FACULTAD DE DERECHO

EL USO SECUNDARIO DE LOS DATOS DE SALUD EN EL NUEVO MARCO LEGAL DEL REGLAMENTO EUROPEO

¿Un nuevo paradigma en la protección del interés general?

Autor: Alfredo Lafita Sáenz-Diez
5º E3 B
Derecho Constitucional
Tutor: Federico de Montalvo Jääskeläinen

Madrid
Abril 2019

RESUMEN

El uso secundario de datos sanitarios es esencial para el progreso de la investigación médica –y, por tanto, para el interés general– pues facilita a los investigadores el acceso a información clínica esencial para sus estudios. Sin embargo, este uso secundario puede atacar el derecho a la intimidad de los titulares de los datos. Ante semejante conflicto, la solución tradicional adoptada por el legislador ha sido el conocido como "paradigma del consentimiento o la anonimización", según el cual el uso secundario exige el previo consentimiento informado de los titulares de los datos o la anonimización de los mismos.

No obstante, el *big data* aplicado al mundo de la medicina parece haber agotado este paradigma. Dado que las ventajas de esta herramienta digital son inmensas, pero también sus riesgos, es necesario construir un nuevo paradigma para el nuevo contexto tecnológico. En este sentido, destaca el Reglamento General de Protección de Datos de 2016, cuya aportación más significativa en relación con la investigación médica es la seudonimización, una técnica que oculta la identidad del titular de los datos, pero permite reidentificarlo en caso de que sea necesario.

PALABRAS CLAVE

Uso secundario, *big data*, Reglamento General de Protección de Datos, consentimiento informado, anonimización y seudonimización.

ABSTRACT

The secondary use of health data is essential for the progress of medical research –and therefore for the general interest– as it provides researchers with access to clinical information essential to their studies. However, this secondary use may attack the right to privacy of data subjects. In the face of such a conflict, the traditional solution adopted by the legislator has been the so-called "consent or anonymization paradigm", according to which secondary use requires the prior informed consent of the data subjects or the anonymization of the data.

However, big data applied to the world of medicine seems to have exhausted this paradigm. Given that the advantages of this digital tool are immense, but also its risks, it is necessary to construct a new paradigm for the new technological context. In this sense, the General Data Protection Regulation of 2016 stands out, whose most significant contribution in relation to medical research is pseudonymization, a technique that hides the identity of the data subject but allows him or her to be re-identified if necessary.

KEYWORDS

Secondary use, big data, General Data Protection Regulation, informed consent, anonymization and pseudonymization.

ÍNDICE

LISTADO DE ABREVIATURAS

CE	Constitución Española
OCDE	Organización para la Cooperación y el Desarrollo Económicos
STC	Sentencia del Tribunal Constitucional
TJUE	Tribunal de Justicia de la Unión Europea

1. INTRODUCCIÓN

El mundo de la medicina genera a diario enormes cantidades de información de todo tipo, como análisis de sangre, radiografías, informes clínicos o muestras genéticas. El uso secundario de esta información en el ámbito de la investigación es esencial, pues evita que los investigadores tengan que recolectar nuevos datos cada vez que llevan a cabo un estudio, lo que resultaría caro e ineficiente. Como la investigación es indispensable para el progreso de la ciencia médica y, por tanto, para el interés general, existe un paradigma que ha venido conciliando en las últimas décadas dicho interés general con el interés individual de los sujetos cuyos datos se emplean, que tienen derecho a que se respete su intimidad y privacidad. Así, de acuerdo con este paradigma, los investigadores sólo pueden emplear datos médicos en sus estudios si han recibido el consentimiento informado de sus titulares o si los datos han sido previamente anonimizados.

Dicho esto, cada vez se genera más y más información clínica, pues además de las fuentes convencionales mencionadas en el párrafo anterior, en la actualidad también existen otras mucho más revolucionarias, como los datos biométricos recolectados por dispositivos inteligentes o las publicaciones en redes sociales. Todo esto hace que hoy en día el conocimiento médico se caracterice por cinco propiedades: el volumen, la variedad, la velocidad, la veracidad y el valor. Estas características se conocen como las cinco uves del *big data* y hacen que el sector de la salud sea ideal para el uso de esta tecnología. El problema es que dicho uso parece suponer el agotamiento del paradigma tradicional del consentimiento o anonimización.

Por este motivo, el objetivo de este trabajo es estudiar el nuevo paradigma del uso secundario de datos médicos en la investigación en la era del *big data*. Este nuevo paradigma ha sido introducido en Europa por el nuevo Reglamento (UE) 2016/679 de Protección de Datos[1] (en adelante, "el Reglamento General de Protección de Datos" o "el Reglamento"), una norma que ha buscado, precisamente, adaptar el régimen legal al nuevo contexto tecnológico. Por ello, el Reglamento ha ahondado, principalmente, en la anonimización, desarrollando una nueva técnica, la seudonimización. Además, el

[1] Reglamento (UE) 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 y por el que se deroga la directiva 95/46/CE (Diario Oficial n° L 110 de 4/5/2016, pp. 1-88).

consentimiento también ha sufrido ligeras modificaciones. En el mismo sentido, las Cortes Generales españolas aprobaron recientemente una nueva ley orgánica con unos objetivos similares a los del Reglamento: la Ley Orgánica 3/2018, de Protección de Datos[2] (en adelante, "la Ley Orgánica de Protección de Datos de 2018" o "la Ley Orgánica de 2018").

Para poder estudiar adecuadamente el nuevo paradigma, ha resultado indispensable contextualizar antes el problema. Por ello, se ha construido un marco teórico en el que, en primer lugar, se ha analizado en profundidad el *big data* en el ámbito de la medicina, con especial énfasis en sus características, ventajas y riesgos. Además, el marco teórico también ha desarrollado los antecedentes legislativos del Reglamento, de entre los que destaca la Directiva 95/46/CE, de Protección de Datos[3] (en adelante, "la Directiva de Protección de Datos" o "la Directiva") y la Ley Orgánica 15/1999, de Protección de Datos[4] (en adelante, "la Ley Orgánica de Protección de Datos de 1999" o "la Ley Orgánica de 1999").

Las principales fuentes a las que se ha acudido para llevar a cabo el presente estudio son diversas normas europeas y españolas en materia de protección de datos, tanto vigentes en la actualidad, como ya derogadas. También ha resultado útil recurrir a la literatura especializada para analizar las ventajas y desventajas del uso del *big data* en la medicina y el marco normativo e impacto de las distintas leyes de protección de datos.

Por lo que se refiere a la estructura del trabajo, éste se divide en siete apartados, incluyendo el presente capítulo introductorio. El segundo profundiza en la importancia de la tecnología en la medicina, con especial énfasis en el *big data*, mientras que el tercero se centra en los riesgos de esta herramienta. A continuación, el cuarto capítulo realiza un recorrido legislativo de algunas normas de protección de datos ya derogadas, a saber, la Directiva de Protección de Datos y la Ley Orgánica de Protección de Datos de 1999. El quinto capítulo analiza en profundidad el actual Reglamento General de Protección de

---

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

[3] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial n° L 281 de 23/11/1995, pp. 0031-0050).

[4] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14 de diciembre de 1999).

Datos. Seguidamente, el sexto capítulo explica la evolución del paradigma del uso secundario de datos en la investigación médica hasta alcanzar la situación actual. Para terminar, el estudio finaliza con un capítulo de conclusiones, donde se discuten las principales averiguaciones alcanzadas.

2. LOS BENEFICIOS DEL USO DE LA TECNOLOGÍA EN LA MEDICINA. ESPECIAL ÉNFASIS EN EL *BIG DATA*

Desde hace décadas, nuestra civilización está siendo partícipe de una revolución tecnológica sin paragón en la historia: podemos cruzar el Atlántico en apenas seis horas, construir edificios de varios cientos de metros, comunicarnos instantáneamente con personas en otros continentes o fabricar cohetes capaces de viajar a Marte.

Como no puede ser de otra manera, el mundo de la medicina está siendo actor y parte de esta revolución. Así, se han experimentado numerosos avances de los últimos tiempos, algunos de los cuales han supuesto incluso *"el nacimiento de nuevas áreas de la ciencia médica, como la genómica, la biología molecular, la medicina genética o la farmacogenética, además de complejas técnicas de diagnóstico e información"*.[5] Por lo tanto, no estamos hablando de pequeños desarrollos que profundizan en ámbitos ya conocidos, sino de una verdadera revolución que nos permite investigar áreas hasta ahora inexploradas.

El Proyecto Genoma Humano es un ejemplo del impacto del desarrollo tecnológico en la medicina. Impulsado por un organismo gubernamental estadounidense, el Centro Nacional para la Investigación del Genoma Humano,[6] en colaboración con otras instituciones norteamericanas e internacionales, este proyecto consiguió secuenciar las tres mil millones de bases de ADN que constituyen el genoma del ser humano.[7] Un informe del año 2011 del Instituto Battelle que analizaba el impacto económico del proyecto destacó que algunos de los avances tecnológicos resultantes del mismo, como el secuenciamiento rápido de ADN, han posibilitado la introducción de nuevas tecnologías en el ámbito hospitalario, como los test genéticos para enfermedades monogénicas o las proteínas terapéuticas.[8]

---

[5] Crabu, S. "Biomedicalization. Technoscience, Health and Illness in the U.S.", *Tecnoscienza*, vol. 2, n. 2, 2010, p. 119.

[6] Hoy, el Instituto Nacional de Investigación del Genoma Humano.

[7] Green, E. D., Watson, J. D. y Collins, F. S., "Human Genome Project: Twenty-five years of big biology", *Nature*, vol. 526, n. 7571, 2015, p. 29.

[8] Tripp, S. y Grueber, M., "Economic Impact of the Human Genome Project", *Battelle Memorial Institute*, 2011, p. 55 (disponible en: https://www.battelle.org/docs/default-source/misc/battelle-2011-misc-economic-impact-human-genome-project.pdf; última consulta 28/01/2019).

Más importante todavía que los extraordinarios avances de los últimos años es el hecho de que la medicina es un área donde se prevé que la tendencia innovadora se mantenga en el tiempo. En este sentido, se espera que el futuro depare nuevos descubrimientos que trasladarán la frontera del saber médico a horizontes insospechados. Por ejemplo, el *big data*, uno de los grandes avances tecnológicos de los últimos años, tiene el potencial de revolucionar el conocimiento médico.

2.1. El *big data* médico

El *big data* es un concepto abstracto y sobre el que no existe un consenso en la literatura. De acuerdo con un informe del McKinsey Global Institute, se puede definir el *big data* como aquellas bases de datos que por su tamaño, complejidad y variedad de información que contienen no pueden ser almacenas y gestionadas mediante *software* tradicional, sino que necesitan del uso de herramientas específicas.[9]

El ámbito médico ofrece numerosas oportunidades en relación con el *big data*, pues es un sector que genera a diario enormes cantidades de datos. Cabe destacar que cuando se habla de datos médicos no sólo se está haciendo referencia a datos de carácter convencional, como los análisis de sangre o las pruebas de rayos X, sino también a fuentes innovadoras en términos clínicos, como los registros procedentes de dispositivos *wearables* o incluso la información de los pacientes en las redes sociales. Pues bien, el *big data* permite que los investigadores, en uso de las herramientas adecuadas, empleen esta amplia gama de datos para buscar patrones, correlaciones y tendencias, con el objetivo de mejorar la salud y la calidad de vida las personas, a la vez que se reduce el coste de los tratamientos.[10]

---

[9] Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. y Hung Byers, A., "Big data: The next frontier for innovation, competition and productivity", *McKinsey Global Institute*, 2011, p. 1 (disponible en: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation; última consulta 03/02/2019).

[10] Raghupathi, W. y Raghupathi, V., "Big data analytics in healthcare: promise and potential", *Health Information Science and Systems*, vol. *2,* n. 3, 2014, p. 9.

2.1.1. Las 5 uves del big data

El *big data* se suele asociar con cinco características fundamentales que en conjunto constituyen las conocidas como cinco uves del *big* data: el volumen, la variedad, la velocidad, la veracidad y el valor.[11] Estas propiedades se aplican a cualquier sector en el que opere el *big data*, no sólo en el clínico, pero si se analiza en detalle cada uno de ellos en relación con el mundo de la medicina, uno comprende por qué el *big data* ofrece increíbles oportunidades en esta área del conocimiento.

a. Volumen

La primera de estas uves es el volumen: para explotar el *big data* en un determinado ámbito científico, es necesario que existan enormes cantidades de datos a analizar. Pues bien, como ya se ha mencionado brevemente en la introducción, en el mundo se generan a diario millones de datos médicos. Para tratar de entender la verdadera magnitud de la información generada, cabe destacar que el tamaño del sistema sanitario estadounidense alcanzó los 150 exabytes –1,5 x 10^{11} gigabytes– en el año 2011.[12] Sin ir más lejos, en España, a raíz de la implantación de la Historia Clínica Digital del Sistema Nacional de Salud,[13] casi el 80% de la población tiene referencias dentro del mismo, lo que se traduce en que éste aloja más de 175 millones de documentos.[14] Además, se espera que en los próximos años el número de datos crezca de manera exponencial, especialmente como resultado del uso de *"nuevas plataformas de secuenciación de alto rendimiento, imágenes en tiempo real y dispositivos de punto de atención, así como tecnologías wearables de salud móviles"*.[15]

---

[11] Comité Internacional de Bioética, "Report of the IBC on Big Data and Health", 2017, p. 3 (disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000248724; última consulta 02/02/2019).

[12] Institute for Health Technology Transformation, "Transforming Health Care Through Big Data", 2013, p. 5 (disponible en: http://c4fd63cb482ce6861463-bc6183f1c18e748a49b87a25911a0555.r93.cf2.rackcdn.com/iHT2_BigData_2013.pdf; última consulta 02/02/2019).

[13] Sistema que permite a pacientes y médicos acceder a su documentación sanitaria en línea.

[14] Ministerio de Sanidad, Servicios Sociales e Igualdad, "Proyecto HCDSNS Historia Clínica Digital del Sistema Nacional de Salud", 2017, p. 30 (disponible en: https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf; última consulta 07/02/2019).

[15] Andreu-Perez, J., Poon, C. C. Y., Merrifield, R. D., Wong, S. T. C. y Yang, G. Z, "Big Data for Health", *IEEE Journal of Biomedical and Health Informatics*, vol. 19, n. 4, 2015, p. 1193.

Por lo tanto, como el mundo médico ha generado históricamente y continúa generando un enorme volumen de datos analizables digitalmente, es un sector que presenta enormes oportunidades para el *big data*.

b. Variedad

La segunda uve del *big data* es la variedad, característica que hace referencia a que no sólo es necesario que exista un enorme volumen de datos con los que trabajar, sino que también es importante que éstos sean de diversa tipología. De nuevo, el mundo de la medicina es ideal en este aspecto, pues en él se genera todo tipo de información, como registros de pacientes, análisis de sangre, pruebas de ADN, ensayos clínicos, ecografías, escáneres médicos y un largo etcétera.

Toda esta información médica solía tener, tradicionalmente, carácter estático: se obtenía el dato de manera aislada y se almacenaba, sin existir relación entre éste y otro posterior. Sin embargo, hoy en día cada vez se genera más información de tipo dinámico, guardando los datos recogidos en distintos momentos relación entre sí. Son, principalmente, datos obtenidos en seguimientos médicos (por ejemplo, la evolución de la presión arterial en un paciente a lo largo de los meses) o recolectados por dispositivos *wearables* (el iPhone, por ejemplo, registra el número de pasos de su dueño al día).[16] Por lo tanto, la información médica no es variada únicamente porque existen distintos tipos de datos en cuanto a su clase, sino que también es importante que haya datos estáticos y dinámicos.

Dentro del apartado de variedad también debemos hablar de las distintas formas en que se encuentra almacenada la información médica. Así, aunque por supuesto abundan los datos organizados y estructurados, que pueden ser fácilmente analizados y manipulados por un ordenador, también hay enormes cantidades de datos desestructurados y semiestructurados.[17] Estos últimos son al mismo tiempo una ventaja, pues supone el acceso a un mayor volumen de datos, y una dificultad, porque es difícil procesar esta

[16] Menasalvas, E., Gonzalo, C. y Rodríguez-González, A., "Big Data En Salud: Retos Y Oportunidades", *Economía Industrial*, n. 405, 2017, p. 88.

[17] Raghupathi, W. y Raghupathi, V., *cit.*, p. 4.

información. Por suerte, el *big data* también ofrece herramientas para trabajar con la información de tipo desestructurada.

c. Velocidad

En tercer lugar, llegamos a la uve de la velocidad, que se asocia con la enorme velocidad a la que se genera, se transforma y se transmite la información en la actualidad.[18] De hecho, se puede incluso hablar de que todo el proceso ocurre en tiempo real en múltiples ocasiones. Por supuesto, esta característica también es aplicable a la información médica. Pensemos, por ejemplo, en un sujeto parte de un experimento médico sobre afecciones cardiacas, al que se le proporciona un Apple Watch que envía de manera continua su pulso sanguíneo a un laboratorio, lo que permite un estudio simultáneo de su condición.

La velocidad de los datos clínicos supone un enorme reto para los investigadores, que tienen que adaptarse a un flujo continuo de información, de tal manera que siempre hay algo que investigar, algo que descubrir, algo que no conocen. Sin embargo, también les brinda una enorme oportunidad, pues en uso de las herramientas adecuadas tienen la posibilidad de recibir y procesar información de manera instantánea.

d. Veracidad

La cuarta uve del *big data* es la veracidad, propiedad que hace referencia al hecho de que no toda la información que forma parte de una base de datos de *big data* es veraz. De nuevo, es una característica propia del *big data* en el mundo de la medicina. En concreto, se trata de un desafío: el desafío de la veracidad del *big data* médico. Y es que en el ámbito de la medicina, como en cualquier ámbito científico, se cometen errores; por ejemplo, una equivocación de un médico a la hora de recetar un medicamento o un error de lectura de un instrumento. En consecuencia, se puede asegurar con certeza que una parte de la información que compone el *big data* médico no es veraz, por lo que ésta *"se*

[18] Jee, K. y Kim, G. H., "Potentiality of big data in the medical sector: focus on how to reshape the healthcare system", *Healthcare Informatics Research*, vol. 19, n. 2, 2013, p. 81.

debe interpretar con precaución y en su contexto, si se busca que sea clínicamente útil".[19] Además, por las enormes consecuencias que tienen las decisiones clínicas sobre la vida y la salud de los pacientes, los médicos y profesionales tienen un especial deber de diligencia a la hora de manipular los datos.

e. Valor

Finalmente, la quinta y última uve del *big data* es la uve del valor, que hace referencia a la utilidad y valía indudable del *big data*. De hecho, en el mundo de la medicina, si se usa de manera adecuada, el *big data* puede traer enormes beneficios para los pacientes, investigadores y sistemas de salud, pudiendo mejorar el servicio médico, favorecer los estudios científicos y reducir los costes, entre otras muchas ventajas.[20] Un estudio de la revista Health Affair estima que el *big data* aplicado al mundo de la salud tiene el potencial de generar más de 300 mil millones de dólares al año en concepto de valor adicional para los servicios sanitarios, principalmente gracias a la reducción de costes.[21] Dicho lo cual, el mismo estudio considera que, como paso previo a la generación de dicho valor, es necesario que los legisladores y proveedores de salud definan un nuevo marco en el que se facilite el intercambio de información médica.

2.1.2. Oportunidades que ofrece el big data

Las oportunidades que ofrece el *big data* en el mundo de la medicina son innumerables. De hecho, muchas de ellas todavía son desconocidas, pues el potencial de esta herramienta no ha sido desarrollado plenamente por el momento. Por lo tanto, dado su inabarcabilidad, conviene centrase en algunas de las más interesantes.

---

[19] Litman, R.S., "Complications of laryngeal masks in children: big data comes to pediatric anesthesia", *Anesthesiology*, vol. 119, n. 6, 2013, p. 1239.

[20] Andreu-Perez, J. *et al.*, *cit.*, pp. 1202-1204.

[21] Roski, J., Bo-Linn, G. W. y Andrews, T. A., "Creating Value In Health Care Through Big Data: Opportunities And Policy Implications", *Health Affairs*, vol. 33, n. 7, 2014, p. 1116.

En primer lugar, destacan las posibilidades del *big data* en el ámbito de la salud pública. En este sentido, ya se ha demostrado que el análisis masivo de datos mediante herramientas de *big data* permite monitorizar epidemias o incluso prevenirlas, permitiendo a las autoridades una respuesta rápida y eficaz. Por ejemplo, un estudio de la Universidad de Iowa en el año 2011 se basó en la información del tablón de Twitter para examinar, por un lado, la opinión pública en la red social sobre la propagación de la gripe A, y por otro, la propagación efectiva de la epidemia, encontrando una alta correlación entre ambas mediciones.[22] Por tanto, quedó demostrado el potencial del análisis de las publicaciones de los usuarios en redes sociales para responder a epidemias u otros problemas relacionados con la salud pública. Además, este ejemplo vuelve a demostrar que el *big data* médico no incluye estrictamente datos médicos convencionales, sino que información a priori tan irrelevante desde un punto de vista clínico como puede ser aquella procedente de las redes sociales también puede ser útil.

La genética es otro ámbito donde el *big data* puede contribuir al avance del conocimiento médico. Como consecuencia de las investigaciones llevadas a cabo en el marco del Proyecto Genoma Humano, del que ya se ha hablado, la secuenciación de ADN es una tarea cada vez más asequible, por lo que existe una proliferación de muestras a disposición de los investigadores. De esta forma, como los futuros avances en el área de la genética dependerán en gran parte de la posibilidad de analizar estas muestras de manera masiva, el *big data* se presenta como la herramienta idónea para llevar a cabo esta tarea.[23]

El conocimiento médico también está comenzando a experimentar los beneficios resultantes del desarrollo del *big data*, pues proporciona a los investigadores las herramientas adecuadas para gestionar la información médica. Para entender esta idea, conviene volver a destacar las ingentes cantidades de datos clínicos a disposición de los investigadores que existen hoy en día, en todo tipo de formatos y actualizados en tiempo real. De hecho, la literatura especializada pronostica que para el año 2020 un profesional

---

[22] Signorini, A., Segre, A. M. y Polgreen, P. M., "The Use of Twitter to Track Levels of Disease Activity and Public Concern in the U.S. during the Influenza A H1N1 Pandemic", *PLoS ONE*, vol. 6, n. 5, 2011, pp. 7-9.

[23] O'Driscoll, A., Daugelaite, J. y Sleator, R. D., "Big data, Hadoop and cloud computing in genomics", *Journal of Biomedical Informatics*, vol. 46, n. 5, 2013, p. 775.

de la salud sólo podrá conocer una veinteava parte de toda la información disponible de su especialidad, e incluso menos si nos centramos en las especialidades más generalistas; se habrá generado tanto conocimiento que ni los propios médicos lo podrán dominar.[24] Por este motivo, el *big data* se presenta como la solución ideal, pues suple las limitaciones naturales del conocimiento humano y permite la gestión eficiente del conocimiento, facilitándole a los profesionales de la medicina el acceso al saber científico.

Otra de las indiscutibles ventajas del *big data* es que contribuirá a democratizar el acceso a la medicina en el mundo. En este sentido, De Montalvo señala que "*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"*.[25]

Y es que muchos seres humanos, por no disponer de los recursos económicos suficientes, no pueden acceder a los servicios médicos más avanzados, o incluso ni siquiera a los más básicos. Frente a esto, la digitalización del conocimiento médico se presenta como una prometedora solución, pues abarata enormemente su coste, facilitando así su difusión.[26]

A más abundamiento, el *big data* aplicado al mundo de la salud no solo beneficia a los pacientes en tanto en cuanto que democratiza el acceso a la medicina; también les empodera, pues permite que éstos se conviertan en dueños de sus datos. Hasta ahora, los centros hospitalarios y las aseguradoras, en general grandes multinacionales o entes públicos, han sido los encargados de custodiar la información médica de los pacientes, que no tienen más remedio que confiar en la buena ética profesional de estas entidades. Sin embargo, en el futuro, el paciente puede desarrollar un roll más activo, siendo él mismo el custodio de su información clínica, que podría unir al resto de su información personal (identificación, educación, residencia, etc.), lo que permitiría encontrar patrones y correlaciones interesantes desde un punto de vista médico.[27]

---

[24] Hernández-Medrano, I. y Carrasco, G., "El profesional de la salud ante el mundo del Big Data", *Revista de Calidad Asistencial*, vol. *31*, n. 5, 2016, p. 251.

[25] De Montalvo Jääskeläinen, F. "¿Puede la máquina sustituir al hombre ?", *Razón y Fe*, vol. 278, n. 1436, 2018, p. 327.

[26] Hernández-Medrano, I. y Carrasco, G., *cit.*, p. 251.

[27] Murdoch, T. B. y Detsky, A., "The Inevitable Application of Big Data to Health Care", *Journal of the American Medical Association*, vol. 309, n. 13, p. 1352.

Dicho o cual, no sólo los pacientes disfrutarán de las ventajas del *big data*; se espera que otros agentes de la industria, como las aseguradoras, las farmacéuticas o los grupos hospitalarios, participen también de su potencial. Por tanto, como se prevé que sea una industria que crezca exponencialmente en los próximos años, estos agentes deben adaptar sus tecnologías y herramientas con el objetivo de implementar el *big data* en sus procedimientos, corriendo el riesgo en caso de no hacerlo de renunciar a beneficios estimados de miles de millones de euros.[28]

A modo de cierre de este análisis global de las ventajas que ofrece el *big data* en el campo de la salud, cabe destacar que por supuesto que los beneficiados individuales son muchos, destacando los investigadores, que tendrán mejores herramientas para analizar los datos, o los pacientes, que podrán acceder de una manera democrática a los cuidados que necesitan. Sin embargo, por encima de este beneficio individual, hay un claro ganador: el interés general.

[28] Lavalle, S., Lesser, E., Shockley, R., Hopkins, M. S. y Kruschwitz, N., "Big Data, Analytics and the Path From Insights to Value", *MIT Sloan Management Review*, vol. *52*, 2011, p. 32.

3. RIESGOS DEL *BIG DATA* EN EL ÁMBITO MÉDICO

Pese a las ventajas analizadas en el apartado anterior, amén de otras muchísimas no mencionadas por su carácter inabarcable, el uso del *big data* en el ámbito médico también presenta algunos riesgos que conviene analizar. En relación con este trabajo, son especialmente interesantes aquellos relacionados con el derecho a la intimidad de la persona, pero sin olvidar que el *big data* también provoca problemas en otros ámbitos.

3.1. Riesgos en relación con el derecho a la intimidad

El artículo 18 de la Constitución Española recoge el derecho a la intimidad personal y familiar, mencionado en su apartado cuarto que *"[l]a ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*. Por tanto, se aprecia como ya en la década de los 70 los padres constitucionales previeron los riesgos de un mal uso de la informática en relación con la intimidad de la persona. Este riesgo se ha visto acervado desde entonces, pues el desarrollo tecnológico, además de innumerables ventajas, también ha resultado en un aumento de los ataques que sufre la esfera íntima personal.

En el caso concreto del *big data* en relación con el ámbito médico, los principales problemas se refieren a la falta de consentimiento en el uso de los datos, a las posibles vulneraciones de la privacidad y a la pérdida de la propiedad de la información por parte de los sujetos titulares.

3.1.1. La falta de consentimiento informado

El problema del consentimiento informado en relación con los estudios médicos se refiere a la falta de autorización con conocimiento de causa emitida voluntariamente por un

sujeto para que sus datos clínicos sean empleados en el marco de una investigación científica.[29]

Un ejemplo muy interesante de este problema es el Estudio del Contagio Emocional, una investigación en la que el equipo científico de Facebook buscaba estudiar cómo las emociones expresadas por los usuarios de la red social afectaban a otros, basándose para ello en la información publicada por éstos en su tablón de noticias.[30] Este estudio, con un legítimo interés médico, fue duramente criticado por dos motivos. En primer lugar, la propia investigación informaba de que *"manipuló la medida en que las personas estaban expuestas a expresiones emocionales en su tablón"*.[31] Teniendo en cuanta que el experimentó tuvo un alcance de más de 600.000 personas, surge la inevitable pregunta de si es legal, o cuanto menos ético, que una red social use su poder para manipular el tablón de noticias de más de medio millón de usuarios sin su consentimiento ni conocimiento. Dicho esto, el lector de este trabajo puede pensar, razonablemente, que un usuario que se registra en Facebook acepta unos términos y condiciones al hacerlo que permiten a la compañía llevar a cabo esta clase de investigaciones. Sin embargo, aquí surge el segundo problema del estudio: Kashmir Hill, una periodista de la revista Forbes, descubrió que Facebook no añadió la palabra *investigación* a sus términos de uso hasta cuatro meses después de que hubiese concluido la investigación, pese a que el estudio afirmaba lo contrario.[32] En otras palabras, la compañía utilizó los datos de los usuarios sin que éstos hubiesen prestado su consentimiento informado para participar en un estudio de investigación.

Es interesante destacar que, por lo general, el problema del consentimiento no es un problema de privacidad, sino de autonomía. La gente considera que su información personal (ya sea médica, psicológica o de navegación en internet) es suya, por lo que lo

---

[29] Grady, C., "Enduring and Emerging Challenges of Informed Consent", *The New England Journal of Medicine*, vol. 372, n. 9, 2015, p. 855.

[30] Kramer, A. D. I., Guillory, J. E. y Hancock, J. T., "Experimental evidence of massive-scale emotional contagion through social networks", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 111, n. 24, 2014, p. 8790.

[31] *Ibid.*, p. 8788.

[32] Hill, K., "Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study", *Forbes*, 30 de junio de 2014 (disponible en: https://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/#6b9796777a62; última consulta 26/02/2019).

único que quieren es ser preguntados antes de que ésta sea usada.[33] Por lo tanto, y siempre hablando en términos generales, la mayoría de la población no está en contra de que se use su información para llevar a cabo estudios médicos o de otro tipo, pero creen que se les debe pedir permiso para ello.

Dicho esto, la solución no es tan sencilla como simplemente pedir permiso a la gente. De hecho, pese a que las encuestas parecen corroborar esta predisposición de la población a permitir que los investigadores accedan a su información, la realidad es que muy poca gente consiente efectivamente tal acceso cuando se les solicita.[34]

Por otra parte, incluso si asumimos que la mayoría simplemente quiere que se les pida permiso para acceder a sus datos, surge la pregunta de cómo se debe pedir dicho consentimiento. Un estudio publicado en el American Journal of Medical Sciences demuestra que los pacientes a los que se les pide el consentimiento no suelen ni siquiera tomarse la molestia de leer los documentos en donde se les solicita porque los consideran incomprensibles y, si lo intentan, suelen afirmar que se tratan de textos legales ilegibles.[35] Al igual que es indudable que la desidia o el desconocimiento de los pacientes no justifica que los investigadores usen su información sin su permiso, también es indudable que las investigaciones son beneficiosas para la humanidad. Por lo tanto, es necesario llegar a una avenencia donde se protejan los derechos de los individuos, pero también el interés general.

El consentimiento también presenta otro problema muy específico en relación con el *big data* médico. En este sentido, ya se ha mencionado que las herramientas para analizar el *big data* buscan encontrar correlaciones entre los datos, pero muchas veces estas correlaciones son imprevisibles. Por este motivo, resulta imposible solicitar el consentimiento de los sujetos para usar su información, pues ni siquiera aquellos que recogen la información saben los posibles usos que ésta puede tener o las correlaciones

---

[33] Rothstein, M. A., "Ethical Issues in Big Data Health Research: Currents in Contemporary Bioethics", *The Journal of Law, Medicine & Ethics*, vol. 43, n. 2, 2015, p. 427.

[34] Topol, E. J., "The big medical data miss: challenges in establishing an open medical resource", *Nature Reviews Genetics*, vol. 16, n. 5, 2015, p. 254.

[35] Henderson, G., "Is Informed Consent Broken?", *American Journal of Medical Sciences*, vol. 342, n. 4, 2011, p. 271.

que van a averiguar.[36] De hecho, ni siquiera se podría solicitar el consentimiento para "posibles investigaciones futuras", pues si son desconocidas en el momento en el que éste se presta, no sería un consentimiento específico, explícito y libre, por lo que se consideraría inválido.[37]

Por ejemplo, imaginemos una mujer de 53 años que se hace un análisis de sangre en una revisión rutinaria en el año 2009. Una década más tarde, un médico investiga una posible correlación entre el cáncer de mama en mujeres mayores de 50 años y niveles bajos de vitamina D. Si ese médico quiere llevar a cabo un estudio de muestras de sangre para comprobar empíricamente su descubrimiento, surgiría un problema fundamental: es imposible que la mujer, al hacerse los análisis en 2009, hubiese prestado su consentimiento para que se usase su información en una investigación sobre el cáncer del año 2019. Además, en el caso de que hubiese prestado su consentimiento para cualquier investigación futura, dicho consentimiento no se podría considerar informado, por lo que sería inválido.

Imaginemos que el investigador, ante la falta de consentimiento válido en el 2009, decide buscar a esa persona para conseguir el consentimiento en 2019. Claramente, es una solución poco razonable, pues sería un proceso laborioso, caro y cuyo resultado es incierto. Además, no sólo tendría que obtener el consentimiento de dicha mujer, sino también el del resto de sujetos parte del estudio. Por lo tanto, se puede señalar un nuevo inconveniente del consentimiento: conseguirlo *a posteriori* es una tarea tremendamente laboriosa o incluso imposible.[38]

Conviene destacar una última dificultad en relación con el consentimiento: el conocido como sesgo del consentimiento. Es un problema que, de acuerdo con la Academia Nacional de Medicina, se produce cuando *"los sujetos que dan permiso para que se acceda a su información médica difieren del grupo de individuos que se muestran*

---

[36] Mittelstadt, B. D. y Floridi, L., "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts", *Science and Engineering Ethics*, vol. 22, n. 2, 2016, pp. 312-316.

[37] Mostert, M., Bredenoord, A. L., Biesaart, M. C. I. H. y van Delden, J. J. M., "Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach", *European Journal of Human Genetics*, vol. 24, n. 7, 2016, p. 957.

[38] *Ibídem*.

contrarios a dar permiso a que su información médica se use en investigación".[39] Es decir, los grupos compuestos por aquellos dispuestos a ceder su información médica en el marco de una investigación tienden a ser distintos de los compuestos por aquellos que se oponen (por ejemplo, habrá más jóvenes entre el grupo que cede su información y más ancianos entre el grupo que se opone). Es fácil comprender los peligros que entraña este sesgo en relación con la investigación médica, pudiendo conducir, por ejemplo, a correlaciones espurias.

Para concluir con este epígrafe, cabe señalar que hoy en día existen nuevas fórmulas de consentimiento que, precisamente, buscan solucionar los problemas que se han señalado y conciliar el interés individual y el interés general. En concreto, destacan el *broad consent*, el *dynamic consent* y el *opt-out consent*, conceptos que se analizarán en detalla en el sexto capitulo, cuando se discuta el nuevo paradigma del consentimiento en la investigación médica.

3.1.2. Las violaciones de la privacidad. La anonimización de los datos.

El uso de datos médicos para la investigación y el derecho a la intimidad de los sujetos también entran en conflicto con el derecho de la persona a la privacidad. Así, Markowetz *et al.* señalan que, a pesar de los innumerables beneficios del *big data* en el ámbito médico, esta herramienta puede ser un arma muy peligrosa en las manos equivocadas.[40] En concreto, estos autores destacan que permite conocer a una persona hasta desnudarla, de tal manera que, por ejemplo, una aseguradora podría usar esa información médica privada para rechazar a un solicitante. Realmente, de lo que se está hablando es de una invasión en toda regla de la esfera privada e íntima de la persona. Este problema es fruto del enorme volumen de información que abarca el *big data*. Al final, es una tecnología que *"absorbe una masiva cantidad de datos generados por un usuario* […] *susceptibles de ofrecer una visión de la persona que supera con mucho al conocimiento que la persona*

[39] Institute of Medicine, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*, The National Academies Press, Washington, D.C., 2009, p. 209.

[40] Markowetz, A., Błaszkiewicz, K., Montag, C., Switala, C. y Schlaepfer, T. E., "Psycho-Informatics: Big Data shaping modern psychometrics", *Medical Hypotheses*, vol. 82, n. 4, 2014, p. 405.

tiene de sí misma".[41] De este modo, la máquina puede llegar a saber más sobre la persona que la propia persona.

Uno de los métodos tradicionales que se ha empleado para asegurar la privacidad de la información de los individuos es la anonimización. Con este término se hace referencia a *"todas aquellas técnicas empleadas para proteger la identidad de los individuos en un conjunto de datos"*.[42] Una de las principales ventajas de los datos que han sido anonimizados es que no se consideran datos personales, por lo que no es necesario que su tratamiento cumpla los requisitos que fija la legislación de los distintos Estados para el tratamiento de datos personales.[43]

Sin embargo, un informe del Comité Internacional de Bioética sostiene que la anonimización tal y como se entiende hoy en día puede no ser suficiente para proteger la identidad de los titulares de la información en la era del *big data*.[44] En concreto, el estudio menciona el problema de la reidentificación, según el cual, al tener el *big data* acceso a ingentes cantidades de información, es posible que se encuentren correlaciones entre los datos anonimizados que posibiliten identificar al sujeto titular de los mismos.

Dicho esto, la anonimización irreversible también es posible, pero igualmente causa problemas en relación con la investigación médica. En concreto, supone la renuncia a la correlación de los datos clínicos con su titular o con alguna variable importante para el estudio, además de que hace imposible la actualización temporal de los datos, pues no se sabe de quién es cada uno.[45] Existe una solución a este problema, la seudonimización, que será analizada en detalle en el sexto capítulo del trabajo.

El *big data* y la privacidad también pueden entrar en conflicto en relación con los grupos. A medida que las bases de datos disponen de más y más información, es fácil hacer perfiles de conjuntos sujetos que, aunque anónimos de manera individual, presentan unas

---

[41] Hernández-Medrano, I. y Carrasco, G., *cit.*, p. 253.

[42] El Emam, K. y Arbuckle, L., *Anonymizing health data: case studies and methods to get you started*, O'Reilly, Sebastopol, 2013, p. 4.

[43] Ziegler, S., Evequoz, E. y Huamani, A. M. P., "The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities" en Aagaard, A. (Ed.), *Digital Business Models*, Cham, Springer International Publishing, 2019, p. 210.

[44] Comité Internacional de Bioética, *cit.*, p. 14.

[45] Mostert, M. *et al*., "Big Data in…", *cit.*, p. 958.

características comunes por su condición de miembros de un grupo.[46] De este modo, si se produce un ataque al grupo, son sus miembros individuales los que sufren las consecuencias de dicha agresión. Por ejemplo, el análisis de los datos de un conjunto de individuos anonimizados puede encontrar una correlación entre un determinado gen y la obesidad, de tal manera que una aseguradora que accediese a dichos datos podría basarse en la información de dicho perfil para rechazar a los solicitantes que presentan el gen, aunque no padezcan de sobrepeso, simplemente por el riesgo de que pueda ocurrir. De este modo, pese a que no se revelaría la identidad de ningún individuo de la muestra, éstos sufrirían las consecuencias directas de la decisión tomada.

Fruto de estos problemas de privacidad, que dependen fundamentalmente de la recolección masiva de datos, se puede llegar incluso a hablar de que la mera recolección indiscriminada puede vulnerar también la privacidad de las personas. Y es que a pesar de que la obtención de información ha estado limitada tradicionalmente por la propia percepción humana, el individuo no es consciente en la actualidad de cuándo puede estar generando datos susceptibles de uso no intencionado por su parte.[47]

3.1.3. La propiedad de la información

También constituye un grave atentado contra la intimidad de la persona un uso no autorizado de su información personal. Así, mientras que en el primer epígrafe de este capítulo se señalaron los problemas del uso no consentido de los datos del interesado, en este caso se habla de un uso consentido de dichos datos, pero para otro fin totalmente ajeno al autorizado. Sucede así que el individuo, al ceder los datos para un uso concreto (por ejemplo, una investigación sobre enfermedades cardiovasculares), pierde totalmente la propiedad de los mismos, pasando éstos a pertenecer a grandes instituciones, como multinacionales, gobiernos o centros académicos. De hecho, un estudio de la Universidad de Harvard acerca de los riesgos de la confidencialidad en relación con la investigación genómica descubrió que más de la mitad de los sujetos participantes estaban

---

[46] Mittelstadt, B., "From Individual to Group Privacy in Biomedical Big Data", en Cohen, I., Lynch, H., Vayena, E. y Gasser, U. (eds.), *Big Data, Health Law, and Bioethics*, Cambridge University Press, Cambridge, 2018, p. 176.

[47] Mittelstadt, B. D. y Floridi, L., *cit*, p. 318.

especialmente concernidos por un posible uso no deseado de su información.[48] Esto representa un grave riesgo para la investigación médica, pues si los pacientes tienen la sensación de que su información cedida va a ser usada ilegítimamente, lo más probable es que se nieguen a aportarla.

La pérdida de la propiedad también es un tema conflictivo cuando es el propio sujeto titular de la información y no un tercero el que quiere acceder a sus datos y beneficiarse de los mismos.[49] En la gran mayoría de los casos, cuando una persona cede sus datos médicos para una investigación, no tiene derecho a emplear dichos datos o recuperarlos, ni tampoco tiene por qué resultar beneficiado por el estudio en el que son empleados. Por tanto, si hablamos del derecho a la propiedad, también deberíamos hablar del derecho del sujeto a acceder a su información para modificarla, eliminarla o emplearla para cualquier otro uso que desee.

A este respecto, sin embargo, cabe oponer que el *big data* en el contexto de la medicina difiere sustancialmente del *big data* en general. Es un ámbito donde, por supuesto, hay que proteger el derecho a la privacidad de los sujetos titulares de la información en la medida de lo posible, pero donde también hay un claro interés de salud pública que merece ser protegido. Por ello, como el *big data* médico tiene una clara función de interés general, pues sus segundos usos pueden estar orientados hacia la salud pública, su tratamiento tiene que ser diferente.[50] Esto no sucede, por ejemplo, con el *big data* de las redes sociales, cuyos segundos usos suelen estar relacionados con la publicidad, por lo que el sujeto titular de los datos merece una protección especial.

---

[48] Beskow, L., Hammack, C., Brelsford, K. y McKenna, K., "Thought-Leader Perspectives on Risks in Precision Medicine Research" en Cohen, I., Lynch, H., Vayena, E. y Gasser, U. (eds.), *Big Data, Health Law, and Bioethics*, Cambridge University Press, Cambridge, 2018, p. 167.

[49] Tene, O. y Polonetsky, J., "Big Data for All: Privacy and User Control in the Age of Analytics", *Northwestern Journal of Technology and Intellectual Property*, vol. 11, n. 5, 2013, p. 260.

[50] Vayena, E., Salathé, M., Madoff, L. C. y Brownstein, J. S., "Ethical Challenges of Big Data in Public Health", *PLoS Computational Biology*, vol. 11, n. 2, 2015, pp. 2-3.

3.2. Otros riesgos

Tras haber analizado los principales riesgos del *big data* en el ámbito médico en relación con el derecho a la intimidad, conviene mencionar brevemente otros problemas que presenta esta tecnología.

Cabe señalar, en primer lugar, el hecho de que se trata de una herramienta poco madura, que se encuentra todavía en una etapa inicial de su desarrollo, por lo que puede presentar fallos y errores importantes. Por poner un ejemplo, Google desarrolló a principios de esta década una tecnología, *Google Flu Trends*, que estimaba el número de visitas a hospitales de pacientes con gripe en una determinada región mediante el análisis de *big data*.[51] En el año 2013, numerosos periódicos y revistas se hicieron eco de que esta herramienta estaba estimando más del doble de casos de los que efectivamente se estaban produciendo.[52] Realmente, este error no tuvo consecuencias médicas graves, pero puso de manifiesto que incluso una compañía como Google, siempre a la vanguardia del desarrollo tecnológico, pueda cometer fallos graves. Por tanto, es inevitable pensar en la posibilidad de que en el mundo de la medicina puedan producirse errores con graves consecuencias para los pacientes. Por este motivo, algunos autores sostienen que la intervención humana siempre es necesaria, pues *"la máquina ayuda, pero nunca sustituye; mejora, pero no completa el análisis y las conclusiones"*.[53]

Para concluir, hay que destacar que la mayoría de los inconvenientes que se han señalado tienen relación con la información excesiva que existe sobre la persona en las bases de datos. Sin embargo, paradójicamente, también hay quien habla de que el *big data* no es lo suficientemente grande. En este sentido, ya se han desarrollado en detalle algunos de los enormes beneficios para la salud que presenta esta tecnología. Desgraciadamente, puede que estos avances no lleguen por igual a toda la población, pues el *big data* contiene mucha menos información sobre algunos grupos sociales, como las minorías raciales o aquellos con menos recursos, que suelen carecer de seguros médicos privados o no acceden con la misma facilidad a los sistemas públicos de salud en aquellos países donde

---

[51] Información obtenida de la página web de Google Flu Trends: https://www.google.org/flutrends/about/.

[52] Lazer, D., Kennedy, R., King, G. y Vespignani, A., "The Parable of Google Flu: Traps in Big Data Analysis", *Science*, vol. 343, n. 6176, 2014, p. 1203.

[53] De Montalvo Jääskeläinen, F., *cit.*, p. 325.

no es universal.[54] Así, como no se genera tanta información sobre ellos, el *big data* no les beneficia por igual. Por lo tanto, las autoridades e instituciones competentes deben impulsar las medidas adecuadas para democratizar el *big data* en el ámbito de la medicina.

[54] Malanga, S., Loe, J., Robertson, C. y Ramos, K., "Who's Left Out of Big Data?" en Cohen, I., Lynch, H., Vayena, E. y Gasser, U. (eds.), *Big Data, Health Law, and Bioethics*, Cambridge University Press, Cambridge, 2018, pp. 101-103.

4. UN RECORRIDO A TRAVÉS DE LA HISTORIA DE LA PROTECCIÓN DE DATOS

Una vez analizadas las ventajas e inconvenientes del uso de los datos personales en el ámbito médico, queda claro que existe un conflicto entre dos posturas legítimas. Por un lado, se ha demostrado la necesidad del uso y análisis de dicha información mediante herramientas de *big data*, pues los beneficios para el interés general y la investigación médica que aportan son innumerables. Al mismo tiempo, también es obvio que el *big data* es un arma de doble filo que presenta graves riesgos con respecto al derecho a la intimidad.

A pesar de que este trabajo se ha centrado, principalmente, en las ventajas y riesgos del uso del *big data* en la medicina, este conflicto entre el interés general y el interés particular en relación con los datos personales ya existía antes del surgimiento de esta tecnología. Además, es un conflicto presente en multitud de sectores, no sólo en el mundo de la medicina. Por ello, en la segunda mitad del siglo XX comenzaron a surgir iniciativas de protección de datos que planteaban distintas soluciones. Por su especial incidencia en el ordenamiento jurídico español, se desarrollarán a continuación dos normas históricas de protección de datos, ambas ya derogadas: la Directiva de Protección de Datos y la Ley Orgánica de Protección de Datos de 1999. Además, se comentará sucintamente la sentencia del Tribunal Constitucional 290/2000[55] (en adelante, "la STC 290/2000"), que declaró la inconstitucionalidad de dos artículos de la Ley Orgánica de 1999.

4.1. La Directiva de Protección de Datos

Antes de la promulgación de la Directiva de Protección de Datos, hubo unas primeras aproximaciones a la regulación de la protección de datos en Europa, tanto a nivel regional como nacional. Así, en la década de los setenta, Suecia y el estado federado alemán de Hesse aprobaron sendos estatutos de protección de datos.[56] A partir de este hito, diversas naciones europeas sancionaron sus propias normas de protección de datos, hasta que en

[55] Sentencia del Tribunal Constitucional de 30 de noviembre, 290/2000.

[56] Blume, P., "An EEC Policy for Data Protection", *Computer Law Journal*, vol. 11, n. 3, 1992, pp. 399 y 401.

1980 surgió la primera gran iniciativa internacional, cuando la OCDE publicó las *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales*.[57] Tras alguna otra iniciativa menor a nivel nacional e internacional, la Comisión Europea publicó finalmente en 1990 el borrador de lo que se acabaría convirtiendo en 1995 en la Directiva de Protección de Datos.[58]

4.1.1. El marco normativo de la Directiva de Protección de Datos

La Directiva fue un documento tremendamente novedoso del que destaca, en primer lugar, la definición amplia y general que se dio a los conceptos de "datos personales" (*"toda información sobre una persona física identificada o identificable"*) y de "tratamiento de datos personales" (*"cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales"*).[59] De este modo, queda claro que la norma buscaba que su regulación tuviese un amplio alcance, afectando a virtualmente cualquier tipo de operación de tratamiento de datos personales.

Con respecto a los principios relativos a la calidad de los datos, el artículo 6 de la Directiva ordenaba a los Estados miembros que se encargasen de que los datos personales fuesen *"tratados de manera leal y lícita [y] recogidos con fines determinados, explícitos y legítimos, y no […] tratados posteriormente de manera incompatible con dichos fines"*. Dicho esto, el mismo artículo afirmaba que un tratamiento posterior para fines científicos no se consideraba incompatible. El artículo 7 continuaba con los principios relativos al tratamiento legítimo de los datos, exigiendo que el interesado hubiese prestado su consentimiento, que fuese algo jurídicamente exigible o que se buscase proteger el *"interés vital del interesado"*, el *"interés público"* o el *"interés legítimo perseguido por el responsable del tratamiento"*. Asimismo, en su artículo 8, la Directiva se pronunciaba

---

[57] Cate, F. H., "The EU Data Protection Directive, Information Privacy, and the Public Interest", *Iowa Law Review*, vol. 80, 1994, p. 431.

[58] Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (92), 18 de octubre de 1992, 422 final.

[59] *Vid*: Directiva 95/46/CE, *cit.*, arts. 2.a) y 2.b).

sobre el tratamiento de algunas categorías especiales de datos, como aquellos que revelasen el origen racial o las opiniones políticas de su titular.

Este texto legal también fue innovador en cuanto al catálogo de derechos que reconocía al sujeto titular de los datos, compuesto por el derecho de información, el derecho de acceso a los datos, el derecho de rectificación, el derecho de oposición y el derecho de no sometimiento a decisiones automatizadas.[60] Cabe hacer especial hincapié en el último de ellos, que la Directiva de Protección de Datos enunciaba como el derecho de las personas *"a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos"*.[61] Este derecho guarda una íntima relación con el problema mencionado en el capítulo anterior acerca de que el *big data* es todavía una tecnología reciente, por lo que puede conducir a errores. De este modo, resulta interesante descubrir que ya en 1995 existían mecanismos legales para proteger a los más desconfiados y reticentes de las nuevas tecnologías, que podían oponerse a verse sometidos a decisiones automatizadas.

4.1.2. Valoración de la Directiva de Protección de Datos

En el año 2009, la Oficina del Comisario de Información preparó un informe en el que se analizaba el impacto de la Directiva.[62] Por un lado, destacaba sus principales fortalezas, resaltando el hecho de que se trataba de un texto exhaustivo, ampliamente redactado y que establecía un marco básico de protección que dibujó unos altos estándares de protección de los datos de las personas, llegando incluso a considerarse un derecho humano.[63] Sin embargo, el informe también examinaba profusamente sus principales carencias, señalando sus objetivos poco claros y un enfoque insuficiente en detrimento, riesgo y aplicación práctica.[64]

---

[60] *Vid*: Directiva 95/46/CE, *cit.*, arts. 10-15.

[61] *Vid*: Directiva 95/46/CE, *cit.*, art. 15.

[62] Robinson, N., Graux, H., Botterman, M. y Valeri, L. *"Review of the EU Data Protection Directive: Summary"*, *Oficina del Comisionado de Información*, 2009.

[63] *Ibid.*, p. 9.

[64] *Ibídem*.

También hay quien opinaba que la Directiva era un texto obsoleto para el siglo XXI, pues su marco legal se planteó creyendo que la informática era mucho más limitada y rastreable.[65] La elección de la figura de la directiva frente a la del reglamento también fue un hecho cuestionado en su momento, pues la concesión de amplias prerrogativas de desarrollo a los Estados se tradujo en una inevitable desarmonización.[66]

Una de las principales críticas a la Directiva llegó procedente de Estados Unidos, cuando la norma acababa de entrar en vigor, pues las empresas de origen estadounidense temían que la norma les prohibiese enviar información de sus clientes a sus sedes en el continente americano, aunque ésta hubiese sido recolectada ética y legalmente.[67] Por suerte, en el año 2000, la Comisión Europea y el Departamento de Comercio estadounidense crearon un programa de "puerto seguro" que permitía a las empresas americanas hacer negocios en Europa si se comprometían a una serie de prácticas garantes de los derechos de los particulares.[68]

En global, gracias a sus fortalezas y a pesar de sus carencias, se considera que la Directiva de Protección de Datos fue un documento con una enorme trascendencia. De hecho, inspiró sustancialmente las normas de protección de datos de otros muchos Estados, como Australia, Israel y Japón.[69]

4.2. La Ley Orgánica de Protección de Datos de 1999

En 1992, España aprobó su primera norma de protección de datos, la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los datos de carácter personal,[70] que desarrollaba por primera vez el artículo 18.4 de la CE. Sin embargo, una vez se aprobó la

---

[65] Omer T, "Privacy: The new generations", *International Data Privacy Law*, vol. 1, n. 1, 2011, p. 15.

[66] De Hert, P. y Papakonstantinou, V., "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, vol. 28, n. 2, 2012, p. 132.

[67] Cate, F. H., *cit.*, p. 437.

[68] Birnhack, M. D., "The EU Data Protection Directive: An engine of a global regime", *Computer Law & Security Review*, vol. 24, n. 6, 2008, p. 515.

[69] *Ibid.*, pp. 512-514.

[70] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE 31 de octubre de 1992).

Directiva de Protección de Datos en 1995 y dadas las evidentes discrepancias entre esta norma y la española, se decidió elaborar una nueva ley orgánica: la Ley Orgánica de Protección de Datos de 1999.

Desgraciadamente, este proceso y su resultado fueron, cuanto menos, deficientes. De hecho, para hacerse una idea de la falta de interés del legislador español en adaptar el ordenamiento interno a la nueva norma europea, es interesante destacar que el Parlamento esperó para transponer la Directiva *"a que se agotara en su práctica totalidad el plazo de tres años previsto por la propia Directiva para que los Estados dieran cumplimiento a lo en ella establecido"*.[71] A más abundamiento, la norma ni siquiera contó con la correspondiente exposición de motivos, por lo que el legislador incumplió su deber de informar a los ciudadanos de que la aprobación de la Ley Orgánica de 1999 era la consecuencia de una obligación de la Directiva de Protección de Datos.[72]

También se puede apreciar la baja calidad legislativa de la Ley Orgánica de 1999 en que, en general, era bastante similar a la Directiva, llegando incluso a copiar literalmente partes de su articulado. Lo que es peor es que algunas de las diferencias que introdujo la norma española supusieron un claro retroceso. Por poner un ejemplo, el Título IV de la norma nacional distinguía entre los ficheros de titularidad pública y los ficheros de titularidad privada, previendo una regulación algo más laxa para los segundos. Sin embargo, la Directiva no contemplaba tal distinción, *"[c]onsiderando que los principios de la protección deben aplicarse a todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario"*.[73] Realmente, no existía una justificación razonable para flexibilizar la protección de los ficheros de titularidad privada, especialmente si se tiene en cuenta que las grandes multinacionales podían –y pueden– llegar a tener incluso más poder que el propio poder público. [74] Por lo tanto, las amenazas a la intimidad de los particulares procedentes del sector privado merecían, como mínimo, la misma protección

---

[71] Murillo de la Cueva, P. L., "La construcción del derecho a la autodeterminación informativa", *Revista de estudios políticos*, n. 104, 1999, p. 59.

[72] Sánchez Bravo, Á., "La Ley Orgánica 15/1999, de Protección de datos de carácter personal: diez consideraciones en torno a su contenido", *Revista de Estudios Políticos*, n. 111, 2001, p. 205.

[73] *Vid*: Directiva 95/46/CE, *cit*., considerando 12.

[74] Pérez Luño, A. E., *Manual de informática y derecho*, Ariel, Barcelona, 1996, p. 74.

que las amenazas del sector público, protección que fue negada por la Ley Orgánica de 1999.

Dicho todo esto, la mayor demostración de la imperfección de esta norma fue la declaración de inconstitucionalidad de dos de sus artículos a raíz de la STC 292/2000, que merece un análisis específico.

4.3. La STC 292/2000

La STC 292/2000 fue la respuesta del Tribunal Constitucional al recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo respecto de los artículos 21.1 y 24 de la Ley Orgánica de Protección de Datos de 1999.

El primero de estos artículos afirmaba que las Administraciones públicas podían comunicar a otras Administraciones públicas los datos de carácter personal de los particulares *"cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso"*.[75] El Defensor del Pueblo argumentó que dicho artículo abría la puerta a que una norma de rango inferior a ley consintiese la cesión de datos personales de los particulares, lo que contravenía el artículo 53.1 de la CE, que afirma que sólo por ley se pueden regular los derechos y libertades recogidos en el capítulo segundo de la norma fundamental.[76] Como no podía ser de otra manera, el Tribunal Constitucional declaró la inconstitucionalidad del citado artículo.[77]

Por su parte, el artículo 24 fue recurrido por el Defensor del Pueblo porque consideró que abría la posibilidad a que se limitasen los derechos de los ciudadanos sin demarcar claramente las instancias en que aquello podía ocurrir, pues la norma empleaba una serie de conceptos jurídicos indeterminados para hacer referencia a las situaciones que justificaban dicha medida. Por ejemplo, permitía excepcionar el derecho de información del afectado cuando su ejercicio "*impida o dificulte gravemente el cumplimiento de las*

---

[75] *Vid*: Ley Orgánica 5/1992, *cit.*, art. 21.1.

[76] Alguacil González-Aurioles, J., "La libertad informática: aspectos sustantivos y competenciales (SS.T.C 290 y 292/2000)", *Teoría y Realidad Constitucional*, n. 7, 2001, p. 384.

[77] *Vid*: Sentencia del Tribunal…, *cit.*, f.j. 14.

funciones de control y verificación de las Administraciones públicas", sin aclarar cuándo se podía considerar que aquello ocurría.[78] Ante este atropello, el Tribunal Constitucional determinó también la inconstitucionalidad del artículo, aclarando que la ley debe delimitar con precisión los supuestos en que un derecho fundamental queda restringido, quedando en caso contrario el individuo a merced de aquel que la aplica.[79]

En cualquier caso, lo más interesante de esta sentencia es que el Tribunal Constitucional afirmó que "*el derecho fundamental a la intimidad (art. 18.1 CE) no aport[a] por sí sólo una protección suficiente frente a esta nueva realidad derivada del progreso tecnológico"*.[80] Por este motivo, reconoce el derecho fundamental a la protección de datos, derecho establecido en el artículo 18.4 de la CE y desarrollado por la Ley Orgánica de 1999, que busca que la persona tenga *"un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"*.[81]

[78] *Vid*: Ley Orgánica 5/1992, *cit*., art. 24.1.
[79] *Vid*: Sentencia del Tribunal…, *cit.*, f.j. 15.
[80] *Ibid.*, f.j. 4.
[81] *Ibid.*, f.j. 6.

5. EL NUEVO REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El 25 de mayo de 2016 entró en vigor en todo el territorio de la Unión Europea el nuevo Reglamento General de Protección de Datos, un texto legal que derogó la anterior Directiva de Protección de Datos y ha creado un nuevo escenario para la protección de los datos personales de los ciudadanos europeos.

5.1. El porqué del Reglamento General de Protección de Datos

De entre todos los problemas de la Directiva de Protección de Datos que se han analizado en el capítulo anterior, la necesidad de reforma se debe principalmente a dos. Por una parte, su obsolescencia tecnológica, considerándose que ya no era el documento óptimo para abordar los problemas provocados por los últimos avances tecnológicos, como el *big data* o el potencial de los motores de búsqueda. Por otra, el tipo de norma, pues el uso de la figura legal de la directiva frente a la del reglamento derivó en una inevitable desarmonización regulatoria entre los distintos Estados miembros.

Ante este panorama, la Comisión Europea propuso en 2012 iniciar un procedimiento para definir un nuevo marco normativo europeo en materia de protección de datos, determinándose que la figura legal adecuada para este nuevo proyecto era la del reglamento.[82] Durante los cuatro años siguientes, la Comisión, el Parlamento y el Consejo se intercambiaron distintos planes y borradores, hasta que el 4 de mayo de 2016 se publicó definitivamente el nuevo Reglamento General de Protección de Datos en el Diario Oficial de la Unión Europea.[83] Dicho lo cual, con el objetivo de que los Estados, las instituciones europeas y cualquier interesado tuviese tiempo de adaptarse al nuevo régimen legal, se retrasó su aplicación hasta el 25 de mayo de 2018.[84]

Para finalizar con el estudio del porqué del Reglamento, es importante volver a destacar la importancia del tipo de norma empleado, el reglamento, que persigue un doble objetivo. En primer lugar, un reglamento, a diferencia de una directiva, limita enormemente la

---

[82] Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century, COM (2012), 3 de septiembre de 2012, 9 final.

[83] *Vid*: Reglamento (UE) 2016/679, *cit*.

[84] *Ibid.*, art. 99.2.

autonomía legislativa de los Estados miembros, por lo que es claro que su uso persigue una fuerte armonización en materia de protección de datos a nivel europeo.[85] Este primer objetivo nos lleva al segundo: el Reglamento demuestra un cambio de concepción respecto a la protección de datos, que deja de considerarse un problema nacional e individual de los Estados para pasar a ser una preocupación conjunta de la Unión.[86]

5.2. El marco normativo del Reglamento General de Protección de Datos

5.2.1. Definición de datos personales

En líneas generales, la definición de datos personales que recoge el Reglamento es muy similar a la propia de la Directiva. De hecho, el inicio de la definición es el mismo en ambos documentos: *"datos personales"* es *"toda información sobre una persona física identificada o identificable"*.[87]

Dicho esto, el Reglamento introduce algunos matices, como el reconocimiento de que una persona también tiene una *"identidad genética"*, algo que no contemplaba la Directiva. Además, el Reglamento también busca aclarar cuándo se considera que una persona física está identificada, señalando el recital 26 que debe analizarse *"si existe una probabilidad de que se utilicen medios para identificar a una persona física [teniendo] en cuenta todos los factores"*. Este aspecto guarda relación con uno de los problemas del *big data* anteriormente destacados: el análisis de ingentes cantidades de datos hace posible identificar, en algunas circunstancias, a personas cuyos datos estaban, en teoría, anonimizados. Por lo tanto, el Reglamento busca atajar este problema, obligando a que se tengan en cuenta factores tecnológicos, como el *big data*, a la hora de valorar si una serie de datos merecen o no el calificativo de datos personales.

---

[85] De Hert, P. y Papakonstantinou, V., "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", *Computer Law & Security Review*, vol. 32, n. 2, p. 182.

[86] *Ibídem*.

[87] *Vid*: Reglamento (UE) 2016/679, *cit*. art. 4.1).

5.2.2. Principios

En cuanto a los principios que recoge el capítulo II del Reglamento, conviene acudir, en primer lugar, a los principios relativos al tratamiento. El articulado del Reglamento vuelve a ser notablemente similar al de la Directiva, pero destacando además algunas matizaciones o profundizaciones. Así, a la exigencia de la Directiva de que los datos fuesen "*tratados de manera leal y lícita"*,[88] el Reglamento ordena que dicho tratamiento también sea *"transparente en relación con el interesado"*.[89] De igual manera, mientras que la Directiva buscaba que los datos fueran *"adecuados, pertinentes y no excesivos"*,[90] el Reglamento se centra en que estos sean *"adecuados, pertinentes y limitados a lo necesario en relación con los fines"*.[91] Por lo tanto, el Reglamento introduce dos nuevos principios relativos al tratamiento en estos dos artículos, el principio de transparencia y el principio de minimización, que fijan restricciones y obligaciones con respecto al uso de datos personales, buscando una mayor protección de su titular.

En segundo lugar, el capítulo II del Reglamento también destaca una serie de principios sobre la licitud del tratamiento. Así, el primer apartado del artículo 6 se pronuncia en términos similares al artículo 7 de la Directiva, indicando que el tratamiento de datos personales sólo será lícito si responde al consentimiento previo del interesado, a una obligación legal o contractual o a la protección de intereses vitales del interesado, del interés público o de un interés legítimo del responsable del tratamiento. En cambio, el Reglamento sí que introduce una novedad en los apartados segundo y tercero del artículo 6, exigiendo un desarrollo legislativo en los Estados miembros o en la Unión cuando el tratamiento responda a una obligación legal o a la protección del interés general. De esta manera, aunque se use la figura legal del reglamento, se les sigue concediendo a los Estados miembros un cierto nivel de autonomía en materia de protección de datos, aunque indudablemente inferior a la que existía con la Directiva.

Finalmente, es interesante detenerse a analizar el régimen introducido por el Reglamento sobre las condiciones de manifestación del consentimiento por parte del interesado acerca

---

[88] *Vid*: Directiva 95/46/CE, *cit.*, art. 6.1.a).

[89] *Vid*: Reglamento (UE) 2016/679, *cit.*, art. 5.1.a).

[90] *Vid*: Directiva 95/46/CE, *cit.*, art. 6.1.c).

[91] *Vid*: Reglamento (UE) 2016/679, *cit.*, art. 5.1.c).

del uso de sus datos personales. Es un régimen totalmente novedoso, pues la Directiva no se pronunciaba en absoluto sobre este asunto. Uno de los aspectos más interesante de la nueva regulación es que el Reglamento exige que el responsable sea capaz de demostrar que el titular de los datos prestó su consentimiento para el tratamiento.[92] Además, "*[s]i el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos"*.[93] Al hacer esto, la norma busca atajar solicitudes de consentimiento confusas, ininteligibles o perdidas en extensos documentos de términos y condiciones. En último lugar, el Reglamento también le permite al interesado *"retirar su consentimiento en cualquier momento"*, operación que debe ser tan fácil como fue el proceso de prestarlo.[94]

5.2.3. Derechos del interesado

Como se ha señalado anteriormente, la Directiva ya recogía un decálogo relativamente detallado de derechos del interesado, teniendo éste la potestad de informarse, de acceder a los datos, de exigir su rectificación, de oponerse a ciertos tratamientos y de no verse sometido a decisiones automatizadas. El Reglamento, como no podía ser de otra manera, incluye todos estos derechos, desarrollándolos en mayor profundidad. Por ejemplo, en relación con el derecho de información del interesado, a los requisitos ya incluidos en la Directiva se añade la obligación de proporcionarle al interesado *"información necesaria para garantizar un tratamiento de datos leal y transparente"*.[95]

Pero eso no es todo; el Reglamento también presenta nuevas incorporaciones al catálogo de derechos, de entre los que cabe destacar dos: el derecho de transparencia y el derecho al olvido. El primero de estos es un mandato a los responsables del tratamiento de los datos personales, según el cual éstos deben tomar *"las medidas oportunas para facilitar al interesado toda información indicada"* en el Reglamento.[96] El segundo le confiere al

---

[92] *Ibid.*, art. 7.1.
[93] *Ibid.*, art. 7.2.
[94] *Ibid.*, art. 7.3.
[95] *Ibid.*, art. 14.2.
[96] *Ibid.*, art. 12.1.

titular de los datos el *"derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan"*.[97] Este derecho fue objeto de un fuerte interés mediático unos años antes de que se aprobase el Reglamento, cuando la Gran Sala del TJUE declaró que los motores de búsqueda, como Google, son responsables del contenido que muestran, por lo que un particular puede exigir que se borren las referencias que incluya en relación con su persona.[98]

5.3. Valoración del Reglamento General de Protección de Datos

Del análisis del nuevo marco jurídico que introduce el Reglamento se puede concluir, sin temor a equivocación, que pone de manifiesto un claro compromiso de las instituciones europeas en la protección de datos de sus ciudadanos. Los más optimistas afirman que no sólo cambiará la protección de datos a nivel europeo, sino que todo el mundo se verá beneficiado, pues numerosas compañías han decidido adaptar sus mecanismos internos para cumplir con el Reglamento no sólo a nivel europeo, sino en su proyección global.[99] Otros en cambio se muestran escépticos, pues creen que las flexibilidades que permiten a los Estados miembros crear normas especiales en algunos campos impedirán alcanzar la deseada armonización, creándose una situación análoga a la existente con la ya derogada Directiva de Protección de Datos.[100] Dicho esto, todavía es pronto para juzgar si el Reglamento se materializará en una mejor protección de los datos de los usuarios o se quedará en una mera manifestación de buenas intenciones.

Como último apunte, es importante mencionar que España actualizo su ordenamiento jurídico para adaptarse al nuevo escenario, aprobando el 5 de diciembre de 2018 una nueva ley, la Ley Orgánica de Protección de Datos de 2018.

---

[97] *Ibid.*, art. 17.1.

[98] Sentencia de 13 de mayo de 2014, Google España, C-131/12, EU:C:2014:317, apartado 88.

[99] Albrecht, J. P., "How the GDPR Will Change the World", *European Data Protection Law Review*, vol. 3, 2016, p. 287.

[100] Goddard, M., "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact", *International Journal of Market Research*, vol. 59, n. 6, 2017, p. 704.

6. UN NUEVO PARADIGMA PARA LA PROTECCIÓN DE DATOS

6.1. La importancia del uso secundario de datos médicos

A lo largo de este trabajo, se han ido desarrollando algunas de las innumerables ventajas de la aplicación del *big data* a la investigación médica. Dicho esto, para que estas ventajas se vean realizadas, resulta indispensable que los investigadores tengan acceso a datos que cumplan las cinco uves del *big data*; es decir, que sean voluminosos, variados, veloces, veraces y valiosos. El problema es que, como para un investigador es inviable material y económicamente recolectar datos nuevos que presenten estas características cada vez que lleva a cabo un estudio médico, éstos suelen recurrir a lo que se conoce como "uso secundario de datos". En términos generales, se define como uso secundario de datos a cualquier uso diferente del originalmente consentido por el titular de los datos.[101] En el ámbito concreto de la medicina, se define como

> el uso no directo de datos de salud personal, incluido, entre otros, analíticas, pruebas de investigación, mediciones de calidad o seguridad, salud pública, pagos, certificaciones o acreditaciones de proveedores e información de actividades de marketing o empresariales, incluidas actividades estrictamente comerciales.[102]

De este modo, si un investigador necesita, por ejemplo, 1.000 muestras de saliva para investigar una patología, el uso secundario de datos hace que no sea necesario que recolecte dichas muestras, sino que puede acudir a registros que contengan la información que necesita.

El riesgo del uso secundario de datos médicos es que cabe la posibilidad de que suponga la materialización de alguno de los peligros asociados al *big data* que se han analizado en el tercer capítulo del presente trabajo. Volviendo al ejemplo de las muestras de saliva, el uso de datos provenientes de registros puede vulnerar el derecho a la intimidad de los pacientes a los que se les extrajo la muestra, que desconocían su uso futuro en otra investigación. De este modo, a pesar de que es deseable que la medicina progrese y cabría pensar que la inmensa mayoría de la población estaría dispuesta a ceder sus datos de salud

---

[101] Rumbold, J. M. M. y Pierscionek, B., "The Effect of the General Data Protection Regulation on Medical Research", *Journal of Medical Internet Research*, vol. 19, n. 2, 2017, p. 50.

[102] 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, p. 2.

para ayudar a otras personas, dicho planteamiento no se puede asumir como válido en cualquier circunstancia, por lo que el legislador tiene el deber de garantizar el derecho a la intimidad de los titulares de los datos médicos empleados en las investigaciones clínicas.[103]

A pesar de que se acaba de analizar el problema del uso secundario de datos médicos en relación con el *big data*, este problema ya existía antes del surgimiento de esta tecnología. De hecho, dadas sus innumerables ventajas, los investigadores llevan empleado secundariamente datos médicos desde hace décadas.[104] El problema es que la solución que existía antes del desarrollo del *big data* para conciliar el interés general y el derecho a la intimidad individual se ha demostrado obsoleta, por lo que surge la necesidad de formular un nuevo paradigma para el uso secundario de datos médicos.

6.2. El agotamiento del paradigma tradicional

La solución tradicional que ha posibilitado el uso secundario de datos en la investigación médica se conoce como el paradigma del consentimiento o la anonimización.[105] De acuerdo con este paradigma, los investigadores tienen dos alternativas a la hora de usar datos para sus estudios: o bien obtienen el consentimiento informado de los titulares de los datos, o bien anonimizan los datos para que éstos no se consideren datos personales merecedores de protección. Sin embargo, en el tercer capítulo de este trabajo se ha visto como ambas soluciones están cuestionadas en la era del *big data*.

Con respecto al consentimiento informado se ha destacado, por ejemplo, que la mayor parte de la población no cede sus datos cuando tiene la oportunidad de hacerlo, pese a que las encuestas afirman que la mayoría de las personas estarían dispuestas a compartir su información para la investigación médica. Además, como el *big data* permite descubrir

---

[103] Meystre, S. M., Lovis, C., Bürkle, T., Tognola, G., Budrionis, A. y Lehmann, C. U., "Clinical Data Reuse or Secondary Use: Current Status and Potential Future Progress", *Yearbook of Medical Informatics*, vol. 26, n. 1, 2017, p. 40.

[104] McArt, E. W., & McDougal, L. W., "Secondary Data Analysis-A New Approach to Nursing Research", *Journal of Nursing Scholarship*, vol. 17, n. 2, 1985, p. 54.

[105] Laurie, G., "Liminality and the limits of law in health research regulation: what are we missing in the spaces in-between?", *Medical Law Review*, vol. 25, n. 1, 2016, p. 52.

correlaciones entre variables *a priori* imperceptibles para el ojo humano, también se ha resaltado la dificultad de los investigadores a la hora de solicitar el consentimiento informado para estudios específicos, pues no se sabe en qué área concreta se va a usar la información cedida hasta que ésta se emplea efectivamente. Por otra parte, al ser un uso secundario de datos, cabría argumentar que el consentimiento informado se podría solicitar cuando se produjese dicho uso, pero ya se ha demostrado que es una tarea inviable económica y temporalmente. Finalmente, se ha señalado que el consentimiento informado conduce al problema del sesgo del consentimiento, por el que *"los sujetos que dan permiso para que se acceda a su información médica difieren del grupo de individuos que se muestran contrarios a dar permiso a que su información médica se use en investigación"*.[106]

Por otro lado, por lo que respecta a la anonimización, se ha hecho referencia a un informe del Comité Internacional de Bioética que afirma que puede no ser una herramienta idónea para proteger a las personas en la época actual, pues el *big data* analiza y relaciona tal cantidad de datos que, aunque estén anonimizados, se puede llegar a identificar a su titular. Además, incluso en el caso de que la anonimización sea realmente irreversible, se ha destacado que también provoca problemas en la investigación médica, pues suele ser necesario hacer un seguimiento a los titulares de los datos para estudiar la evolución de los parámetros objeto del estudio. Finalmente, el último problema de la anonimización que se ha puesto de manifiesto es que abre la posibilidad a que los miembros individuales de grupos que presentan unas características comunes sean atacados tras el estudio de sus datos anonimizados.

6.3. Un nuevo paradigma para la investigación médica

Ante el agotamiento del paradigma tradicional, surge la necesidad de construir un nuevo paradigma que concilie el interés general y los derechos individuales de las personas en la era del *big data*. Este nuevo paradigma debe actuar por dos vías: reformulando el consentimiento o actualizando la anonimización.

---

[106] Institute of Medicine, *cit.*, p. 209.

6.3.1. Nuevas formas de consentimiento

Para que las nuevas formas de consentimiento sean eficaces en el contexto actual, deben facilitar el uso de los datos en las investigaciones manteniendo el respeto a la intimidad de los pacientes.[107] En este sentido, el Comité Internacional de Bioética destaca tres nuevas formas de consentimiento, que corrigen los principales problemas del consentimiento informado y que serán analizadas en las siguientes líneas en base al informe de dicho organismo sobre el impacto del *big data* en la salud.[108]

La primera se conoce como *broad consent* y supone que el titular de los datos consiente para que éstos sean usados en un amplio marco de investigaciones.[109] Es importante aclarar que no equivale a un consentimiento abierto por el que los datos pueden ser usados para cualquier estudio, pero sí supone un aumento condiderable de las posibilidades que ofrece el consentimiento tradicional, según el cual cada estudio individual debe ser autorizado por el titular de los datos para que su consentimiento sea informado. El Comité aclara que para que el *broad consent* sea válido se necesita algún tipo de garantía; por ejemplo, *"un comité que revisa las propuestas para garantizar que los derechos e intereses de las personas están protegidos adecuadamente o que las salvaguardias exigidas por las legislaciones han sido implementadas"*.

La segunda forma de consentimiento es el *opt-out consent*, *"según la cual la información clínica [de los sujetos] puede ser usada en la investigación salvo que manifiesten afirmativamente su oposición a ello"*. Esta es una opción muy favorable para los investigadores, pues la opción fijada por defecto les permite acceder a los datos de los pacientes. Sin embargo, puede ser poco garante de los derechos de los titulares de la información, por lo que éstos deben ser informados de la posibilidad de modificar la opción predeterminada.

Finalmente, la última forma de consentimiento es el *dynamic consent*, *"que permite a los participantes dar su consentimiento para nuevos proyectos o alterar sus opciones de*

---

[107] Comité Internacional de Bioética, *cit.*, p. 11.

[108] *Ibid.*, pp. 11-13.

[109] Steinsbekk, K. S., Kåre Myskja, B. y Solberg, B., "Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?", *European Journal of Human Genetics*, vol. 21, 2013, p. 897.

consentimiento en tiempo real a medida que cambian sus circunstancias".[110] Es una opción fácil de implementar en la actualidad, pues las tecnologías de la información permiten una comunicación continua con el titular de los datos. Además, éste permanece como un sujeto activo a lo largo de toda la relación, pudiendo adaptar su posición en función del contexto.

6.3.2. Actualizando la anonimización: la seudonimización

A lo largo del presente trabajo se ha insistido en la idea de que una anonimización eficaz impide volver a identificar al sujeto titular de los datos, lo que puede resultar interesante en el contexto de la investigación médica. Frente a este problema surge la seudonimización, una técnica definida como

> el 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.[111]

En otras palabras, la seudonimización *"oculta la identidad pero permite volver a identificarla en caso necesario"*.[112] Por lo tanto, cuando los investigadores necesitan profundizar en el estudio de un sujeto particular, ya sea para actualizar datos que ya poseen, ya sea para recolectar otros nuevos, la seudonimización les permite llegar a dicho sujeto. De igual modo, el interesado no ve comprometida su información personal en ningún momento, pues esta herramienta exige que se implementen una serie de medidas de protección.

Sin embargo, cabe destacar que la seudonimización no aporta ninguna mejoría frente a la anonimización en lo que se refiere al problema de la reidentificación. De esta forma, un

---

[110] Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H. y Melham, K., "Dynamic consent: a patient interface for twenty-first century research networks", *European Journal of Human Genetics*, vol. 23, 2015, p. 143.

[111] *Vid*: Reglamento (UE) 2016/679, *cit.*, art. 4.5).

[112] Romana García, M. L. y Hernández Pardo, B., "Protección de datos: la 'seudonimización' inexistente", *Estudios*, vol. 28, n. 1, 2018, p. 93.

mayor desarrollo de las técnicas de anonimización y seudonimización es esencial para garantizar la protección de los datos personales de las personas en la era del *big data*.

6.3.3. El nuevo paradigma en el Reglamento General de Protección de Datos

El Reglamento pone de manifiesto la consciencia del legislador europeo de la importancia del uso secundario de datos. En este sentido, el recital 157 afirma que

> combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas [por lo que], para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos.

Sin embargo, a pesar de este compromiso con la investigación científica –y médica, por tanto–, el Reglamento no profundiza de la misma manera en el consentimiento y en la anonimización, frente al anterior régimen incluido en la Directiva de Protección de Datos.

Con respecto al consentimiento, al estar los datos relativos a la salud incluidos dentro de las categorías especiales de datos personales del artículo 9, el Reglamento prohíbe su tratamiento excepto si *"el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales"*.[113] Dado que este requisito es acumulativo a los propios del consentimiento general del artículo 7, parece que el legislador no tiene ninguna intención de flexibilizar el consentimiento en relación con la investigación médica, manteniendo por tanto el consentimiento informado como regla. Dicho esto, el recital 33 de la norma afirma que *"debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica"*, por lo que parece que el Reglamento admite el *broad consent* como una forma válida de consentimiento. Sin embargo, existe la duda de si dicho recital se refiere exclusivamente al consentimiento general del artículo 7 o si también es de aplicación al consentimiento para las categorías especiales de datos del artículo 9.[114] Sólo en el caso de que la segunda postura sea la aceptada podrá el *broad consent* ser empleado en relación con los datos médicos.

---

[113] *Vid*: Reglamento (UE) 2016/679, *cit.*, art. 9.2.

[114] Mostert, M., "A new regulatory landscape for Big Data health research: Safeguards and research exemptions in the GDPR" en Mostert, M. (Ed.), *Big Data health research: Safeguarding rights and interests*, Utrecht University, Utrecht, 2018, p. 60.

Por lo que se refiere a la anonimización, el Reglamento sí que actualiza el régimen preexistente, permitiendo la seudonimización y desarrollando su régimen. Uno de los aspectos más interesantes de esta figura es que los datos que han sido seudonimizados se siguen considerando *"información sobre una persona física identificable"*, por lo que están sujetos al Reglamento, a diferencia de los datos que han sido anonimizados.[115] Aún así, el tratamiento de los datos seudonimizados es sustancialmente más laxo que el general previsto en el Reglamento. Así, el derecho de la Unión o el de los Estados miembros puede establecer excepciones a los derechos de acceso, rectificación, limitación del tratamiento y oposición.[116] Por lo tanto, se facilita la investigación científica, reduciendo las obligaciones de los investigadores en el tratamiento de los datos personales.

En global, el Reglamento se pronuncia de una manera muy favorable sobre esta técnica, buscando *"incentivar la aplicación de la seudonimización en el tratamiento de datos personales"*[117] y afirmando que *"[l]a aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos"*.[118]

En resumen, el Reglamento parece haber optado por un nuevo paradigma donde se busca favorecer el interés general potenciando la anonimización, a través de la seudonimización. En cambio, el consentimiento no sufre mayores cambios en el campo de la investigación médica, a la espera de determinar si el *broad consent* es una solución aplicable a este tipo de estudios.

---

[115] *Vid*: Reglamento (UE) 2016/679, *cit.*, recital 26.
[116] *Ibid.*, art. 89.2.
[117] *Ibid.*, recital 29.
[118] *Ibid.*, recital 28.

6.3.4. El nuevo paradigma en la Ley Orgánica de Protección de Datos de 2018

La Ley Orgánica de 2018, en su disposición adicional decimoséptima, donde analiza el tratamiento de los datos de salud, se pronuncia en unos términos similares al Reglamento con respecto al nuevo paradigma.

Así, con respecto al consentimiento, se indica que *"[e]l interesado […] podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud"*.[119] Por suerte, no es necesario que los sujetos presten el consentimiento para cada investigación concreta, sino que puede prestarlo para *"categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora"*.[120] Por lo tanto, la norma española admite el *broad consent* en el uso secundario de datos médicos. Este planteamiento queda reafirmado en el artículo 2.c) de la disposición adicional, que afirma que

> [s]e 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.

Por lo tanto, la Ley Orgánica de 2018 flexibiliza hasta cierto punto el consentimiento en el marco de una investigación médica, pero siempre garantizando la protección de los derechos individuales de los sujetos cuyos datos son empleados. Además, de la redacción literal del artículo 2.c) de la disposición adicional, parece que sólo se justifica el *broad consent* para aquellos casos en que los datos han sido originalmente recogidos en el marco de una investigación, no cuando han sido obtenidos de pacientes médicos.

Sobre la anonimización, la Ley Orgánica de 2018, como es lógico, también permite la seudonimización al afirmar que *"[s]e considera lícito el uso de datos personales seudonimizados con fines de investigación en salud"*.[121] Además, si recordamos el epígrafe anterior sobre el nuevo paradigma en el Reglamento, en él se explicó como la nueva norma comunitaria abría la posibilidad a que el derecho de los Estados miembros

---

[119] *Vid*: Ley Orgánica 3/2018, *cit.*, disposición adicional 17ª, art. 2.a).

[120] *Ibídem*.

[121] *Ibid.*, art. 2.d).

pudiese establecer excepciones a una serie de derechos en el contexto de investigaciones médicas. Pues bien, la Ley Orgánica de 2018 hace ejercicio de esta prerrogativa y declara que sólo se podrán excepcionar tales derechos si éstos son ejercidos ante los investigadores y en relación con los resultados de una investigación cuyo objeto es un interés público esencial.[122] Además, parece que la norma justifica la seudonimización tanto para el caso de que los datos hayan sido obtenidos originalmente en el marco de una investigación, como para cuando hayan sido obtenidos de pacientes.

Se puede afirmar, por tanto, que la norma española facilita la labora de los investigadores frente al régimen anterior, en parte gracias a la flexibilización del consentimiento con la aceptación del *broad consent*, pero sobre todo con la introducción de la seudonimización como alternativa a la anonimización de los datos.

[122] *Ibid.*, art. 2.e).

7. CONCLUSIÓN

El uso secundario de datos médicos es esencial para el progreso de la medicina, pues abre la posibilidad a los investigadores de acceder a fuentes de información esenciales para llevar a cabo sus estudios. En caso contrario, éstos tendrían que obtener los datos de manera primaria para cada investigación, lo que resultaría caro y excesivamente laborioso. Por este motivo, y dado el innegable valor de la investigación médica para el interés general, se ha venido permitiendo dicho uso secundario siempre y cuando los titulares de los datos hubiesen prestado su consentimiento informado para la investigación o, en su defecto, éstos hubiesen sido anonimizados. De hecho, la Directiva de Protección de Datos y Ley Orgánica de Protección de Datos de 1999, dos normas ya derogadas, recogían esta visión.

Sin embargo, el *big data* ha revolucionado este paradigma. Es una herramienta que se basa en el análisis de datos voluminosos, variados, veloces, veraces y de valor y que ofrece unas posibilidades increíbles en el mundo de la medicina. En este sentido, permite, por ejemplo, prevenir y monitorizar epidemias, analizar de manera masiva muestras genéticas, gestionar el conocimiento médico o democratizar el acceso a la medicina. Dicho esto, el *big data* también presenta una serie de riesgos, pues puede conducir a la vulneración del derecho a la intimidad de los sujetos cuyos datos se emplean, ignorando su consentimiento o atacando su privacidad.

Por ello, el nuevo Reglamento General de Protección de Datos, aplicable desde mayo de 2018, actualiza su régimen para adaptarse al nuevo contexto. La novedad más importante de esta norma en relación con la investigación médica es la seudonimización, una técnica por la que los datos no se pueden atribuir a su titular sin emplear información adicional que no se encuentra en posesión de los investigadores. Es una evolución esencial pues, dado que la investigación médica exige en ocasiones un seguimiento de los pacientes, la seudonimización permite a los investigadores identificar a los titulares de los datos en caso de que su información sea relevante para el estudio. De este modo, se preserva el interés general, pues se facilita la investigación médica, pero también el interés particular de los titulares de los datos, cuyos datos no pueden atribuirse a ellos salvo que sea esencial para el estudio.

También hubiera sido interesante que el Reglamento modificase el consentimiento, permitiendo nuevas formas de prestarlo, como el *broad consent*, el *opt-out consent* o el *dynamic consent*. Sin embargo, la norma europea parece optar por continuar exigiendo que el consentimiento sea informado y específico, desconfiando de un posible mal uso de los datos particulares. Dicho esto, queda abierta la posibilidad a que el *broad consent* sea una forma válida de consentimiento en el marco de las investigaciones médicas.

La Ley Orgánica de Protección de Datos de 2018 se pronuncia en términos similares al Reglamento, recogiendo en su disposición adicional décimo séptima la seudonimización como una nueva alternativa para los investigadores. Además, la norma española sí que se muestra favorable al *broad consent* para aquellas instancias en que los datos han sido originalmente obtenidos en el contexto de una investigación.

Dicho esto, todavía queda camino por recorrer en esta materia, pues las posibilidades del *big data* aplicable a la medicina parecen ser infinitas. Por lo tanto, en defensa del interés general, es esencial facilitar el trabajo de los investigadores, de tal manera que puedan usar de manera secundaria datos clínicos en sus estudios, pero siempre con las adecuadas garantías para la protección de la intimidad de los particulares.

8. REFERENCIAS BIBLIOGRÁFICAS

8.1. Legislación

Amended proposal for a council directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM (92), 18 de octubre de 1992.

Constitución Española.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Diario Oficial n° L 281 de 23/11/1995, pp. 0031-0050).

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE 31 de octubre de 1992).

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE 14 de diciembre de 1999).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

Reglamento (UE) 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 y por el que se deroga la directiva 95/46/CE (Diario Oficial n° L 110 de 4/5/2016, pp. 1-88).

8.2. Jurisprudencia

Sentencia del Tribunal Constitucional de 30 de noviembre, 290/2000.

Sentencia de 13 de mayo de 2014, Google España, C-131/12, EU:C:2014:317.

8.3. Doctrina

Aagaard, A. (Ed.), *Digital Business Models*,Cham, Springer International Publishing, 2019.

Albrecht, J. P., "How the GDPR Will Change the World", European Data Protection Law Review, vol. 3, 2016, pp. 287-289.

Alguacil González-Aurioles, J., "La libertad informática: aspectos sustantivos y competenciales (SS.T.C 290 y 292/2000)", *Teoría y Realidad Constitucional*, n. 7, 2001, pp. 365-385.

Andreu-Perez, J., Poon, C. C. Y., Merrifield, R. D., Wong, S. T. C. y Yang, G. Z, "Big Data for Health", *IEEE Journal of Biomedical and Health Informatics*, vol. 19, n. 4, 2015, pp. 1193-1208.

Birnhack, M. D., "The EU Data Protection Directive: An engine of a global regime", *Computer Law & Security Review*, vol. 24, n. 6, 2008, pp. 508-520.

Blume, P., "An EEC Policy for Data Protection", *Computer Law Journal*, vol. 11, n. 3, 1992, pp. 399-440.

Cate, F. H., "The EU Data Protection Directive, Information Privacy, and the Public Interest", *Iowa Law Review*, vol. 80, 1994, pp. 431-443.

Cohen, I., Lynch, H., Vayena, E. y Gasser, U. (eds.), *Big Data, Health Law, and Bioethics*, Cambridge University Press, Cambridge, 2018.

Comité Internacional de Bioética, "Report of the IBC on Big Data and Health", 2017 (disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000248724; última consulta 02/02/2019).

Crabu, S. "Biomedicalization. Technoscience, Health and Illness in the U.S.", *Tecnoscienza*, vol. 2, n. 2, 2010, pp. 119-123.

De Hert, P. y Papakonstantinou, V., "The new General Data Protection Regulation: Still a sound system for the protection of individuals?", Computer Law & Security Review, vol. 32, n. 2, pp. 179-194.

De Hert, P. y Papakonstantinou, V., "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, vol. 28, n. 2, 2012, pp. 130-142.

De Montalvo Jääskeläinen, F. "¿Puede la máquina sustituir al hombre ?", *Razón y Fe*, vol. 278, n. 1436, 2018, pp. 323-334.

El Emam, K. y Arbuckle, L., *Anonymizing health data: case studies and methods to get you started*, O'Reilly, Sebastopol, 2013.

Goddard, M., "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact", *International Journal of Market Research*, vol. 59, n. 6, 2017, pp. 703-705.

Grady, C., "Enduring and Emerging Challenges of Informed Consent", *The New England Journal of Medicine*, vol. 372, n. 9, 2015, pp. 855-862.

Green, E. D., Watson, J. D. y Collins, F. S., "Human Genome Project: Twenty-five years of big biology", *Nature*, vol. 526, n. 7571, 2015, pp. 29-31.

Henderson, G., "Is Informed Consent Broken?", *American Journal of Medical Sciences*, vol. 342, n. 4, 2011, pp. 267-272.

Hernández-Medrano, I. y Carrasco, G., "El profesional de la salud ante el mundo del Big Data", *Revista de Calidad Asistencial*, vol. *31*, n. 5, 2016, pp. 250-253.

Hill, K., "Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study", *Forbes*, 30 de junio de 2014 (disponible en: https://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/#437bdf767a62; última consulta 26/02/2019).

Institute for Health Technology Transformation, "Transforming Health Care Through Big Data", 2013, (disponible en: http://c4fd63cb482ce6861463-bc6183f1c18e748a49b87a25911a0555.r93.cf2.rackcdn.com/iHT2_BigData_2013.pdf; última consulta 02/02/2019).

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

Jee, K. y Kim, G. H., "Potentiality of big data in the medical sector: focus on how to reshape the healthcare system", *Healthcare Informatics Research*, vol. 19, n. 2, 2013, pp. 79-85.

Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H. y Melham, K., "Dynamic consent: a patient interface for twenty-first century research networks", *European Journal of Human Genetics*, vol. 23, 2015, pp. 141-146.

Kramer, A. D. I., Guillory, J. E. y Hancock, J. T., "Experimental evidence of massive-scale emotional contagion through social networks", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 111, n. 24, 2014, pp. 8788-8790.

Laurie, G., "Liminality and the limits of law in health research regulation: what are we missing in the spaces in-between?", *Medical Law Review*, vol. 25, n. 1, 2016, pp. 47-72.

Lavalle, S., Lesser, E., Shockley, R., Hopkins, M. S. y Kruschwitz, N., "Big Data, Analytics and the Path From Insights to Value", *MIT Sloan Management Review*, vol. *52*, 2011, pp. 20-32.

Lazer, D., Kennedy, R., King, G. y Vespignani, A., "The Parable of Google Flu: Traps in Big Data Analysis", *Science*, vol. 343, n. 6176, 2014, pp. 1203-1205.

Litman, R.S., "Complications of laryngeal masks in children: big data comes to pediatric anesthesia", *Anesthesiology*, vol. 119, n. 6, 2013, pp. 1239-1240.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C. y Hung Byers, A., "Big data: The next frontier for innovation, competition and productivity", *McKinsey Global Institute*, 2011 (disponible en: https://www.mckinsey.com/business-functions/digitalmckinsey/our-insights/big-data-the-next-frontier-for-innovation; última consulta 03/02/2019).

Markowetz, A., Błaszkiewicz, K., Montag, C., Switala, C. y Schlaepfer, T. E., "Psycho-Informatics: Big Data shaping modern psychometrics", *Medical Hypotheses*, vol. 82, n. 4, 2014, pp. 405-411.

McArt, E. W., & McDougal, L. W., "Secondary Data Analysis-A New Approach to Nursing Research", *Journal of Nursing Scholarship*, vol. 17, n. 2, 1985, pp. 54-57.

Menasalvas, E., Gonzalo, C. y Rodríguez-González, A., "Big Data En Salud: Retos Y Oportunidades", *Economía Industrial*, n. 405, 2017, pp. 87-97.

Meystre, S. M., Lovis, C., Bürkle, T., Tognola, G., Budrionis, A. y Lehmann, C. U., "Clinical Data Reuse or Secondary Use: Current Status and Potential Future Progress", *Yearbook of Medical Informatics*, vol. 26, n. 1, 2017, pp. 38-52.

Ministerio de Sanidad, Servicios Sociales e Igualdad, "Proyecto HCDSNS Historia Clínica Digital del Sistema Nacional de Salud", 2017 (disponible en: https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf; última consulta 07/02/2019).

Mittelstadt, B. D. y Floridi, L., "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts", *Science and Engineering Ethics*, vol. 22, n. 2, 2016, pp. 303-341.

Mostert, M., Bredenoord, A. L., Biesaart, M. C. I. H. y van Delden, J. J. M., "Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach", *European Journal of Human Genetics*, vol. 24, n. 7, 2016, pp. 956-960.

Mostert, M. (Ed.), *Big Data health research: Safeguarding rights and interests*, Utrecht University, Utrecht, 2018.

Murdoch, T. B. y Detsky, A., "The Inevitable Application of Big Data to Health Care", *Journal of the American Medical Association*, vol. 309, n. 13, pp. 1351-1352.

Murillo de la Cueva, P. L., "La construcción del derecho a la autodeterminación informativa", *Revista de estudios políticos*, n. 104, 1999, pp. 35-60.

O'Driscoll, A., Daugelaite, J. y Sleator, R. D., "Big data, Hadoop and cloud computing in genomics", *Journal of Biomedical Informatics*, vol. 46, n. 5, 2013, pp. 774-781.

Pérez Luño, A. E., *Manual de informática y derecho*, Ariel, Barcelona, 1996.

Raghupathi, W. y Raghupathi, V, "Big data analytics in healthcare: promise and potential", *Health Information Science and Systems*, vol. *2,* n. 3, 2014, pp. 1-10.

Robinson, N., Graux, H., Botterman, M. y Valeri, L. *"Review of the EU Data Protection Directive: Summary"*, *Oficina del Comisionado de Información*, 2009.

Romana García, M. L. y Hernández Pardo, B., "Protección de datos: la 'seudonimización' inexistente", *Estudios*, vol. 28, n. 1, 2018, pp. 92-103.

Roski, J., Bo-Linn, G. W. y Andrews, T. A. "Creating Value In Health Care Through Big Data: Opportunities And Policy Implications", *Health Affairs*, vol. 33, n. 7, 2014, pp. 1115-1122.

Rothstein, M. A., "Ethical Issues in Big Data Health Research: Currents in Contemporary Bioethics", *The Journal of Law, Medicine & Ethics*, vol. 43, n. 2, 2015, pp. 425-429.

Rumbold, J. M. M. y Pierscionek, B., "The Effect of the General Data Protection Regulation on Medical Research", *Journal of Medical Internet Research*, vol. 19, n. 2, 2017, pp. 47-55.

Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century, COM (2012), 3 de septiembre de 2012.

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. 1-9.

Sánchez Bravo, Á., "La Ley Orgánica 15/1999, de Protección de datos de carácter personal: diez consideraciones en torno a su contenido", *Revista de Estudios Políticos*, n. 111, 2001, pp. 201-214.

Signorini, A., Segre, A. M. y Polgreen, P. M., "The Use of Twitter to Track Levels of Disease Activity and Public Concern in the U.S. during the Influenza A H1N1 Pandemic", *PLoS ONE*, vol. 6, n. 5, 2011, pp. 1-10.

Steinsbekk, K. S., Kåre Myskja, B. y Solberg, B., "Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem?", *European Journal of Human Genetics*, vol. 21, 2013, pp. 897-902.

Tene, O. y Polonetsky, J., "Big Data for All: Privacy and User Control in the Age of Analytics", *Northwestern Journal of Technology and Intellectual Property*, vol. 11, n. 5, 2013, pp. 239-273.

Topol, E. J., "The big medical data miss: challenges in establishing an open medical resource", *Nature Reviews Genetics*, vol. 16, n. 5, 2015, pp. 253-254.

Tripp, S. y Grueber, M., "Economic Impact of the Human Genome Project", *Battelle Memorial Institute*, 2011 (disponible en: https://www.battelle.org/docs/default-source/misc/battelle-2011-misc-economic-impact-human-genome-project.pdf; última consulta 28/01/2019).

Omer T, "Privacy: The new generations", *International Data Privacy Law*, vol. 1, n. 1, 2011, pp. 15-27.

Vayena, E., Salathé, M., Madoff, L. C. y Brownstein, J. S., "Ethical Challenges of Big Data in Public Health", *PLoS Computational Biology*, vol. 11, n. 2, 2015, pp. 1-7.