

INTERNATIONAL JOURNAL OF OPEN GOVERNMENTS

REVUE INTERNATIONALE DES GOUVERNEMENTS OUVERTS

Vol. 5 - 2017

 **IMODEV**
LES ÉDITIONS

ISSN 2553-6869

International Journal of Open Governments
Revue internationale des gouvernements ouverts

Direction :
Irène Bouhadana & William Gilles

ISSN : 2553-6869

IMODEV
49 rue Brancion 75015 Paris – France
www.imodev.org
ojs.imodev.org

*Les propos publiés dans cet article
n'engagent que leur auteur.*

*The statements published in this article
are the sole responsibility of the author.*

Droits d'utilisation et de réutilisation

Licence Creative Commons – Creative Commons License -



Attribution

Pas d'utilisation commerciale – Non Commercial

Pas de modification – No Derivatives

À PROPOS DE NOUS

La **Revue Internationale des Gouvernements ouverts (RIGO)/ the International Journal of Open Governments** est une revue universitaire créée et dirigée par Irène Bouhadana et William Gilles au sein de l'IMODEV, l'Institut du Monde et du Développement pour la Bonne Gouvernance publique.

Irène Bouhadana, docteur en droit, est maître de conférences en droit du numérique et droit des gouvernements ouverts à l'Université Paris 1 Panthéon-Sorbonne où elle dirige le master Droit des données, des administrations numériques et des gouvernements ouverts au sein de l'École de droit de la Sorbonne. Elle est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Elle est aussi fondatrice et Secrétaire générale de l'IMODEV.

William Gilles, docteur en droit, est maître de conférences (HDR) en droit du numérique et en droit des gouvernements ouverts, habilité à diriger les recherches, à l'Université Paris 1 Panthéon-Sorbonne où il dirige le master Droit des données, des administrations numériques et des gouvernements ouverts. Il est membre de l'Institut de recherche juridique de la Sorbonne (IRJS). Il est aussi fondateur et Président de l'IMODEV.

IMODEV est une organisation scientifique internationale, indépendante et à but non lucratif créée en 2009 qui agit pour la promotion de la bonne gouvernance publique dans le cadre de la société de l'information et du numérique. Ce réseau rassemble des experts et des chercheurs du monde entier qui par leurs travaux et leurs actions contribuent à une meilleure connaissance et appréhension de la société numérique au niveau local, national ou international en analysant d'une part, les actions des pouvoirs publics dans le cadre de la régulation de la société des données et de l'économie numérique et d'autre part, les modalités de mise en œuvre des politiques publiques numériques au sein des administrations publiques et des gouvernements ouverts.

IMODEV organise régulièrement des colloques sur ces thématiques, et notamment chaque année en novembre les *Journées universitaires sur les enjeux des gouvernements ouverts et du numérique / Academic days on open government and digital issues*, dont les sessions sont publiées en ligne [ISSN : 2553-6931].

IMODEV publie deux revues disponibles en open source (ojs.imodev.org) afin de promouvoir une science ouverte sous licence Creative commons **CC-BY-NC-ND** :

- 1) la *Revue Internationale des Gouvernements ouverts (RIGO)/ International Journal of Open Governments* [ISSN 2553-6869] ;
- 2) la *Revue internationale de droit des données et du numérique (RIDDN)/International Journal of Digital and Data Law* [ISSN 2553-6893].

ABOUT US

The **International Journal of Open Governments / Revue Internationale des Gouvernements ouverts (RIGO)** is an academic journal created and edited by Irène Bouhadana and William Gilles at IMODEV, the Institut du monde et du développement pour la bonne gouvernance publique.

Irène Bouhadana, PhD in Law, is an Associate professor in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where she is the director of the master's degree in data law, digital administrations, and open governments at the Sorbonne Law School. She is a member of the Institut de recherche juridique de la Sorbonne (IRJS). She is also the founder and Secretary General of IMODEV.

William Gilles, PhD in Law, is an Associate professor (HDR) in digital law and open government law at the University of Paris 1 Panthéon-Sorbonne, where he is the director of the master's degree in data law, digital administration and open government. He is a member of the Institut de recherche juridique de la Sorbonne (IRJS). He is also founder and President of IMODEV.

IMODEV is an international, independent, non-profit scientific organization created in 2009 that promotes good public governance in the context of the information and digital society. This network brings together experts and researchers from around the world who, through their work and actions, contribute to a better knowledge and understanding of the digital society at the local, national or international level by analyzing, on the one hand, the actions of public authorities in the context of the regulation of the data society and the digital economy and, on the other hand, the ways in which digital public policies are implemented within public administrations and open governments.

IMODEV regularly organizes conferences and symposiums on these topics, and in particular every year in November the Academic days on open government and digital issues, whose sessions are published online [ISSN: 2553-6931].

IMODEV publishes two academic journals available in open source at ojs.imodev.org to promote open science under the Creative commons license **CC-BY-NC-ND**:

1) the *International Journal of Open Governments/ la Revue Internationale des Gouvernements ouverts (RIGO)* [ISSN 2553-6869] ;

and 2) the *International Journal of Digital and Data Law / la Revue internationale de droit des données et du numérique (RIDDN)* [ISSN 2553-6893].

OPEN DATA EN EL ÁMBITO SANITARIO Y SU COMPATIBILIDAD CON LA PRIVACIDAD DEL PACIENTE

par M^a Belén ANDREU MARTÍNEZ, Profesora Titular de
Derecho Civil de la Universidad de Murcia, España¹.

El ámbito de la salud ha estado hasta hace no mucho tiempo ajeno a la apertura de los datos, entre otros, por los riesgos derivados del tratamiento de información muy sensible. Pero la apertura de datos es ya un hecho y el sector salud es uno de los ámbitos en el que esta apertura puede tener un mayor impacto en los próximos años. Podemos decir que uno de los focos de atención del open data está puesto precisamente en el sector sanitario.

Actualmente estamos asistiendo a una auténtica revolución (también de los datos) en la salud, no solo en cuanto a la reutilización y apertura de los datos o la generalización de las *wearables* y las aplicaciones sobre salud y bienestar, sino también por la irrupción de herramientas de realidad virtual, inteligencia artificial y técnicas de big data sanitario. Se puede comprobar este hecho si observamos la cantidad de noticias cada vez mayor² (además de las declaraciones al respecto en informes oficiales³) sobre cuestiones de salud, revolución tecnológica y tratamiento de datos que se pueden encontrar en los últimos años, hasta el punto de que términos como “medicina de precisión” o “medicina personalizada”, “empoderamiento del paciente” (unido a otros como eficiencia del sistema, mejora en la toma de decisiones, reducción de costes...) han pasado a un primer plano.

Los cambios culturales, demográficos, sociales (envejecimiento de la población, aumento de la cronicidad y comorbilidad, etc.) y, por supuesto, tecnológicos tienen un reflejo evidente en esta realidad. Y con todo ello se pretende contribuir a posibilitar lo que se consideran los principales retos de los sistemas sanitarios en los próximos años⁴:

¹ Este trabajo se enmarca en el proyecto de investigación financiado por la Fundación SENECA de la Región de Murcia (España) «E-salud y autonomía del paciente vulnerable a la luz del Bioderecho» (Ref. 19486/PI/14).

² Por citar algunas: <http://datos.gob.es/es/noticia/datos-abiertos-y-salud-conclusiones-extraidas-del-iode-2016>; <http://www.expansion.com/economia-digital/innovacion/2016/12/13/584ed22222601de9658b45a5.html>; <http://www.hospitaldigital.com/2013/06/28/open-data-en-salud-retos-y-oportunidades/>

³ A título de ejemplo, a nivel europeo se puede citar el «Plan de Acción sobre salud electrónica de 2012-2020: atención sanitaria innovadora para el siglo XXI», de la Comisión europea, de 6-12-2012. Y en España, el informe del Consejo Asesor de Sanidad del Ministerio de Sanidad, Servicios Sociales e Igualdad «La E-salud. Prioridad estratégica para el sistema sanitario», de abril de 2014.

⁴ M. ROVIRA, «Las TIC en la coordinación entre los sistemas social y sanitario», *Informática+Salud*, n° 116, 2016, p. 6.

- Reforzar la prevención y la salud pública: se busca una medicina más proactiva y no tanto reactiva. Se pretende retrasar la aparición de las enfermedades o de las situaciones de dependencia. Y ello implica una mayor “responsabilización” del ciudadano en la gestión de su propia salud.
- Asegurar la continuidad asistencial a lo largo de la vida: con la finalidad de conseguir una atención sanitaria continuada y de calidad. Esto supone, entre otros, una mayor disponibilidad de la información sobre salud de las personas.
- Unido con lo anterior también se señala la necesidad de conseguir una mayor coordinación socio-sanitaria: se trataría de superar el actual marco de la sanidad para establecer puentes con las estructuras sociales (lo que implica también un mayor trasvase de datos).

En las siguientes páginas nos centraremos en el open data como instrumento que puede contribuir a conseguir los objetivos citados, señalando, por un lado, los beneficios y el valor que puede aportar el open data en salud y su grado de desarrollo actual, así como los principales riesgos y obstáculos a los que se enfrenta; y, por otro, si la situación legislativa propicia o no esta apertura, analizando algún ejemplo de open data sanitario en España. En última instancia, este análisis nos permitirá comprobar cuáles son los mecanismos que se arbitran para proteger la privacidad del paciente en un escenario de open data sanitario y en qué medida éste dispone de herramientas para controlar el uso que se hace de su información sanitaria.

§ 1 – LA REALIDAD DEL OPEN DATA EN EL ÁMBITO SANITARIO

A) Los beneficios declarados del open data en salud y su grado de desarrollo

Se han puesto de relieve de forma reiterada los beneficios que el open data y la reutilización de datos reporta tanto a los ciudadanos como a los poderes públicos y a las propias empresas. Beneficios que se extienden también al ámbito de la salud.

De forma muy resumida se ha señalado que el open data debería permitir a los gobiernos una mejora en la toma de decisiones en el sector salud (aumentando la eficiencia del sistema y reduciendo costes, entre otros) y un incremento de la transparencia en la gestión pública. Por lo que hace al paciente, al estar mejor informado, debería involucrarse más en la toma de decisiones. Por otra parte, se dice que los pacientes más informados y formados deberían responder mejor a los tratamientos, lo que repercutiría en una mejora del sistema sanitario. En definitiva, una mayor participación, responsabilidad y compromiso por parte del paciente (“empoderamiento” del paciente)⁵. Por último, también

⁵ Como herramienta a disposición de pacientes, científicos, médicos, etc. se cita, entre otras muchas, el proyecto Open Trials, con el que se crea una base de datos abierta y

se ha destacado la creación de nuevos modelos de negocio con base en el open data. En el ámbito sanitario permitiría crear nuevas herramientas y aplicaciones de salud basadas en los datos abiertos (ej., para evaluar la calidad de los servicios de salud, costes de prestaciones, etc.)⁶.

Por su parte, el Servicio Público de Salud inglés ha analizado los beneficios de la apertura de datos en salud, señalando seis aspectos (propuestas de valor) que se verían afectados positivamente por esta apertura de datos: responsabilidad, elección, eficiencia, resultados, servicio al cliente y satisfacción del paciente, innovación y crecimiento económico⁷.

Hay que tener en cuenta, por otra parte, que el sector salud genera un volumen ingente de datos y por muchos actores y que la cantidad de datos relacionados con la salud y la sanidad ha crecido de forma exponencial en los últimos años. En España, el volumen mayor de datos se concentra en manos de las Administraciones públicas (principales prestadores de la asistencia sanitaria; con información asistencial, datos administrativos, pero también de costes y otros). Aunque cada vez generan mayor información otros proveedores de salud, la industria sanitaria (en particular, la industria farmacéutica), etc. Por otra parte, también va creciendo el número de datos de salud que generan los dispositivos móviles y las aplicaciones sobre salud y bienestar, junto con las *wearables*⁸.

Ahora bien, desde el punto de vista del open data ¿qué información en el ámbito de la salud se encuentra disponible en la

colaborativa con información extraída de ensayos clínicos de todo el mundo (accesible en: <https://opentrials.net/>).

⁶ Se ha señalado que la reutilización de datos permitiría, entre otros, trazar tendencias epidemiológicas. En este ámbito es preciso hacer mención a la herramienta «Google Flu Trends», con la que se pretendía detectar brotes de gripe con base en las búsquedas de los usuarios en el buscador. Aunque estuvo funcionando durante un tiempo (y los datos siguen disponibles), la herramienta se cerró por ciertos fallos.

⁷ En su documento de mayo de 2014 «The open data era in health and social care» (elaborado junto con The GovLab -New York University-). Así, la apertura de datos en el entorno sanitario puede permitir una mayor rendición de cuentas a nivel económico, político. Permitirá a los ciudadanos buscar los servicios que mejor se adapten a sus necesidades de salud individuales; y elegir entre proveedores y tratamientos, lo que conduce a la mejora de la satisfacción del paciente, de la calidad y de los estándares e indicadores de los sistemas sanitarios. La disponibilidad de datos puede obligar a ser más rentables y responsables en la forma de actuar. La publicación de resultados de los distintos componentes del sistema de salud puede impulsar la competencia entre profesionales, lo que puede suponer una mejora en la calidad de la atención y en la innovación. Mejorar el acceso del paciente a los datos y la prestación de servicios orientados al cliente, permite conseguir un servicio de calidad y aumentar la eficiencia. Por lo que hace a la innovación y crecimiento económico, la obtención de datos de salud es difícil y a veces cara. Recolectar y distribuir datos de manera abierta permite convertirse en un foco para atraer la investigación e innovación.

⁸ Información que actualmente está en manos de empresas privadas y de la que puede hacerse un uso comercial. Sobre el tema pueden consultarse, entre otros, diversos textos producidos por organismos europeos: Green Paper on mobile health ("mHealth") and the Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps, 10-4-2014; Opinion 8/2014 on the on Recent Developments on the Internet of Things, 16 Septiembre 2014, Article 29 Data Protection Working Party; Opinion 1/2015 on Mobile Health, 21 may 2015, European Data Protection Supervisor. Vid. igualmente V. ALARCÓN SEVILLA /M.B. ANDREU MARTÍNEZ, «La vulnerabilidad de los datos de salud en tecnología móvil», *Revista Aranzadi de derecho y nuevas tecnologías*, n° 42, 2016, pp. 135 y ss.

actualidad de forma estructurada? Sobre todo, lo que se encuentra son indicadores estadísticos sobre diferentes aspectos relacionados con la salud. Un ejemplo de ello es el *European Core Health Indicators* (ECHI) de la Comisión Europea, que recoge 88 indicadores esenciales de salud, de entre los que se dispone de datos razonablemente comparables para alrededor de 60; estos indicadores están segmentados -cuando ello es posible- por sexo, edad, estatus socio-económico y territorio⁹. Estos indicadores permiten establecer comparaciones (ej. comparar indicadores de salud en relación con la mortalidad infantil con factores demográficos, como la población y la tasa de nacimiento para un país específico). Además, la Comisión también proporciona una herramienta para explotar estos datos (*EHCI data tool*), que permite crear gráficos y realizar cálculos con la información¹⁰. Ahora bien, en lo que hay un mayor retraso es en el hecho de que esta información se convierta en productos de valor añadido para el ciudadano.

A nivel nacional el país más avanzado en esta materia es el Reino Unido, con el portal de datos del Servicio público de salud (NHS)¹¹. No solo presenta datos e indicadores estadísticos, sino también valoraciones de cada centro sanitario, coste de tratamiento, resultados de tratamientos clínicos, incidencia de enfermedades, etc. Con ello, los ciudadanos pueden ver el impacto de sus impuestos en sanidad y comparar el nivel de asistencia médica de cada área, al igual que dota a las Administraciones de información para la toma de decisiones y mejora de los servicios¹².

En España, esta cuestión no acaba de despegar. Llama la atención la gran cantidad de herramientas que se han producido para la mejora de la gestión y de la asistencia sanitaria. Ha habido importantes avances en telemedicina, en la puesta en funcionamiento de las historias clínicas electrónicas, recetas electrónicas, etc. Su implantación en las organizaciones sanitarias ha sido y está siendo un reto importante, pero cambiar hacia una cultura de datos abiertos en salud, todavía lo es más. Por el momento, lo que tenemos son algunos indicadores estadísticos en

⁹ https://ec.europa.eu/health/indicators/echi_es. Los indicadores aparecen agrupados en cinco epígrafes: 1) situación demográfica y socioeconómica; 2) situación sanitaria; 3) factores determinantes de la salud; 4) intervenciones sanitarias: servicios sanitarios; 5) intervenciones sanitarias : promoción de la salud.

¹⁰ Otro ejemplo sería el portal de datos del observatorio mundial de la salud (GHO), dependiente de la OMS, que publica de forma abierta indicadores estadísticos relacionados con la salud. Véase <http://www.who.int/gho/es/>

¹¹ <https://www.nhs.uk/service-search/Performance/DataProviders>. Similar al existente en EEUU, que ha creado una plataforma digital denominada Health Data (que agrega bases de datos sanitarias dependientes de instituciones públicas sanitarias estadounidenses, como CDC o la FDA). Véase <https://www.healthdata.gov/>

¹² Cita el NHS (en su documento «The open data era in health and social care») como ejemplo de impacto del open data en la mejora de la asistencia sanitaria la publicación por parte de la Sociedad de Cirujanos Cardiorráquicos de los resultados de las cirugías realizadas por los médicos en todo el Reino Unido, con una mejora rápida de los resultados. En el informe de la citada Sociedad se vinculaba dicha mejora de forma directa al proceso de registrar, reportar y publicar resultados de los médicos a nivel individual.

materia de salud en los Portales de Transparencia del Instituto Nacional de Estadística, el Portal Estadístico del Sistema Nacional de Salud (SNS), la iniciativa Aporta del Gobierno de España y los observatorios y webs oficiales de las Comunidades Autónomas¹³.

B) Los obstáculos a la implantación

Visto lo anterior ¿Cuáles son las razones por las que no hay una mayor disponibilidad de información en abierto en salud? Los obstáculos con los que se encuentra el open data también han sido señalados (entre otros, por el NHS inglés):

– Las barreras institucionales, burocráticas y culturales a la apertura de datos. La cultura de los datos abiertos requiere un cambio de percepción e incluso cambio cultural en algunos casos. Se está pidiendo a las administraciones, proveedores de salud y pacientes que se adapten a una nueva forma de recolectar y usar los datos. En España hay que contar, además, con una escasa cultura en open data en general (buena muestra de ello es que la ley de transparencia y acceso a la información pública no se aprobó hasta el año 2013), lo que dificulta aún más su aplicación al ámbito sanitario.

– Otra de las más importantes barreras es la protección de la privacidad. En el ámbito de la salud se está tratando con datos sensibles y, desde luego, hay desconfianza hacia un uso incorrecto de estos datos que pueda ser perjudicial para la persona.

– Además, también existe desconfianza a que la apertura de datos lleve realmente a una toma de decisiones adecuada (la necesidad de un “buen análisis”). Buenos datos no siempre significan buenas decisiones, pues al final siempre hay un componente de análisis e interpretación humana.

– Y, evidentemente, también se han puesto de relieve los obstáculos relacionados con estándares técnicos y la interoperabilidad, que puede producir que la apertura de datos no sea efectiva. Se habla en este sentido de la necesaria “liquidez de los datos”, esto es, de la capacidad de los datos de fluir fácilmente entre proveedores, pacientes y otros grupos que intervienen en la asistencia sanitaria.

Un reflejo de lo anterior son las dificultades con las que se encuentra en la práctica la puesta en marcha de proyectos de open

¹³ El INE, en su portal de transparencia (<http://transparencia.gob.es/>), ha publicado algunos informes en materia de salud como el relativo al Big data en salud digital (<http://www.ontsi.red.es/ontsi/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf>). El portal estadístico del SNS recoge datos estadísticos varios agrupados por temáticas (<http://www.mssi.gob.es/estadEstudios/estadisticas/sisInfSanSNS/tablasEstadisticas/home.htm>). La iniciativa Aporta está destinada a promocionar la cultura de apertura de información e incorpora una sección dedicada a la salud (<http://datos.gob.es/es/catalogo>). En cuanto a las Comunidades Autónomas el panorama es muy diverso; la mayoría de los portales de transparencia replican datos estatales y, en ocasiones, lo único que se hace es añadir información básica de centros sanitarios. Algunas Comunidades Autónomas publican resultados asistenciales, pero en formato no reutilizable y alguna otra, como la asturiana, cuenta con información ampliada en un observatorio de salud.

data en el ámbito sanitario¹⁴. En España (en concreto, en Cataluña) ha habido una experiencia incipiente de apertura de datos, sobre todo de reutilización de datos de salud del sistema público catalán, que se denominó en su origen Visc+ y que fue objeto de una gran controversia a nivel político y social¹⁵. El proyecto se fue modificando con el tiempo y “restringiendo” antes las críticas de una posible “venta” de datos de las historias clínicas públicas¹⁶ y en la actualidad se encuentra como tal paralizado y ha sido sustituido por otro programa (denominado PADRIS), sobre el que volveremos más adelante.

Como se ha puesto de relieve, el riesgo evidente que se percibe en este tipo de proyectos es el derivado del uso de información en origen altamente sensible, basado en técnicas de anonimización que no pueden asegurar al 100% la no reidentificación, unido a la aplicación de técnicas de análisis masivo de datos, con el riesgo de una posible discriminación basada en perfiles y patrones de comportamiento creados con fines que el afectado no puede controlar¹⁷. En cualquier caso, estas experiencias ponen de relieve lo delicado de los proyectos que impliquen el tratamiento de información sanitaria de los ciudadanos y nos plantean la necesidad no solo de cumplir con la normativa aplicable y prever las herramientas adecuadas para garantizar el respeto de los derechos de los pacientes, sino también de una correcta toma de decisiones en la gestión de los datos, de la necesidad de transparencia, información en los procesos (tanto a los profesionales, como a los pacientes) y, en definitiva, de lograr que se siga manteniendo la confianza en el sistema, confianza que es la base última de las relaciones en el ámbito sanitario.

¹⁴ La dificultad de tratar con los datos de los historiales médicos por las suspicacias que suscita se puso de relieve también en el Reino Unido a propósito del programa Care.data en el año 2013 por parte del NHS, que buscaba centralizar datos médicos y sociales de los pacientes y le permitía compartir información con terceros fuera del NHS. A instancia de la National Data Guardian for Health and Care (que puso en cuestión el modelo de consentimiento y el opt-out propuesto), el NHS decidió cerrar el programa y trasladar la labor iniciada a la National Information Board para reforzar la confianza ciudadana en esta materia. Véase <https://www.england.nhs.uk/ourwork/tsd/care-data/> y <https://www.england.nhs.uk/digitaltechnology/info-revolution/>

¹⁵ Se trataba de una licitación de un contrato de colaboración público-privada para la implantación y operacionalización de un modelo de gestión para dar valor a la información del sistema sanitario catalán en el marco de políticas públicas. Ya la propia denominación (oscura) fue criticada.

¹⁶ Todo el procedimiento fue muy azaroso: se aprobó mediante un acuerdo del Gobierno catalán. El Parlamento solicitó la suspensión de la licitación hasta que no se abriera un proceso público y participativo para debatir el proyecto. El Gobierno siguió adelante con el mismo, sometiéndolo a distintos órganos (Agencia catalana de protección de datos; Observatorio de Bioética de Cataluña), suscitando adhesiones y llamadas de atención por parte de distintos agentes sociales. La Agencia pública encargada de gestionar el proyecto publicó un listado con los centros de investigación y asistenciales públicos con los que se había suscrito convenios de cesión de información. Y finalmente en mayo de 2016 se canceló el proceso de licitación. Un análisis crítico del proyecto puede consultarse en M.M. SERRANO PÉREZ, «Big data o la acumulación masiva de datos sanitarios: derechos en riesgo en el marco de la sociedad digital», *Revista Derecho y Salud*, nº 25, 2015, pp. 51 y ss.

¹⁷ Vid. M.R. LLÁCER, M. CASADO, L. BUISÁN (coords.), “Documento sobre bioética y big data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública”, del Observatorio de Bioética y Derecho de la Universidad de Barcelona, Barcelona, 2015, accesible en: <http://hdl.handle.net/2445/104585>.

§ 2 – PRIVACIDAD Y OPEN DATA

A) Panorama normativo para el acceso y tratamiento de los datos de salud

En España, aunque el panorama legislativo en materia de tratamiento de datos de salud es disperso y se encuentra fragmentado¹⁸, podemos considerar que las dos normas básicas de referencia serían la LOPD (Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal) y la LAP (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), que regula entre otros el acceso a la historia clínica. Pues bien, ambas normas están pensando en un tratamiento de los datos de salud en un contexto de asistencia sanitaria que podemos denominar “clásico” y, por tanto, en un tratamiento que se realiza con la finalidad básicamente de atención sanitaria en una relación individual médico-paciente (con algunas excepciones, como la utilización por terceros con funciones de evaluación, acreditación o planificación del sistema; o con fines epidemiológicos, de salud pública y de investigación o docencia, fundamentalmente con datos disociados). En cualquier caso, esta regulación está basada en un uso de los datos de salud en el contexto sanitario previo a la introducción masiva de las TIC en este ámbito, a la época big data o a la cultura del open data y, por lo tanto, no dan una respuesta satisfactoria a los interrogantes que se pueden plantear en el actual escenario. De hecho, ambas normas deben ser objeto de una revisión importante, entre otras cuestiones, en el ámbito del tratamiento de datos de salud a la vista de la aprobación del Reglamento General de Protección de Datos europeo (Reglamento UE 2016/679, de 27 abril 2016; RGPD), y se espera un anteproyecto de LOPD para los próximos meses.

Por su parte, la LTAIPBG (Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, arts. 5.3, 15) y la LRISP (Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, arts. 3.3.a y 3.4) contienen las excepciones clásicas al acceso y la reutilización de datos en poder de las Administraciones públicas cuando se trate de datos de carácter personal y, si son sensibles (como es el caso que nos ocupa), se inclinan por la disociación de datos para permitir el acceso y reutilización de los mismos.

¹⁸ Para un conocimiento más en detalle de la normativa española en el tratamiento de datos de salud, así como en transparencia, acceso y reutilización de la información sanitaria puede consultarse J. VALERO TORRIJOS, «Acceso, reutilización y gestión avanzada de la información sanitaria en el ámbito de la Administración sanitaria: implicaciones jurídicas desde la perspectiva de la innovación tecnológica», en J. VALERO TORRIJOS y M. FERNÁNDEZ SALMERÓN, *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*, Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2014, pp. 643 y ss.; U. ABERASTURI GORRINO, *La protección de datos en la sanidad*, Thomson Reuters-Aranzadi, Cizur Menor (Navarra), 2013, pp. 73 y ss.

En Europa, la tendencia es clara en el sentido de permitir una mayor utilización de los datos de salud, más allá del contexto tradicional de la atención sanitaria al paciente. Ello se ve claramente reflejado en el RGPD que incorpora no solo una definición de datos de salud (así como de datos genéticos y biométricos, arts. 4.13 a 4.15; a diferencia de su predecesora, la Directiva 95/46/CE), sino que presta una atención mucho más amplia al tratamiento de estos datos. A priori, el principio del que parte el RGPD es similar al de la Directiva 95/46/CE, esto es, la prohibición del tratamiento de las categorías especiales de datos (los llamados “datos sensibles”), entre los que se encuentran los datos de salud, estableciendo ciertas excepciones. Ahora bien, se ha ampliado el número de excepciones que pueden incidir en el tratamiento de datos de salud y, además, estas se regulan de forma más amplia. Así, por ejemplo, la excepción clásica del tratamiento de datos de salud en el ámbito de la prestación de la asistencia sanitaria incluye ahora, entre otros, el tratamiento con fines de medicina preventiva o laboral; y junto al tratamiento para la prestación de la asistencia sanitaria y la gestión de los servicios sanitarios, se incluye también la referencia a la asistencia “social” (art. 9.2.h). Adicionalmente, otros dos supuestos pueden tener una incidencia especial en este ámbito: el tratamiento de datos por razones de interés público en el ámbito de la salud pública (art. 9.2.i RGPD); y el tratamiento con fines de investigación científica (arts. 9.2.j, 89 RGPD), que incluye los estudios realizados en interés público en el ámbito de la salud pública (considerando 159 RGPD)¹⁹. Junto a lo anterior, el RGPD dedica un artículo específico a la necesidad de conciliar el derecho de acceso a los documentos públicos y el derecho a la protección de datos personales, aunque remitiendo al derecho de la UE o nacional aplicable (art. 86).

De la lectura de los preceptos señalados se puede vislumbrar cómo en la reciente regulación europea de protección de datos parece haber calado la nueva realidad a la que se enfrentan los modernos sistemas sanitarios y las nuevas necesidades en cuanto a los usos de los datos de salud, siendo sensible a ellas y apostando por una mayor utilización y reutilización de estos datos; todo ello sin perjuicio de la adopción de las medidas de garantía adecuadas de los derechos de los particulares. Y el testigo debería ser recogido por las legislaciones nacionales a las que el propio Reglamento remite en múltiples ocasiones a lo largo de su articulado.

¹⁹ Esta mayor atención del RGPD al tratamiento de los datos de salud se puede observar también en la parte expositiva del texto, con diversos considerandos dedicados a esta cuestión (vid., entre otros, los considerandos 33 a 35, 52 a 54, 73, 156, 157 o 159). En ellos se deja ver esa mayor apertura al tratamiento de estos datos y, en particular, la relevancia otorgada a las finalidades de salud pública y de investigación científica como bases jurídicas para el tratamiento de los datos de salud.

B) La postura de la Agencia española de protección de datos sobre la reutilización de datos del sector público

La Agencia española de protección de datos (AEPD) también parece ir en esta línea. En su reciente documento “Orientaciones sobre protección de datos en la reutilización de la información del sector público”²⁰, se reconoce el valor de la información del sector público y su importancia de cara a la reutilización para la provisión de nuevos productos y servicios. De ahí la necesidad de formular propuestas que permitan compatibilizar ambos derechos: favorecer la reutilización, minimizando los riesgos.

La AEPD opta, siguiendo las orientaciones del Grupo de Trabajo del Artículo 29²¹, por la anonimización como fórmula para compatibilizar ambos derechos; si bien, como se reconoce, la normativa en materia de protección de datos personales exige un alto nivel de anonimización, de forma que la disociación de datos resulte irreversible. Se trata de un resultado muy complejo, pues implica que la imposibilidad de identificación se produzca no solo con los medios de que dispone el responsable del tratamiento, sino también por terceros (considerando 26 Directiva 95/46/CE); y, además, en perspectiva dinámica, pues las TIC evolucionan con el tiempo, y lo que no es posible hoy, puede serlo el día de mañana.

Ante ello, se establece la necesidad de hacer una evaluación de los riesgos de reidentificación²². Además, dadas las dificultades que puede conllevar esta tarea para algunas Administraciones públicas, prevé la AEPD que el reutilizador pueda colaborar con la Administración en cuestión y que pueda llevar a cabo su propia evaluación de impacto o riesgos de reidentificación una vez obtenida la información. Para la evaluación de estos riesgos hay que tener en cuenta factores como la evolución de las TIC a la que ya se ha hecho referencia, la disponibilidad de grandes volúmenes de datos de origen diverso, el valor económico de la información personal de que se trate y de los perfiles de conducta que se puedan obtener.

En cualquier caso, la existencia de estos riesgos no debe excluir, a criterio de la AEPD, la posibilidad de reutilizar la información pública (potenciada por el propio legislador europeo), sino que deben aplicarse garantías jurídicas adicionales a las medidas técnicas y organizativas. Compromisos jurídicos adicionales serían la indicación expresa al reutilizador en el sentido de prohibir la

²⁰ Accesible en:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_proteccion_datos_Reutilizacion.pdf

²¹ Opinion 6/2013, on open data and public sector information (PSI) reuse, 5 June 2013.

²² Las evaluaciones de impacto se consideran una medida adecuada cuando el reutilizador utiliza datos personales y no son, por tanto, necesarias en el caso de datos anonimizados. Otra cosa es que se aconseje acudir a la anonimización como medida adecuada para equilibrar los intereses en juego, acompañada además de una evaluación de riesgos sobre las posibilidades de revertir la disociación de datos.

reidentificación y/o la utilización de los datos personales para la adopción de medidas o la elaboración de perfiles. Y entre los instrumentos dirigidos a garantizar estos compromisos se señalan, entre otros: la evaluación periódica de los riesgos de reidentificación; auditorías sobre el uso de la información reutilizada ; la obligación de notificar al organismo público la posibilidad de reidentificación ; medidas coercitivas, como las penalizaciones económicas o la posibilidad de suspender o impedir la reutilización de documentos.

De entre las modalidades de reutilización que prevé la normativa en la materia, se considera que la opción más apropiada en estos casos para exigir los compromisos jurídicos mencionados es la concesión de licencias específicas (que incluirán información sobre la finalidad concreta para la que se concede la reutilización, si es comercial o no, duración de la licencia, obligaciones del beneficiario y de la entidad concedente, etc.). Y ello frente a fórmulas más abiertas que se potencian en la legislación (como la de obtener la información en un portal de datos abiertos).

Las anteriores indicaciones en materia de reutilización de información del sector público y su compatibilidad con la protección de datos personales que, como hemos visto, pivotan sobre la anonimización de los datos y las evaluaciones de impacto (riesgos de reidentificación), se completan con otro documento sobre “Orientaciones y garantías en los procedimientos de anonimización de datos personales”²³. En él se establecen de forma detallada los principios de anonimización, las fases del procedimiento (con la definición del equipo de trabajo, la evaluación de riesgos, la viabilidad del proceso, definición/eliminación /reducción de variables de identificación, la selección de la técnica de anonimización...), la formación e información al personal implicado, las garantías, auditorías del proceso, etc. En este documento se señala algo que se viene repitiendo incansablemente en los últimos años, que no es posible garantizar al 100% el anonimato absoluto (sobre todo a lo largo del tiempo). Por ello, la fortaleza de la anonimización habrá que sustentarla en medidas de muy diverso tipo: evaluaciones de impacto, organizativas, de seguridad, tecnológicas y en cualquier otra que permita atenuar los riesgos y paliar las consecuencias en el caso de que estos se materialicen.

En definitiva, los documentos mencionados de la AEPD recogen las líneas que se están imponiendo en esta materia con el fin de permitir el uso de la información pública y favorecer el desarrollo

²³ Accesible en:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf. En este documento se siguen, entre otras, las indicaciones contenidas en: Opinion 5/2014, on Anonymisation Techniques, 10 April 2014, Article 29 Data Protection Working Party. Por otra parte, la AEPD señala que la finalidad de la anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados, pero al mismo tiempo mantener la veracidad de los resultados del tratamiento. Es decir, el procedimiento también debe garantizar que un tratamiento que se realice con los datos anonimizados no conlleve una distorsión de los datos reales.

económico (garantizando al mismo tiempo un nivel “aceptable” de protección de la privacidad de las personas)²⁴: anonimización de datos y evaluaciones de riesgos de reidentificación, partiendo de la necesidad de poner en valor la información y de la aceptación de que el anonimato absoluto no es posible.

C) Lo que podemos aprender de la experiencia catalana en reutilización de datos de salud

La principal experiencia en España en materia de apertura de datos de salud hasta el momento es el proyecto para la reutilización de datos del sistema sanitario público catalán (anteriormente denominado Visc+, al que se ha hecho ya referencia, en la actualidad proyecto PADRIS –Programa público de analítica de datos para la investigación y la innovación en salud²⁵). La implantación de este proyecto ha generado una intensa discusión acerca de determinadas cuestiones que, a nuestro entender, nos pueden orientar sobre cuáles son los elementos básicos a dilucidar en esta materia. Entre otros, se puede señalar:

- El ámbito objetivo de aplicación: determinar qué información sanitaria de la que dispone el sistema público de salud se va a poner a disposición. En este sentido, se señala la necesidad de excluir, por ejemplo, los datos genéticos. También plantean dudas las medidas a adoptar respecto de otro tipo de datos (ej. relacionados con enfermedades que pueden tener un carácter especialmente discriminatorio, como pueda ser las enfermedades mentales o de transmisión sexual).
- La forma en que se ponen a disposición los datos: la regla general será la anonimización. Pero ¿cabría también la cesión de datos personales con el previo consentimiento del interesado?
- En cuanto a la gestión de este tipo de proyectos, se destaca la necesidad de que dicha gestión recaiga en entidades públicas, discutiéndose el papel a otorgar a los colaboradores externos ante la posible externalización de tareas. Igualmente se plantea la existencia de mecanismos de control externos de que la gestión se lleve a cabo correctamente.
- Un elemento fundamental son las finalidades para las cuales se pueden obtener los datos. Dentro del ámbito sanitario destacan las de tipo asistencial, administración y gestión de centros sanitarios y de la administración sanitaria, inspección, estudios epidemiológicos, docencia...
- Y un aspecto especialmente polémico son los clientes finales o destinatarios de la información.

En relación con estas dos últimas cuestiones, el proyecto catalán parece limitarlas a las finalidades de evaluación del sistema de

²⁴ El propio documento de la AEPD sobre orientaciones en los procesos de anonimización destaca cómo el desarrollo de técnicas de anonimización adquiere una importancia vital para garantizar la privacidad en el desarrollo de estudios e investigaciones de interés social, científico y económico.

²⁵ http://aquas.gencat.cat/es/projectes/analitica_dades/

salud o de investigación científica. Y en cuanto a los destinatarios, se ha decantado por centros de investigación acreditados, agentes del sistema sanitario de utilización pública catalana, centros de investigación universitarios públicos y la propia Administración sanitaria (con exclusión de farmacéuticas, aseguradoras, empresas de marketing o consultoras). El acceso a los datos exige el cumplimiento de los criterios establecidos para garantizar el respeto a los principios éticos, de seguridad y de análisis de riesgos y deberá contarse con el aval de un Comité ético de investigación. En este sentido, los proyectos de investigación deben identificar las necesidades de información y los objetivos de la investigación, con descripción del interés científico del estudio, su alineamiento con los planes estratégicos y el beneficio potencial en la salud de la ciudadanía y en el sistema sanitario. Igualmente deben publicarse los proyectos que utilicen estos datos, así como sus resultados.

Una cuestión polémica es el papel que se le otorga al consentimiento de los interesados y la posibilidad de incluir un sistema opt-out. Se discute la relación entre la autonomía y los principios de justicia y beneficencia y en qué medida en un sistema de salud público la ciudadanía debe ceder altruistamente los datos para que se puedan hacer investigaciones en beneficio de todos, siempre que se garantice la seguridad de los mismos.

De esta manera, frente al consentimiento parece cobrar especial relevancia la información al ciudadano sobre qué, quién y para qué se van a tratar sus datos anonimizados y garantizar que no habrá una explotación privada para otras finalidades (comercialización de datos o usos ilícitos). La información debería incluir también la advertencia al ciudadano de la imposibilidad de garantizar una anonimización total y añadirse garantías jurídicas adicionales (compromiso de no reidentificación).

CONCLUSIONES

La apertura de datos en el sector salud es ya un hecho y parece imparable, cuenta con el apoyo legislativo y la simpatía de los poderes públicos ante los beneficios declarados que puede tener para una gestión más eficiente, mejora de los servicios, reducción de costes, impulso a la innovación e investigación y, en definitiva, para una mayor satisfacción de los individuos con el sistema de salud. Ahora bien, no está desprovista de controversia ética y jurídica, debido a lo sensible de la información que se está manejando y a la imposibilidad de garantizar al cien por cien el anonimato y a la dificultad de controlar el uso que a la postre se hace de ella.

Frente a opciones que maximizan la autonomía del sujeto, dándole prevalencia a su consentimiento (consentimiento que, en principio, podría parecer innecesario dada la anonimización de los datos), las herramientas que se ponen a disposición del individuo para “controlar” el uso que se hace de su información sanitaria pasan más bien por potenciar la transparencia e información y

utilizar mecanismos que reduzcan los riesgos (de reidentificación, de usos ilícitos...). El “control”, por tanto, se pone a la hora de determinar quién accede a los datos, por y para qué, en qué condiciones, etc.; traspasando la “responsabilidad” a quien accede (a través, entre otros, de compromisos jurídicos asumidos en el uso de los datos) o a quién los detenta (con planes sobre gestión, uso y reutilización de los datos de que dispone como responsable). Nos encontramos, así, con la paradoja de que el empoderamiento del individuo pasa desde luego por una información de calidad, pero al mismo tiempo se disminuyen sus facultades de controlar el uso que se hace de su información sanitaria. Está por ver que las garantías que se disponen para proteger la información sean suficientes para evitar un uso con fines comerciales u otros no deseados.

