

**UNA REFLEXIÓN DESDE LA TEORÍA
DE LOS DERECHOS
FUNDAMENTALES SOBRE EL USO
SECUNDARIO DE LOS DATOS DE
SALUD EN EL MARCO DEL BIG DATA**

FEDERICO DE MONTALVO JÄÄSKELÄINEN

SUMARIO

I. Introducción. II. Despejando algunos mitos: ¿conservará el ser humano un papel esencial en la lucha contra las enfermedades en los tiempos del Big Data? III. El impacto de las oportunidades del Big Data en el conflicto entre derechos individuales e intereses colectivos. IV. La necesaria superación del paradigma Helsinki en el uso secundario de los datos de salud con salvaguarda de los derechos de las personas. V. ¿Ha optado la nueva Ley Orgánica por este nuevo paradigma? VI. Conclusiones.

Fecha recepción: 30.04.2019
Fecha aceptación: 19.09.2019

UNA REFLEXIÓN DESDE LA TEORÍA DE LOS DERECHOS FUNDAMENTALES SOBRE EL USO SECUNDARIO DE LOS DATOS DE SALUD EN EL MARCO DEL BIG DATA

FEDERICO DE MONTALVO JÄÄSKELÄINEN¹

Profesor propio agregado, Derecho Constitucional, UPCOmillas (ICADE)
Presidente del Comité de Bioética de España y miembro del IBC (UNESCO)

I. INTRODUCCIÓN

El Big Data ofrece en general y, especialmente, en el ámbito de la investigación en salud, muchas alternativas y oportunidades². La explotación masiva de los datos de salud tradicionales e, incluso, su interrelación con los no tradicionales, va a permitir avanzar en la lucha contra las enfermedades y a favor de la prevención y predicción en unos términos que seguramente no van a encontrar parangón en la Historia de la Medicina y de la humanidad. Los resultados derivados de la explotación de datos que hasta hace pocos años se tardaban décadas en obtener ahora pueden conseguirse en meses, incluso, días, y ello, además, a un precio muy asequible. Los algoritmos van a permitir comparar un ingente número de procesos asistenciales ofreciendo unas conclusiones que permitirán conocer con mayor precisión, por volumen, cuáles son los mejores tratamientos para cada una de las enfermedades y sus diagnósticos. El Big Data permite avanzar en el campo de la medicina basada en la evidencia, entendida

¹ Profesor propio agregado, Derecho Constitucional, UPCOmillas (ICADE). Facultad de Derecho. C/ Alberto Aguilera 23 - 28015 Madrid. Email: fmontalvo@icade.comillas.edu

² Señala la Agencia Española de Protección de Datos en el Código de Buenas Prácticas en Protección de Datos para Proyectos Big Data elaborado conjuntamente con el ISMS Fórum Spain que “Existen múltiples definiciones de Big Data de diversas fuentes. En síntesis, con dicho término se hace referencia al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo. Al Big Data frecuentemente se le caracteriza mediante tres ‘v’: Volumen, Variedad y Velocidad”.

ésta como el proceso de revisión sistemática, evaluación y utilización de los resultados de investigación clínica para impulsar una prestación de atención sanitaria óptima para el paciente. El Big Data evita, además, el problema que plantean muchos ensayos clínicos que bien seleccionan pacientes que muchas veces no suelen compartir el perfil de la media poblacional que padece una determinada enfermedad que se está tratando de investigar o bien no permiten valorar correctamente la adherencia farmacológica, ya que mientras la mayor parte de los pacientes que siguen un ensayo clínico cumplen fielmente las pautas de tratamiento prescritas, éstas no son condiciones reales de comportamiento en la vida real. A este respecto, la mitad de la población con pluripatología no sigue la suficiente adherencia al tratamiento y, por tanto, los ensayos clínicos se realizan en condiciones ideales que difieren sustancialmente de la práctica habitual. Y aquí es precisamente donde Big Data puede hacer una aportación fundamental a la práctica médica ya que, por su propia idiosincrasia, Big Data no hace una selección de pacientes a los que sitúa en unas condiciones artificiales ideales, sino que se consideran todos los enfermos y sus particularidades reales, es decir, sus condiciones reales de salud y sus comportamientos reales respecto a su estilo de vida, su gestión de la enfermedad y su adherencia a los tratamientos³.

Como apunta el Consejo Nacional de Ética de Alemania (*Deutscher Ethikrat*), en la investigación biomédica, el análisis de grandes volúmenes de datos relevantes para la salud facilitará una mejor comprensión de importantes procesos científicos y de sus conexiones. Entre las aplicaciones más importantes, en lo que a los datos se refiere, se encuentran los procedimientos modernos de obtención de imágenes y de biología molecular, como los empleados en los llamados ómicos (por ejemplo, genómica o proteómica)⁴. Esta misma idea aparece reflejada en el propio Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, el Reglamento UE), señalando su Considerando 157, de manera muy gráfica, que “Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la

³ SAN SEGUNDO ENCINAR, J.M., *Big Data en salud digital. Informe de resultados*, Red.es, Madrid, 2017, pp. 42 y 43.

⁴ German Ethics Council, *Big Data and health. Data sovereignty as the shaping informational freedom*, Opinion, Executive Summary and Recommendations, Berlín, 2018, p. 9.

eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros”.

El Big Data abre, pues, una nueva era para mejorar la prestación de servicios de salud, ofreciéndose nuevas oportunidades, tanto para el diagnóstico y el tratamiento de multitud de problemas de salud y la capacidad, aún incipiente, de proporcionar nuevos servicios personalizados mediante su detección en tiempo real y la adecuación de los tratamientos desde una perspectiva hipersegmentada⁵.

La explotación masiva de datos permitirá obtener unos resultados con un valor diferente de los mismos resultados analizados singularmente. Como señala muy gráficamente y con excepcional metáfora la profesora Vanesa Morente, el uso de la herramienta técnica del Big Data proporciona una mirada más profunda, una mirada de calado, que va más allá de lo evidente, como sucede en los cuadros de Giuseppe Arcimboldo, donde aparece un rostro o un perfil humano si observamos el bodegón en su conjunto y no como un mero conglomerado de frutas y hortalizas individuales y diferenciadas. La finalidad primera del Big Data supone por tanto una mirada que no solo ve, sino que descubre, se trata de una mirada transformadora que obtiene un valor donde solo hay información en bruto, sin pulir⁶. Y ello, en el ámbito de la Medicina y de la salud en general tiene un valor cualificado, dado que se trata de un campo de investigación en el que el método cuantitativo, a diferencia de otros, ostenta un valor especialmente relevante, pese a que, también es cierto que, como habitualmente se dice, no existen enfermedades sino enfermos. En todo caso, para el avance en la mejora de los tratamientos médicos, la oportunidad de correlacionar millones de procesos asistenciales es irrenunciable, sin olvidar que dichos resultados deben ser después contextualizados e individualizados.

Por otro lado, si atendemos a que la salud, según la definición ofrecida por la Organización Mundial de la Salud hace ya unos años, es “*un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades*”, ello refuerza un enfoque holístico de la salud que desdibuja la línea entre la salud en el campo médico y el estilo de vida. Y así, el Big Data ofrece la oportunidad técnica de apoyar una visión tan holística, al no limitar la explotación de datos a los estricta o tradicionalmente asistenciales, como son los contenidos en las historias clínicas, pudiendo incorporar también datos sobre estilos y hábitos de vida e, incluso, el entorno.

Por ello, puede afirmarse que el dato clínico deja de ser un mero recordatorio del proceso asistencial y se convierte en principal fuente de conocimiento y avance en la Medicina y Biología. El dato de salud puede ser considerado ya el verdadero *tesoro* de la investigación biomédica frente al *tesoro* que constituían en la pasada década las muestras biológicas. El dato no tiene ahora interés en el estricto ámbito de la asisten-

⁵ SAN SEGUNDO ENCINAR, J.M., *Big Data en salud digital. Informe de resultados*, op. cit., p. 5.

⁶ MORENTE PARRA, V., “Big data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales”, *Revista Derechos y Libertades*, número 41, época II, julio 2019 (en prensa), p. 2.

cia sanitaria o en el marco concreto de un ensayo clínico, como soporte documental de los hechos más relevantes de la asistencia prestada, de las decisiones adoptadas durante la misma o de los diagnósticos y conclusiones alcanzadas, sino también para su explotación secundaria, es decir, al margen de los fines principales para los que fue el dato facilitado. El paciente cede sus datos para un fin concreto y tales datos cobran interés para fines secundarios, su uso secundario, a través de las herramientas que ofrece el Big Data.

Pero es que, además, las oportunidades que ofrece el uso masivo de datos de salud cobran incluso mayor relevancia en sistemas de salud como el español que se caracteriza tanto por su gestión y prestación esencialmente públicas (modelo basado en la fórmula Beveridge) como por el reciente proceso de digitalización de los documentos e historias clínicas, lo que nos permite disponer de millones de datos en una única base o, al menos, en bases que son fáciles de interrelacionar. No nos estamos refiriendo, pues, exclusivamente a los datos que fueron obtenidos de un proyecto de investigación en seres humanos o ensayo clínico, sino al uso secundario de los datos puramente asistenciales cuyo número y, posiblemente, valor es superior a los primeros.

Pese a dicha relevancia del Big Data en general y del Big Data en salud en particular, no existen regulaciones específicas sobre el fenómeno en los marcos legales nacionales e internacionales, como señalara el International Bioethics Committee (IBC) de la UNESCO en su Informe sobre Big Data y salud de 2017, parcialmente redactado, por cierto, en España durante su sesión de trabajo desarrollada en la sede de la Universidad Pontificia Comillas. Sin embargo, añade el mismo IBC, que ello no obsta para que sí exista un marco regulatorio completo para la protección de datos personales en muchas jurisdicciones, principalmente en Europa, del que pueden ser aplicables muchas reglas en el área de Big Data, aunque es una nueva realidad que pudiera exigir soluciones más específicas⁷. Por lo tanto, no hay una falta de regulación general, dado que varios de los conflictos y dilemas legales están jurídicamente cubiertos por la regulación de la protección de datos, sino de disposiciones específicas y quizás de nuevos principios que sean adecuados para regular las nuevas características del Big Data.

Este nuevo panorama se nos ofrece, además, en momentos en los que surgen nuevas incertidumbres sobre cómo se desenvuelven muchas enfermedades que, aunque sean muy antiguas, como el cáncer, ofrecen nuevos paradigmas acerca del desarrollo celular y de proteínas, y, al mismo tiempo, nuevas enfermedades, muchas de ellas huérfanas aún de tratamiento. Las interacciones entre los factores determinantes de muchas enfermedades son extremadamente complejas. El Big Data permite a los investigadores integrar y agregar información diversa de múltiples fuentes⁸. La oportunidad es, pues, indiscutible desde la perspectiva de la protección de la vida, lo que

⁷ IBC, Report on Big Data and Health, UNESCO, París, 2017, p. 4. Puede accederse a dicho Informe a través de la página web del IBC, en <https://unesdoc.unesco.org/ark:/48223/pf0000248724>.

⁸ German Ethics Council, *Big Data and health. Data sovereignty as the shaping informational freedom*, cit., p. 10.

obliga, en palabras de Ricard Martínez, a renunciar a un enfoque apriorístico en el que cualquier tratamiento de datos de salud es concebido negativamente⁹.

Junto a las oportunidades también aparecen los riesgos para los derechos de las personas. Pablo Lucas Murillo de la Cueva los resumía hace unos años en los siguientes términos: “Hay que advertir que el peligro potencial y real al que nos enfrentamos radica, por una parte, en el volumen de información, a menudo aparentemente irrelevante, que sobre nosotros se maneja. Por la otra, en la posibilidad cierta de obtener -mediante el tratamiento de esos datos- nuevos elementos informativos que nos afectan. En tercer lugar, en que tales procedimientos permiten lograr el conocimiento de aspectos de nuestra vida que, además de ser personales, merecen ya el calificativo de íntimos. Por último, existe el riesgo de que, a partir de ese cúmulo informativo, se elaboren o construyan perfiles de nuestra personalidad en función de los cuales se tomen decisiones sobre nuestros derechos y expectativas”¹⁰.

Por todo ello, el Consejo Nacional de Ética de Alemania señala que el Big Data representa un reto importante para el sistema legal y, en concreto, para el Derecho Constitucional¹¹. Sin embargo, estos riesgos siempre han estado presentes en relación con la información personal, más aún, en ámbitos como el sanitario en el que se trata de datos especialmente sensibles, pero las características del Big Data potencialmente los incrementarán¹². Y es que los riesgos no solo quedan circunscritos al ámbito del derecho a la intimidad, dado que la información sobre el estado de salud puede afectar a otros derechos e intereses como los del acceso al empleo, al crédito o al aseguramiento¹³.

II. DESPEJANDO ALGUNOS MITOS: ¿CONSERVARÁ EL SER HUMANO UN PAPEL ESENCIAL EN LA LUCHA CONTRA LAS ENFERMEDADES EN LOS TIEMPOS DEL BIG DATA?

Todo lo que hemos expuesto en la introducción no creemos que pueda interpretarse en clave de que las nuevas tecnologías y, entre ellas, el Big Data, la Inteligencia Artificial y la robótica vengán a suplir por completo el papel de los profesionales en el ámbito de las luchas contra las enfermedades. Esta transformación digital nos ofrece una doble conclusión que, en cierto modo, resulta paradójica: por un lado, es

⁹ MARTÍNEZ, R., “Big data, investigación en salud y protección de datos personales ¿Un falso debate?”, *Revista Valenciana d'Estudis Autonòmics*, núm. 62, año 2017, p. 236.

¹⁰ LUCAS MURILLO DE LA CUEVA, P., “La construcción del derecho a la autodeterminación informativa”, *Revista de Estudios Políticos*, núm. 104, abril-junio 1999, p. 38.

¹¹ German Ethics Council, *Big Data and health. Data sovereignty as the shaping informational freedom*, *cit.*, p. 14.

¹² CHAN, S., “Bioethics in the big data era: health care and beyond”, *Rev Bio y Der.*, vol. 41, año 2017, p. 10.

¹³ MARTÍNEZ, R., “Big data, investigación en salud y protección de datos personales ...”, *cit.*, p. 236.

innegable que la lucha contra muchas de las enfermedades pasa por la explotación masiva de datos. Sin embargo, por otro lado, cada vez nos convencemos más de que la tecnología nos ayuda, pero, en modo alguno, nos sustituye. La máquina puede completar el conocimiento humano, pero nunca suplirlo. No podemos hablar de una nueva época de máquinas, sino de seres humanos ayudados por máquinas en sus quehaceres. Como metafóricamente se ha señalado en relación con el Big Data, las estadísticas, las correlaciones masivas de datos, son como la farola para un borracho, más que luz ofrece apoyo¹⁴. Watson puede ser un útil compañero pero no creemos que el responsable único o último del proceso asistencial. La máquina lleva décadas en el ámbito sanitario y, singularmente, en el hospitalario y no ha sido nunca capaz de sustituir al profesional.

Un ejemplo paradigmático que nos aporta el Derecho en relación con este dilema entre máquina y conocimiento humano lo encontramos en el propio Reglamento UE, el cual ha dotado al acervo jurídico de un nuevo derecho que, junto a otro novedoso como es el derecho al olvido, deben ahora entenderse ya plenamente incorporados desde mayo de 2018 a los que tradicionalmente se han considerado incluidos dentro del artículo 18.4 de la Constitución que regula el denominado *habeas data*. Se trata del derecho de oposición a las decisiones adoptadas de manera meramente automatizada (art. 22 del Reglamento UE). Este nuevo derecho es recogido, como no podía ser de otro modo, también por la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante, la Ley Orgánica) que en su artículo 18 dispone que el “derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluidas la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE)”.

Aunque hemos tildado de novedoso el citado derecho de oposición, el mismo encuentra un precedente en la propia Ley Orgánica 15/1999, de 13 de diciembre, de la que es sucesora la actual Ley Orgánica 3/2018. Así, el artículo 13 de aquélla recogía ya el derecho a no verse sometido a una decisión con efectos jurídicos que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad, tenor literal que no se separa mucho del que se recoge en el artículo 22 del Reglamento UE, donde se dispone que todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. La novedad, pues, estaría en la extensión del reconocimiento del derecho que no se limitaría al tratamiento para la elaboración de perfiles.

Para la Agencia Española de Protección de Datos este derecho de oposición se proclama con la finalidad de garantizar que no seamos objeto de una decisión basada únicamente en el tratamiento de nuestros datos, incluida la elaboración de perfiles,

¹⁴ GIL, E., *Big Data, privacidad y protección de datos*, Boletín Oficial del Estado, Madrid, 2016, p. 41.

que produzca efectos jurídicos sobre nosotros o nos afecte significativamente de forma similar¹⁵. Es decir, podemos oponernos a las consecuencias que respecto de nuestros derechos o intereses pretendan derivarse del mero resultado de la explotación automatizada de datos sin que haya intervenido la razón humana a posteriori para verificar el resultado o solución propuesta por la máquina. La presencia del ojo clínico es para la Ley, pues, no sólo conveniente o recomendable, sino jurídicamente exigible, lo que da buena cuenta de lo increíble que se muestra el Reglamento respecto del paradigma tecnológico.

Este nuevo derecho es, como decíamos antes, un buen ejemplo de cómo la intuición, el llamado ojo clínico, seguirá ostentando un papel protagonista en este nuevo mundo. La máquina ayuda, pero nunca sustituye, mejora, pero no completa, el análisis y las conclusiones. Si bien el Big Data a través de la explotación masiva de datos hace posible localizar patrones que permitan realizar predicciones futuras, es, sin embargo, muy importante determinar cuál es la verdadera relación entre las variables para poder crear un modelo predictivo¹⁶. En su defecto, estaremos dando por patrón válido lo que es una mera casualidad, es decir, lo que se denomina causalidad espuria. La correlación puede ser tanto causal como casual y sólo la primera permite establecer un patrón predictivo. Y la determinación de ello, en los términos empleados por el propio Reglamento, parece que solamente puede establecerla con cierta confianza el cerebro humano, el llamado ojo clínico. Además, el problema se agravará a medida que avancemos en el análisis masivo de datos. Cuanto más “big” sean los “data” más expuestos estaremos a las falsas causalidades y más necesario será, por ende, el ojo clínico, véase, el factor humano.

Como señalara el Parlamento Europeo en 2017, la información revelada por los análisis de los macrodatos no ofrece una visión general objetiva e imparcial de ninguna materia y que es tan fiable como lo permitan los datos subyacentes; resalta que los análisis predictivos basados en macrodatos únicamente pueden ofrecer una probabilidad estadística y que, por ello, no pueden predecir siempre con precisión la conducta individual; resalta, por ello, que son fundamentales normas científicas y éticas estrictas para gestionar la recopilación de datos y valorar los resultados de esos análisis¹⁷.

Las causalidades espurias no son meras fantasías. La divertida página web de *spurious correlations* en www.tylervigen.com, nos muestra con gran humor cómo existe una correlación casi exacta entre el incremento de las personas que mueren ahogadas al caerse a una piscina con el número de películas en las que aparece el actor Nicolas Cage, entre el aumento del consumo per cápita de margarina con el de la tasa

¹⁵ Vid. página web de la Agencia Española de Protección de Datos; en concreto, <https://www.aepd.es/reglamento/derechos/index.html>.

¹⁶ GIL, E., *Big Data, privacidad ...*, *op. cit.*, pp. 32 y 33.

¹⁷ Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

de divorcios en el bello Estado de Maine o entre el consumo de queso mozzarella y el número de doctores en ingeniería premiados. Las palabras casualidad y causalidad son gramaticalmente casi exactas, pero en ningún modo sinónimas y eso lo sabemos bien, entre otros, los que nos dedicamos al mundo del Derecho, sobre todo, cuando tratamos de imputar responsabilidades legales.

Por ello, hay que evitar tanto despreciar o minusvalorar este nuevo panorama como considerarlo como un paradigma único y excluyente de la sabiduría humana, muchas veces más intuitiva que puramente racional, que conserva el ser humano. La que hace unos años Leon Kass tildara gráficamente de “sabiduría de la repugnancia” que más recientemente ha recuperado en cierto modo el último premio Princesa de Asturias de Ciencias sociales, Michael Sandel en su libro “Contra la perfección: la ética en la era de ingeniería genética”, no se desvanece ni ha perdido actualidad, por muy conservadora que pueda sonar¹⁸. No se trata de parar el avance de la ciencia y de la tecnología, sino tan sólo de situar en su justo lugar las ventajas que puede ofrecer.

III. EL IMPACTO DE LAS OPORTUNIDADES DEL BIG DATA EN EL CONFLICTO ENTRE DERECHOS INDIVIDUALES E INTERESES COLECTIVOS

Este nuevo panorama del uso masivo de datos en el ámbito de la salud y la lucha contra las enfermedades ofrece, salvado el valor del ojo clínico, muchas e importantes oportunidades, como ya apuntábamos al comienzo, aunque no exentas de riesgos, sobre todo, para la intimidad de las personas y la confidencialidad de los datos. Sin dejar de ser ello cierto, también lo es el que no podemos seguir operando en este ámbito con postulados o paradigmas propios de contextos distintos al actual en los que los riesgos superaban con creces a las ventajas. En el momento actual, la explotación masiva de datos genera ciertos riesgos en relación con los derechos de los individuos, pero, por otro lado, ofrece verdaderas posibilidades de curación o prevención también para la comunidad. Especialmente en el ámbito de la salud, el Big Data muestra como todos estamos relacionados. Compartimos genes, exposiciones medioambientales, hábitos y comportamientos. De este modo, los datos obtenidos de un grupo de individuos pueden predecir la enfermedad y los patrones de evolución de otros grupos de individuos¹⁹.

Como menciona el Consejo Nacional de Ética de Alemania, el modelo de protección de datos que ha estado vigente estas últimas décadas se fundamentaba en la necesidad de garantizar que los datos serían usados para el fin específico para el que

¹⁸ Vid. SANDEL, M., *Contra la perfección: la ética en la era de ingeniería genética*, Marbot, Madrid, 2016.

¹⁹ VAYENA, E., “Protecting health privacy in the world of Big Data”, en GLENN COHEN, I., FERNÁNDEZ LYNCH, H., VAYENA, E. y GASSER, U. (Edit.), *Big Data, Health Law and Bioethics*, Cambridge University Press, Cambridge, 2018, p. 158.

fueron cedidos, siendo fácil preestablecer cuáles eran dichos fines de antemano. Sin embargo, en la actualidad, en los tiempos del Big Data, los fines ya no son previsibles a priori²⁰. Si el paradigma y, por ende, la regla general pretendemos que siga siendo el de la cesión para un fin específico, podemos afirmar que las ventajas que ofrece el Big Data no serán aprovechadas lo que, sin duda, irá en detrimento de la lucha contra las enfermedades y de la efectiva protección de la vida y salud de las personas. El mismo Comité Internacional de Bioética (IBC) de la UNESCO señala que, en el área de la investigación con grandes datos, el uso secundario potencial de datos en el futuro no se puede predecir. También implica interrelaciones entre fuentes de datos múltiples y cambiantes, tanto médicas como no médicas, lo que llama a un nuevo modelo más apropiado²¹.

El mantener una posición que ignore el beneficio colectivo y prime no tanto la autonomía sino, incluso, el egoísmo y narcisismo tampoco parece aceptable, desde una perspectiva ético-legal. A este respecto Barbara J Evans señala que aquellos que invocan su derecho a no compartir sus datos en cualquier circunstancia, incluso cuando la salud de terceros puede depender de ellos, pueden estar difuminando la línea entre la autonomía individual y el narcisismo²².

El seguir asentando el modelo legal en el postulado de que la enfermedad y sus datos sólo les pertenecen a quienes sufren aquélla y no a los demás es, en nuestra opinión, ignorar la realidad. A este respecto, debemos recordar que la protección de datos no es, ni nunca ha sido, un fin en sí misma, sino que, más bien, sirve para proteger a la persona en el libre desarrollo de su personalidad, tanto en su esfera privada como en la esfera pública. Sin embargo, también es importante recordar que dicho libre desarrollo de la personalidad se produce en un entorno social de interrelaciones, de manera que tan plausible es la autonomía como la propia responsabilidad y la solidaridad.

El propio International Bioethics Committee (IBC) de la UNESCO en su Informe sobre el Big Data en salud de 2017, ya citado, señala que el Big Data puede considerarse ya un bien común de la humanidad (literalmente, “Big Data can be framed as a common good of humankind”). Los avances y las nuevas oportunidades proporcionadas por la ciencia y la tecnología podrían ayudar a reducir y no profundizar las desigualdades que impiden a muchos seres humanos disfrutar del más alto nivel posible de salud, tanto a nivel nacional como internacional²³. El dato de salud,

²⁰ German Ethics Council, *Big Data and health. Data sovereignty as the shaping informational freedom*, cit., p. 16.

²¹ IBC, Report on Big Data and Health, cit., p. 11. Puede accederse a dicho Informe a través de la página web del IBC, en <https://unesdoc.unesco.org/ark:/48223/pf0000248724>.

²² EVANS, B.J., “Big Data and individual responsibility”, en GLENN COHEN, I., FERNÁNDEZ LYNCH, H., VAYENA, E. y GASSER, U., (Edit.), *Big Data ...*, op. cit., p. 21.

²³ IBC, Report on Big Data and Health, cit., p. 15. Puede accederse a dicho Informe a través de la página web del IBC, en <https://unesdoc.unesco.org/ark:/48223/pf0000248724>.

en la etapa del Big Data, puede decirse que es ya un verdadero patrimonio de la humanidad, aunque ello se expresa en términos meramente metafóricos.

El conflicto de derechos cobra una nueva perspectiva desde el momento que la explotación masiva de mis datos puede salvar la vida de otros. No se trata de poner riesgo o sacrificar la intimidad y el derecho a la confidencialidad y protección de datos en pos de otros valores y derechos de no tal trascendencia constitucional e impacto en la dignidad del ser humano como aquéllos, sino de limitarlos en pos de la protección de la vida e integridad de terceros. Si el Big Data ofrece la oportunidad de conocer cuáles son los mejores tratamientos y, por tanto, cuál es la mejor oportunidad de superar la enfermedad para aquellos que la están sufriendo o que pueden desgraciadamente sufrirla en el futuro, ¿podemos seguir sosteniendo el paradigma de la protección de los datos como valor supremo? Parece que el Big Data no solo ha alterado sustancialmente la forma y método de investigación en Medicina, sino también la naturaleza de los derechos en conflicto y, como vamos a sostener aquí, su resolución.

En todo caso, el Instituto de Medicina de Estados Unidos acertadamente nos recuerda que el conflicto entre la esfera individual y colectiva en el ámbito de la investigación con datos en el ámbito de la salud es relativo, ya que tanto la dignidad que se protege con la privacidad tiene una dimensión colectiva, como que el propio avance de la Medicina lo tiene a nivel individual²⁴.

Ciertamente, el interés general no permite el sacrificio del derecho individual, en este caso, el derecho a la intimidad y a la protección de datos del sujeto cuyos datos pretenden ser usados en beneficio de la salud de terceros. Sin embargo, sí cabe una decisión ponderada en la que la limitación a tal derecho sea capaz de superar el test de proporcionalidad. Y en relación con dicho test, el subprincipio de proporcionalidad en sentido estricto puede quedar salvaguardado, una vez acreditada que la medida es idónea y necesaria, lo que no debe ofrecer mayores dificultades, a través de una medida que permita salvaguardar el núcleo esencial del derecho. Así, la nueva figura de la seudonimización creemos que es la fórmula que permite superar en el conflicto concreto la proporcionalidad.

Como señala Pablo Lucas Murillo de la Cueva, una cosa es el pragmatismo y la preocupación por la eficiencia y otra distinta la reducción de los niveles estrictamente jurídicos de tutela, ya que no es lo mismo perseguir el respeto a las normas que establecen los derechos de los afectados ante quienes pretenden servirse de sus datos personales por vías que promueven o estimulan en términos positivos su más amplio cumplimiento, que rebajar el contenido de esos derechos en sí mismos considerados²⁵. Se trata, pues, de buscar un equilibrio entre ambos intereses, el individual y el colectivo, que permita avanzar en la lucha contra las enfermedades sin verdadero detrimento de los derechos de los individuos.

²⁴ Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009, p. 1.

²⁵ LUCAS MURILLO DE LA CUEVA, P., "La protección de los datos de carácter personal en el horizonte de 2010", *Anuario de la Facultad de Derecho*, Universidad de Alcalá, núm. 2, año 2009, p. 138.

IV. LA NECESARIA SUPERACIÓN DEL *PARADIGMA HELSINKI* EN EL USO SECUNDARIO DE LOS DATOS DE SALUD CON SALVAGUARDA DE LOS DERECHOS DE LAS PERSONAS

Para Barbara J Evans, nuestro modelo legal se ha asentado en la fuerza del consentimiento informado como garantía de la intimidad del individuo. Sin embargo, este modelo responde a una realidad distinta de la que ahora se nos ofrece porque la investigación actual, a diferencia de aquella que diera lugar a los grandes documentos bioéticos vinculados a la investigación como fueron el Código Nuremberg o la Declaración de Helsinki, no pretende actuar sobre la integridad de las personas, sino sobre sus datos. No se toca a la persona sino a sus datos. No estamos enfrentando integridad física del individuo e interés colectivo, lo que difícilmente superaría el test de proporcionalidad, y, sobre todo, el límite de la dignidad como núcleo esencial del derecho, sino la intimidad. Se trata de un nuevo *informational research* que, ni ética ni legalmente, puede ser equiparado a los ensayos clínicos que pueden poner en riesgo la integridad del sujeto. En los entornos del Big Data, las normas tradicionales de consentimiento informado individual ya no pueden cumplir el objetivo principal para el que fueron diseñadas²⁶.

No podemos aplicar a la investigación a través del Big Data los principios y valores ético-legales que hemos desarrollado frente a la tradicional investigación en seres humanos, en la que los derechos expuestos eran los consagrados en el artículo 15 de la Constitución. Proponer sacrificar la vida o integridad del individuo en beneficio del interés colectivo, aunque el valor colectivo fuera precisamente la vida o integridad, es harto difícil que supere el test de proporcionalidad. Sin embargo, cuando el derecho a limitar frente a la salud de terceros son los derechos consagrados en el artículo 18 de la Constitución, el subprincipio de proporcionalidad en sentido estricto es más sencillo considerar que se ha respetado, más aún, cuando se han adoptado medidas para evitar que el sacrificio no se traduzca en la afectación del derecho, sino en el mero riesgo de serlo.

El denominado *paradigma Helsinki* hace referencia a los postulados bioéticos e incluso normativos promovidos tras los acontecimientos acaecidos en el ámbito de la investigación con seres humanos a finales de la primera mitad del siglo XX e, incluso, pocos años después. Así, debemos recordar, resumidamente, que si bien en el ámbito del denominado Derecho Sanitario se encuentran ya precedentes remotos en las sentencias dictadas por los Tribunales sobre la responsabilidad civil de los médicos, destacando como verdadero *seminal case* la dictada por el sefardí Cardozo en 1914

²⁶ EVANS, B.J., “Big Data and individual responsibility”, en GLENN COHEN, I., FERNÁNDEZ LYNCH, H., VAYENA, E. y GASSER, U. (Edit.), *Big Data ...*, *op. cit.*, pp. 26 y 27. Esta distinción ya fue establecida hace una década por el Instituto de Medicina de Estados Unidos, señalando que habría que distinguir entre “interventional research and research that is exclusively information based”. Vid. Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009, p. 3.

(Schloendorff v Society of New York Hospital), la Bioética y el Bioderecho se inauguraron como áreas específicas del conocimiento con ocasión de los execrables atentados a la dignidad y a los derechos humanos de cierta medicina de finales de la primera mitad del siglo XX e, incluso, de pocas décadas después (véanse, Willowbrook State School, Jewish Chronic Disease Hospital Of New York o Tuskegge Syphilis Study, como ejemplos tristemente paradigmáticos). La reflexión bioética y la biojurídica surgen como muros de contención o de prevención frente a los abusos que pueden cometerse en el ámbito de la investigación, expresando con la *contrafrase* erróneamente atribuida a Maquiavelo, o, al menos, con el significado peyorativo con el que habitualmente se usa, de que los fines no justifican los medios ni el interés colectivo el sacrificio de la dignidad del individuo.

Ambas, Bioética y Bioderecho, nacen como áreas del conocimiento con un fin fundacional: el desarrollo de garantías para la dignidad humana en el ámbito de la investigación con seres humanos. Y dichas garantías se recogieron en el Código Nuremberg, elaborado al amparo de los juicios contra los responsables del Nazismo y concretamente el juicio contra los médicos, y la Declaración de Helsinki que fue aprobada por Asociación Médica Mundial en 1964. En ambos se inaugura un modelo estricto de protección del interés individual, como reacción frente a los abusos de los que traen causa ambos textos.

Y éste, precisamente, es uno de los problemas a los que nos enfrentamos. El consentimiento informado, nacido esencialmente como garantía frente a las atrocidades cometidas a finales de la primera mitad del siglo XX, ha acabado por postular el principio de autonomía como el prevalente, obviando cuál es el contexto en el que se pretende que opere el mismo. Los problemas que la doctrina del consentimiento informado ha presentado en su evolución vienen motivados sustancialmente porque surge al amparo de la investigación médica con seres humanos, pretendiéndose implantar con la misma extensión y efectos en los demás ámbitos como serían el de la medicina asistencial ordinaria o el de la investigación con datos. Si bien un cumplimiento extraordinariamente riguroso del consentimiento informado cobra pleno sentido en una relación entre investigador y sujeto en la que aquél va a actuar sobre la vida e integridad física de éste y en la que individuo tiene que adoptar una decisión de tanto compromiso ético-legal como es la de participar o no en un proyecto de experimentación, cuyo beneficio individual, más allá del comunitario es incierto, en la relación clínica asistencial ordinaria o en la mera investigación con datos, tales exigencias no parecen tan necesarias.

Además, cabría preguntarse si este modelo normativo, basado esencialmente en el interés del individuo, responde también a los deseos de los ciudadanos. A este respecto, ya hay trabajos que muestran que los ciudadanos no mantienen una posición contraria a compartir los datos; antes al contrario, como señala Haug, los pacientes desean que sus datos se compartan rápidamente, especialmente para garantizar que otros pacientes conozcan los posibles efectos secundarios de los tratamientos. Y si bien es cierto que también desean mantener cierto control sobre cómo se comparten aqué-

llos, ello se produce especialmente cuando los fines que se persiguen por los estudios son esencialmente comerciales y no tanto cuando son los propios sistemas públicos de salud los que pretenden recurrir a ellos para mejorar los tratamientos médicos o la atención a otros pacientes ²⁷. Porque, de hecho, recibir atención médica siempre implica una pérdida de privacidad. Los pacientes deben exponer su información personal para obtener ayuda, y esa ayuda generalmente se basa en el conocimiento adquirido a partir de las experiencias de pacientes anteriores que han revelado información personal ²⁸. El problema no está tanto en el uso, sino en la exigencia de un uso responsable.

El modelo, como puede verse, parece más asentado en el parecer de los legisladores y la doctrina de algunos académicos que en la verdadera voluntad de los ciudadanos.

Todo lo que venimos exponiendo, obviamente, no puede suponer primar el interés colectivo en total detrimento y exposición del interés individual, sino en buscar una fórmula equilibrada que permita conjugar ambos. Y precisamente esta fórmula puede lograrse flexibilizando, con salvaguarda de los derechos de los individuos involucrados, uno de los dos requisitos que se exige cumplir en el modelo jurídico de protección de datos; véase, bien el requisito del consentimiento informado, o bien el de la anonimización.

En este contexto en que se plantea un dilema entre riesgos y oportunidades, entre interés individual e interés colectivo, surge como debate estelar el del uso secundario de los datos de salud, y no sólo de los que proceden del ámbito de la investigación biomédica y con fármacos, sino también de los obtenidos con ocasión de la asistencia sanitaria, cuyo volumen es muy superior al de aquéllos. El debate se centra en determinar si el nuevo modelo que pretendemos desarrollar, sobre todo, a partir de la implementación del Reglamento UE y la aprobación de la Ley Orgánica, debe seguir fundamentado, como garantías principales, en la doble alternativa de previo consentimiento informado para el nuevo fin o, en su defecto, estricta anonimización de los datos, lo que podríamos denominar el *paradigma Helsinki*, o en un nuevo modelo que, sin quitar un ápice de valor a la dignidad humana y a los derechos del individuo, permita conjugar el interés individual con el colectivo, de manera que el dato de salud deje de ser considerado ya como un dato estrictamente personal y cobre sentido como verdadero patrimonio de la humanidad, como dato que tiene un impacto en el futuro de la salud de la colectividad.

Recuérdese que, en el modelo tradicional, el uso secundario de los datos de salud para fines distintos de aquellos para los que fueron cedidos exigía, bien el consentimiento expreso del interesado, o bien su estricta anonimización. A este respecto, puede verse lo dispuesto en la Ley 14/2007, de 3 julio, de investigación biomédica,

²⁷ HAUG, C.J., "Whose Data Are They Anyway? Can a Patient Perspective Advance the Data-Sharing Debate?", *NEJM*, 26 de abril 2016, p. 1.

²⁸ *Ibidem*, p. 2.

que en su artículo 5 que regula precisamente la protección de datos personales y garantías de confidencialidad se remite a lo dispuesto en la ya ahora derogada Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, explicitando que “3. Se prohíbe la utilización de datos relativos a la salud de las personas con fines distintos a aquéllos para los que se prestó el consentimiento”. Así pues, la citada Ley no autoriza el uso secundario de los datos de salud, salvo, claro está, que se obtenga un nuevo consentimiento específico del interesado para dicho nuevo uso o, en su defecto, se proceda a anonimizar los datos de manera que quedarían fuera de la regulación y, por tanto, de los requisitos de la Ley Orgánica de protección de datos de carácter general.

En todo caso, tampoco podemos olvidar que fue la propia Ley de investigación biomédica la que inauguraba un nuevo paradigma, distinto del denominado Helsinki, al comenzar proclamando en su Preámbulo que “La investigación biomédica y en ciencias de la salud es un instrumento clave para mejorar la calidad y la expectativa de vida de los ciudadanos y para aumentar su bienestar, que ha cambiado de manera sustancial, tanto metodológica como conceptualmente, en los últimos años. La aparición de nuevas herramientas analíticas ha llevado a grandes descubrimientos que permiten albergar fundadas esperanzas sobre el tratamiento e incluso la curación en un futuro no muy lejano de patologías hasta ahora inabordables”, no siendo “España, que ya participa de manera decidida en la generación del conocimiento biomédico, ... ajena al interés por estas investigaciones y al debate que suscitan”. Y añade, a continuación, que “Ante este panorama, es necesario disponer del marco normativo adecuado que dé respuesta a los nuevos retos científicos al mismo tiempo que garantice la protección de los derechos de las personas que pudiesen resultar afectados por la acción investigadora. Y “tanto en el ámbito internacional como en el seno de la sociedad española algunos de los aspectos más sensibles relacionados con la investigación biomédica han sido objeto de debate abierto y extenso, lo que ha permitido deducir principios y criterios, de cada vez más amplia aceptación, a partir de los cuales construir normas y reglas de conducta que logren establecer el necesario equilibrio entre las necesidades de los investigadores y la confianza de la sociedad en la investigación científica. De acuerdo con este espíritu, esta Ley tiene como uno de sus ejes prioritarios asegurar el respeto y la protección de los derechos fundamentales y las libertades públicas del ser humano y de otros bienes jurídicos relacionados con ellos a los que ha dado cabida nuestro ordenamiento jurídico, de forma destacada la Constitución Española y el Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina, suscrito en Oviedo el día 4 de abril de 1997, y que entró en vigor en España el 1 de enero de 2000”.

Sin embargo, este nuevo paradigma queda limitado, por la propia materia a la que viene fundamentalmente referida la citada Ley, la investigación y tratamiento de muestras biológicas humanas, precisamente, a dicho ámbito de la investigación biomédica y no tanto, como vimos antes, a la investigación con datos personales de salud.

Así pues, el artículo 58.1 regula la obtención y uso de las muestras biológicas, disponiendo en su apartado 1 que “La obtención de muestras biológicas con fines de investigación biomédica podrá realizarse únicamente cuando se haya obtenido previamente el consentimiento escrito del sujeto fuente y previa información de las consecuencias y los riesgos que pueda suponer tal obtención para su salud”, a lo que añade a continuación en el apartado 2 que “El consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización”. El modelo, por tanto, supone, incluso, un régimen más estricto, al no eximir la anonimización del requisito del nuevo consentimiento específico que autorice los nuevos fines para los que pretenden usarse secundariamente las muestras.

Sin embargo, a continuación, el mismo precepto en el párrafo segundo del apartado dos, relativiza mucho lo dicho anteriormente, ya que señala que “No obstante lo anterior, de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i) de esta Ley. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación correspondiente, el cual deberá tener en cuenta, como mínimo, los siguientes requisitos: a) Que se trate de una investigación de interés general; b) Que la investigación se lleve a cabo por la misma institución que solicitó el consentimiento para la obtención de las muestras; c) Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente; d) Que no conste una objeción expresa del mismo; e) Que se garantice la confidencialidad de los datos de carácter personal”.

La Ley de investigación biomédica instaura, al menos, en lo que se refiere concretamente al uso secundario de las muestras biológicas un modelo más flexible, aunque, obviamente, no con carácter general, sino excepcionalmente, en aquellos casos, en los que, entre otros requisitos, pero con sustancial relevancia, estemos ante una investigación de interés general para la salud de la comunidad.

Este nuevo paradigma se recoge igualmente en el artículo 60 de la misma Ley que regula el consentimiento sobre la utilización de la muestra biológica y dispone en su apartado 2 que “El consentimiento específico podrá prever el empleo de la muestra para otras líneas de investigación relacionadas con la inicialmente propuesta, incluidas las realizadas por terceros”, y en el artículo 62 de la misma Ley de investigación biomédica que habilita el uso secundario de muestras sin requerir un nuevo consentimiento ni la anonimización estricta, cuando se pretenda investigación secundariamente con la muestra dentro de la misma línea de investigación que aquella en el marco de la cual la muestra fue lícitamente cedida. El concepto “línea de investigación” supone un concepto jurídicamente algo indeterminado porque permite una mayor o menor flexibilización en función de cómo sea interpretado por el operador jurídico. Así, puede considerarse que la investigación en cáncer o en determinada

modalidad de cáncer supone una misma línea de investigación, sin que obviamente la norma exija que sea el mismo proyecto de investigación o ensayo clínico u otro posterior derivado y conectado con éste. Puede aceptarse que el requisito se cumple, dados los términos en los que se expresa el artículo, cuando se trata de un proyecto o ensayo distinto del inicial, pero que tiene como fin investigar en la misma área de enfermedad o conocimiento.

Puede afirmarse, por tanto, que la Ley de investigación biomédica inaugura un nuevo paradigma en el uso secundario de las muestras biológicas que supera el tradicional paradigma Helsinki y hay que ver si dicho cambio se extiende igualmente a los datos personales de salud en el Reglamento y la Ley Orgánica. Avanzamos ya que la respuesta debe ser afirmativa, ya que el nuevo modelo aplicable a las muestras biológicas hay que entenderlo referido también a los datos personales de salud, pese a la aparente contradicción entre lo previsto en el artículo 5 y los artículos 58, 60 y 62, como nos recuerda la propia Agencia Española de Protección de Datos que en el Informe de su Gabinete Jurídico acerca de la incidencia que en el ámbito de la investigación biomédica pudiera producir la plena aplicación a partir del 25 de mayo de 2018 del Reglamento, así como la aprobación de una nueva Ley Orgánica de Protección de Datos, teniendo en cuenta el texto del Proyecto que fue remitido a las Cortes Generales por el Gobierno el día 10 de noviembre de 2017, y ello a la vista de la preocupación manifestada en diversos foros por las sociedades científicas (Informe 073667/2018). Dicho Informe del Gabinete Jurídico señala, literalmente, que en el caso de la investigación biomédica, y particularmente en la llevada a cabo a partir de muestras biológicas procedentes del mismo, nos encontraremos ante el tratamiento de datos relativos a la salud de los sujetos fuente, toda vez que el artículo 4.15 del Reglamento los define como “datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud”²⁹.

La propia Agencia Española de Protección de Datos opta por un modelo más flexible en el que el paradigma no se asiente en la dualidad del consentimiento o anonimización, sino en el del consentimiento frente a la seudonimización, que es precisamente el modelo que promueve en el ámbito del uso secundario de los datos personales de salud tanto el Reglamento como la Ley Orgánica. Y así, en el Informe del Gabinete Jurídico, se dispone que “los requisitos de especificidad y carácter inequívoco para la prestación del consentimiento no deben ser interpretados en el ámbito de la investigación científica de un modo restrictivo, limitado a una concreta investigación de la que se facilite toda la información disponible, sino que cabe considerar que concurren en los supuestos en los que el consentimiento se presta en relación con un determinado campo de investigación, pudiendo extenderse en el futuro ese consentimiento, sin que ello lo vicie en modo alguno, incluso a “finalidades” o

²⁹ Puede accederse a dicho Informe a través de la página web de la Agencia Española de Protección de Datos, en <https://www.aepd.es/media/informes/2018-0046-investigacion-biomedica.pdf>

áreas de investigación que ni siquiera hubieran podido determinarse en el momento en que se prestó sin que sea necesario recabar un nuevo consentimiento del sujeto fuente, teniendo en cuenta los beneficios para los individuos y la sociedad en su conjunto que pueden derivarse de tal investigación no prevista”.

Más aún, el mismo Informe ofrece una interpretación muy amplia del concepto “misma línea de investigación” que antes comentamos. Y así señala que “De este modo, por poner un ejemplo, no sería preciso, para garantizar el carácter inequívoco y específico del consentimiento, que el mismo fuese prestado para la realización de una investigación concreta; ni siquiera para la realización de investigaciones en una rama muy delimitada, como por ejemplo, un determinado tipo de cáncer, sino que, teniendo en cuenta la interpretación derivada directamente del propio Reglamento, será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación, como por ejemplo, la investigación oncológica, o incluso para ámbitos más extensos”. Es decir, definir la misma línea de investigación como investigación en cáncer o, incluso, en términos más amplios (y el anterior ya lo es) es perfectamente factible en atención a lo dispuesto en el ordenamiento jurídico.

Lo relevante en este nuevo modelo no será tanto que el individuo haya otorgado su consentimiento previo para el nuevo fin al que pretenden destinarse los datos o que el dato esté estrictamente anonimizado, como que el origen de los datos sea legítimo, que su uso secundario revista un interés muy relevante para la salud de la colectividad y que se implementen garantías suficientes que impidan que terceros no legitimados puedan acceder a través del dato a la identidad del individuo, sin exigir necesariamente dicha estricta anonimización. Y ello parece que, jurídicamente, puede lograrse a través de lo que se viene ahora en denominar seudonimización, entendida ésta, en palabras del Reglamento UE, como aquel tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Puede considerarse que esta definición de seudonimización resulta algo paradójica, en la medida que es restrictiva pero amplia al mismo tiempo. Es restrictiva en el sentido de que excluye procesos que no pueden garantizar que los datos personales no se atribuyan a una persona física identificable. Sin embargo, es también amplia como decimos ya que la mera separación de la información adicional del dato parece sujetar el tratamiento de éstos a un régimen jurídico muy próximo o casi similar al del dato anonimizado, lo que se traduce en la no exigencia del consentimiento informado.

Las profesoras de la Universidad Pontificia Comillas, Romana García y Hernández Pardo, en su muy esclarecedor que, a la par, brillante trabajo sobre la nueva figura de la seudonimización señalan que este proceso (el de seudonimizar) no va más allá de una mera recodificación, sustituyendo unos códigos identificables por otros

que no lo sean. Sin embargo, el lector experto, posiblemente, no está interpretando este simple efecto, sino que está entendiendo que hablamos de un proceso que no constituye una auténtica anonimización, esto es, una especie de anonimización desleída, que se le acerca, pero no llega a serlo. Y esta interpretación le lleva de manera natural a acuñar la palabra *seudo + anonimización*, igual que hablamos por ejemplo de «seudociencia», «seudointelectuales» o «seudoliteratura», siempre en el sentido de una versión desvirtuada del original. Y así, en lugar de interpretar el procedimiento en el sentido de una recodificación, los especialistas piensan en una versión suave de la anonimización, sin ser conscientes del malentendido³⁰.

Seudonimizar no puede, por tanto, equipararse a pseudoanonimización, como una especie de anonimización algo más débil, sino como la exigencia legal de ocultar el nombre del dato con un seudónimo, es decir, un código, de manera que el concepto equivaldría más al de una disociación más compleja o fuerte. Eso es lo que sostiene, por ejemplo, el Instituto de Medicina de Estados Unidos cuando señala que la seudonimización es un método utilizado para reemplazar las identidades verdaderas (nominativas) de individuos u organizaciones en bases de datos por pseudo-identidades (pseudo-identificaciones) que no se pueden vincular directamente a sus identidades nominativas correspondientes, siendo el beneficio de utilizar la seudonimización en la investigación en salud que al mismo tiempo que protege las identidades de los individuos, permite a los investigadores vincular los datos personales a través del tiempo y el lugar. Y añade el mismo Instituto que la mayoría de los métodos de seudonimización utilizan un tercero de confianza para realizar el proceso de seudonimización. Esto hace que al menos tres entidades participen en la creación de cada base de datos. Existe la fuente de datos que tiene acceso a datos personales nominativos, el tercero de confianza y el registro de datos que utiliza los datos seudonimizados para la investigación³¹.

El Grupo de Trabajo sobre Protección de Datos del artículo 29, en su Dictamen de 10 de abril de 2014 sobre técnicas de anonimización, señala que la seudonimización no es un método de anonimización; simplemente, reduce la vinculabilidad de un conjunto de datos con la identidad original del interesado y es, en consecuencia, una medida de seguridad útil (pág. 3) y añade, a continuación, que uno de los errores consiste en pensar que los datos seudonimizados son datos anonimizados ... los datos seudonimizados no constituyen información anonimizada, ya que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. La probabilidad de que el pseudoanonimato admita la identificabilidad es muy alta; por ello, entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos. Sin embargo, como vamos a ver el modelo que implanta el Reglamento UE e implementa la Ley Orgánica opta por la doble opción de un nuevo consentimiento informado

³⁰ ROMANA GARCÍA, M.L. y HERNÁNDEZ PARDO, B., “Protección de datos: La “seudonimización” inexistente”, *Derecho y Salud*, vol. 28, núm. 1, 2018, pp. 93.

³¹ Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009, p. 103.

o la seudonimización. Es decir, el dato seudonimizado estaría bajo el marco regulador de la protección de datos, no como el dato anonimizado, pero su uso secundario en el ámbito de la salud, cuando el interés general sea relevante, no exigiría la obtención de un nuevo consentimiento informado.

Así, el nuevo modelo optaría por permitir el uso secundario sin nuevo consentimiento informado y sin la exigencia de destruir el vínculo entre el dato y la persona. No se exige una supresión absoluta del riesgo de vincular el dato con un individuo concreto, sino una extraordinaria minimización de aquél. Es, en cierto modo, el modelo que sugiriera una década atrás Ohm cuando afirmaba que la anonimización debía abandonarse como objetivo regulatorio, así como la tradicional distinción entre datos personales y no personales (anónimos)³².

Las virtudes que ofrece la seudonimización frente a la tradicional estricta anonimización son evidentes desde la perspectiva del interés de la salud de la colectividad, ya que, al mantenerse el vínculo entre el dato y la persona, aún cuando sea extraordinariamente difícil que un tercero pueda descodificarlo, se permite no sólo ampliar los datos que se utilizan en la investigación a otros que inicialmente podían no considerarse trascendentes (ampliación de datos) sino, lo que es muy importante en el estado actual de la ciencia del Big Data, contrastar los resultados de la explotación de datos con, por ejemplo, la verdadera evolución de los pacientes (verificación de resultados)³³. La seudonimización es, a la postre, la única garantía frente a las causalidades espurias que ya hemos mencionado antes que es uno de los principales riesgos del Big Data.

Ello es compartido por Ohmann, Banzi, Canham, et al., cuando señalan que es recomendable compartir datos seudonimizados y no estrictamente anonimizados, debiendo ser ésta la regla general³⁴. Incluso, puede afirmarse que existe una obligación legal para los patrocinadores de la investigación de mantener el conjunto de datos seudonimizados. Las principales opciones para compartir datos son seudonimizar o anonimizar efectivamente el conjunto de datos antes de que se comparta, reemplazando los identificadores usados en la prueba con otro conjunto independiente y no reteniendo ninguna información de enlace entre los dos. La ventaja de compartir datos seudonimizados es que, si el investigador usuario de dichos datos descubre buenas razones para aclarar, expandir o unir algunos de los datos, o incluso para realizar nuevas investigaciones con parte de la población de origen, pueden contactar con los titulares de los datos. Esto no significa que la información identificable se transfiera

³² OHM, P., “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization”, *UCLA Law Review*, núm. 57, año 2010, pp. 1755.

³³ Para el Nuffield Council, máximo órgano consultivo en materia de Bioética en el Reino Unido, la seudonimización ofrece tres ventajas en el uso secundario de los datos de salud: “to feed back information to an individual within a cohort who is discovered to be at particular risk, or to validate an analytical procedure, or to enable further data about individuals to be added over time”. Vid. Nuffield Council on Bioethics, *The collection, linking and use of data in biomedical research and health care: ethical issues*, Londres, febrero 2015, p. 68.

³⁴ OHMANN, C., BANZI, R., CANHAM, S. et al., “Sharing and reuse of individual participant data from clinical trials: principles and recommendations”, *BMJ Open*, 7, 2017, p. 11.

a un usuario secundario, a menos que haya un consentimiento explícito del participante para que esto ocurra. Solo significa que se puede regresar a las personas involucradas para solicitar un consentimiento adicional.

El propio Reglamento UE hay que entender que se postula a favor de este nuevo modelo si atendemos a los términos en los que se expresa en sus artículos 6 y 9. Coincide con nuestra opinión, la profesora Vanesa Morente, la cual señala que el Reglamento contempla la posibilidad de tratar datos relativos a la salud sin la previa obtención del consentimiento cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, y cuando el tratamiento tiene como finalidad la investigación científica, aunque apunta que el propio Reglamento deja un margen de decisión a los Estados miembros al permitirles introducir condiciones adicionales, incluso limitaciones, con respecto al tratamiento de los datos genéticos, datos biométricos o datos relativos a la salud³⁵.

También ha apostado por este nuevo paradigma en la flexibilización del requisito de la anonimización, y ya desde una perspectiva estrictamente ética, el Comité Internacional de Bioética (IBC) de la UNESCO en el Informe al que antes hemos hecho referencia. En su Informe de 2017 sobre Big Data y Salud señala que, si bien el uso secundario de los datos de salud exige un nuevo consentimiento específico, tal regla encuentra una excepción cuando se implementen procedimientos técnicos adecuados que eviten que los investigadores o terceros accedan a los datos personales, como sería la seudonimización. Los términos literales en los que se expresa dicho Informe son los siguientes (apartado 59): “In case research is intended that falls outside the range of the broad consent that was obtained for the use of this data, specific consent is necessary for secondary data processing. This is an essential principle to guarantee confidentiality and data privacy. However, secondary analysis of data could be ethically admissible without a new informed consent for such secondary use provided that all the following requirements are met: 1) appropriate legal foundation; 2) evaluation by the Research Ethics Committee (REC); 3) adequate technical procedures in order to prevent researchers and third parties from accessing personal data, such as pseudo-anonymisation; 4) overriding public interest in this health research; 5) infeasible to obtain a new consent; and 6) data must have been collected according to ethical and legal requirements”.

Como puede comprobarse a través del criterio emitido por el que constituye el único Comité a nivel global, no se trata meramente de permitir la investigación sin el requisito de un nuevo consentimiento informado o de la anonimización, sino que deben concurrir junto al de la seudonimización unos requisitos, tales como la previsión normativa previa, el origen legal de los datos, la evaluación por un Comité de Ética (habrá de entenderse, en el caso de España, un Comité de Ética de la Investiga-

³⁵ MORENTE PARRA, V., “Big data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales”, *cit.*, pp. 26 y 27.

ción, CEI), las dificultades en obtener un nuevo consentimiento y el interés público en la investigación.

En similares términos, acaba de expresarse igualmente el Comité de Ministros del Consejo de Europa en su Recomendación CM/Rec(2019)2 sobre protección de los datos de salud, adoptada el 27 de marzo de 2019, y en la que se establece que “Where scientific research purposes allow, data should be anonymised; where research purposes do not allow this, pseudonymisation of the data — with intervention of a trusted third party at the separation stage of the identification — is among the measures that should be implemented to safeguard the rights and fundamental freedoms of the data subject. These measures must be carried out where the purposes of the scientific research can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects (ap. 15.9).

Y así además parecen haberlo entendido dos Estados tan relevantes en el ámbito de los derechos humanos, con sus diferentes sensibilidades históricas, como el Reino Unido y Alemania. La Cámara de los Comunes en su Informe de 2016 sobre *The Big Data Dilemma* señala (ap. 101) que la nueva regulación UE parece abrir el uso secundario de datos a través de la seudonimización, si concurre un interés público en ello³⁶. Tal parece se ha plasmado, además, en la reciente Ley de Economía Digital de 2017 que en su artículo 64 acerca de la “Disclosure of information for research purposes”, dispone, literalmente, que “(1) *Information held by a public authority in connection with the authority’s functions may be disclosed to another person for the purposes of research which is being or is to be carried out*”, y añade, a continuación, que “(2) *If the information is personal information it may not be disclosed under subsection (1) unless the following conditions are met*”, para concluir que “(3) *The first condition is that, if the information identifies a particular person, it is processed before it is disclosed so that- (a) the person’s identity is not specified in the information, and (b) it is not reasonably likely that the person’s identity will be deduced from the information (whether by itself or taken together with other information)*”.

Y, por su lado, la nueva Ley alemana de protección de datos de 2017 recoge un artículo 22 en el que dispone que, si el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, para garantizar altos niveles de calidad y seguridad de la asistencia sanitaria, las medidas para implementar para proteger la privacidad de los datos pueden incluir la seudonimización de los datos personales.

Frente a dicho modelo que opta, como venimos sosteniendo, por flexibilizar el requisito de la estricta anonimización en favor del nuevo concepto legal de seudonimización, hay autores que proponen, por el contrario, poner el peso del cambio de paradigma en el requisito del consentimiento informado, promoviendo fórmulas más flexibles, tales como el denominado *broad consent*, consentimiento amplio, que encajaría en lo que antes hemos comentado acerca de la posibilidad del uso secundario de los datos de salud para la misma o similar línea de investigación (se consiente el uso

³⁶ Puede accederse a dicho Informe a través de la página web de la Cámara de los Comunes, en <https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf>.

para un fin y otros en la misma línea o área de investigación), o el *dynamic consent*, consentimiento dinámico que aprovecha la propia naturaleza dinámica de las nuevas tecnologías para ajustarse precisamente a ellas, de manera que a través de herramientas tecnológicas o aparatos como el propio teléfono móvil, el sujeto pueda ser permanentemente informado de los nuevos usos secundarios y permitirlos o no.

Esta posición de articular el nuevo paradigma sobre la base de un modelo más flexible de consentimiento informa lo ha defendido en el ámbito de los datos de salud la profesora Vanesa Morente. Así, dicha autora señala que sería más adecuado implementar un modelo de consentimiento presunto, o modelo “opt-out”, en el ámbito de la investigación científica y sanitaria. Este modelo de consentimiento que implica que los datos de salud admitirían usos secundarios vinculados a la investigación científica, a menos que el individuo lo rechace expresamente, podría aplicarse o bien de manera restrictiva debiendo atender a dos criterios: en primer lugar, que se trate de investigación dirigida a satisfacer un interés general; y, en segundo lugar, que no tenga un ánimo de lucro de carácter privado. O bien de manera amplia, si el modelo de consentimiento presunto estuviera sujeto únicamente al criterio del interés general, en cuyo caso se posibilita el uso privativo de un bien público como es la información sanitaria³⁷.

Nosotros, por el contrario, sostenemos que debe ser el requisito de la anonimización el que debe ser flexibilizado en garantía de los derechos de los individuos, como, además, creemos que se recoge el propio Reglamento UE. La flexibilización del consentimiento puede suponer un claro detrimento de los derechos de las personas en un ámbito tan sensible como es el de los datos de salud. A la postre, dicho modelo puede llevar a un uso en abierto o con una mera disociación de los datos, es decir, con verdadero riesgo para la intimidad de las personas, a través el mero cumplimiento de un hipotético consentimiento, como sería el caso del *broad consent* o consentimiento amplio, que no le permite al individuo controlar a posteriori, sino tan solo a priori, el uso que va a hacer de sus datos de salud.

En cuanto al modelo de *opt-out*, si bien el mismo muestra la virtualidad de que el silencio opera en favor de la investigación científica, también muestra el riesgo de dejar a la voluntad de los ciudadanos la decisión de optar por participar o no con sus datos en la investigación. Nosotros, por el contrario, consideramos que un modelo en el que el derecho a la protección de la salud está reconocido como un derecho constitucional, pese a que lo sea, en su caso, bajo la modalidad de derecho social, y en el que el modelo asistencial es prácticamente universal, no se sostiene ni ética ni legalmente que los ciudadanos no acepten que sus datos puedan ser empleados en beneficio de la salud de terceros, cuando la confidencialidad queda prácticamente garantizada a través de la figura de la seudonimización. No proponemos una cesión obligatoria y apertura absoluta de los datos en detrimento de la intimidad de las

³⁷ MORENTE PARRA, V., “Big data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales”, *cit.*, p. 31.

personas y de la confidencialidad de sus datos, sino promover un compromiso ético-legal, en el marco del principio de solidaridad en el que se asienta el Estado social y el sistema público asistencial, por el que los ciudadanos aporten sus datos, con garantías de la confidencialidad, en el bien de la salud de la colectividad.

El problema de asentar el modelo en el consentimiento de los individuos, por mucho que flexibilizemos dicho requisito, y no en el requisito de la anonimización, radica, por un lado, en que la protección de la intimidad de las personas y de la confidencialidad de sus datos puede no ser verdaderamente efectiva, ya que por un mero consentimiento amplio en el pasado o por su silencio, sus datos podrían quedar expuestos de manera desproporcionada, y, por el otro, en que, a la postre, estamos dotando a los individuos de la facultad de decidir, *prima facie*, si comparten o no sus datos, lo que en un modelo social y sanitario como el nuestro no nos parece que sea sostenible ética y legalmente.

En todo caso, como hemos venido sosteniendo, del Reglamento UE precisamente no se deriva una flexibilización del requisito del consentimiento informado como fundamento del tratamiento de datos personales, sino antes al contrario, se apuesta por una fórmula más estricta que la recogida en la Directiva a la que viene a sustituir aquél. Los términos del Reglamento son meridianamente claros, sobre todo, si atendemos a lo dispuesto en el Considerando 32 que dispone que “El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales”.

Y añade a continuación que “el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta”.

V. ¿HA OPTADO LA NUEVA LEY ORGÁNICA POR ESTE NUEVO PARADIGMA?

Si antes hemos concluido que el Reglamento UE ha incorporado a la regulación del tratamiento de datos de salud el nuevo paradigma que promueve una flexibilización de los requisitos legales de la anonimización a través del nuevo concepto legal

de la seudonimización, sería difícil, dada la naturaleza de la norma comunitaria y su carácter vinculante, que el ordenamiento español hubiera regulado en un diferente sentido dicho tratamiento. Sin embargo, es importante recordar que, pese a tratarse la norma comunitaria de un reglamento, una lectura de la misma permite concluir que, si bien formalmente recibe dicha denominación, materialmente los términos en los que se expresa son muy próximos, por la flexibilidad de los propios requisitos que incorpora, a una directiva. Como nos recordara el Consejo de Estado en su Dictamen 757/2017, de 26 de octubre, sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, el Reglamento contiene, pese a su intensa vocación armonizadora, hasta cincuenta y seis remisiones de diverso alcance al Derecho de los Estados miembros³⁸.

Esta cierta flexibilidad del Reglamento UE es recogida por la recientemente aprobada Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, al disponer en su Preámbulo que, pese a la naturaleza reglamentaria de la nueva norma UE y no de Directiva, ello no excluye “la intervención del Derecho interno. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo”.

La nueva regulación que se contiene en dicha Ley Orgánica aborda específicamente el nuevo régimen legal del tratamiento de los datos de salud y así viene a incorporar un marco específico para dichos datos, como lo hace el propio Reglamento UE, en su disposición adicional 17.^a. Esta disposición adicional hay que recordar que ha ido precedida de un arduo debate parlamentario en Comisión, ya que el proyecto enviado por el Gobierno no recogía tal regulación específica para los datos de salud, lo que generó cierto desconcierto y preocupación en el sector sanitario. Fruto de la presión ejercida por diferentes colegios profesionales, sociedades científicas y otros grupos de interés que veían en la falta de dicho régimen específico un riesgo para aprovechar las ventajas del uso masivo de datos de salud, la Comisión y posteriormente el Pleno optaron por incorporar de forma ciertamente singular la mencionada disposición adicional.

Una de las ventajas desde la perspectiva del avance de la ciencia en el ámbito de la lucha contra las enfermedades que podemos encontrar en dicha regulación conte-

³⁸ Puede accederse a dicho Dictamen a través de la página web del Consejo de Estado y específicamente en el siguiente enlace: <https://www.boe.es/buscar/doc.php?id=CE-D-2017-757>. Se recoge un resumen de dicho Dictamen en JIMÉNEZ ASENSIO, R., *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*, IVAP, Oñati, 2019, pp. 24 a 26.

nida en la disposición es que la misma no se limite a tratar el uso secundario de los datos de salud procedentes de la investigación biomédica, sino también de la mera asistencia sanitaria, de manera que no se reforma la Ley de investigación biomédica, sino lo que es realmente importante, la Ley de autonomía del paciente y su régimen de acceso a los datos por razones secundarias a la asistencia sanitaria. La propia disposición adicional inicia su tenor señalando que se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento UE los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados, entre otras y por lo que aquí interesa, en las siguientes leyes y sus disposiciones de desarrollo: Ley 14/1986, de 25 de abril, General de Sanidad, Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, Ley 14/2007, de 3 de julio, de Investigación biomédica, y Ley 33/2011, de 4 de octubre, General de Salud Pública. Así, el nuevo régimen de uso secundario de datos personales de salud no queda, como decíamos, circunscrito a los datos derivados de la investigación biomédica o con fármacos, sino también a los datos asistenciales.

Desde la perspectiva de la técnica normativa, la citada Disposición no es precisamente un ejemplo de buen hacer, tanto por la forma extraña de inserción en el ordenamiento jurídico, a través de la mera aprobación de una adicional, sin modificación del texto de las normas a las que, en principio, viene a completar o afectar la misma, como por la propia redacción que exige el sobreesfuerzo intelectual de leerla en varias ocasiones para alcanzar a entender sus previsiones.

De la nueva regulación contenida en la disposición adicional es importante destacar su apartado 2 que, si bien, señala que la reutilización de datos en la investigación en salud podrá basarse la precitada fórmula del *broad consent* (“c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial”), añade a continuación, en la siguiente letra que “d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica”.

La posibilidad de ir más allá de la flexibilización del consentimiento informado en su modalidad de consentimiento amplio, el cual permitiría el uso secundario de datos en proyectos de investigación que vengan referidos a la misma o similar área de investigación de aquel en el marco del cual los datos fueron cedidos, y admitir también dicho uso secundario a través de la seudonimización muestra la virtud de que posibilita aprovechar no solo los datos de la investigación, en los que puede haberse otorgado la autorización de un uso posterior, sino los puramente asistenciales. En lo que se refiere a éstos, habitualmente ni habrá previo consentimiento expreso, solamente tácito, ni menos aún un consentimiento amplio. La virtualidad del consentimiento amplio queda reducida a los datos derivados de la investigación, pero no al

uso secundario de los asistenciales y, como ya hemos señalado antes, precisamente estos ofrecen, por volumen e integración, un gran potencial para la investigación en salud.

Así pues, el apartado 2 d) de la disposición adicional permite el uso secundario de los datos de salud, tanto procedentes de la investigación como de la asistencia, siempre que se proceda a su seudonimización. Es decir, la Ley opta por un cambio del paradigma del uso secundario de los datos de salud. El paradigma anterior que exigía optar por cumplir con un nuevo consentimiento del titular de los datos o proceder a su anonimización, se ve ahora sustituido por otro que flexibiliza tanto el consentimiento informado, admitiendo para la reutilización una fórmula amplia basada en similares áreas de investigación, como el requisito de la anonimización, a través del novedoso concepto de la seudonimización. No se exige ya, pues, la anonimización, sino la seudonimización que recordemos que en traducción de su versión original en lengua inglesa no significa que otra cosa que poner un seudónimo a los datos, es decir, una disociación compleja. Seudonimizar no se equipara a seudoanonimización, como una especie de anonimización algo más débil, sino como la exigencia legal de ocultar el nombre del dato con un seudónimo, es decir, un código, de manera que el concepto equivaldría más al de una disociación más compleja o fuerte. La seudonimización se aproxima más a la disociación, aunque más compleja, que a la anonimización.

Por otro lado, la Ley Orgánica también ha modificado en su disposición final 9.^a la Ley de autonomía del paciente (41/2002), en concreto, lo que se refiere al acceso a la historia clínica regulado en el artículo 16 y así dispone ahora que la obligación de preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, quedando asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos no será de aplicación en los supuestos de investigación previstos en el apartado 2 de la ya citada disposición adicional 17.³⁹

En nuestra opinión, lo relevante en este modelo que viene a consagrar la nueva Ley no será tanto que el individuo haya otorgado su consentimiento previo para el nuevo fin al que pretenden destinarse los datos o que el dato esté estrictamente anonimizado, como que el origen de los datos sea legítimo, su uso secundario revista un interés muy relevante para la salud de la colectividad y se implementen garantías suficientes que impidan que terceros no legitimados puedan acceder a través del dato a la identidad del individuo, sin exigir necesariamente dicha estricta anonimización. Y ello, jurídicamente, se logra a través de la seudonimización.

Las virtudes que ofrece la seudonimización frente a la tradicional estricta anonimización son evidentes desde la perspectiva del interés de la salud de la colectividad, ya que, al mantenerse el vínculo entre el dato y la persona, es decir, la trazabilidad, se permite no sólo ampliar los datos que se utilizan en la investigación a otros que inicialmente podían no considerarse trascendentes (ampliación de datos) sino, lo que

³⁹ Sobre los efectos de esta modificación legislativa, vid. Informe del Gabinete Jurídico de la Agencia 121/2018.

es muy importante, contrastar los resultados de la explotación de datos con, por ejemplo, la verdadera evolución de los pacientes (verificación de resultados). La seudonimización es, a la postre, la única garantía frente a las causalidades espurias, uno de los principales riesgos del Big Data, sobre todo, en sus inicios.

El nuevo modelo se sujeta, además, a la garantía de la evaluación por parte de los Comités Éticos de Investigación, lo que exigirá trabajar en el seno de dichos Comités en comprender cuál es el nuevo modelo que se implanta, sabiendo equilibrar los intereses en conflicto y responder a las necesidades de la lucha contra las enfermedades y por la mejora de los tratamientos médicos.

VI. CONCLUSIONES

En definitiva, en este nuevo panorama de grandes oportunidades para la lucha en contra de las enfermedades y la mejora de la salud de las personas, es importante promover nuevos paradigmas que, sin caer en lo tecnológico, no sólo como algo esencialmente bueno, sino como absolutamente excluyente de la intuición y sabiduría humana, tampoco olviden que el contexto es muy distinto al existente pocos años atrás y que las enormes ventajas que puede ofrecer el tratamiento masivo de datos han de trascender a una visión exclusivamente basada en el interés individual en detrimento del bien común. Un punto de equilibrio entre ambas posturas parece mostrarse, al igual que ocurre en muchos otros ámbitos, como la verdadera virtud.

Además, el debate debe plantearse en términos en los que el contexto no se pierda de vista. En los modelos de protección de la salud desarrollados en la Europa occidental tras la Segunda Guerra Mundial y, sobre todo, en los basados en la fórmula más socialdemócrata como es la Beveridge, resulta un contrasentido mantener una posición que únicamente atiende a la dimensión individual o subjetiva, cuando el modelo tiene rasgos esenciales de comunitarismo. Acudir a un Hospital y ver resuelto un grave problema de salud con cargo a los presupuestos públicos exige también de los ciudadanos un ejercicio de responsabilidad y ésta se manifiesta en el contexto actual del avance de la tecnología en el deber moral de compartir los datos para que, aquellos otros que no han logrado tan fácilmente la curación, puedan obtenerla.

Por lo tanto, se trata de desarrollar un nuevo paradigma que, salvando alguno de los postulados en los que se asienta el denominado paradigma Helsinki, permita beneficiar a la colectividad en el avance de la medicina, para lo que la explotación masiva de datos se ofrece como un instrumento indispensable, sin menoscabo de los derechos fundamentales de los individuos. Es decir, un modelo responsable tanto desde la perspectiva de los investigadores y la industria, como de los propios ciudadanos. Obviamente, no debe promoverse un modelo de responsabilidad punitiva, sino

un concepto de responsabilidad como deber de ayuda a los demás, en términos acuñados muy recientemente por Yascha Mounk⁴⁰.

BIBLIOGRAFÍA

- BOLLIER, D., *The promise and peril of Big Data*, The Aspen Institute, Maryland, 2010.
- CHAN, S., “Bioethics in the big data era: health care and beyond”, *Rev Bio y Der.*, vol. 41, año 2017, pp. 3 a 32.
- COTINO HUESO, L., Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales, *Dilemata*, núm. 24, año 9, 2017, pp. 131-150.
- GERMAN ETHICS COUNCIL, *Big Data and health. Data sovereignty as the shaping informational freedom*, Opinion, Executive Summary and Recommendations, Berlín, 2018.
- GIL, E., Big Data, privacidad y protección de datos, Boletín Oficial del Estado, Madrid, 2016.
- GLENN COHEN, I, FERNÁNDEZ LYNCH, H, VAYENA, E. y GASSER, U. (Edit.), *Big Data, Health Law and Bioethics*, Cambridge University Press, Cambridge, 2018.
- HAUG, C.J., Whose Data Are They Anyway? Can a Patient Perspective Advance the Data-Sharing Debate?, *NEJM*, 26 de abril 2016.
- HOUSE OF COMMONS, Science and Technology Committee, *The Big Data dilemma*, Fourth Report of Session 2015-16, Londres, 2016.
- INTERNATIONAL BIOETHICS COMMITTEE (IBC) UNESCO, *Report on Big Data and Health*, París, 2017.
- INSTITUTE OF MEDICINE, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009.
- JIMÉNEZ ASENSIO, R., *Introducción al nuevo marco normativo de la protección de datos personales en el sector público*, IVAP, Oñati, 2019.
- LUCAS MURILLO DE LA CUEVA, P., “La construcción del derecho a la autodeterminación informativa”, *Revista de Estudios Políticos*, núm. 104, abril-junio 1999.
- LUCAS MURILLO DE LA CUEVA, P., “La protección de los datos de carácter personal en el horizonte de 2010”, *Anuario de la Facultad de Derecho*, Universidad de Alcalá, núm. 2, año 2009, pp. 131 a 142.
- KAPLAN, B., “How should health data be used? Privacy, secondary use, and Big Data sales”, *Yale University Institute for Social and Policy Studies*, Working Paper

⁴⁰ Vid. MOUNK, Y., *The age of responsibility. Luck, choice and the Welfare State*, Harvard University Press, Cambridge, 2017.

- núm. 14-025, *Cambridge Quarterly of Healthcare Ethics*, vol. 25, núm. 2, año 2016, pp. 312-329.
- MARTÍNEZ, R., “Big data, investigación en salud y protección de datos personales ¿Un falso debate?”, *Revista Valenciana d’Estudis Autonòmics*, núm. 62, año 2017, pp. 235 a 280.
- MAYER-SCHÖNBERGER, V. y CUKIER, K., *Big Data*, Turner, Madrid, 2013.
- MORENTE PARRA, V., “Big data o el arte de analizar datos masivos. Una reflexión crítica desde los derechos fundamentales”, *Revista Derechos y Libertades*, número 41, época II, julio 2019 (en prensa).
- MOUNK, Y., *The age of responsibility. Luck, choice and the Welfare State*, Harvard University Press, Cambridge, 2017.
- NUFFIELD COUNCIL ON BIOETHICS, *The collection, linking and use of data in biomedical research and health care: ethical issues*, Londres, febrero 2015.
- OHM, P., *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, *UCLA Law Review*, núm. 57, año 2010, pp. 1701-1777.
- OHMANN C, BANZI R, CANHAM S, et al., “Sharing and reuse of individual participant data from clinical trials: principles and recommendations”, *BMJ Open*, 7, 2017, pp. 1 a 24.
- REBOLLO DELGADO, L. y SERRANO PÉREZ, M.M., *Manual de protección de datos*, 3.^a ed., Dykinson, Madrid, 2019.
- RESOLUCIÓN DEL PARLAMENTO EUROPEO, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).
- ROMANA GARCÍA, M. L. y HERNÁNDEZ PARDO, B., “Protección de datos: La “seudonimización” inexistente”, *Derecho y Salud*, vol. 28, núm. 1, 2018, pp. 92 a 103.
- SAFRAN, C., BLOOMROSEN, M., HAMMOND, W. E., LABKOFF, S., MARKEL-FOX, S., TANG, P. C. y DETMER, D. E., “Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper”, *Journal of the American Medical Informatics Association*, vol. 14, n. 1, 2007, pp. 1 a 9.
- SAN SEGUNDO ENCINAR, J.M., *Big Data en salud digital. Informe de resultados*, Red.es, Madrid, 2017.
- STALLA-BOURDILLON, S. y KNIGHT, A., *Anonymous data v. personal data—a false debate: an EU perspective on anonymization, pseudonymization and personal data*, *Wisconsin International Law Journal*, 2017. Available at SSRN: <https://ssrn.com/abstract=2927945>

Title:

A reflection from the theory of fundamental rights on the secondary use of health data in the framework of Big Data

Summary:

I. Introduction. II. Solving some myths: will the human being retain an essential role in the fight against disease in the days of Big Data? III. The impact of Big Data opportunities in the conflict between individual rights and common good. IV. The necessary overcoming of the Helsinki paradigm in the secondary use of health data safeguarding people's rights. V. Have the new Spanish Regulation of data protection opted for the new paradigm? VI. Conclusions

Resumen:

El Big Data ofrece en el ámbito de la investigación en salud grandes oportunidades. La interrelación y explotación de los datos de salud, incluso, correlacionándolos con los no tradicionales, va a permitir avanzar en la lucha contra las enfermedades y a favor de la prevención y predicción en unos términos que seguramente no van a encontrar parangón en la Historia de la Medicina y de la humanidad. Sin embargo, el modelo en el que se han asentado tradicionalmente tanto la investigación en salud, el denominado *paradigma Helsinki* por referencia a la Declaración del mismo nombre, suscrita por la 18ª Asamblea Médica Mundial en 1964, como la propia regulación jurídica de la protección de los datos de salud parecen no mostrarse adecuados para poder aprovechar tales oportunidades. El equilibrio entre los riesgos para los derechos del individuo y los beneficios para el interés colectivo parece haberse transformado. Ello nos exige reflexionar sobre si cabe desarrollar un nuevo paradigma que permita conjugar las ventajas que para la salud tiene la investigación masiva de datos con la exigida protección de los derechos de las personas. Se trata, en definitiva, de optar, dentro de los márgenes que ofrece la regulación de la protección de datos, por el marco legal más adecuado, atendiendo a las novedades que, al respecto, ofrecen el Reglamento UE y la Ley Orgánica. Como sostenemos en nuestro trabajo, consideramos que el nuevo concepto de la seudonimización ha de ocupar un papel principal dentro de este nuevo modelo.

Abstract:

Big Data offers great opportunities in the field of health research. The interrelation and exploitation of health data, even, correlating them with non-traditional ones, will allow progress in the fight against diseases and in favor of prevention and prediction in terms that are surely not going to find a match in the History of the Medicine and humanity. However, the traditionally settled model, so-called Helsinki paradigm by reference to the Declaration of the same name, signed by the 18th World Medical

Assembly in 1964, and the legal regulation of the protection of health data do not appear to be adequate to take advantage of such opportunities that Big Data offers. The balance between risks for individual rights and benefits for common interest seems to have been transformed. This requires us to reflect on whether a new paradigm can be developed that allows us to combine the health benefits of massive data research with the required protection of individual rights. In other words, to choose, within the margins offered by the regulation of data protection, for the most appropriate legal framework, taking into account the developments that, in this regard, offer the EU Regulation and the Spanish specific new regulation of data protection. As we are maintaining in our work, we consider that the new concept of pseudonymization has to play a leading role within this new model.

Palabras clave:

Big Data; análisis de datos; datos de salud; algoritmos; privacidad; habeas data; intimidad; confidencialidad; uso secundario; seudonimización; consentimiento informado.

Key words:

Big Data; data análisis; health data; algorithms; privacy; habeas data; privacy; confidentiality; secondary use; pseudonymization; informed consent.