Capítulo 8

El valor y el precio de los datos personales de salud en la sociedad digital

Itziar de Lecuona Ramírez
Universidad de Barcelona
María Villalobos-Quesada
Universidad de Barcelona

SUMARIO: I. INTRODUCCIÓN. II. LA RESPUESTA DE LA UNIÓN EUROPEA A LA INVESTIGACIÓN CON BIG DATA A PARTIR DEL 2018: EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS. III. LOS PROYECTOS VISC+ Y PADRIS: LECCIONES APRENDIDAS CONTRA LA MONETIZACIÓN DE DATOS PERSONALES DE SALUD EXPLOTADOS A ESCALA MASIVA EN INVESTIGACIÓN. IV. CONCLUSIONES Y PROPUESTAS. V. REFERENCIAS.

Resumen. El cambio de paradigma hacia una economía guiada por el dato para mejorar la toma de decisiones en la sociedad digital, potencia el uso y la mercantilización de conjuntos de datos personales, entre los cuales los datos de salud son de especial interés, por el valor intrínseco que poseen y por el que pueden adquirir mediante su explotación a escala Big Data. El poder que confiere el acceso a esta información y su adecuada explotación por parte de terceros, estén situados en el ámbito de la iniciativa pública o en el de la privada, o una alianza entre ambas, merece ser objeto de reflexión en una sociedad en la que las capacidades informáticas deshumanizan al individuo mediante la recolección y cruce de datos de distinta índole de forma algorítmica, para luego ofrecerle atención y servicios automatizados e hiperpersonalizados aparentemente a coste cero. La intimidad es un valor a proteger que se ha convertido en un bien con el que comerciar. Ambas posibilidades son hoy comúnmente aceptadas, no planteándose *a priori* que la intimidad deba estar fuera del tráfico mercan-

til, sino que se busca compatibilizar dos situaciones irreconciliables bajo la lógica del mercado. Frente al imperio de esta lógica, de lo que se trata es de evitar la acumulación injustificada de datos personales, incluyendo los de salud, e impedir su mercantilización, con el fin de que la intimidad no se vea menoscabada.

I. INTRODUCCIÓN

El Big Data se refiere al tratamiento de grandes volúmenes de datos mediante el desarrollo de algoritmos matemáticos, para establecer correlaciones entre datos, incluidos los personales y determinar patrones de comportamiento que permitan predecir tendencias para mejorar la toma de decisiones (Llàcer et al. 2015: 29-49). La definición de datos masivos, o Big Data como se les conoce en inglés, se establece a partir de los grandes volúmenes de datos, que se manejan entre terabytes y petabytes de magnitud. Para referirnos a magnitudes que podamos imaginar, un terabyte es la capacidad de 1500 CDs, mientras que un petabyte es la capacidad de 1.5 millones de CDs aproximadamente. El manejo de estos increíbles volúmenes de información ha venido de la mano de avances teóricos y tecnológicos en áreas tales como informática, matemática, electrónica y computación. Los datos masivos también se pueden caracterizar por su alta variedad (lo que se denomina alta heterogeneidad estructural), velocidad (en referencia a su generación y análisis), variabilidad (variaciones en las tasas de transferencia de datos) y complejidad (porque se origina de muy diversas fuentes) (Gandomi y Haider 2015: 137-144).

El valor de la información contenida en los datos masivos reside en las asociaciones y relaciones que pueden ser utilizadas para tomar decisiones, un proceso que algunos han llamado en inglés Big Data to knowledge (BD2K) (Margolis et al. 2014: 957-958). De esta forma, el uso de los datos masivos puede afectar a los individuos a nivel personal, llámese micro-escenario, y social, macro-escenario (Comisión de las Comunidades Europeas 2004: 4-23, Mantelero y Vaciago 2015: 104-109). Cuantos más datos estén disponibles de forma fiable y organizada, más poderosos son los análisis que se pueden realizar (Casanovas et al. 2017: 335-349). En una base de datos, el individuo se convierte en una referencia a la que se le asigna un conjunto de variables. Las variables de un grupo de individuos se pueden analizar para proponer relaciones o asociaciones. Los individuos serán categorizados en subgrupos, de los que se pueden derivar conclusiones basadas en probabilidades estadísticas. Estos análisis por ejemplo, pueden establecer patrones de acuerdo con el lugar de residencia, edad, género, etnicidad, nivel de ingresos o nivel educativo.

La explotación a escala masiva de conjuntos de datos, incluidos los datos personales y de salud, es una de las prioridades de la Unión Europea (UE). Así, se destinan fondos para proyectos de Big Data en el contexto del Programa Horizonte 2020 y se persigue la creación de un mercado digital, una economía y una sociedad guiada por el dato que sea competitiva y a la vez respetuosa de los derechos e intereses en juego (European Commission 2017: 5-45). El objetivo es situar a Europa a la cabeza de los mercados y de la investigación más puntera. Para conseguir estos fines, se ha visto como necesaria la reutilización de datos del sector público (Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa a la reutilización de la información del sector público). Por esto es comprensible que los estados miembros hayan priorizado iniciativas de explotación de datos a escala masiva en el contexto de la salud, con sistemas de consentimiento presunto en el que todos los ciudadanos están incluidos en una base de datos para fines de investigación sanitaria, a no ser que manifiesten su consentimiento en sentido contrario. Los conjuntos de datos personales de salud adquieren valor por la información que aportan *per se* y por aquella que se pueden desentrañar; lo cual nos enfrenta con situaciones en las que lejos de ser utilizados para el bien común, se instrumentalizan para obtener el máximo rendimiento económico, persiguiendo intereses con fines de lucro vestidos de innovación e investigación. Esta situación se analizará más adelante a propósito de los proyectos sobre analítica de datos masivos de salud VISC+ y PADRIS, impulsados por el gobierno catalán desde el año 2013 hasta la actualidad.

Así, nuevas aplicaciones de la ciencia y tecnología han dado paso a una economía basada en el uso y la mercantilización de datos personales, incluidos los de salud. Para muestra, basta con entrar en las plataformas de descarga de aplicaciones móviles y constatar la ingente cantidad de aplicaciones (apps) de salud y bienestar. Estas apps se basan en la acumulación y explotación de información personal de múltiples fuentes, como los datos sociodemográficos, de geolocalización y de salud. Es habitual que esta información sea liberada, con o sin el conocimiento del titular de los datos, a terceros que acumulan y ponen precio a esos datos, generando nuevos modelos de negocio fundamentados en el acceso a la intimidad de las personas (Casino 2017). Estas apps pueden incorporar biometría y conectarse al Internet de las cosas (the Internet of Things), sensores y vestibles. Son muchas las combinaciones y posibilidades que además permiten una observación de los patrones de comportamiento de individuos en tiempo real a través de la geolocalización, pues los flujos de datos están a disposición de quienes quieran explotarlos en perímetros en los que no se puede asegurar la confidencialidad de los datos personales.

En esta ocasión nos centramos en el tratamiento a escala masiva de datos que incluyen información relativa a la salud. Por ejemplo, las historias clínicas informatizadas. El proceso de digitalización de las historias clínicas transforma la información médica, antes fragmentada y almacenada en diferentes lugares y formatos, digitales y analógicos, en una colección única a la que se puede acceder desde diferentes lugares para garantizar una asistencia adecuada y eficiente. Aunque este tipo de información ha sido tradicionalmente utilizada en áreas de salud pública, actualmente ha adquirido gran valor para la investigación, innovación y desarrollo, actividades que involucran a los sectores público y privado. Las historias clínicas informatizadas pueden contribuir al desarrollo de la medicina personalizada, a conocer en menor tiempo los efectos adversos de los medicamentos, a predecir pandemias y a determinar la susceptibilidad de las personas de sufrir determinadas enfermedades.

Las historias clínicas se pueden enriquecer con otras fuentes de información, como otras bases de datos de índole diversa y colecciones de muestras biológicas de origen humano. Los biobancos son entidades donde convergen estas diferentes fuentes de información. Por ejemplo, los biobancos suelen incorporar numerosos tipos de muestras biológicas, historias médicas, datos genómicos e información sobre el estilo de vida. Esta es una dinámica con tendencia al alza que responde al concepto integral de la salud y a un alejamiento del reduccionismo genético que predominó durante el tiempo de la publicación del genoma humano. La vasta información en manos de los biobancos posee gran potencial biomédico, incluyendo el de contribuir a la medicina personalizada y al esclarecimiento de problemas complejos como la transición salud-enfermedad y la influencia del estilo de vida en la salud (Gottweis 2012: 12-39).

El caso de la explotación a escala masiva de datos de salud, como son las historias clínicas, es particularmente interesante y delicado, puesto que se trata de información personal altamente sensible. Si esta información no se protege adecuadamente y no se controla su tratamiento durante todo el ciclo de vida de los proyectos de investigación de las iniciativas basadas en la innovación, puede monetizarse y ser objeto de lucro por parte de terceros ajenos a la actividad investigadora. De valores como el bien común y el altruismo en investigación en salud se transita velozmente a generar nichos de mercado de datos personales. Efectivamente, proyectos que utilizan datos de salud se han enfrentado a fuertes críticas antes y después de ser aprobados, precisamente por carecer de las medidas suficientes para garantizar la protección de los derechos e intereses de los ciudadanos, especialmente de la intimidad, y por allanar el terreno a potenciales discriminaciones de individuos en función de sus datos, por ejemplo los

genéticos, en nombre de la investigación científica, la excelencia y la innovación. Las críticas también se han centrado en la falta debates sociales informados, los cuales deberían servir tanto al público para formar un criterio esclarecido, como para informar la toma de decisiones políticas y estratégicas. Por ejemplo, las posiciones de los ciudadanos deberían verse reflejadas en las políticas de promoción de la investigación médica, que es la base del sistema público de salud. Lo anterior corresponde al concepto de investigación e innovación responsable, que reconcilia la investigación e innovación con los valores, necesidades y expectativas de la sociedad, lo cual se logra mediante la cooperación entre todos los grupos implicados en investigación e innovación, incluyendo al público en general. Además, esta se fundamenta en la transparencia, gobernanza, educación y divulgación científica, ética, accesibilidad, acceso abierto e igualdad de género (Casado et al. 2016: 43-57, European Commission 2017: 5-45).

II. LA RESPUESTA DE LA UNIÓN EUROPEA A LA INVESTIGACIÓN CON BIG DATA A PARTIR DEL 2018: EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

En el mes de mayo del 2018 entra en vigor el Reglamento General de Protección de Datos (RGPD), el cual trata de dar respuesta a los tratamientos de datos de carácter personal y a la utilización del Big Data, en áreas como la investigación e innovación. El RGPD reconoce que la protección de los individuos en relación con el procesamiento de datos personales es un derecho fundamental. El propósito de esta nueva regulación es armonizar las políticas y medidas para proteger a los ciudadanos de la UE de violaciones de su información personal e intimidad, en un mundo que gira alrededor de los datos y el conocimiento. El RGPD supone cambios relevantes en cuanto al proceso de información y de solicitud de consentimiento informado. Este último debe convertirse en un proceso claro, comprensible y accesible, dejando atrás los formularios largos y llenos de jerga jurídica. Además, el consentimiento deberá ser tan fácilmente otorgado como revocado y habrá de evitarse relaciones asimétricas entre compañías y los usuarios.

Uno de los cambios con mayores implicaciones es que el RGPD ha extendido su jurisdicción a cualquier compañía que procese datos provenientes de individuos que residen en la UE, sin importar dónde esté localizada la empresa. Lo que significa la protección de datos personales europeos más allá de las fronteras europeas. Asimismo, el RGPD establece elevadas sanciones, hasta de 4% del beneficio anual de la compañía o €20 millones, que funcionarán como un mecanismo real de conformidad.

El RGPD también reconoce el derecho al olvido y genera cambios dramáticos hacia la transparencia de las compañías con respecto a sus usuarios. Por ejemplo, le brinda a los usuarios el derecho de recibir copia de los datos personales utilizados y recibir información sobre dónde y para qué están siendo utilizados.

El Reglamento establece una serie de medidas para garantizar que los derechos y libertades de los implicados no sean menoscabados. Introduce un principio de responsabilidad activa, la exigencia de una evaluación del posible impacto que el tratamiento de los datos pueda tener en los derechos de los afectados. Esta evaluación debe hacerse *a priori* y puede repetirse a lo largo del ciclo de vida de la iniciativa que se propone, dependiendo de su naturaleza. Además, en la explotación de datos a escala masiva se introduce como obligatoria la figura del Delegado de Protección de Datos que asesora en esta materia. Las iniciativas deben detallar las medidas técnicas y organizativas por implementar, desde los principios de "privacidad desde el diseño" y "privacidad por defecto", los cuales se refieren a minimizar los datos que se vayan a utilizar, a no acumularlos desproporcionadamente y a garantizar el tratamiento confidencial y seguro de ellos. Esta situación implica que hay que tener previstas las posibles violaciones de seguridad de los datos y los mecanismos de respuesta, de manera que se reduzcan al máximo los riesgos. Una cuestión fundamental es la vigilancia de los datos: es decir, la posibilidad de rastrear en todo momento la situación de los mismos, en especial en cuanto a quién los accede y trata, y con qué propósitos. Este punto es de especial importancia ante las más que habituales externalizaciones de tratamientos de datos y las posibles transferencias internacionales de datos para su explotación por parte de terceros.

El espíritu del RGPD se ve reflejado en otros antecedentes europeos que son indicativos de la evolución de la gobernanza de los datos personales. Por ejemplo, la Agencia Europea de Seguridad de las Redes y de la Información (ENISA por sus siglas en inglés) ha analizado en profundidad los riesgos que suscita el uso de los datos masivos, donde explícitamente se incluyen los datos sanitarios. En un informe publicado en 2015, la ENISA aboga por los "datos masivos con privacidad", lo que implica adoptar los principios de protección de datos y privacidad como "valores esenciales" de los datos masivos: en otras palabras, "privacidad desde el diseño". Desde la concepción de los proyectos, la protección de la intimidad de los implicados debe ser pilar fundamental, lo que conduce a articular medidas organizativas y estructurales, medidas tangibles sobre cómo protegerla y no meros pactos entre caballeros que puedan generar falsas seguridades. La ENISA declara que esto servirá no sólo a los indivi-

duos, sino también a la prosperidad de las actividades que se derivan del análisis de estos mismos datos (ENISA 2015: 9-50). Alcanzar la "privacidad desde el diseño" y la interoperabilidad de los datos masivos a nivel de la UE, enfrenta grandes retos imposibles de eludir. Los Estados Miembros deberán de trabajar en conjunto para establecer no sólo "privacidad desde el diseño" sino "privacidad desde la interoperabilidad".

En este contexto de flujo de datos, cobran sentido los principios de transparencia y rendición de cuentas que establece el RGPD. No se trata ya de que el titular consienta o rechace que se le den usos particulares a sus datos, que también es un principio fundamental sobre el que se asienta la normativa, sino que se trata de que el proveedor de los datos personales pueda tener el control de los mismos y ejercitar los derechos de acceso, rectificación, cancelación y oposición. Especialmente el derecho al borrado, al olvido y a objetar a la toma de decisiones automatizada.

Igualmente, se han sentado precedentes de la superioridad de los derechos individuales, y especialmente del derecho a la privacidad. En el 2014 el Tribunal de Justicia de la UE, mediante la resolución C-131/12, reconoció que intereses económicos no pueden justificar la interferencia del derecho a la protección de datos y acuñó el "derecho al olvido". En otras palabras, el derecho de los individuos sobre su información personal prevalece sobre del derecho de los recolectores de datos (Rees y Heywood 2014: 574-578). Asimismo, la posición del Tribunal es congruente con el Grupo Europeo de Ética (EGE por sus siglas en inglés) en Ciencia y Nuevas Tecnologías de la Comisión Europea. El EGE sostiene que el principio de "limitación de finalidad" debe ser un estándar para organizaciones públicas y privadas. Este principio establece que en lo que respecta a datos personales, estos sólo deben ser recolectados para fines específicos y legítimos, y los fines comerciales requieren consentimiento explícito (EGE 2014: 81-91).

En una sociedad digital como la nuestra es necesario contar con herramientas y capacidades para indagar qué nichos de mercado están fundamentados en datos personales de salud y qué objetivos persiguen, precisamente para evitar la discriminación y una mayor estigmatización social. Este es un reto extraordinario en el contexto de investigación e innovación, ya que en muchas ocasiones los agentes que intervienen en los procesos de tratamiento de datos, tienen distintos intereses en diferentes conjuntos de datos. Aún más importante, no todos los actores persiguen los fines para los que inicialmente se recopilaron los datos. Esos fines primarios son usualmente legítimos, persiguiendo el interés común; como puede ser mejorar la calidad de vida o el tratamiento de una enfermedad

determinada. Sin embargo, ante el posible conflicto de intereses entre los diversos agentes que intervienen en el tratamiento de los datos, es necesario establecer medidas para evitar la mercantilización de la intimidad y la monetización de los conjuntos de datos de carácter personal. Puesto que los datos de salud, incluidos los datos genéticos, dicen tanto sobre nosotros, estos son ansiados por terceros para informar la toma decisiones con objetos comerciales, incluso en contra de nuestra voluntad o desde nuestro más completo desconocimiento, permitiéndoles situarse en una posición de dominio en el mercado.

III. LOS PROYECTOS VISC+ Y PADRIS: LECCIONES APRENDIDAS CONTRA LA MONETIZACIÓN DE DATOS PERSONALES DE SALUD EXPLOTADOS A ESCALA MASIVA EN INVESTIGACIÓN

Para entender los retos y las tensiones a los que nos enfrentamos desde la perspectiva ética, jurídica y social en cuanto a la protección de datos personales de salud cuando se explotan a escala masiva en investigación, se analizan a continuación los proyectos VISC+ y PADRIS auspiciados por el gobierno catalán. Los proyectos apuntan a situar a Cataluña a la cabeza de la investigación y la innovación en salud, mediante la reutilización de datos almacenados en el sistema público, acorde con las directrices europeas. Este estudio se considera oportuno en tanto que asistimos a un cambio de paradigma en la protección de los datos de carácter personal en la UE por la inminente aplicación Reglamento General de Protección de Datos. El Reglamento trata de dar respuesta al uso que actualmente se le da a los datos personales en investigación, en la que el no tan nuevo Big Data rompe los moldes y desbarata las reglas sobre los que se asentaba la ya desfasada normativa sobre protección de datos de carácter personal. Un ejemplo de esa normativa es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal del estado español, abreviada LOPD.

Actualmente nos enfrentamos a situaciones en las que se declara querer dar valor a los datos personales relativos a la salud, lo que con frecuencia hace referencia a su capitalización. Los proyectos VISC+ y PADRIS resultan cautivadores porque ejemplifican el forcejeo por proteger los intereses y derechos individuales, en entornos que tienden a la digitalización y a la monetización de datos personales de salud. Dejan patente también la falta de anticipación y previsión. Asimismo ponen de manifiesto la necesidad de integrar la reflexión ética y el impacto social involucrando a los implicados desde el inicio, exigencias que promueve la Unión Europea desde

el concepto de investigación e innovación responsable (Casado et al. 2016: 43-57, European Commission 2017: 5-45).

El acrónimo VISC+ (Més Valor a la Informació de Salut de Catalunya) permite un sugerente juego de palabras, puesto que visc significa vivo. El proyecto VISC+ fue paralizado en el 2016, entre otras razones, por no haber analizado detenidamente las implicaciones éticas, legales y sociales de la explotación de datos a escala masiva en investigación y por abrir la puerta a posibles transferencias de datos de salud con ánimo de lucro. Posteriormente, en el 2017 se aprobó el PADRIS (Programa Públic d'Analítica de Dades per a la Recerca i la Innovació en Salut), también promovido por la Agencia de Calidad y Evaluación Sanitarias de Cataluña (AQuAS por sus siglas en catalán).

Los proyectos VISC+ y PADRIS están basados en el uso secundario de información sanitaria almacenada en distintas bases de datos que podrían correlacionarse entre sí y con otras bases de datos externas. Una de sus fuentes primarias de información es el Sistema de Información para el desarrollo de la Investigación en Atención Primaria (SIDIAP) y la Historia Clínica Compartida de Cataluña (HC3). El SIDIAP es un sistema de información que contiene datos de la historia clínica informatizada de Cataluña (Instituto Catalán de Salud) así como de fuentes complementarias para apoyar la investigación en atención primaria. Además, el SIDIAP potencia la investigación y la evaluación sanitaria, y contribuye a mejorar la gestión clínica mediante el conocimiento generado. La HC3 una base de datos sanitaria en la que ya participaban la práctica totalidad de los centros de salud catalanes en 2016 (CatSalut 2016: 9).

La red de la HC3 asegura la protección de datos mediante la LOPD antes mencionada, que establece una serie de derechos básicos conocidos como ARCO, el derecho de los ciudadanos al acceso, rectificación, cancelación y oposición (Solans Fenández et al. 2017: 1-18). La HC3 se estableció como una medida necesaria para modernizar los sistemas de salud y alcanzar interoperabilidad en y entre sistemas de salud, proyecto que ha sido ampliamente impulsado por la UE (eHealth Network 2015: 1-24). La HC3 se estableció en Cataluña sin haberse llevado a cabo debates abiertos o campañas que informaran sobre el análisis de riesgo-beneficio; tampoco se ofrecieron aclaraciones sobre el modelo elegido para almacenar y acceder a los datos en el contexto clínico y asistencial (Buisan 2003: 1-99).

El proyecto VISC+ precisaba avales éticos, por lo que se solicitó opinión al Comité de Bioética de Cataluña (CBC). En los términos en los que fue presentado, el "objetivo del proyecto es relacionar la información de salud que se genera en Cataluña de una manera totalmente anonimizada

y segura con el fin de impulsar y facilitar la investigación, la innovación y la evaluación en ciencias de la salud". El CBC identificó puntos importantes que el VISC+ necesitaba mejorar respecto a gobernanza, limitación de propósito, derechos ARCO y transparencia. Después de que estos cambios fueran asumidos, el VISC+ recibió el aval del CBC. El proyecto se consideró como "una oportunidad para mejorar la calidad y la sostenibilidad del sistema público de salud que requiere la contribución anónima y solidaria de los ciudadanos, que son contribuyentes y beneficiarios" (traducción de las autoras) (Comité de Bioética de Cataluña 2015: 5-35, Morlans et al. 2015: 1-21). Posteriormente el VISC+ fue aprobado discretamente por el gobierno al inicio de las vacaciones de Semana Santa, a pesar de que el valor que se le deseaba dar a los datos de salud de Cataluña incluía intenciones comerciales, las cuales estaban claramente ausentes de los objetivos para los que se crearon las bases de datos de salud que se pretendían utilizar.

Otro inconveniente que planteaba el VISC+ es la pretendida anonimización. Es pretendida pues la explotación a escala masiva permite reidentificar a las personas con parámetros mínimos como el sexo, la fecha de nacimiento o el código postal (Sweeney, 2000: 1-34). Por ello conviene no utilizar una terminología obsoleta, que induce a confusión, además de generar una falsa seguridad en quienes confían en el sistema y en el anonimato como válvula de seguridad definitiva.

A pesar de la aparente solidez que le daba el respaldo del gobierno, el proyecto fue objeto de críticas, entre las que se incluye el estudio realizado por el Observatorio de Bioética y Derecho de la Universidad de Barcelona, que publicó recomendaciones que posteriormente fueron incluidas en la reformulación del proyecto por parte del gobierno catalán (Llàcer et al. 2015: 29-49). Además, plataformas como Marea Blanca para la defensa de la Salud Pública de Cataluña, se expresaron en contra del proyecto. Se generó así suficiente presión sobre el gobierno como para llegar a invalidar la decisión legislativa que aprobó el VISC+. De hecho, ya en 2014 el Parlamento Catalán había pedido frenar la licitación del VISC+ hasta que se realizara un proceso participativo (Moció 150/X), y en 2016 solicitó detener definitivamente el proyecto para transformarlo en una iniciativa pública en la que los datos de salud de los catalanes no se pudiesen vender a compañías privadas ni ser usados para fines comerciales (Moció 49/XI).

La retractación del VISC+ demuestra que iniciativas que manejan datos personales sensibles, necesitan de una extendida participación pública, acompañada de las voces y debates de expertos desde enfoques interdisciplinares, que abarquen los ámbitos social, económico, ético, jurídico,

técnico, científico, y otros. De esta forma es posible identificar riesgos y beneficios y tomar decisiones informadas respecto de este tipo de proyectos.

Poco después del abandono del VISC+, se presentó la propuesta PADRIS. El visible cambio de nombre pone en evidencia que el rechazo que suscitó el VISC+ no se podía remediar con simples modificaciones, sino que un cambio radical era necesario. El proyecto se justificó de manera similar al VISC+, haciendo referencia a la necesidad de mejorar el sistema de salud y a promover la investigación biomédica. Actualmente, el PADRIS atraviesa por la fase de concepción y definición (Generalitat de Catalunya 2017: 1-37).

Un punto crítico para el PADRIS ha sido determinar la función de aquellos terceros que desde la iniciativa privada pueden participar en la explotación de datos. AQuAS ha declarado que solo los centros CERCA (Centros de Investigación de Cataluña), que son instituciones financiadas por la Dirección General de Investigación de la Generalitat de Cataluña, serán los que exploten los datos de salud de los usuarios del sistema público sanitario catalán a escala masiva. Sin embargo, no se ha explicado que la investigación que se efectúa en esos centros no es siempre puramente pública pues participa activamente el sector privado y por todos es conocida la apuesta político-económica por generar parternariados público-privados en investigación (véase la Ley 14/2007, de 3 de julio, de Investigación Biomédica). Tampoco se ha aclarado que a menudo se necesita la intervención de agentes de distinta índole para el tratamiento de los datos. No todos estos agentes están vinculados al deber de confidencialidad, como sí lo están los profesionales sanitarios, y pueden tener intereses muy diferentes en los distintos conjuntos de datos. Ante esta situación, no se ha aclarado qué hacer con los casos en los que existan investigaciones apoyadas por capital privado o con colaboraciones con instituciones privadas (Generalitat de Catalunya 2017: 1:37). Esta situación genera enorme confusión acerca de las dinámicas que rigen la investigación en ese contexto, pues, como ya se ha dicho, no es ni puramente pública ni privada. Es necesario que el PADRIS aclare su posición en relación con este punto, pues de lo contrario la puerta a la posible mercantilización de datos personales sigue abierta.

Otra debilidad por superar por el PADRIS, es asegurar un proceso de inclusión popular, el cual fue claramente requerido por el Parlamento. AQuAS organizó tres actividades de consulta popular para orientar la propuesta del PADRIS. Dos de ellas se realizaron en Barcelona y otra fue mediante un formulario electrónico (Generalitat de Catalunya 2017: 1-37).

Estas actividades fueron un buen comienzo, pero insuficientes como única medida para promover el debate social que demanda un proyecto de la magnitud del PADRIS. Hubiera sido deseable una estrategia más inclusiva y estable en el tiempo, de tal forma que permitiera desarrollar mecanismos de gobernanza a lo largo de la vida de los proyectos que eventualmente accedieran al PADRIS. Parte de esta estrategia podría haber incluido a los ciudadanos para, por ejemplo, decidir la priorización de la agenda de investigación.

El proceso de información y discusión pública no debe ser ni menospreciado, ni subestimado; tampoco debe ser rebajado a meros formalismos para seguir avanzando en propósitos políticos que, por muy lícitos que sean, no cuentan con la confianza de la ciudadanía, ni con su implicación. Es necesario recordar que los ciudadanos son los titulares de la información y los proveedores de los que depende la innovación e investigación en salud. Resulta todavía más grave que tampoco se hayan discutido los proyectos que se aprobaron en la ventana en el que el VISC+ estuvo activo. Esta era una valiosa oportunidad de análisis, para debatir las ventajas e inconvenientes del proyecto, riesgos inherentes y para determinar si el modelo de consentimiento presunto establecido, es el más adecuado para el PADRIS. En el caso de que el consentimiento presunto se aceptara, es necesario discutir la implementación de sólidos mecanismos de gobernanza, transparencia y rendición de cuentas que permitan un control sobre el uso del dato y asegurar que los objetivos que se persiguen y los resultados alcanzados puedan ser beneficiosos para la población. También hubiera sido conveniente revisar anteriores proyectos como el caso islandés de cesión de datos médicos y genéticos de la población a una empresa privada (DeCode Genetics) mediante una concesión administrativa previa aprobación parlamentaria (Winickoff 2006: 80-105).

El PADRIS todavía debe perfilar adecuadamente el proceso de salida de la base de datos, para que la petición de retirada sea simple y accesible, tratada con las máximas garantías de confidencialidad y sin necesidad de justificación alguna. Es inaceptable que el mecanismo para darse de baja del sistema se efectúe por correo electrónico o solicitar las razones de la oposición al titular de los datos. La protección de la intimidad y la confidencialidad de los datos personales de salud no queda garantizada en estas condiciones, ni tampoco la autonomía en el ámbito sanitario. Se plantea así cómo proteger estos datos tan preciados de usos no deseados o ilícitos, los cuales pueden tener tremendas implicaciones para los proyectos de vida de los titulares de los datos puesto que la información de salud, incluida la genética, dice muchísimo sobre nosotros y nuestras familias. Por lo tanto, si no somos conscientes y no controlamos su uso,

nuestra información personal puede ser utilizada contra nuestros propios intereses, y por ejemplo, abrir la puerta a posibles discriminaciones en el ámbito laboral o de los seguros de vida. No se trata únicamente de evitar los usos comerciales de los datos públicos de salud, se trata de situar en primera línea los valores y derechos fundamentales de nuestra sociedad, los cuales deben ser protegidos y promovidos por quienes manejan la información. El ciudadano no debería cargar con toda la responsabilidad, precisamente porque no cuenta con la visión panorámica que compete a la administración pública ni tampoco tiene la obligación de velar por los intereses colectivos. Además, es evidente la gran asimetría que existe entre el nivel de información que poseen los titulares de los datos y aquellos operadores de las bases de datos donde se almacena esa información para ser explotada, por ejemplo a escala masiva (Pasquale 2015: 1-320).

Los proyectos VISC+ y PADRIS nos enseñan que la protección de la dignidad de la persona a través de la protección de los datos personales de salud, debe guiar la legislación y cualquier iniciativa política que pretenda explotar tan preciada materia prima. También nos alerta sobre el peligro de priorizar otros intereses en contextos de recursos escasos y especialmente de crisis económica, puesto que el proyecto el VISC+ se concibió también como una oportunidad para salir de una coyuntura económica muy desfavorable. No hace falta abundar sobre decisiones que tomadas por motivo de la crisis económica global, han traído consigo efectos locales devastadores.

Para establecer las condiciones de gobernanza de iniciativas que utilizan datos personales de salud, de manera que se logre un uso responsable y respetuoso, se necesita tomar en cuenta el impacto social e individual. Es necesario implementar sistemas organizados de debate social, en un enfoque que llamamos bioética en acción. Este tipo de actividades son clave para fomentar la participación pública en los marcos de gobernanza y generar más confianza para poder avanzar hacia sólidos sistemas de consentimiento presunto y de responsabilidad compartida referente a la gobernanza del dato (Nuffield Council on Bioethics 2015: 1-225).

El recurso a los comités de ética de la investigación como únicos evaluadores y garantes del sistema puede ser perverso e ineficaz, ya que puede dar falsas seguridades a investigadores y titulares de la información y afectar negativamente el progreso social. La AQuAS debería establecer bajo el paraguas del proyecto PADRIS los requisitos específicos para la evaluación de proyectos de investigación que utilicen analítica de datos masivos relativos a la salud. El proyecto PADRIS, como hizo el VISC+ en su momento, confiaba en exceso en la función de estos comités. El mayor

problema es que, en estos momentos, esos comités no están preparados para afrontar los retos que plantea el Big Data en el ámbito de la investigación en salud, puesto que funcionan todavía con dinámicas propias de la investigación del siglo XX en la que la anonimización era posible (de Lecuona 2017: 267-295). No es objeto de este trabajo analizar los retos y las oportunidades para el cambio de estas instancias interdisciplinares. Sí conviene apuntar que es necesario que se produzcan cambios en la composición de los comités para integrar científicos de datos que contribuyan a una adecuada evaluación de los aspectos técnico-científicos. Los científicos de datos son de especial importancia porque muchos de los problemas que presentan las investigaciones de Big Data son debilidades técnicas y porque el análisis ético dependerá de esa evaluación. Desde luego no se puede olvidar que se requiere que todos los miembros del comité tengan una formación interdisciplinaria, actualizada y continua. En este momento específico, es de particular importancia ponerse al día con las nuevas dinámicas establecidas por el Reglamento General de Protección de Datos.

En resumen, el acceso a los datos contenidos en el PADRIS debería guiarse por los principios de necesidad, proporcionalidad, equidad, minimización de datos, propósito limitado, consentimiento informado y transparencia. Puesto que esa evaluación está en manos de los comités de ética de la investigación acreditados, estos deben de estar preparados. Estos comités deberán revisar su composición y desarrollar protocolos de actuación y de evaluación para evitar entre otras cuestiones, la mercantilización de los datos personales de salud. Por ejemplo, deben estar preparados para identificar posibles mercados de datos disfrazados de investigación. Además, estos organismos deben velar por proteger la intimidad y la autonomía de las personas en el marco de proyectos de investigación. Los intereses de los participantes deben anteponerse a los fines que persiguen los proyectos, por lo que es necesario evaluar cuidadosamente las garantías que les son dadas.

IV. CONCLUSIONES Y PROPUESTAS

Hasta hace unas décadas, el sistema económico estaba basado en artículos tangibles o servicios que eran fáciles de controlar. Actualmente, la economía basada en el conocimiento ha pasado a organizarse alrededor de los datos y no de los procesos, como lo hacía anteriormente. Los datos digitales son fácilmente publicados, compartidos, copiados, transferidos, analizados, formateados, editados, actualizados y borrados. La información personal se ha convertido en el nuevo petróleo que puede ser ex-

plotado y monetizado con distintos intereses y en diferentes ámbitos. La datificación de la sociedad digital nos obliga a reflexionar sobre qué reglas del juego son las más adecuadas para proteger la dignidad y la intimidad de la persona, y especialmente su libertad para tomar decisiones. Proteger los datos personales, incluidos los de salud, en estos procesos de investigación e innovación, es proteger la dignidad de las personas. Se trata de evitar que las personas sean deshumanizadas, convertidas en conjuntos de datos que son de interés para múltiples actores. Es precisamente esa deshumanización la que puede dar paso a convertir en bienes con los que comerciar, la identidad individual y colectiva, y la intimidad propia y la de las generaciones futuras.

La economía digital que ha sido promovida por la UE implica desarrollar iniciativas y modelos de negocio que utilizan datos personales relativos a la salud. Los sectores público y privado, con el apoyo de los gobiernos, han centrado sus esfuerzos en proteger la propiedad de los datos que almacenan, y de los productos y servicios derivados, todo esto en nombre de la innovación y la competitividad, reduciendo a objeto al titular de los conjuntos de datos. El esfuerzo precipitado por recuperar las economías y hacerlas más competitivas, no ha propiciado estudios de riesgo-beneficio y de las consecuencias sociales e individuales derivadas del uso de la información personal. En los casos en los que este tipo de estudios ha sido realizado, las legislaciones nacionales no han respondido de forma ágil. Por ejemplo, en algunos casos los estados han recurrido al uso de las leyes generales de protección de datos ya establecidas para gobernar los datos relativos a la salud. Estas legislaciones no son siempre suficientes en los nuevos contextos tecnológicos y mercantiles actuales. Muy especialmente cuando se trata de información relacionada con la salud, por su naturaleza altamente sensible, la autonomía individual no puede servir de excusa para justificar el uso no reglamentado de datos personales.

El Reglamento General de Protección de Datos da un giro hacia el empoderamiento del ciudadano frente a los intereses económicos, un cambio radical en sociedades de mercado como las nuestras, en donde las dinámicas de empresa se tienden a anteponer sobre otros intereses. Este es un cambio que puede aportar beneficios porque retorna el control a los titulares de los datos, para por ejemplo, en el caso de investigación biomédica, priorizar los objetivos de investigación de acuerdo a los intereses y necesidades de los participantes. Se trata de un auténtico reto social que exige una responsabilidad compartida en materia de salud entre los estados y los distintos agentes involucrados, lo cual incluye los sectores público y privado, los titulares de los datos y quienes dan uso a las bases de datos de información personal.

La investigación científica es el principal acicate para el desarrollo de los estados en términos de conocimiento, terapias e intervenciones beneficiosas para los ciudadanos. Sin embargo, el derecho a la libertad de investigación debe ejercerse en condiciones de seguridad y con las más altas garantías de confidencialidad en cuanto a los datos personales de salud. Conviene entonces plantearse que si terceros ajenos al ámbito investigador en salud acceden y participan en la explotación de datos personales de salud a escala masiva, se les debe exigir las mismas garantías de confidencialidad que a los investigadores en salud. Asimismo se deben establecer las medidas necesarias para que esas garantías sean efectivas, condiciones técnicas a articular para que se de una efectiva protección de los derechos de los implicados.

Proyectos como el VISC+ y el PADRIS deben ser objeto de estudio porque en información relativa a la salud, los ciudadanos están preparados para participar asumiendo ciertos riesgos siempre que se garantice que su información no es objeto de lucro. Entre estos riesgos se sitúa la posible re-identificación de personas a través de los conjuntos de datos. Así, respecto al anonimato de los datos personales que hasta ahora garantizaba la confidencialidad, se ha generado suficiente evidencia para demostrar que la anonimización ya no es posible. Es apropiado dejar de utilizar conceptos obsoletos que aportan falsas seguridades en el nuevo paradigma datificado, no permitan comprender la realidad en la que estamos inmersos, oscurezcan la identificación de problemas y entorpezcan aportar soluciones.

El entusiasmo tecnológico que caracteriza a nuestra época no debe primar sobre los intereses del individuo, especialmente por la asimetría que existe entre los potenciales participantes y los que explotan sus datos personales. Tampoco conviene someter a la lógica del mercado bienes públicos como son los datos de salud para convertirlos en mercancías. Lograr un uso responsable y respetuoso de los datos personales de salud y una adecuada explotación a escala masiva significa apostar por mecanismos de gobernanza y una responsabilidad social compartida. Estos no sólo dependen de la voluntad del estado y del impulso de la iniciativa privada o público-privada, sino que el ciudadano debe ser parte central, no un mero espectador. La explotación de datos de salud y de carácter sociodemográfico no puede guiarse por criterios mercantiles ni debe ceder los principios de solidaridad, transparencia y rendición de cuentas. Esta posición está en línea con lo propuesto por el Reglamento General de Protección de Datos. La comercialización y la privatización de los recursos de la sociedad no debiera permitirse. Tampoco conviene obsesionarse con el requisito del consentimiento informado como si fuera la única solución.

La concepción de la persona y el valor que le damos a la intimidad en la sociedad digital, subyacen en este análisis. También se demuestra que en proyectos donde se explota a escala masiva información personal, incluidos datos de salud, hay una necesidad imperante de incorporar la reflexión ética desde el inicio y de adoptar mecanismos que permitan la gobernanza y el control de los datos personales. No se trata de meras formalidades que queden en papel mojado. Tampoco resulta útil castigar conductas, porque el daño que puede provocarse a nivel de derechos fundamentales es irreparable y no hay indemnización que solucione la excesiva exposición de la tan preciada vida privada y familiar. La reputación del sistema de ciencia y tecnología está en juego. También están en jaque valores fundamentales como la libertad y el libre desarrollo de la personalidad, sobre los que se asientan las sociedades democráticas.

El análisis que se aquí se efectúa muestra la necesidad de incorporar la reflexión ética y los impactos individuales y sociales desde el diseño de los protocolos de investigación y proyectos que utilicen datos de salud. La investigación e innovación responsable que propugna la Unión Europea solo puede hacerse realidad si la investigación y la innovación en salud se efectúan integrando los intereses de los afectados y mecanismos de gobernanza eficaces que permitan un adecuado control, lo que generaría la necesaria confianza en el sistema. Asimismo, las iniciativas de datos masivos deben desplegar medidas técnicas y organizativas que permitan una adecuada gestión del dato, que incluye el respeto por el derecho a la intimidad y el tratamiento confidencial. Involucrar al público en la definición de estos proyectos es clave, de manera que se asegure la protección de sus intereses y de valores tan importantes como la intimidad. Más aún porque los ciudadanos son titulares, proveedores y potenciales beneficiarios o consumidores de la materia prima más preciada, la información de carácter personal y en particular los datos relativos a la salud de cada uno de nosotros.

V. REFERENCIAS

Buisan, L. (2003): La confidencialitat en l'assistència sanitària. Del secret mèdic a la història clínica compartida a Catalunya. Barcelona, Publicacions i Edicions de la Universidad de Barcelona.

Casado, M. et al. (2016): Declaración sobre integridad científica en investigación e innovación responsable. Observatorio de Bioética y Derecho, UNESCO. Publicacions i Edicions de la Universidad de Barcelona.

Casanovas, P. et al. (2017): "Regulation of Big Data: Perspectives on strategy, policy, law and privacy". Health Technology, 7.

Casino, G. (2017): "Sobre el uso de datos médicos en investigación y otros fines menos altruistas". Escepticemia, 26 Septiembre, 2017. Disponible en: *http://www.esteve.org/en/escepticemia-35/* (acceso: febrero 2018).

CatSalut. (2016): Memòria 2015. Servei Català de la Salut. Generalitat de Catalunya, Departament de Salut.

Comisión de las Comunidades Europeas. (2004): La salud electrónica – hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. Bruselas.

Comité de Bioética de Cataluña. (2015): Memòria Any 2015. Disponible en: *http://comitebioetica.cat/memoria-del-comite-de-bioetica-de-catalunya/* (acceso: febrero 2018).

De Lecuona, I. (2017): "La tendencia a la mercantilización de partes del cuerpo humano y de la intimidad en investigación con muestras biológicas y datos (pequeños y masivos)", en M. Casado, coord., *De la solidaridad al mercado. El cuerpo humano y el comercio biotecnológico*. Barcelona, Publicacions i Edicions de la Universidad de Barcelona: 267-295.

EGE. (2014): Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Group on Ethics in Science and New Technologies. European Commission.

eHealth Network. (2015): Refined eHealth European Interoperability Framework. Brussels.

ENISA. (2015): Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics. European Union Agency for Network and Information Security.

European Commission. (2017): Science with and for Society. Horizon 2020, Work Programme 2018-2020. European Commission Decision C(2017)7124 of 27 October 2017.

Gandomi, A. y Haider, M. (2015): "Beyond the hype: Big data concepts, methods, and analytics". International Journal of Information Management, 35.

Generalitat de Catalunya. (2017): Programa públic d'analítica de dades

per a la recerca i la innovació en saluta Catalunya – PADRIS –. Agència de Qualitat i Avaluació Sanitàries de Catalunya (AQuAS). Barcelona.

Gottweis, H. et al. (2012). Biobanks for Europe. A challenge for governance. Luxembourg, Publications Office of the European Union.

Llàcer, M. R. et al. (2015): Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública. Observatorio de Bioética y Derecho, UNESCO. Publicacions i Edicions de la Universidad de Barcelona.

Mantelero, A. y Vaciago, G. (2015): "Data protection in a big data society. Ideas for a future regulation". Digital Investigation, 15.

Margolis, R. et al. (2014): "The National Institutes of Health's Big Data to Knowledge (BD2K) initiative: capitalizing on biomedical big data". Journal of the American Medical Informatics Association, 21(6).

Morlans, M. et al. (2015): Principis Ètics i Directrius per a la Reutilització de la Informació del Sistema de Salut Català en la Recerca, la Innovació i l'Avaluació. Grup de treball del Comitè de Bioètica de Catalunya. Generalitat de Catalunya. Barcelona.

Nuffield Council on Bioethics. (2015): The collection, linking and use of data in biomedical research and health care: ethical issues. Medical Research Council, the Nuffield Foundation, and the Wellcome Trust.

Pasquale, F. (2015): The Black Box Society. The Secret Algorithms That Control Money and Information. England, Harvard University Press.

Rees, C. y Heywood, D. (2014): "The 'right to be forgotten' or the 'principle that has been remembered'". Computer Law & Security Review, 30(5).

Solans Fenández, O. et al. (2017): "Shared Medical Record, Personal Health Folder and Health and Social Integrated Care in Catalonia: ICT Services for Integrated Care". New Perspectives in Medical Records. TELe-Health book series.

Sweeney, L. (2000): Simple Demographics Often Identify People Uniquely. DataPrivacy Working Paper 3. Pittsburgh, Carnegie Mellon University.

Winickoff, D. E. (2006): "Genome and Nation. Iceland's Health Sector Database and its Legacy". Innovations. Technology, Governance, Globalization. MIT Press.