativos a la propiedad de la historia clínica, pero también su utilización. De manera destacada, determinan que el titular de la información que contiene la historia clínica es el paciente y que sólo podrán ser informados de este contenido otras personas en caso que el paciente expresa o tácitamente lo consienta. En el artículo 11 de la citada Ley 21/2000 se hace referencia a los usos de la historia clínica, y en ningún lugar consta que pueda haber cesión de datos sin consentimiento del paciente, ya que los apartados 1 y 2 sólo se refieren el acceso a la historia clínica por parte de los profesionales asistenciales implicados en un episodio clínico de un paciente. El apartado 3 trata del acceso con fines epidemiológicos, de investigación o docencia, y los apartados 4 y 5 tratan, respectivamente, de los datos a los que tiene acceso el personal de administración y gestión de los centros sanitarios, así como el personal al servicio de la Administración sanitaria que ejerce funciones de inspección.

Además, la Ley 16/2010, de 3 de junio, de modificación de la Ley 21/2000, de 29 de diciembre, consta de un único artículo de modificación del anterior artículo 12, que en su punto 5, habla de intercambio de datos entre los dispositivos asistenciales de las diferentes comunidades autónomas, por lo que cabe entender que puede haber, efectivamente, cesión de los datos de salud. En la disposición adicional de esta ley[2], se da un plazo de cuatro años para garantizar la existencia de la historia clínica compartida, así como para el acceso a la misma. Hay que entender, naturalmente, que los profesionales sanitarios podrán acceder a los datos de los pacientes que sean necesarios para la asistencia sanitaria y que los pacientes podrán acceder a sus datos de salud contenidos en la historia clínica compartida.

La Ley 41/2002, de 14 de noviembre, *básica reguladora de la autonomía del enfermo y de los derechos y obligaciones en materia de información y documentación clínica*, limita, en el artículo 16

[2] Véase en: Disposición adicional de la Ley 16/2010, del 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.*

(apartados 3 y 5), los supuestos de cesión de datos de la historia clínica a terceros ajenos a la asistencia sanitaria en los siguientes términos:

Artículo 16

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

En el mismo reglamento de la LOPD,[3] en su artículo 10, apartado 5 parte final, se afirma que "no es necesario el consentimiento de la persona interesada para la comunicación de datos personales sobre la salud, inclusive por medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando dicha comunicación se lleve a cabo para la atención sanitaria de las personas, de acuerdo con lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud". De la lectura de este texto normativo se desprende, sin lugar a dudas, que se autoriza la cesión de datos de salud, sin el consentimiento del interesado, entre organismos, centros y servicios del Servicio Nacional de Salud cuando dicha cesión se realice al amparo y en el marco de la atención sanitaria de los ciudadanos.

[3] Real Decreto 1720/2007, de 21 de diciembre, por el cual se aprueba *el Reglamento que desarrolla la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos Personales.*

2. Autonomía del enfermo *versus* tratamiento de los datos de salud de la historia clínica compartida sin su consentimiento

Como se acaba de exponer, el Real Decreto 1720/2007, de 21 de diciembre, ya citado, autoriza la cesión de datos de salud entre organismos, centros y servicios del SNS, sin el consentimiento de las personas afectadas, cuando ello se realice para la atención sanitaria de estas personas.

Este planteamiento abre un conjunto de preguntas que se pueden sintetizar así:

- ¿Cómo queda afectado el deber de respetar la autonomía de las personas en los ámbitos sanitarios catalán y español?
- ¿Deben los ciudadanos renunciar necesariamente a parte de su intimidad con el fin de poder acceder a la asistencia sanitaria pública?
- ¿Podemos saber los ciudadanos quién puede acceder, o ya ha accedido, a nuestros datos de salud, a qué datos concretos y con qué objetivo?

Para responder a estos interrogantes, hay que analizar primero quién puede tener acceso a la historia clínica compartida.

3. El acceso a la historia clínica compartida: ¿quién debe poder acceder?

Según el artículo 113 del RLOPD, el acceso a la documentación se limitará exclusivamente al personal autorizado, por lo que se establecerán los mecanismos que permitan determinar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios, como es el caso de la historia clínica compartida. Pero este mismo Reglamento establece, en su apartado 3, que el acceso de personas no incluidas en el párrafo anterior debe quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

De acuerdo con este último requisito, se desprende que debe quedar constancia de los accesos a cada una de las historias clínicas por los distintos profesionales, lo que lleva a formular la siguiente pregunta: cuando una persona solicita el acceso a su historia clínica, ¿puede exigir también que se le informe de qué personas han accedido a la misma con anterioridad?

Si bien la regulación del derecho de acceso permite al afectado saber, entre otra información, las comunicaciones de datos que se han hecho, es decir cesiones a terceros (art. 15

LOPD y 27 RLOPD), estos preceptos legales no incluyen dentro del derecho de acceso el derecho a conocer la identidad de las personas que han accedido lícitamente a la información, como es el caso de los profesionales sanitarios. Por lo tanto, cualquier petición en estos términos efectuada al amparo del derecho de acceso, según la LOPD, tendrá una respuesta desfavorable.

San José,[4] en un artículo dedicado a la custodia y gestión de las historias clínicas, analiza el supuesto de que la persona afectada sospechara de accesos indebidos o no autorizados. En este caso, podría plantear esta cuestión al centro sanitario para que el personal responsable compruebe qué accesos se han efectuado y si estos están suficientemente justificados. Igualmente, la persona afectada podría poner su caso en conocimiento de la APDCAT para que los funcionarios inspectores lleven a cabo las comprobaciones necesarias, entre ellas la verificación del registro de accesos.

En la compartición de datos entre los hospitales y centros médicos de Cataluña mediante la historia clínica compartida debe haber diferentes niveles de información según los diferentes profesionales, ya sean estos asistenciales, gestores, administrativos, investigadores o docentes, aunque la finalidad principal del proyecto de historia clínica compartida es que los profesionales de la salud puedan acceder a diagnósticos, informes, estudios, y otros materiales relacionados con la salud de un paciente y que hayan sido realizados en otros centros adscritos al proyecto para una mejor calidad asistencial. La finalidad aquí es evitar la duplicidad de pruebas complementarias, con lo cual disminuirá la yatrogenia inherente a las mismas, aumentando la seguridad del paciente y con un gasto eficiente.

3.1. Los profesionales sanitarios

De lo dicho hasta ahora se deduce claramente que: *a)* todos los profesionales sanitarios que necesiten los datos del contenido de la historia clínica compartida deben poder acceder a la misma a fin de garantizar la continuidad asistencial del enfermo; *b)* el ciudadano es el titular o propietario de la información que consta en su historia clínica compartida y, por tanto, debe poder tener acceso a toda la información sobre su salud que contiene.[5]

[4] SAN JOSÉ, C. "Medidas de seguridad en la custodia y gestión de las historias clínicas", en BUISAN, L. y SÁNCHEZ URRUTIA, A. (coords.) *Intimidad, confidencialidad y protección de datos de salud*, Navarra: Aranzadi, 2011.

[5] Ley 21/2000, de 29 de diciembre (texto consolidado).

Ahora bien, el usuario de la sanidad pública es un ciudadano que, en ejercicio de su autonomía personal, tiene el derecho a decidir a qué parcela de su intimidad permite acceder a otras personas y, en consecuencia, también debería tener la posibilidad de decidir qué profesionales pueden acceder a sus datos de salud.

Sin embargo, la cuestión relevante aquí es si en la historia clínica compartida se pueden tratar los datos de los usuarios sin el consentimiento explícito de los mismos, amparándose en la legislación vigente, con lo que quedaría anulada la confidencialidad en la relación entre médico y paciente —por imposibilidad de poder mantenerla tal y como clásicamente se ha entendido—, al pasar los datos de salud de los ciudadanos a "la nube" en que esté realmente ubicada su historia clínica compartida.

¿Qué sentido tiene en este contexto el secreto médico? La LOPD, en su artículo 10, establece el deber del secreto para el responsable del fichero y para cualquier otra persona que intervenga en cualquier fase del tratamiento de un paciente. El conflicto ético que con ello se plantea es si el paciente tiene que aceptar, sólo por el hecho de que exista una ley que lo posibilita, que cualquier persona pueda acceder de manera legítima a sus datos de salud. ¿No sería preferible que el enfermo tuviera que autorizar expresamente quién puede acceder a ciertos contenidos de su historia clínica, tanto en el centro donde es atendido como en los nuevos repositorios que se generen en el futuro? O bien, ¿sería mejor que existiera un acceso restringido para ciertos problemas de salud y /o sociales, para cuyo acceso el propio paciente autorizara sólo a quien crea oportuno, como pueden ser los supuestos relacionados con la salud mental, adicciones, ámbito laboral, enfermedades de transmisión sexual, datos genéticos y similares?

La alternativa más idónea para proteger la intimidad del paciente es, a juicio de quien esto escribe, que haya diferentes niveles de datos encriptados. Ante todo es, pues, necesario definir estos diferentes niveles de encriptación para que cualquier profesional asistencial que trate los datos de salud pueda situarse al nivel que les corresponda. Conviene acordar también quién y para qué podrá acceder a cada nivel, así como quién asume la responsabilidad de registrar y actualizar la información y, sobre todo, quién se hace responsable de la calidad de esta información.

Según Ancochea, el paciente debe poder pedir que una información determinada no conste en su historia clínica compartida. En la práctica, esto sucede a menudo y, en este caso, el médico suele no grabarla y, si se trata de una información relevante, advierte al paciente de los riesgos de esconder la información negociando qué y cómo se incorpora primero a la historia clínica y, posteriormente, a la historia clínica compartida.

3.2. Las instituciones sanitarias

Las instituciones sanitarias tienen sus propios sistemas y, además, la cesión de datos entre las mismas está legalmente permitida con una única finalidad: la asistencial, de acuerdo con lo que establece el Capítulo V de la Ley 16/2003, de 28 de mayo, de *cohesión y calidad del Sistema Nacional de Salud*. En su artículo 54, que trata de las redes de comunicación del Sistema Nacional de Salud, concreta que por medio de esta red circularán las alertas y emergencias sanitarias. Intercambiará también la información necesaria para la gestión del fondo de cohesión sanitaria, así como toda aquella imprescindible para las necesidades de información sanitaria del Sistema Nacional de Salud, pero siempre que ello se realice para la atención sanitaria de las personas, es decir, exclusivamente con fines asistenciales para lo que no se requiere el consentimiento del interesado.

En el artículo 56 de esta misma ley se prevé el intercambio de información de salud entre los diferentes organismos, centros y servicios del SNS, permitiendo tanto al interesado como a los profesionales que participen en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de la asistencia y la confidencialidad e integridad de la información, con independencia de cuál sea la Administración que la proporcione.

3.3. Actividades de investigación, epidemiología y docencia

Las actividades de investigación y docencia vienen reguladas por el artículo 11 (Investigación y docencia) de la Ley 44/2003, de 21 de noviembre, *de ordenación de las profesiones sanitarias.* Como ya se ha dicho, en los usos no asistenciales de la historia clínica compartida en Cataluña, esta es también el soporte informativo imprescindible para la investigación clínica, porque facilita las actuaciones encaminadas a obtener un mayor conocimiento de las enfermedades y / o la aplicación de nuevas terapias. Así, el artículo 11.2, establece que "Las administraciones sanitarias, en coordinación con las administraciones educativas, promoverán las actividades de investigación y docencia en todos los centros sanitarios, como elemento esencial para el progreso del sistema sanitario y de sus profesionales". Ahora bien, tanto en la investigación clínica como en la docencia la totalidad de los datos de salud que contiene la historia clínica compartida están protegidos por la LOPD y por el RLOPD.

La historia clínica compartida también es fuente de datos de morbilidad y mortalidad, y además se puede utilizar —como de hecho se utilizan— para determinar los recursos sanitarios que se necesitan para atender la demanda asistencial y así llevar a cabo tareas de planificación

sanitaria, pero también para estudios epidemiológicos y de salud pública, y en general para la prevención y mejora del estado de salud de la población, así como para la realización de estadísticas sanitarias tanto a nivel nacional como internacional.

En este punto, mi valoración es que hay que insistir una vez más en la importancia de la anonimización de los datos tanto con fines de investigación clínica como epidemiológica. Pero como los datos de la historia clínica compartida están en una "nube", no existe esta anonimización y se puede identificar fácilmente el titular. El personal asistencial que se dedica a tareas de investigación debe estar muy atento al hecho de que nunca se pueda identificar al titular de los datos sensibles.

3.4. Los usuarios

Actualmente ya no es motivo de discusión que el propietario o titular de la información que contiene la historia clínica, y también la de la historia clínica compartida, es el ciudadano. Por tanto, este debe tener la capacidad para poder gestionar esta información referida a sus datos de salud y debe tener la posibilidad de hacerlo. La capacidad depende del ciudadano, pero la accesibilidad depende de la Administración sanitaria que ha puesto en marcha la historia clínica compartida. Por ello, es imprescindible que la Administración dé respuesta, por lo menos, a las siguientes preguntas:

¿Cómo podrá el ciudadano gestionar los datos que contiene la historia clínica compartida si los desconoce? ¿Cómo se accede a los datos de la propia historia clínica compartida? ¿Dónde puede encontrar la información imprescindible para poder acceder a la misma? ¿A qué datos puede acceder y cómo hacerlo? ¿Puede conocer el ciudadano quién ha accedido a su historia clínica compartida y a qué documentos?

Todas estos interrogantes plantean cuestiones que resultan aún más pertinentes si se cumple lo que afirma María Rovira[6]: "Hoy por hoy, se ha planteado la historia clínica compartida como una herramienta asistencial y un índice para la compartición de datos, pero en el futuro hay quien considera que debería permitirse también otro tipo de explotaciones". Esta misma autora considera, además, que el tema de la calidad de los datos es otro de los puntos importantes en el contenido de la historia clínica compartida.

[6] ROVIRA, M, Coordinadora Grupo de Expertos Área de Documentación Médica. Fundació Doctor Robert. Sistemes d'Informació. Oficina d'Estàndards i Interoperabilitat. Departament de Salut.

Ante estos conflictos y dilemas, en este artículo se defiende que el hecho de facilitar el acceso del ciudadano al contenido de sus datos de salud que contiene la historia clínica compartida es el elemento primordial para que el ciudadano pueda gestionarlos, de la misma manera que todo ciudadano puede gestionar sus otros datos sensibles. Si esta accesibilidad no es real, el ciudadano queda imposibilitado para el ejercicio del derecho de acceso que contempla la LOPD y que se analiza en el apartado siguiente.

Ante todo debe regularse el acceso: quién puede acceder, a qué y por qué motivos. Sin olvidar que el objetivo es lograr compaginar tres finalidades distintas:

- que los profesionales sanitarios puedan hacer su trabajo.
- que los enfermos tengan un buen servicio.
- que los enfermos puedan ejercer sus derechos ARCO.

4. Los derechos ARCO: explicación general de los derechos de los usuarios de la sanidad en el tratamiento de datos sensibles

La información que contiene una historia clínica, a pesar de ser recogida y estructurada por los profesionales asistenciales, hace referencia a los datos de salud del paciente, datos que le pertenecen y están protegidos, como datos de carácter personal que son, por la legislación estatal y autonómica en la materia y especialmente por la Ley Orgánica de Protección de Datos y el Reglamento que la desarrolla, por lo que no es raro que las entidades asistenciales reciban peticiones relacionadas con el ejercicio de los derechos que esta ley reconoce: derecho de acceso, de rectificación, de cancelación y de oposición, conocidos conjuntamente como derechos ARCO.

Estos derechos ARCO constituyen una facultad de control de los datos personales que otorga el ordenamiento jurídico al titular de los mismos con el fin de impedir un tratamiento ilícito y lesivo para la dignidad y el derecho del afectado. En definitiva, a través del ejercicio de estos derechos —hecho conocido como *habeas data*— se hace efectivo el poder de disposición que tiene el afectado sobre sus datos personales. Los derechos ARCO, son derechos personalísimos que solo pueden ser ejercidos por el afectado o por su representante legal, si así lo acredita, y nunca en otros supuestos.

Esta especial protección que la LOPD atribuye a los datos relativos a la salud se refiere especialmente a las medidas de seguridad que hay que tomar para garantizar su integridad y

confidencialidad, cuestión que también hay que tener en cuenta a la hora de tomar decisiones sobre la gestión de estos datos.

Los derechos ARCO son un conjunto de derechos que el paciente puede ejercer en relación con sus datos sensibles, es decir, son las herramientas de que dispone para garantizar que sus datos de salud se traten de acuerdo con la legislación y con pleno respeto a su intimidad.

4.1. Derecho de acceso

De acuerdo con la normativa vigente (art. 15 LOPD y 27-30 RLOPD), es el derecho del afectado a ser informado por el responsable del fichero o tratamiento acerca de si sus datos son objeto de tratamiento, la finalidad de este, cómo se han obtenido los datos y acerca de las cesiones a terceros efectuadas o previstas. El responsable del fichero o tratamiento debe responder a la solicitud del interesado en el plazo de un mes, y en caso de estimarse necesario hacerlo efectivo en el plazo de 10 días.[7]

En el artículo 13 de la Ley 21/2000, y en la disposición adicional de la Ley 16/2010, de 3 de junio, de modificación de la Ley 21/2000, de 29 de diciembre, *sobre los derechos de información concerniente la salud y la autonomía del paciente y la documentación clínica*, se establece un plazo de cuatro años como máximo para que los enfermos puedan acceder al contenido de su documentación médica personal incluida en la historia clínica compartida.

El derecho de acceso se debe facilitar en cualquier caso, ya que en caso contrario tampoco se podrán ejercer el resto de los derechos ARCO. Si el ciudadano desconoce el contenido de sus datos de salud que constan en ficheros automatizados y que son objeto de tratamiento, difícilmente podrá ejercer el derecho de rectificación, oposición y cancelación de los mismos. Podemos afirmar, en consecuencia, que de todos los llamados derechos ARCO, el de acceso es el más importante, pues constituye un prerrequisito imprescindible para el ejercicio efectivo de los demás derechos.

[7] BUISAN, L y SANCHEZ URRUTIA, A. *op. cit.*

4.2. Derecho de rectificación

Según el artículo 16 de la LOPD y 31-33 del RLOPD, este derecho permite que se modifiquen los datos que sean inexactos o incompletos. Una vez ejercido este derecho, se hará efectivo en el plazo de 10 días, salvo que proceda la desestimación.

4.3. Derecho de cancelación

Siguiendo lo establecido en el artículo 16 de la LOPD y 31-33 del RLOPD, este derecho faculta al titular de los datos para solicitar la supresión de las mismos cuando sean inadecuados, es decir, cuando se trate de datos que no guardan relación con la finalidad para la que en su momento se recogieron, o bien cuando sean excesivos en el sentido de que se tratan más datos de los estrictamente necesarios para la finalidad del tratamiento médico. En este caso, este derecho se hará efectivo en el plazo de 10 días, salvo que proceda la desestimación de la petición.

4.4. Derecho de oposición

Atendiendo al artículo 6.4 de la LOPD y los artículos 34-36 del RLOPD, se refiere al derecho del titular de los datos a que no se lleve a cabo un determinado tratamiento de los mismos cuando haya motivos fundados y legítimos relacionados con alguna situación personal. Una vez ejercido, se hará efectivo también en el plazo de 10 días, salvo que proceda la desestimación.

En resumen, se trata del derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal, o se cese en el mismo, cuando los datos hayan sido recogidos sin su consentimiento explícito, como es el caso de los datos clínicos, y existan causas que justifiquen dicha oposición.

4.5. El derecho al olvido

4.5.1. Como derecho de las personas físicas

Lo que se ha llamado derecho al olvido es un derecho subjetivo de titularidad individual que hace referencia a la facultad de poder elegir cuándo y dentro de qué límites procede revelar datos e

informaciones que forman parte de la identidad de una persona. En este caso, el bien jurídicamente protegido es la libertad de actuación y el libre desarrollo del proyecto vital de cada uno y, por tanto, es más amplio de lo que se protege con la protección de los datos personales, porque su fundamento radica en el artículo 10 de la CE y en el derecho al libre desarrollo de la personalidad. Este derecho subjetivo al olvido debe complementarse, sin embargo, con el deber de los demás a respetar este olvido y su incumplimiento puede generar responsabilidad civil por culpa.

De manera general, representa la garantía individual frente a hechos pasados que no respondan a un interés público actual y que puedan, en cambio, condicionar el libre desarrollo de la personalidad. La Agencia Española de Protección de Datos (AEPD) en el litigio que interpuso contra Google, invocó el derecho al olvido defendiendo que ningún ciudadano que no tenga la condición de personaje público, ni sea objeto de hecho noticiable de relevancia pública, no tiene por qué resignarse a soportar que sus datos de carácter personal se difundan por la red sin poder reaccionar ni enmendar su inclusión en un sistema de comunicación global como es Internet.

Mediante el ejercicio de este nuevo derecho, el ciudadano tendría la posibilidad de exigir la supresión o cancelación de determinada información o la constancia de unos hechos. Por tanto, no sólo se incluirían datos personales sino también noticias pasadas que pueden afectar al futuro de las personas y que han sido publicadas en el pasado.

Si analizamos el derecho comparado, vemos que hay una gran divergencia entre los países de tradición civilista (entre los que se incluye el nuestro) y los seguidores de la *common law*. En la cultura de la *common law* se niega el derecho al olvido, por lo que todos los archivos que son públicos pueden ser publicados sin problemas en Internet aunque contengan datos personales, como por ejemplo los archivos de los tribunales que son considerados como a fuentes públicas de información. La tradición jurídica civilista ha ligado el derecho al olvido con la prescripción adquisitiva y a la extintiva que contienen los códigos civiles. Con el argumento de que ambas prescripciones tienen unos plazos para ejercerse, cuando éstos finalizan olvidan las acciones y las antiguas titularidades. En el caso de España, la regulación de la prescripción y la cancelación de los antecedentes delictivos refuerza los argumentos a favor del derecho al olvido.

El Tribunal Constitucional español considera la dignidad humana como el punto de partida, el "prius lógico y ontológico para la existencia y especificación de los demás Derechos", porque el artículo 10 CE encabeza el título destinado a tratar los derechos y deberes fundamentales. Por tanto, la dignidad humana es un valor jurídico inspirador de los derechos fundamentales, que en todo caso garantiza el derecho de cada uno a determinar su vida de forma autónoma y responsable, con total libertad para decidir su proyecto vital. El TC también ha detallado que los

derechos contenidos en el artículo 18 CE tienen la consideración de "derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la dignidad de la persona que reconoce el art. 10 CE".

Así pues, el derecho al olvido se configura como un derecho del ciudadano de poder elegir cuándo y dentro de qué límites procede revelar datos e informaciones que forman parte de su identidad. Este derecho nace como el derecho a la autodeterminación informativa (derecho fundamental), dirigido a satisfacer una necesidad básica de toda persona como es tener el control de la información referente a sí misma. Esto no es otra cosa que el derecho de *habeas data*: decidir qué datos personales de un individuo pueden ser tratadas y consultadas por otros, entendido como desarrollo del *habeas corpus* sobre el que se ha basado históricamente la libertad personal. Lo que se quiere proteger con el derecho al olvido es la libertad de desarrollar el propio proyecto vital sin que éste se vea hipotecado por información que no tiene ninguna relevancia pública actual. Entendido así, encaja perfectamente en el amplio concepto de autodeterminación informativa en la medida que se define como el derecho a controlar la divulgación de datos personales propios, decidir cuáles pueden ser tratados por otros y cuáles no, con el fin de que no condicionen el futuro de los ciudadanos.

4.5.2. El derecho al olvido digital y la historia clínica compartida

La AEPD acoge el derecho al olvido digital en el marco del principio de finalidad en materia de protección de datos. Sin embargo, los datos personales que se recogen en la historia clínica compartida —sin consentimiento del afectado, porque hay una ley que lo habilita— deberían enmarcarse dentro del derecho al olvido digital y no en el derecho de protección de datos, porque el bien jurídicamente protegido es, como ya se ha dicho, la libertad de actuación y el libre desarrollo del proyecto vital personal y, en este sentido, abarca un ámbito más amplio de lo que se quiere proteger con el derecho a la protección de datos personales, al tener su fundamento en el art. 10 de la CE y en el libre desarrollo de la personalidad. Los datos de salud que contiene la historia clínica compartida, exceptuando los que hacen referencia a enfermedades de declaración obligatoria, nunca tienen relevancia pública y, como resultado, en el marco del derecho al olvido digital el enfermo debe poder oponerse a fin de conseguir que sean borradas (y no meramente encriptadas).

El hecho de que el usuario de la sanidad pública hoy por hoy no pueda tener el control y la gestión de los datos de salud que están compartidos en la historia clínica compartida y colgados en el *cloud* sanitario por un profesional sanitario sin su consentimiento, imposibilita el ejercicio del derecho a oponerse y, por tanto, de poder cancelarlos a petición del paciente (según el artículo

6.1 de la LOPD). Cancelación que se podría hacer efectiva desde el momento en que estos datos ya no sean necesarios para la finalidad por la cual fueron recogidos y tratados.

5. Proyecto de actualización de la Directiva Europea de Protección de Datos[8]

La propuesta de Reglamento de la Comisión Europea incorpora el derecho al olvido y lo trata como un tema estructural en el ámbito de la protección de datos personales, y regula su ejercicio en el artículo 17 como sigue:

Derecho al olvido y la supresión:

1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernan y se abstenga de darle más difusión, especialmente lo que respecta a datos proporcionados por el propio interesado siendo niño, cuando concurra alguna de las circunstancias siguientes:

a) los datos ya no son necesarios en relación con la finalidad para la que fueron recogidos o tratados;

b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el art.6, apartado 1, letra a), o bien ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;

c) el interesado se opone al tratamiento de datos personales según lo dispuesto en el artículo 19;

d) el tratamiento de datos no se corresponde con el presente Reglamento por otros motivos.

---

[8] El 4 de noviembre de 2010, la Comisión adoptó la comunicación «Un enfoque mundial de la Protección de los Datos personales en la Unión Europea», que se traslada al Supervisor Europeo de Protección de Datos (SEPD) según lo dispuesto en el artículo 41 del Reglamento (CE) 45/2001. Incluso antes de adoptar la Comunicación, el SEPD tuvo ocasión de pronunciarse sobre la comunicación a título informal. Algunas de estas observaciones han sido recogidas en la versión definitiva del documento. Dicha comunicación tiene como objetivo definir un nuevo marco que permita a la Comisión Europea revisar el régimen jurídico en materia de protección de datos. Publicado en el *Diario Oficial de la Unión Europea*, núm. 162, de 22 de junio de 2011. El 25 de enero de 2012, la Comisión hace la propuesta de reglamento general de protección de datos por el que se regula el derecho al olvido en el artículo 17.

Las excepciones a la facultad de suprimir los datos personales se encuentran en el artículo 17 apartado 3.a) y se fundamentan en motivos de interés público en el ámbito de la salud pública, en especial cuando existan riesgos sanitarios transfronterizos graves.

Conseguir la privacidad en un mundo global, donde los ciudadanos (y también empresas, instituciones...) interactúan de forma activa a través de la computerización en un *cloud,* facilita la divulgación de datos personales y, por tanto, la privacidad se ve aún más amenazada, por lo que es urgente que la Directiva en materia de protección de datos contemple estos nuevos retos derivados del uso masivo de las TIC.

Conclusión

La cesión de datos de salud de los ciudadanos sin su consentimiento con fines asistenciales entre centros, organismos y servicios del Servicio Nacional de Salud es ya una realidad, por lo que es imprescindible que la Administración sanitaria facilite al ciudadano el derecho de acceso a la historia clínica compartida y establezca claramente cómo puede gestionar sus datos de salud. Facilitar el acceso del ciudadano a los datos de salud que contiene su historia clínica es el elemento primordial para que pueda gestionarlos. El derecho de acceso debe ser posible en cualquier caso, pues si esta accesibilidad no es real, el ciudadano queda imposibilitado para el ejercicio de los derechos ARCO que contempla la LOPD. Si el ciudadano desconoce el contenido de sus datos de salud almacenados en ficheros automatizados y que son objeto de tratamiento, difícilmente podrá ejercer los derechos de rectificación, oposición y cancelación de los mismos. El médico de familia debe ser quien facilite al ciudadano el derecho de acceso, a fin que éste pueda conocer qué información contienen estos ficheros, así como los documentos, pruebas o informes que se hayan incorporado a los mismos desde cualquier estación de trabajo de un centro hospitalario, de atención primaria o de urgencias.

En el contexto de la historia clínica con compartición de datos, la posibilidad real de ejercer el derecho de oposición por parte del paciente sin que tenga que motivar su decisión es el único medio para que se respete su intimidad. Difícilmente se puede negar el derecho de oposición en el ámbito sanitario y, en general, no se debería denegar a una persona con capacidad de obrar, y por lo tanto autónoma, ningún derecho ARCO. El profesional sanitario debe facilitar al ciudadano que solicita el ejercicio de los derechos ARCO la información más adecuada para que éste sea conocedor del riesgo que le puede suponer, en una eventual atención sanitaria posterior, que los profesionales sanitarios no dispongan de toda la información incorporada a la historia clínica compartida.

Es urgente que la Directiva de la Unión Europea en materia de protección de datos contemple los nuevos retos del uso masivo de las TIC, especialmente en sanidad. Conviene, además, que se incorpore el derecho al olvido digital en el ámbito sanitario, junto con los derechos ARCO, con el fin de favorecer la máxima protección de la intimidad de los ciudadanos. Los datos personales que constan en la historia clínica compartida —sin el consentimiento del afectado, porque hay una ley que lo habilita— deberían enmarcarse dentro del derecho al olvido digital y no dentro del derecho de protección de datos, porque el bien que se quiere proteger es la libertad de actuación y el libre desarrollo del proyecto vital, que se fundamentan en el artículo 10 de la Constitución Española y en el libre desarrollo de la personalidad. Los datos de salud que contiene la historia clínica compartida, exceptuando los relacionados con las enfermedades de declaración obligatoria, nunca tienen relevancia pública, por lo que en el marco del derecho al olvido digital el ciudadano debe poder solicitar y conseguir que dichos datos sean borrados y no meramente encriptados.

Fecha de recepción: 15 de enero de 2016
Fecha de aceptación: 10 de abril de 2016