BIG DATA O LA ACUMULACIÓN MASIVA DE DATOS SANITARIOS: DERECHOS EN RIESGO EN EL MARCO DE LA SOCIEDAD DIGITAL[1]

Mª Mercedes Serrano Pérez
Profesora de Derecho Constitucional
Universidad de Castilla-La Mancha

RESUMEN

Big Data sanitario constituye una acumulación de datos relativos a la salud de los individuos que permite el acceso a un gran volumen de datos y con una gran rapidez. Las ventajas que aporta Big Data en el campo sanitario son muy considerables, pero también pueden verse amenazados los derechos de los individuos. Precisamente por el volumen de datos que se manejan y la facilidad de acceso, el riesgo para la libertad de la persona es mayor. Por ello es preciso extremar las garantías para que la utilización de dicha información no constituya el enemigo a batir, sino el aliado para mejorar la asistencia sanitaria de la población en todas sus vertientes. En España, el proyecto VISC+ configura un Big Data sanitario que no está exento de polémica, precisamente por algunas imprecisiones de las que adolece el proyecto y que pueden suponer una merma para el derecho a la intimidad de los ciudadanos. Reforzar las garantías jurídicas para que ello no suceda es la finalidad que ha de perseguir el Derecho.

PALABRAS CLAVE

Big Data, datos personales, protección, derecho a la intimidad.

ABSTRACT

Big data is an accumulation of data relative to individuals´ health which allows to access to a large volume of data with high speed. The advantage that big data give us in the sanitary case are very considerable, but also, the human rights can be threatened.

Because of the data volume that we are dealing with and the easy access we have, the risk for person freedom is bigger.Because of that, it is necessary to increase the warranties for the use of that information not constitute the enemy to beat, but the ally to improve health care for the population in all its aspects. In Spain, VISC+ is a Big Data that is not without controversy, precisely by some wrong things about the project and that can mean a decrease for the right

1 Ponencia presentada a la Mesa Plenaria: Big data. Acumulación masiva de datos sanitarios, cooperación público-privada y derechos en riesgo en el marco de la sociedad digital, presentada en el XXIV Congreso sobre Derecho y Salud, celebrado en Granada, 10-12 de junio de 2015, titulado Innovación y desarrollo tecnológico en el ámbito de la salud.

Artículo dedicado a mi madre Carmen Ramona, por su incondicional ayuda siempre.

to a citizen's privacy. Strengthening legal warranties for these issues do not happen, it is the goal that law has to pursue.

KEYWORDS

Big Data, personal data, protection, right to privacy.

1.¿QUÉ ES EL BIG DATA? CONCEPTO Y NORMATIVA APLICABLE.

Big Data (BD) constituye una acumulación de datos. Consiste en un macro conjunto de datos relativos a personas que, por su organización y accesibilidad, aportan un gran volumen de información, es decir, BD es un tratamiento de datos de carácter personal cuyo análisis arroja una información precisa y rápida[1]. La dimensión que alcanza este depósito de datos, y a juicio de los partidarios del BD, requiere una normativa específica y una atención particularizada, pues, las reglas y normas convencionales que hasta ahora han delimitado y regulado el uso de la información personal parecen quedar obsoletas al dirigirse e intentar regular este acopio de datos.

BD se sitúa en el contexto de la protección de datos, pues ésta se extiende a la utilización de los datos de carácter personal sometidos a tratamiento que pueden experimentar algún tipo de operación de las que incluyen las normas, nacionales o internacionales, sobre la materia. La Directiva 95/46/CE[2] define el tratamientos de datos personales (art. 2 b) como "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción". De acuerdo con la definición de tratamiento de datos que se ha consolidado tanto en la normativa internacional como en nuestro ordenamiento, BD constituye un tratamiento de datos de carácter personal, aunque a partir de esta inclusión en la definición general señalada, debamos admitir ciertas especificidades en razón de sus características.

Las normas vigentes de protección de datos contemplan la necesidad de proteger los datos de carácter personal en la medida en que estos datos revelan aspectos de la persona y sobre los que el sujeto debe mantener un control y un dominio, con el fin de proteger su propia libertad de actuación, su personalidad, en definitiva sus derechos fundamentales[3]. La protección de datos construye un sistema de garantías que debe permitir al individuo que nadie que él no consienta o desee utilice informaciones relativas a su entorno o a su persona. Mantener el control sobre lo que somos, hacemos o pensamos, y que se ha proyectado en la sociedad actual en forma de informaciones personales –datos de carácter personal- es una faceta de la libertad del individuo del siglo XXI. En efecto, el individuo de la sociedad tecnológica ha visto cómo el tratamiento de datos de carácter personal resulta inevitable, además de necesario para mantener el nivel de vida y servicios propio de las sociedades actuales, pero también es consciente de que este tratamiento de datos ha de estar sometido a criterios y normas que eviten su transformación en una amenaza para el ejercicio de sus derechos.

Por tanto, si a la reducción de lo que somos a un elenco de datos y de informaciones, unimos las

1 Otras definiciones de Big Data: "Big Data se refiere a los conjuntos de datos cuyo tamaño está más allá de las capacidades de las herramientas típicas de bases de datos para capturar, almacenar y analizar" McKinsey Global Insitute; "Big Data es una nueva generación de tecnologías, arquitecturas y estrategias diseñadas para capturar y analizar grandes volúmenes de datos prevenientes de múltiples fuentes heterogéneas a una alta velocidad con objeto de extraer un valor económico a ellos", Consultora IDC, Disponible en la URL: http://www.fundacionctic.org/sat/articulo-que-es-el-big-data (Con acceso el 12.7.2015)

2 Directiva 95/46/CE del Parlamentos Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281, de 23 de noviembre de 1995).

3 La STC 292/2000, de 30 de noviembre, define el contenido esencial de la protección de datos como "el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legitimó que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4)", (STC 292/2000, FJ 5). Para señalar más adelante, de modo más contundente que "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular" (STC 292/2000, FJ 7).

posibilidades de la tecnología[4], disponemos de una manera rápida y fácil de la facultad de manejar información de carácter personal respecto de un elevado número de individuos que aparecerían ante quien tiene capacidad de disponer de esa información absolutamente transparentes y por tanto, en un posible estado de vulnerabilidad que el propio sujeto puede llegar a desconocer. En este contexto de manejo de datos y de necesario control del mismo se sitúa, como decíamos más arriba BD, aunque con unas posibilidades mucho más amplias de las que ofertaba en su estado primigenio la tecnología, fruto de avances a un ritmo vertiginoso y que descubren cada día nuevas posibilidades.

Las normas de protección de datos existentes hasta ahora contemplan un estado de la técnica que, si bien no puede calificarse de viejo, si podemos afirmar que, debido a la evolución de la tecnología, ha devenido obsoleto para incorporar a su protección y criterios algunos procesos novedosos. Las disposiciones de protección de datos contemplan reglas y principios para un estado de la tecnología que atiende a un manejo "sencillo", poco sofisticado de la información, con mecanismos de acceso a los datos de forma particular. Los datos a los que se accede son datos estructurados[5], estáticos, en definitiva forman parte de un estado tecnológico poco complejo. En la actualidad, sin embargo, las posibilidades de la técnica, en lo que a tratamiento de la información personal se refiere, han experimentado una nueva revolución, a la que parece que ya no son aplicables las normas convencionales. El Derecho, de nuevo y como tantas otras veces, debe actualizarse para dar respuesta a los distintos retos que se le plantean, en orden a la protección de los derechos de la persona. Porque esta última finalidad es invariable, tratándose de un Estado de Derecho cuyo propósito es la limitación del poder para garantizar el espacio de libertad de los derechos fundamentales de la persona. Ese es el marco que ha de quedar diseñado también para el tratamiento de los datos a través de BD.

Por tanto, las coordenadas jurídicas en las que se inserta BD están perfectamente definidas: utilización de datos de carácter personal a gran escala (tratamiento), necesidad de regular dicho manejo y protección de los derechos de los sujetos de los que se conoce la información. Todo ello desde la protección máxima que la Constitución brinda a los derechos de los ciudadanos. Está en juego la libertad del individuo, que es el bien más preciado de la persona y con ello el ejercicio de sus derechos.

Junto a ello el BD constituye un gran negocio, pues la información es poder, y compartirla o difundirla puede tener un precio en el mercado. Conocer los gustos de los individuos, su personalidad, sus intereses, etc., abre un abanico de posibilidades infinitas en una sociedad que propugna la libertad de empresa, la libre competencia y el libre mercado. La facilidad de acceso a grandes volúmenes de datos puede mover grandes cantidades de dinero en diversos sectores. En este sentido BD no parece conocer límites, pues lo mismo acumula y trata información sobre el clima, las migraciones, datos sismográficos, el ámbito empresarial o el sanitario. Disponer de esa información, en cada uno de sus contextos, y poder utilizarla coloca en situación ventajosa al sujeto que la conoce frente a quién no lo puede hacer. El negocio estriba en la facilidad para acceder y analizar un gran volumen de datos, lo que permite, en definitiva, adoptar una decisión en el menor tiempo posible, con toda la información sobre los elementos integrados en ella recolectada además en un tiempo record.

La diferencia fundamental del BD con los ficheros de información que almacenan datos personales, y todo el universo que se contempla en las leyes de protección de datos actuales, consiste en la recolección por parte del BD tanto de datos estructurados como no estructurados. Los datos estructurados son los datos a los que hace referencia la LOPD en su art. 3 b) y 5.1 k) RLOPD, el primero de ellos cuando define el concepto de fichero como "todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso". El dato estructurado responde a un criterio específico de organización y de acuerdo a ese criterio se dispone el acceso a los mismos. La novedad que aporta BD consiste en unir a los datos estructurados hasta ahora recogidos en un fichero y tratados de forma organizada, los datos no estructurados. Los datos no estructurados son aquellos datos no almacenados

4 No podemos olvidar que las leyes de protección de datos regulan el tratamiento de datos de carácter personal automatizado o manual, aunque es obvio, que uno y otro no conllevan los mismos riesgos para la persona y sus derechos.

5 La diferencia entre datos estructurados y no estructurados marca también la diferencia en la tecnología y en la respuesta de las leyes de protección de datos. Los datos estructurados están constituidos por la información ordenada y organizada de acuerdo a diversos criterios materiales o funcionales, decididos en la mayoría de los casos por el responsable del fichero; los datos no estructurados son los datos como vídeos, Excel, imágenes, redes sociales, Word, documentos pdf, audio, etc., es decir, datos no almacenados de forma convencional.

en una base de datos tradicional[6]. BD puede recoger y tratar tanto datos estructurados como no estructurados[7], lo que agota prácticamente todas las posibilidades informativas y también de conocimiento de la información relativa a un individuo y para un sector determinado, todo ello a una gran velocidad[8].

2. BIG DATA EN EL SECTOR DE LA SALUD.

BD en el campo de la salud adquiere una importancia trascendental, pues va a modificar (si no lo está haciendo ya) la forma de trabajo en el área de la salud, ya que afectará al tratamiento de la información en la atención médica, investigación, administración hospitalaria, asistencia sanitaria, epidemiología, etc[9]. Las ventajas generales del BD, que consisten no sólo en poner a disposición de los demandantes de información los datos, sino también el conocimiento, se trasladan a la sanidad, lo que facilitará una utilización más racional y eficaz de la información y revertirá en la atención sanitaria al paciente. No sólo repercutirá en el paciente, sino que podrá ser utilizada por los estudiantes de medicina y el personal sanitario, con lo que incrementará el valor de la información al permitirse su reutilización. El giro copernicano que BD aportará al ámbito de la salud se basa en la utilización de datos estructurados junto a datos no estructurados. En el área de la salud los datos estructurados, es decir, los organizados bajo un criterio estático y cuyo almacenamiento permite el acceso singular a los mismos, está formado por los datos del paciente, tanto los personales, como algunos datos relativos a la salud (los que constan en forma de informaciones que relacionan una información sobre la salud de una persona con el sujeto titular de esa información). Por su parte, los datos no estructurados son "las recetas de papel, los registros médicos, las notas manuscritas de médicos y enfermeras, las grabaciones de voz, las radiografías, escáneres, resonancias magnéticas, TAC y otras imágenes médicas, los archivos electrónicos o de contabilidad, y gestión administrativa..."[10]. Por otro lado, los datos generados por las redes sociales, blogs, wikis, etc., pueden constituir también datos no estructurados, así como los datos de los teléfonos inteligentes.

Del informe "*Big Data in digital Health"* de la fundación *Rock Health*[11], de gran valor en el campo de la salud, y su estudio se desprende el cambio radical que provocará trabajar con BD. Así las aplicaciones de BD al área de la salud provocarían una auténtica revolución al permitir el manejo de datos no estructurados especialmente, pues se lograría definir de un mejor modo las causas de las enfermedades y ofrecer una mejor solución. Los datos se utilizarán para predecir, prevenir y personalizar enfermedades y hacer un seguimiento más individual de los pacientes y de su evolución. Aunque todas las áreas sanitarias se verían mejoradas en sus prestaciones por la utilización de BD, el citado informe destaca en particular las siguientes:

6 Entre las características de los datos no estructurados son: "Volumen y crecimiento: el volumen de datos no estructurados y su crecimiento es muy superior al de los datos estructurados; origen de los datos: el origen es muy diverso, puede tratarse de datos generados en redes sociales, en foros, e-mails, documentos internos (word, pdf, ppt); almacenamiento: para almacenarlos no se puede emplear medios tradicionales sino que hay que utilizar la estructura de Big Data. A veces por el tipo de datos se impone el almacenamiento cloud; terminología e idioma: la terminología es una cuestión crítica tratándose de datos no estructurados tipo texto. Es preciso racionalizar la terminología; seguridad: algunos datos no estructurados tipo texto no son seguros. Por otra parte, el control de acceso a los mismos es complejo debido a cuestiones de confidencialidad y la difícil clasificación del dato", Vidal, J., Big Data: Gestión de datos no estructurados, disponible en la URL: http://www.dataprix.com/blog-it/big-data/big-data-gestion-datos-no-estructurados (Con acceso el 23.6.2015).

7 Las principales cuestiones a considerar en el tratamiento de información no estructurada son las siguientes: "Crear una plataforma escalable (infraestructura y procesos), añadir información/estructura complementaria a los datos no estructurados; crear conjuntos reducidos de datos que sean representativos; desarrollo de algoritmos: procesos de depuración/limpiado de datos", http://www.dataprix.com/blog-it/big-data/big-data-gestion-datos-no-estructurados (Con acceso el 23.6.2015)

8 Como se ha puesto de manifiesto, BD "se caracteriza por lo que se conoce como las 3 V's: volumen, pues existe un crecimiento exponencial de datos; variedad: los datos se obtienen de múltiples fuentes (datos tanto estructurados como no estructurados) y velocidad ya que las tecnologías de BD permiten capturar, almacenar y analizar datos a la mayor velocidad posible", disponible en la URL http://www.fundacionctic.org/sat/articulo-que-es-el-big-data (Consulta el 23.06.2015)

9 Según *The Human Face Big Data*, el área de la salud y bienestar es una de las seis áreas en las que se centra este informe y que experimentará un profunda transformación que revertirá en la mejora de la sociedad, disponible en Facebook: www.facebook.com/FaceOfBigData

10 Informe disponible en www.slideshare.net/RockHealth/rock-report-big-data (Consulta el 23-6-2015). El informe es comentado en Poyatos Díaz, J. M., "Big Data y el sector de la salud: el futuro de la sanidad", Disponible en la URL: http://poyatosdiaz.com/index.php/big-data-y-el sector-de-la-salud-el-futuro-de-la sanidad, (Consulta el 3.06.2015).

11 Según las conclusiones del informe hay tres vías mediantes las cuales big data puede cambiar la atención sanitaria, a juicio de Poyatos, J. M.: 1. Transformación de datos en información; 2. Apoyo al autocuidado de las personas; 3. Apoyo a los proveedores de cuidado médicos; 4. Aumento del conocimiento y concienciación del estado de salud; 5. Agrupamiento de los datos para expandir el ecosistema". Disponible en http://poyatosdiaz.com/index.php/big-data-y-el sector-de-la-salud-el-futuro-de-la sanidad, (Consulta el 3.06.2015).

> "La investigación genómica y la secuenciación del genoma; operativa clínica; autoayuda y colaboración ciudadana; mejora en la atención personalizada al paciente; monitorización remota de pacientes; medicina personalizada para todos; autopsias virtuales; seguimiento de pacientes crónicos; mejoras en los procesos médicos."

Las posibilidades y aplicaciones de BD[12] son inmensas, pero, precisamente, por la magnitud del manejo de información se han de incrementar también las medidas de protección de las personas. Ya no cabe ninguna duda que la libertad del individuo del siglo XXI y los derechos de la personalidad, básicamente el derecho a la intimidad, han de incorporar otra forma de protección frente a los canales susceptibles de mover en la actualidad la información personal. La construcción jurídica del derecho a la protección de datos persigue como finalidad proteger los datos del individuo, para así proteger la libertad del ser humano. Mientras podamos mantener protegidos los aspectos del ser humano que desvelan perfiles de su conducta, de sus gustos, de sus actividades laborales, de sus preferencias de ocio, de su situación geográfica, de su salud, etc., quedará a salvo la libertad de la persona. Revelar estos aspectos, por inocuos que nos parezcan, reduce el número de elementos personales que pertenecen a la esfera que controlamos, y nos hacemos más vulnerables, en la medida en que estamos más expuestos a los ojos y a las decisiones de los demás.

En el campo sanitario las posibilidades del BD abren, como decimos, todo un abanico de actuaciones e intervenciones que pueden ser utilizadas de forma positiva, de manera que se trasladen a la mejora de la salud de los ciudadanos, pero también pueden planear como una amenaza para su intimidad, su libertad y para sus derechos. Esa potencial amenaza resulta de la valoración especial que las normas sobre protección de datos han hecho de los datos que recogen la salud de las personas, que son el instrumento esencial que BD almacena y pone a disposición de los usuarios del mismo. En efecto, al calificativo de datos personales, dichas normas añaden el calificativo de sensible[13], precisamente por lo delicado de la información que incorporan, que, como regla general, solamente se comunica al médico para recibir tras ello una asistencia sanitaria y en la seguridad de que va a quedar amparada por la confidencialidad que sostiene la relación médico-paciente[14]. Por ello el Derecho debe regular este macro almacenamiento de datos sobre la salud para evitar lesionar los derechos de los individuos.

3. EL PROYECTO VISC+: LA RESOLUCIÓN SLT 570/2015, DE 16 DE MARZO.

En España la experimentación del BD ha tenido lugar en Cataluña bajo la creación del proyecto VISC+ (Más valor a la información de salud de Cataluña)[15], que pone a disposición de los ciudadanos, empresas, laboratorios y centros de investigación, los datos contenidos en las historias clínicas de pacientes atendidos por la sanidad pública catalana, con el objetivo de mejorar la salud de la población y facilitar la investigación y evaluación sanitaria. En su formulación originaria el Proyecto VISC+ consistía en la licitación de un contrato de colaboración público privada para la implantación de un modelo de gestión de servicios con el fin de dar más valor a la información sanitaria.

El proyecto, así diseñado, contó con un amplio rechazo en el Parlamento catalán[16], y conforma un BD sanitario que pretende poner a disposición de los interesados tanto los datos como el conocimiento que se desprende de los datos de la sanidad pública catalana. El Proyecto fue analizado por la Agencia Catalana de Protección de Datos (APDCAT),

12 Por ejemplo el citado autor cuenta un ejemplo y un caso verídico singular. Como ejemplo, "los profesionales sanitarios pueden utilizar la analítica de big data en tiempo real para saber dónde se está extendiendo un virus de la gripe y a qué ritmo pueden adaptar la respuesta y garantizar el stock de vacunas suficiente para los sitios que lo necesiten", disponible en http://poyatosdiaz.com/index.php/big-data-y-el sector-de-la-salud-el-futuro-de-la sanidad, (Consulta el 3.06.2015).

13 El art. 7.3 LOPD señala que "Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una ley o el afectado consienta expresamente". Por su parte, el art. 5.1 f) define los datos de carácter personal relacionados con la salud como "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".

14 Sobre la especialidad de los datos sobre la salud se puede ver Rebollo Delgado, L. Serrano Pérez, M. M., **Manual de Protección de Datos**, Dykinson S. L., Madrid 2014, pág. 99 y ss; Gómez Sánchez, Y., "Datos de salud como datos especialmente protegidos", **Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,** Troncoso A. (dir.), Thomson Reuters, Cívitas, Madrid 2010, págs. 647 y ss.

15 Proyecto aprobado en sus inicios en septiembre de 2013.

16 BOPC, núm. 421, de 3 de noviembre de 2014, Moción 150/X

dando lugar al Dictamen 34/2014[17]. El Dictamen de la APDCAT incluía varias recomendaciones y sugerencias en orden a la protección de datos personales, de acuerdo con la Ley Orgánica 15/1999, de 13 de diciembre[18], (en adelante LOPD) y el Reglamento de desarrollo de la Ley, el Real Decreto 1720/2007[19], de 21 de diciembre (RLOPD). Ya el Parlamento catalán instaba al Gobierno a paralizar la licitación del Proyecto VISC+ por no incorporar en su contenido las aportaciones de los representantes de los grupos parlamentarios, colegios profesionales de especialidades implicadas, profesionales y direcciones de los centros asistenciales y de investigación, expertos en investigación social y biomédica, y representantes de la APDCAT.

El 14 de enero de 2015 tuvo lugar una jornada de debate sobre la reutilización de datos y el proyecto VISC+ con los representantes de los grupos parlamentarios y representantes de la APDCAT, quienes remarcaron las recomendaciones incluidas en el Dictamen 34/2014. El proyecto VISC+ reelaborado es objeto de un segundo Dictamen 20/2015 por parte de la APDCAT[20] que se pronuncia sobre las modificaciones incorporadas. Antes de la emisión del segundo dictamen se ha publicado la **Resolución SLT 570/2015 de 16 de marzo[21],** por la que se encarga, por parte del Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Catalán de la Salud a la Agencia de Calidad y Evaluación Sanitarias de Cataluña (AQuAS) el inicio de un proceso de anonimización de todos los datos de los pacientes atendidos en la sanidad catalana, para ser puestos a disposición de todos los agentes que tienen posibilidad de intervenir para mejorar la salud de la población a través de acciones de evaluación o investigación. El segundo dictamen de la APDCAT se pronuncia sobre las siguientes cuestiones[22]:

- Sobre la información que se tratará en el Proyecto VISC+
- Sobre el encargo del tratamiento
- Sobre el modelo de gestión.
- Sobre la finalidad del tratamiento, los destinatarios de la información y los servicios previstos.
- Sobre la anonimización de los datos personales en el contexto del Proyecto VISC+.
- Sobre las garantías éticas del uso de los datos.
- Sobre el ejercicio de los derechos ARCO y posibilidades de opt-out.
- Sobre análisis de riegos
- Sobre medidas de seguridad.

Aspectos todos ellos que han experimentado alguna transformación tras el Dictamen 30/2014 de la APDCAT.

Por tanto, el análisis que versa a continuación tratará sobre algunos aspectos del Dictamen de marzo de 2015 de la APDCAT, que analiza las variaciones del proyecto VISC+ y de la Resolución 570, que incorpora en su contenido aspectos de dicho proyecto, y supone la implantación definitiva del mismo.

3.1. Objetivo general.

La Resolución 570 expone en sus manifestaciones la exigencia por parte de la sociedad actual de utilizar la tecnología para mejorar la calidad y disponibilidad de los servicios sanitarios. En efecto, con el objetivo de mejorar la calidad de vida y de prestación sanitaria de los ciudadanos, la tecnología ofrece a un ritmo vertiginoso avances y mejoras que pueden y deben revertir en la sociedad (no otra finalidad debe tener la tecnología, sino ponerse al servicio del ser humano).

A estos fines loables se dirige el VISC+, a poner en valor la cantidad de datos sobre la salud recopilados por el sistema de salud de Cataluña, a mejorar la atención sanitaria gracias a la utilización de la tecnología. Para ello, como reconoce la propia Resolución, se facilita a "los agentes que intervienen o tienen

17 Disponible en http://www.apd.cat/media/dictamen/ca_678.pdf

18 BOE núm., 298, de 14 de diciembre de 1999.

19 BOE núm. 17, de 19 de enero de 2008.

20 Dictamen 20/2015, en relación con el Proyecto para dar valor a la información del sistema sanitario catalán en el marco de las políticas públicas, disponible en http://www.apd.cat/media/dictamen/ca_769.pdf.

21 Resolución 570/2015, de 16 de marzo, por la que se hace público un encargo de gestión que formalizan el Departamento de Salud, el Servicio Catalán de la Salud y el Instituto Catalán de la Salud con la Agencia de Calidad y Evaluación Sanitarias de Cataluña, Diari Oficial de la Generalitat de Catalunya, núm. 6843-1.4.2015.

22 La documentación aportada por el proyecto VISC+ modificada tras las oportunas consideraciones ya comentadas es la siguiente: Memòria del projecte VISC+: més valor a la informació de salut de Catalunya; Garanties ètiques d'us de les dades; Dades i procés d'anonimització; Anàlisi de riscos; Anàlisi dels possibles models per a la gestió del projecte; Estàndards de recol-lecció de dades; Presentació del projecte VISC; todos ellos disponibles en URL http://aquas.gencat.cat/ca/projectes/visc/documentacio (consultado el 10.7.2015)

capacidad para mejorar la salud de la población a través de actuaciones de evaluación o investigación, y mantener al mismo tiempo la necesaria protección de los datos personales que tienen un carácter altamente sensible"[23], el empleo de los datos almacenados y tratados por el Sistema Catalán de salud, por medio de un proceso de anonimización.

3.2. Sujetos con acceso a los datos: sujetos públicos y privados.

Al objetivo citado se puede formular una primera crítica, referida a la alusión a los agentes que intervienen en los procesos sanitarios, que, por su sentido híbrido e inconcreto, puede referirse tanto a agentes públicos como privados. En ningún apartado posterior de la Resolución se concreta el carácter público o privado de los agentes con acceso a los datos sobre la salud, por lo que hay que entender que la posibilidad para los agentes privados está prevista y permitida por la norma. El Dictamen 20/2015 APDCAT consideraba adecuado, en la revisión del proyecto VISC+, la concreción de los clientes finales o destinatarios de la información (centros acreditados de CERCA y Agentes del sistema sanitario integral de utilización pública de Cataluña)[24], concreción que, a mi juicio, desaparece en la Resolución 570 con la referencia amplia e indeterminada efectuada a los agentes que intervienen para mejorar la salud de la población. En efecto, los documentos 3 (apartado 5.2 del Documento) y 5 en los que se reflejaba los sujetos a los que se dirigía la información y que ya no se mencionan en la Resolución son:

- Centros de investigación acreditados por CERCA

- Agentes del sistema sanitario integral de utilización pública de Cataluña (SISCAT), que planteen la necesidad de acceder a los datos en relación con la calidad, efectividad, eficiencia, etc., de los servicios sanitarios o de los tratamientos[25].

El documento núm. 7[26], apartado 2.1, excluye expresamente a determinados peticionarios como farmacéuticas, consultoras, aseguradoras de salud, empresas de colocación o de contratación de personal, empresas publicitarias, de marketing o de prospección comercial, etc. Pese a la razonable consideración de exclusión que realiza la APDCAT de estos tipos de sujetos con acceso a los datos, reflexiona también acerca de la pertinencia de la exclusión de las aseguradoras, teniendo en cuenta que la información sobre la salud puede ser relevante en determinados tipos de seguros como los de vehículos. Si bien esta última consideración que realiza la APDCAT es cierta, podemos señalar que puede haber otro procedimiento por parte de las aseguradoras para conocer los datos de salud de los sujetos, además de no encajar en la misión de las aseguradoras las funciones de evaluación e investigación en las que piensa el proyecto. Por tanto, la recomendación de la APDCAT en relación con los destinatarios de la información abogaba por "a los efectos de transmitir una información lo más clara y coherente posible entre todos los documentos objeto de consulta, convendría añadir la referencia a los Agentes del SISCAT como destinatarios de los servicios de VISC+, en aquellos documentos en que sólo se hace referencia a los centros acreditados de CERCA (entre otros, apartado 6.2 del Documento núm. 3)", sugerencia que, vista la referencia genérica a los agentes que intervienen o tienen capacidad para mejorar la salud de la población, que realiza la Resolución 570, no sólo no se ha observado, sino que ha empeorado considerablemente desde el punto de vista de la precisión, por lo que el daño, de nuevo, recae en la protección de los derechos de los sujetos cuyos datos de salud se manejen, al permitir el acceso a los datos de los sujetos privados y públicos sin ningún tipo de precisión.

Cabe realizar también alguna apreciación más en relación con la posibilidad de uso público o privado de la información. En primer lugar la distinción entre el uso público o el privado no debe alterar el nivel de protección de los datos personales, pues, de lo que se trata es de la protección de un derecho fundamental, protección que no diferencia entre amenazas procedentes del sector público o del sector privado, aunque tradicionalmente el Estado ha sido el vulnerador por excelencia del espacio de protección de los derechos fundamentales, en los últimos años y en parte debido

23 Manifestación núm. 1 de la Resolución 570.

24 La información relativa a los sujetos que tendrán acceso a los datos está contenida en el documento 3 relativo a la Memoria social del proyecto (Memòrie Projecte) y al documento 5 referido a valoración de los modelos de gestión de VISC+ (Anàlisis dels posibles models per a la gestió del projecte), disponibles en URL http://aquas.gencat.cat/ca/projectes/visc/documentacio

25 Referencia que se contiene en el Dictamen de la APDCAT, pág. 11.

26 Documento relativo a las garantías éticas del uso de los datos (código ético), (Garanties ètiques d'ús de les dades) disponible en URL http://aquas.gencat.cat/ca/projectes/visc/documentacio

a las tecnologías, el sector privado es un potencial (real) agresor de la libertad de la persona. Tampoco, en segundo lugar, la LOPD diferencia en las medidas de protección a aplicar a los datos y en los derechos que forman parte del contenido de la protección de datos entre un sector y otro. Las medidas, principios y criterios de protección protegen un derecho fundamental que es predicable de los individuos frente a todos, por tanto, frente a cualquier ámbito del que pueda provenir la amenaza de violación del derecho. Por ello tampoco puede entenderse, en términos jurídicos estrictamente, la desnaturalización que del derecho a la intimidad realiza el Informe del Comité de Bioética[27], al defender la validez y constitucionalidad del Proyecto VISC+, y aludir al derecho a la intimidad como un derecho básico, cuando por su naturaleza jurídico constitucional constituye un derecho fundamental, cualidad que le otorga la más alta protección en el ordenamiento jurídico. Ello no significa que pueda ser considerado como un derecho absoluto, como no lo es ningún derecho fundamental, sino que puede ceder y ver restringido su disfrute y protección ante intereses o derechos constitucionalmente más dignos de protección. La mejor protección de otros derechos justificaría la reducción del derecho a la intimidad o a la protección de datos, sin que esto provoque una lesión en el mismo[28].

3.3. Las finalidades del proyecto.

Las finalidades de evaluación o investigación inciden más todavía en la inconcreción del proyecto. Las citadas finalidades son, además, las que recupera la Resolución 570 en la primera de sus manifestaciones, aunque luego, son ampliamente sobrepasadas en el anexo 2 de la citada norma. Dicho anexo incluye las finalidades a las que podrían ser destinados los datos: asistencial, administración y gestión de centros sanitarios, gestión sanitaria por la Administración sanitaria, inspección por la administración sanitaria, estudios de epidemiología, investigación, docencia, actividad estadística dentro del Plan de Estadística. De hecho la APDCAT expresamente reconoce que en la Resolución 570 y dentro del apartado "servicios encargados incluye no sólo finalidades de investigación y evaluación (de hecho no hay una referencia expresa a la evaluación del sistema sanitario)…". De nuevo, aunque los documentos analizados por la APDCAT resaltan la evaluación e investigación como las finalidades del proyecto VISC+, las ampliaciones que incluye la Resolución son objeto de razonable crítica por parte de la Agencia.

En relación con las exigencias derivadas de la aplicación de la LOPD, el art. 4.1 señala que la información solamente puede ser objeto de tratamiento "en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". Por su parte el art. 4.2 indica que "Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos". Tal y como ya hemos referido en el párrafo anterior, las finalidades de evaluación e investigación, que son legítimas, determinadas y explícitas se diluyen con la ampliación de fines que contempla el anexo 2, pues no todas esas funciones corresponden a las genéricas de evaluación e investigación. En relación con el art. 4.1 LOPD, la APDCAT recuerda la necesidad de mantener los criterios de calidad de los datos recogidos en el art. 4.1 LOPD. Así se destaca que "1 Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas explícitas y legítimas para las que se hayan obtenido".

El principio de proporcionalidad es un principio que acompaña al dato durante toda su vida activa, desde que se recoge y empieza a tratarse, por lo que incluye también la cesión, que constituye una operación más, incorporada al concepto de tratamiento. De hecho la finalidad del tratamiento permite mantener ligado al dato con su tratamiento, pues si la finalidad que motivó y legitimó la recogida llegara a desaparecer o a cumplirse los datos deberán ser cancelados, según dice el art. 4.5 LOPD: "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán

27 En concreto el Documento del Comité de Bioética señala que "la protección de la intimidad es un derecho básico y que se debe preservar la confidencialidad de las historias clínicas…", "Principios éticos y directrices para la reutilización de la información del sistema de salud catalán en la investigación, la innovación y la evaluación", disponible en www.comitebioetica.cat

28 Sobre la limitación del derecho a la intimidad y a la protección de datos para preservar otros bienes o derechos constitucionalmente dignos de protección vid., Serrano Pérez, M. M., en "El derecho al honor, a la intimidad personal y familiar y a la propia imagen. La inviolabilidad del domicilio. La protección de datos", en **Los derechos fundamentales**, García Guerrero, J. L., (coord.), Tirant lo Blanch, Valencia, 2013, págs. 441-490, donde se contiene jurisprudencia del TC sobre la colisión entre los derechos fundamentales citados.

conservados en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados…"

Pues bien, en relación con el anexo 2 la APDCAT, dentro de los servicios encargados, que están más arriba citados, estima que se incluyen no sólo fines de investigación y evaluación, cuando a juicio de la APDCAT no hay una referencia expresa a la evaluación, sino que también se incluyen fines de tipo asistencial, administración y gestión de centros sanitarios, gestión sanitaria para la administración sanitaria, inspección por la administración sanitaria, estudios de epidemiología, docencia y actividad estadística dentro del Plan estadístico. La APDCAT es crítica también con la falta de explicación acerca de las medidas de seguridad a aplicar a los datos que han de ser de nivel alto, como corresponde a los datos que son fuente de información del proyecto VISC+, pero la falta de concreción expresa es interpretada por la APDCAT como permisibilidad para admitir ficheros de nivel de seguridad inferior.

3.4. El encargo del tratamiento.

La Resolución 570 contempla un encargo de tratamiento que ha de ajustarse a lo establecido en el art. 12 LOPD. Por tratarse de un tratamiento de datos hay dos elementos fundamentales que proteger: por una parte los datos, como elementos físicos que incorporan una información, en este caso, especialmente sensible y por otro, a los sujetos a los que se refiere esa información. Respecto de lo primero hay que tener en cuenta el art. 4 LOPD y las medidas de seguridad que han de ser observadas mientras dura el tratamiento (y en este caso también tras su finalización) y en relación con lo segundo la posibilidad de accionar los derechos ARCO, con el fin de mantener el control y el dominio de los datos de carácter personal que han pasado a ser objeto de tratamiento. Esa es la cuestión principal, el contenido esencial del derecho que no puede ser rebasado o desconocido, pues en ese caso el derecho fundamental –a la protección de datos o a la intimidad, a la libertad en definitiva- quedaría desnaturalizado y reducido a la nada. Por tanto, el control por parte del individuo, saber en todo momento qué se hace con sus datos y a qué se destinan, constituye el aspecto fundamental de la protección de datos, ya sea en un BD o en un fichero convencional, el instrumento resulta indiferente, porque el derecho fundamental es digno de protección en cualquier situación y el ordenamiento jurídico no puede hacer excepciones a ello.

Con el objetivo de "mejorar la calidad, seguridad y sostenibilidad del sistema de salud de Cataluña", generando el conocimiento preciso para ello, el Departamento del Salud, el Servicio Catalán de la Salud y el Instituto Catalán de la Salud encargan a la Agencia de Calidad y Evaluación Sanitaria de Cataluña (AQuAS) llevar a cabo el proceso de anonimización de los datos de la salud que están incluidos en los ficheros de datos de carácter personal, al amparo del art. 12 LOPD, como primer paso para facilitar su utilización a todos los agentes implicados en las actuaciones de evaluación o de investigación ya referidas. Todo ello para dar valor a los datos del sector sanitario catalán en el marco de las políticas públicas, dice la norma.

En virtud del contrato celebrado entre el responsable del tratamiento - el Departamento de Salud, el Servicio Catalán de Salud y el Instituto Catalán de la Salud- y el encargado del mismo –AQuAS-, tiene lugar un acuerdo sobre las limitaciones y posibilidades en orden al tratamiento de la información contenida en los ficheros de datos de los responsables citados. El encargado del tratamiento se compromete a:

1. Realizar el proceso de anonimización de los ficheros de datos de carácter personal con los datos de salud incluidos en el Departamento de Salud, del Servicio Catalán de Salud y del Instituto Catalán de la Salud, persiguiendo con ello un interés para la investigación y evaluación médica. La relación de ficheros que se enumera en el anexo 1 de la norma contiene una completa relación de todos los ficheros que incluyen datos sobre la salud en el sistema de salud catalán. Sin embargo, no parece constituir una lista cerrada, en virtud de las ampliaciones contenidas en el anexo 1 y relativas a cada conjunto de ficheros de los respectivos entes públicos. En efecto, tras el inventario detallado de ficheros, en cada enumeración se recoge la posibilidad de su ampliación, con la cláusula de "Y en el futuro cualquier otro fichero de (responsable, cualquiera de ellos) con datos de salud o centros asistenciales de interés siempre que se justifique para algunas de las finalidades señaladas en el anexo 2. La propuesta de inclusión corresponde al responsable del fichero y tiene que contar con la valoración favorable del comité de seguimiento"[29]. El Dictamen 20/2015 APDCAT critica esta fórmula que ya consideró desaconsejable en el Dictamen anterior "desde la

29 Según se contiene en el (FJ XIV del Dictamen 34/2014), FJ V Dictamen 20/2015, pág. 6.

perspectiva del principio de calidad". Pero junto a ello, la APDCAT pone de relieve en el Dictamen del 2015 que el encargo de tratamiento contenido en la Resolución 570 tiene lugar con la observancia de los requisitos del art. 12 LOPD y del que ya ha tenido conocimiento la APDCAT, según señala expresamente la citada Resolución (pacto segundo), afirmación que no es cierta, ya que el Dictamen del 2014 solamente se refería "al proyecto VISC+ que, según se desprende del resto de la documentación adjuntada, incluye la anonimización de datos de salud para su cesión con finalidades de investigación y de evaluación del sistema sanitario"[30], lo que resulta excedido tanto por las finalidades recogidas como por la posibilidad de ceder datos personales, ambos elementos recogidos en la Resolución 570. Por tanto, como dice la APDCAT, "las menciones a cesiones de datos personales y las remisiones a finalidades que van más allá de las de investigación y evaluación, no se ajustan a dicho nuevo enfoque de VISC+".[31]

2. Utilizar la información anonimizada para algunas de las finalidades incluidas en el anexo 2, a las que ya hemos hecho referencia, y que recordemos exceden las finalidades de evaluación e investigación

3. Cesión a terceros de la información anonimizada para algunas de las finalidades del anexo, 2, es decir, de las señaladas anteriormente.

4. Cesión a terceros de información personal, esto es, no anonimizada, para algunas de las finalidades del anexo 2 siempre que se den dos condiciones:

   a) que exista consentimiento previo de cada uno de los sujetos afectados.

   b) que el cesionario disponga de una auditoria en la que se compruebe el cumplimiento de todas las medidas de seguridad exigidas por la LOPD y por el RLOPD.

La cesión de estos datos convierte al cesionario en responsable del tratamiento, asumiendo todas las obligaciones que la LOPD atribuye a los responsables del tratamiento, aunque como ya hemos hecho referencia se trata de una posibilidad que no estaba incluida en el originario proyecto VISC+, y puede provocar una lesión en los derechos del sujeto. De hecho la APDCAT consideraba un acierto del proyecto que comportara la "anonimización de toda la información personal por parte de la entidad, antes de su comunicación a terceros, descartando de esta manera la comunicación de datos personales de salud no anonimizados, a los destinatarios finales"[32], situación que *sensu contrario,* puede, como decimos, constituir una serie amenaza para el sujeto. Dada la importancia de no comunicar datos personales, la APDCAT insistía en el Dictamen 20/2015, en la necesidad de "…remarcar y hacer énfasis que durante el funcionamiento de VISC+ no se utilizarán datos personales, ya que el tratamiento y el análisis estadístico se hará sobre datos anonimizados"[33]. No obstante el proceso de anonimización de datos, respecto del proyecto VISC+ que analiza la APDCAT en el Dictamen de 2015, ésta señala que debería aclararse que VISC+ sí procederá al tratamiento de datos personales en origen, "ya que la anonimización por parte de la entidad es una fase más del "tratamiento" de los datos. Convendría pues matizar la afirmación que VISC+ no utilizará datos personales", afirmación que, a mi modo de ver, sigue siendo aplicable al encargo que contiene la Resolución 570. Es más, la APDCAT indica la conveniencia de que los datos personales que no han sufrido aún el proceso de anonimización tengan que cumplir las medidas de seguridad[34]. Medidas de seguridad que también tendrán que cumplir los datos anonimizados, aunque ya no se trate de datos personales, pero puesto que la anonimización constituye el elemento esencial del proyecto deberá realizarse con las mayores garantías posibles. Dichas garantías deben valorar las potencialidades del BD y las posibilidades de permitir la reidentificación de una persona, para lo que habrá que valorar toda la información disponible, no sólo en el marco del proyecto sino de otros proyectos o la información a disposición del solicitante de la misma. En concreto la APDCAT, en el marco del Documento 2 y del Documento 8, "prevé eliminar la información identificativa de personas físicas (datos identificativos e información genética), eliminar o reducir al mínimo

30 Por lo que la referencia incluida en el pacto segundo de la Resolución 570 es errónea "dado que esta autoridad sólo se ha pronunciado respecto del proyecto VISC+", (FJ V Dictamen 20/2015), pág. 6.

31 FJ V Dictamen 20/2015, pág. 7.

32 Dictamen 20/2015, FJ VIII, pág. 12.

33 Información que se contiene en la pág. 4 del Documento núm. 4, Anàlisi de riscos (Análisis de riesgos), disponible en URL http://aquas.gencat.cat/ca/projectes/visc/documentacio, incidiendo la APDCAT en la necesidad de "transmitir una información a los afectados lo más clara posible, respecto de las implicaciones de VISC+", Dictamen 20/2015, FJ VIII, pág. 13.

34 Dictamen 20/2015, FJ VIII, pág. 13

imprescindible el detalle de la información u otras variables que pueden dar lugar a identificaciones indirectas, así como aplicar las técnicas de alteración de los datos. También se prevé atribuir un código anónimo de personas con el fin de permitir relacionar los diferentes conjuntos de datos y aplicar un segundo código diferente para cada proyecto. Estos códigos se tendrán que crear mediante algoritmos que no permitan que terceras personas puedan relacionarlo con una persona concreta (…) Y también en la línea de lo que ya se puso de manifiesto en nuestro anterior Dictamen, la anonimización debería afectar también a los datos relativos al centro donde ha sido atendido el paciente o códigos geográficos, en línea con lo que ya prevé el apartado 2.9 del Documento núm. 7"[35].

Por último, la Resolución contiene en el pacto octavo del encargo de tratamiento, la posibilidad de reidentificar al sujeto titular de los datos, en caso de posibles peligros para su salud presente o futura, tras la combinación de datos. En este caso el encargado del mismo se obliga, dice la norma, a informar al responsable de los ficheros para adoptar las medidas precisas en orden a salvaguardar la salud del sujeto. La reidentificación, incluso en estos casos de riesgo, está prohibida para el encargado del tratamiento (lo que significa que la posibilidad de realizarla no es improbable). En este sentido el Dictamen 20/2015, en su FJ IX, insiste en la inexistencia de riesgo cero respecto de la reidentificación de la información previamente anonimizada. Por ello, y valorando la reversibilidad del proceso de anonimización recuerda la necesidad de respetar el principio de proporcionalidad, de manera que solamente se puedan acceder a los datos anonimizados mínimos que dan cobertura a la petición, para lo cual la APDCAT aconseja la introducción de la referencia relativa a "los datos de salud de los cuales se pueda derivar unas mayores consecuencias discriminatorias o estigmatizadoras para las personas afectadas".

La Resolución finaliza estableciendo que la utilización de los datos y su cesión, en coherencia con el art. 4 LOPD sobre el principio de la calidad de datos, solamente alcanzará a los datos estrictamente necesarios para cumplir con alguna de las finalidades descritas en el Anexo 2 y que no resulten excesivos. Por último, las cesiones a terceros sólo se efectuarán a entidades dedicadas a la finalidad que justifique la cesión de los datos y que debe ser alguna de las que se recogen en el anexo 2.

Respecto del encargo, tiene sentido aquí manifestarse sobre el mandato recogido en la Resolución 570, aunque la APDCAT se refiere en el Dictamen al encargo del proyecto VISC+ tras las modificaciones incorporadas[36] y alude a la posibilidad de contratar con un tercero, -colaboradores externos-, parte de los servicios encomendados a la Agencia, recomendando, en este sentido, que se explicara el modelo que se escoge (contar con colaboradores externos o no), aunque parece deducirse que es el primero, así como el rol de los colaboradores. En la Resolución estas cuestiones parecen quedar más claras, pues la figura jurídica de encargado de tratamiento del art. 12 LOPD ya permite la posibilidad de subcontratación y así se contempla en el pacto séptimo, donde se alude expresamente a la autorización por parte del responsable del fichero "de forma expresa al encargado del tratamiento a subcontratar a terceras empresas/entidades parte de los servicios indicados en el encabezamiento de este acuerdo"[37], autorización expresa que se contiene en el art. 21.1 RLOPD, salvo que se cumpla la condición del art. 21.2[38]. Ninguna garantía añade el párrafo siguiente, en el que se obliga a que "con anterioridad a la subcontratación por parte del encargado del tratamiento, éste comunique al responsable de los ficheros los datos identificativos de las

35 Dictamen 20/2015, FJ VIII, pág. 14, al igual que la anonimización de los datos de los profesionales sanitarios que han atendido al paciente.

36 En el Dictamen 20/2015, FJ VI, pág. 8 la APDCAT analiza la posibilidad contenida en VISC de contactar con colaboradores externos mediante "un contrato de servicios resultado de un proceso de diálogo competitivo"

37 Esto es: "Medir, evaluar y difundir de forma pública y transparente los resultados globales alcanzados en salud y en el ámbito de la asistencia sanitaria por los diferentes agentes que integran el sistema de salud, a partir de la gestión del sistema integrado de información de salud en Cataluña, configurado por la información de naturaleza administrativa y estadística que contienen los registros y sistemas de información del departamento y los organismos competentes en materia de salud, los de los centros, servicios y establecimientos sanitarios y de los profesionales sanitarios; Desarrollar tareas de investigación en el ámbito de sus funciones; ejercer todas las actividades que sean necesarias para el cumplimiento de sus objetivos, así como también las actuaciones en relación con las citadas funciones que le sean encomendadas". Esta actividad, recuérdese, se precisa en la anonimización de los datos, en la utilización de los datos para las finalidades señaladas en el anexo 2, la cesión a terceros de información personal para algunas de las citadas finalidades y la cesión a terceros e la información anonimizada para las mismas finalidades.

38 Será necesaria autorización expresa salvo que se cumplan las condiciones del art. 21.2 RLOPD, la primera de las cuales no se ajusta a lo previsto en la Resolución 570, a tenor de su redacción "2 a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar", la segunda condición no resulta absolutamente necesaria, pero sí la primera, respecto de los servicios a subcontratar, a los que la Resolución 570 alude como "parte de los servicios a contratar", es decir, con una indeterminación que no permite la subcontratación sin autorización por parte del responsable del tratamiento.

empresas/entidades subcontratistas, además de regular contractualmente el tratamiento realizado por estas terceras entidades de los datos incluidos en los ficheros. Este tratamiento se tendrá que ajustar en todo caso a las instrucciones dictadas por el responsable de los ficheros", que son requisitos a los que se ha de someter la subcontratación según el art. 21 RLOPD, aunque la especificación de los datos de la empresa con la que se va a subcontratar se podrán comunicar tras la subcontratación.

El documento relativo a la Información sobre el tipo de datos y el proceso de anonimización de VISC+, explica que la información que será objeto de tratamiento, es decir, el conjunto de datos de carácter personal y sobre la salud que será objeto de tratamiento está contenido en los ficheros del Departamento de Salud, del Servicio Catalán de Salud y del Instituto Catalán de la Salud (regulados por SLT 25/2014, de 3 de febrero). En concreto en los siguientes ficheros:

- Fichero de encuestas de salud
- Fichero estadístico de estadística de causas de muerte.
- Fichero de la historia clínica.
- Fichero de patologías específicas.
- Fichero de prestación farmacéutica.
- Archivo de registro del conjunto mínimo básico de datos (CMBD)
- Fichero de pacientes del Instituto Catalán de Salud. La APDCAT recomienda hacer referencia clara a los ficheros incluidos en el proyecto, en concreto el Dictamen se refiere al Registro de prestación farmacéutica o al Fichero de Pacientes de la División de Atención Primaria del Instituto Catalán de la Salud, ficheros ambos que no obstante la recomendación siguen apareciendo en la Resolución SLT 570/2015.

3.5 Garantías éticas del uso de los datos.

El documento titulado Garantías éticas de los datos (Garanties ètiques d'us de les dades), aportado como novedad tras la remodelación del proyecto VISC+, establece una serie de principios para el desarrollo del proyecto y para valorar la demanda de información y el seguimiento posterior de su utilización.

El documento 3, en su apartado 5.1[39], habla de un Comité Ético de Investigación Clínica (CEIC), que no parece coincidir exactamente con el Comité de seguimiento del pacto quinto de la Resolución y cuyas funciones se concretan en el pacto noveno del encargo. Este último precisa que corresponde al Comité la genérica función de "analizar la situación del servicio y decidir sobre mejoras en éste", para lo cual analizará la siguiente información:

> "-Utilización de datos directamente por el encargado de tratamiento realizadas y previstas.
> -Cesiones de datos realizadas y previstas a terceros.
> -Conjuntos de datos actualmente disponibles para su utilización según las finalidades señaladas en este anexo.
> -Informes sobre el cumplimiento de los criterios de anonimización.
> -Incidencias.
> -Resultados de auditorías.
> -Cambios en los procedimientos".

La regulación del Comité de seguimiento, que parece ser el órgano que asume una pequeña parte de las funciones que los documentos 3, 7 y 8 atribuyen al CEIC, resulta algo imprecisa y poco efectiva. Ya el Dictamen 20/2015, a la vista de las discordancias de los citados documentos, aconsejaba "calificar el papel del CEIC o de los CEIC en el proceso de gestión de la demanda"[40], lo que no se logra con la regulación que hace la Resolución, que contempla al Comité con funciones de evaluación y de actuación a posteriori, pero no como un órgano dirigido realmente a garantizar la protección de los derechos de los sujetos y a velar por la gestión de las demandas de datos efectuadas.

3.6 Los derechos de los sujetos.

Como hemos dicho en un momento anterior en estas páginas, uno de los elementos o pilares esenciales de la protección de datos lo constituye el abanico de derechos o facultades sobre los que se articula el control por parte del sujeto de sus informaciones personales sometidas a un tratamiento. Los derechos que facilitan el ejercicio del dominio sobre los datos son los derechos de acceso, rectificación, cancelación y oposición (ARCO). Para que los citados derechos

39 Memòria del projecte VISC+: més valor ala información de salut de Catalunya, en URL http://aquas.gencat.cat/ca/projectes/visc/documentacio.

40 Dictamen 20/2015, FJ IX, pág. 15.

puedan articularse es preciso respetar también el derecho de información del art. 5 LOPD y el principio del consentimiento del art. 6 LOPD que legitima un tratamiento de datos.

Pues bien, el Dictamen 20/2015, alude en su FJ X[41] a la posibilidad de ejercitar los derechos ARCO y el opt-out. Hay que aclarar en este momento, como precisa la APDCAT, quizá de modo algo confuso, que cuando se trabaja con datos anonimizados, no se produce la identificación de la persona a la que se refiere la información, por lo que el sujeto de protección ya no existe y por tanto no es de aplicación la LOPD. No se trata ya de datos personales que permiten identificar a una persona, de acuerdo con la definición contenida en la LOPD. El dato es objeto de protección en tanto en cuanto revela información que hace referencia a una persona concreta, pero si el dato es anónimo la información que incorpora no se refiere a ningún sujeto (salvo que el proceso de anonimización sea reversible). Por ello el proyecto VISC+, en lo que respecta a los datos anonimizados no ha de prever el ejercicio de los derechos ARCO. Ahora bien, a mi juicio, si debería estar previsto para las cesiones de datos personales que contempla la Resolución como una posibilidad en el pacto primero d) que, sorprendentemente no contiene ninguna alusión expresa al ejercicio de los derechos ARCO. Aunque la Resolución contiene diferentes remisiones a la aplicación de la LOPD, en mi opinión, en este caso, hubiera sido deseable y más garantista, una referencia explícita al ejercicio de los derechos, siendo su ausencia a mi modo de ver un motivo de disminución de protección para el sujeto. Ahora bien, el hecho de que no sean de aplicación los derechos de acceso, rectificación, cancelación y oposición al proyecto VISC+, por tratarse de datos anonimizados, no significa que con carácter previo al proceso de disociación no puedan ejercitarse. Y así lo recuerda la APDCAT en el Dictamen 20/2015 al señalar que "convendría matizar que los derechos ARCO continúan siendo de aplicación respecto de los datos personales de origen (tratados en los diferentes ficheros y sistemas de información que son fuente de información de VISC+), hasta que se procede a su anonimización por parte de la entidad. Por lo tanto, los derechos ARCO y, en especial el derecho de oposición (art. 6.4 LOPD), tienen que poder continuar ejerciéndose delante de los correspondientes responsables de los tratamientos", facultad que omite completamente la Resolución 570. No hubiera estado de más incluir una referencia a dicha posibilidad, para una mejor protección de los derechos de los sujetos de los que se tratan los datos sobre la salud.

41 Pág. 16.

Por último hay que decir que las partes se comprometen a observar la más estricta confidencialidad sobre las informaciones, datos y documentación a la que tengan acceso en virtud del encargo recibido y no podrán utilizar dicha información para fines y usos diferentes de los previstos en el contrato de encargo, haciendo constar de forma expresa que velarán por el cumplimiento de la normativa de protección de datos (pacto cuarto de la Resolución y pacto quinto del encargo). El pacto quinto contempla la obligación de guardar secreto y confidencialidad de lo conocido a través de la realización de las actividades propias del encargo. Esta obligación de confidencialidad impide la reproducción total o parcial de los datos por ningún medio o soporte, ni su tratamiento, ni edición informática, ni transmisión a terceras personas fuera de la ejecución del encargo. Por tanto, la obligación de secreto incumbe a todos los sujetos que tiene acceso a la información y quedan igualmente obligados a observar todas las medidas técnicas y organizativas tendentes a garantizar la confidencialidad e integridad de la información. Dichas obligaciones subsistirán incluso después de finalizar el acuerdo.

El pacto cuarto alude a las medidas de seguridad que, contenidas en el art. 9 LOPD, han de ser implementadas por el encargado del tratamiento. Se trata de medidas técnicas y organizativas que garanticen la seguridad de los datos personales que están en los ficheros de los responsables y eviten su alteración, pérdida, tratamiento o acceso no autorizado, valorando el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos tanto por parte del hombre como por parte del entorno físico o natural. La concreción de las medidas de seguridad está regulada en el RLOPD. Como medida de seguridad añadida en el acuerdo suscrito, el responsable de los ficheros "podrá solicitar al encargado de tratamiento, en caso de estimarlo conveniente, una copia del preceptivo informe de auditoría con la finalidad de verificar el cumplimiento de las medidas de seguridad reguladas en el Reglamento citado anteriormente", ello sin perjuicio de control que realizará trimestralmente el comité de seguimiento previsto en el pacto décimo del acuerdo.

4. CONCLUSIÓN

En resumen, y tras el análisis realizado de diversas cuestiones relativas a la disposición normativa que recoge la forma jurídica del BD, podemos concluir que el encargo realizado a AQuAS para "medir, evaluar y difundir de forma pública y transparente los

resultados en salud de los distintos agentes que integran el servicio catalán de salud a través de gestión de la información sanitaria", resulta mejorable en aspectos fundamentales en orden a garantizar la protección de los sujetos de los que se recogen y tratan datos relativos a la salud. Las medidas de protección recogidas en el proyecto VISC+ resultan insuficientes para poder hablar de una protección elevada de los derechos de los ciudadanos, por lo que el riesgo del tratamiento de los datos sobre la salud por medio de este BD sanitario no aparece conjurado. Ello no significa, no obstante, que la acumulación masiva de datos en el contexto de la salud, no deba realizarse y que mediante una mejora en los criterios de utilización de los datos y en los fines perseguidos, no pueda conseguirse una reutilización de los datos efectiva y eficaz. El BD introduce indudables beneficios que no deben ni pueden ignorarse, como tampoco la protección de los derechos de los sujetos cuyos datos son manejados. El equilibrio ha de lograrse a través de una regulación jurídica razonable y sensata.

5. BIBLIOGRAFÍA

• Consultora IDC, http://www.fundacionctic.org/sat/articulo-que-es-el-big-data

• Gómez Sánchez, Y., "Datos de salud como datos especialmente protegidos", **Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal**, Dir. Troncoso Reigada, A., Thomson-Reuters, Cívitas Madrid 2010.

• Poyatos Díaz, J. M., "Big Data y el sector de la salud: el futuro de la sanidad", http://poyatos-diaz.com/index.php/big-data-y-elsector-de-la-salud-el-futuro-de-la sanidad

• "Principios éticos y directrices para la reutilización de la información del sistema de salud catalán en la investigación, la innovación y la evaluación", www.comitebioetica.cat

• Proyecto Visc+, http://aquas.gencat.cat/ca/projectes/visc/documental.

• Rebollo Delgado, L., Serrano Pérez M. M., **Manual de Protección de Datos,** Dykinson S. L., Madrid 2014.

• Serrano Pérez, M. M., "El derecho al honor, a la intimidad personal y familiar y a la propia imagen. La inviolabilidad del domicilio. La protección de datos", **Los derechos fundamentales**, Dir. García Guerrero, J. L., Tirant lo Blanch, Valencia, 2015.

• The Human Face Big Data, www.facebook.com/FaceOfBigData

• Vidal, J. Gestión de datos no estructurados, http://www.dataprix.com/blog-it/big-data/big-data-gestion-datos-no-estructurados