Anuario Jurídico y Económico Escurialense, **LVII (2024) 13-62 / ISSN: 1133-3677**

El derecho a la protección de datos en el ámbito de la investigación biomédica: Reflexiones en torno a los retos e implicaciones jurídicas del *Big Data*[*]

The right to data protection in the field of biomedical research: Reflections on the challenges and legal implications of Big Data

Roser ALMENAR RODRÍGUEZ
Investigadora visitante en el Centro Cañada Blanch
London School of Economics and Political Science (LSE)
r.almenar-rodriguez@lse.ac.uk
ORCID: 0000-0002-4228-8888

Resumen: Los grandes avances tecnológicos que se han desarrollado durante los últimos años han cambiado el paradigma normativo existente a nivel de la Unión Europea. La implementación de las tecnologías *Big Data*, caracterizadas por la capacidad de manejar cantidades masivas de datos, ha generado tanto beneficios como preocupaciones en el especial ámbito de la salud. Este estudio, en consecuencia, se centra en analizar el marco legislativo europeo y español que regula la protección de los datos personales en relación con su aplicación a la investigación científica, y, más concretamente, en la disciplina de la biomedicina. Debido al reconocimiento del carácter especial de los datos de salud en la normativa, la legitimación de su tratamiento con estos fines se torna más compleja, si bien el verdadero desafío se encuentra en determinar la adecuación de este marco jurídico a los retos que plantea la incorporación de los sistemas *Big Data* a este campo. En base a esta premisa, procederé a formular una serie de reflexiones en torno a propuestas de criterios de licitud alternativos al actualmente predominante fundado en el consentimiento.

Abstract: The great technological advances that have been developed over the last few years have changed the existing regulatory paradigm at the

[*] Este artículo ha obtenido, el presente año académico 2023-2024, el VIII Premio Reina María Cristina, de carácter internacional, en la modalidad de Derecho, convocado por el Real Centro Universitario Escorial-María Cristina.

European Union level. The implementation of Big Data technologies, characterised by the ability to handle massive amounts of data, has generated both benefits and concerns in the special field of healthcare. This study, consequently, focuses on analysing the European and Spanish legislative framework regulating the protection of personal data in relation to its application to scientific research, and, more specifically, in the discipline of biomedicine. Due to the recognition of the special nature of health data in the regulations, the legitimacy of its processing for these purposes becomes more complex, although the real defiance lies in determining the adequacy of this legal framework to the challenges posed by the incorporation of Big Data systems in this realm. Based on this premise, I will proceed to formulate a series of reflections around proposals for alternative lawfulness criteria to the currently predominant one based on consent.

Palabras clave: Protección de datos, investigación biomédica, consentimiento, legitimación, categorías especiales de datos personales.

Keywords: Data protection, biomedical research, consent, legitimacy, special categories of personal data.

Sumario:

I. INTRODUCCIÓN

Como afirma la Comisión Europea, *"los datos se han convertido en un recurso esencial para el crecimiento económico, la creación de empleo y el progreso social"*[1]. Desde la década de los noventa, la globalización y la creciente evolución tecnológica han devenido factores clave en el ámbito de protección de los datos personales en Europa. La magnitud de estos avances, junto con el aumento en el flujo e intercambio de datos, han tenido como repercusión el planteamiento de nuevos retos para garantizar un alto nivel de protección de los datos personales.

Ya advertía la Ley 14/2007, de 3 de julio, de Investigación biomédica en su exposición de motivos que *"Es necesario disponer del marco normativo adecuado que dé respuesta a los nuevos retos científicos al mismo tiempo que garantice la protección de los derechos de las personas que pudiesen resultar afectados por la acción investigadora"*. Más de quince años después nos encontramos ante nuevos desafíos para la investigación científica, con la idéntica necesidad de buscar soluciones que permitan aprovechar el potencial de las nuevas tecnologías al mismo tiempo que se salvaguardan los derechos fundamentales y libertades públicas de las personas.

Es indudable que la incorporación de métodos *Big Data* en el campo de la salud constituye una herramienta muy provechosa y útil de cara a promover avances para el conocimiento en investigación biomédica, principalmente en el diagnóstico, prevención y tratamiento de enfermedades. No obstante, el optimismo tecnológico derivado de la elevada cantidad de beneficios que genera para la misma no debe opacar los riesgos para la privacidad de los ciudadanos que entraña, y es por ello que resulta indispensable poner en una balanza las ventajas que aporta la utilización de estos sistemas y la necesaria protección de los derechos fundamentales de los pacientes, a fin de lograr un equilibrio que permita la subsistencia de ambos.

Dada la gran importancia que presenta esta cuestión, el propósito de este estudio es examinar la idoneidad y adecuación del consentimiento como base legitimadora en el marco de las investigaciones en biomedicina, explorando la

[1] Vid., COMISIÓN EUROPEA, *A European Strategy for data*, disponible en: https://digital-strategy.ec.europa.eu/en/policies/strategy-data

necesidad de formular una alternativa que sepa dar respuesta a los nuevos retos jurídicos que plantea el *Big Data*, sin dejar de velar por la efectiva observancia de los derechos inherentes a la persona.

II. EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN EL ORDEN CONSTITUCIONAL ESPAÑOL. CONFIGURACIÓN JURÍDICA, OBJETO Y CONTENIDO

Siendo ciertamente conscientes de la importancia progresiva que las nuevas tecnologías comenzaron a adquirir a finales del siglo pasado, los 'padres' de nuestra Constitución de 1978 consideraron pertinente introducir en su articulado una referencia a esta incipiente relación entre los derechos humanos y la tecnología, escogiendo el artículo 18 relativo al derecho a la intimidad personal y familiar como el encuadre idóneo, y dotando al derecho a la privacidad de una serie de garantías en el mundo tangible y, de igual modo, en el entorno digital. Así, el derecho a la protección de datos personales[2] se encuentra regulado en el Título I, Capítulo II, que recoge los derechos considerados "fundamentales" en nuestro ordenamiento jurídico[3].

[2] Para poder entender el objeto de regulación de las diferentes legislaciones que analizaremos en el epígrafe siguiente, resulta necesario definir, en primer lugar, qué se entiende por "datos personales". A efectos del Reglamento General de Protección de Datos, su artículo 4 presenta la siguiente definición: *"toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".* En este sentido, MURILLO DE LA CUEVA publicó en la década de los noventa su obra *El derecho a la autodeterminación informativa* (Madrid, Tecnos, 1990), acerca de la configuración de este derecho como objeto de protección del art. 18.4 CE, donde expone una primera aproximación a este concepto. Así, lo describe como: *"el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia identidad, nuestra dignidad y libertad. En su formulación como derecho, implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito".* Vid., MURILLO DE LA CUEVA, P. L., *Informática y protección de datos personales (estudio sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)*, Madrid 1993, pp. 32 y 51.

[3] CRUZ VILLALÓN describe los "derechos fundamentales" como aquellos derechos subjetivos que encuentran reconocimiento en las Constituciones, *"en la medida en que de este reconocimiento se deriva alguna consecuencia jurídica"*. Vid., CRUZ VILLALÓN, P., "Formación y evolución de los derechos fundamentales", en *Revista Española de Derecho Constitucional,* (Madrid), 25 (1989) 41. Dicha consecuencia jurídica se traduce en la formulación de garantías adicionales para la protección jurisdiccional de los derechos fundamentales y libertades públicas ante los Tribunales, en virtud del art. 53.2 de la Constitución. Respecto a la vía extraordinaria, son elegibles para ser objeto de un recurso de amparo ante el Tribunal Constitucional; y en cuanto a los Tribunales

Dispone el artículo 18.4 CE que: *"La 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"*[4]. Este derecho constitucional a la protección de datos, que podríamos calificar de emergente o de última generación, garantiza que toda persona pueda tener un control sobre el uso de sus datos personales, por lo que podemos advertir que juega un papel de suma importancia tanto para el libre desarrollo de la personalidad como para la defensa de la dignidad humana[5].

En una primera aproximación, el art. 18.4 CE era concebido como una garantía del derecho fundamental a la intimidad personal y familiar (art. 18.1 CE); no obstante, tanto la jurisprudencia de nuestros Tribunales como la de los órganos internacionales ha reconocido la existencia de un derecho subjetivo a la protección de datos[6], que otorga a la ciudadanía la capacidad y el derecho de decidir sobre el uso de sus propios datos personales, incluyendo al conocido como "derecho al olvido"[7]. De este modo, nuestro máximo intérprete de la Constitución ha ido delimitando, a través de su jurisprudencia, el contenido y el objeto de este derecho fundamental en el periodo que transcurre entre los años 1993 y 2000[8].

Así, en una primera Sentencia 254/1993, de 20 de julio, el Tribunal Constitucional concreta el contenido mínimo que debe garantizarse para la efectiva

ordinarios, su protección se lleva a cabo a través de un procedimiento preferente y sumario. Esto significa, en palabras de nuestro Tribunal Constitucional que "*la preferencia implica prioridad absoluta por parte de las normas que regulan la competencia funcional o despacho de los asuntos; por sumariedad, como ha puesto de relieve la doctrina, no cabe acudir a su sentido técnico (pues los procesos de protección jurisdiccional no son sumarios, sino especiales), sino a su significación vulgar como equivalente a rapidez"* (STC 81/1992, de 28 de mayo, FJ 4º).

[4] Es evidente la clara intención del constituyente al utilizar el verbo "limitar" en lugar de "regular", dejando vislumbrar cierto componente negativo a la hora de hacer alusión a la función legislativa sobre el uso de las nuevas tecnologías y su afectación a los derechos fundamentales de la persona. Así lo perciben SANTAMARÍA IBEAS, J. J., "La LORTAD: breve análisis de sus antecedentes", en *Informática y derecho: Revista iberoamericana de derecho informático* (Montevideo), 4 (1994) 262, y LÓPEZ-MUÑIZ GOÑI, M., "La ley de regulación del tratamiento automatizado de los datos de carácter personal", en *Informática y derecho: Revista iberoamericana de derecho informático* (Montevideo), 6-7 (1994) 94.

[5] MARTÍNEZ LÓPEZ-SÁEZ, M., "Repensando el derecho constitucional a la protección de datos ante la mutación de la "informática", en *Constitución, política y administración: España 2017, reflexiones para el debate*, Valencia 2020, p. 164.

[6] AGUILERA VAQUÉS, M. y SERRA CRISTÓBAL, R., *Rights and Freedoms in the Spanish Constitution*, Valencia 2015, p. 103.

[7] El derecho al olvido (o derecho de supresión) está garantizado en el art. 17 del Reglamento General de Protección de Datos, de acuerdo con el cual *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan"*, quedando este último obligado a eliminar los datos personales cuando concurra una de las circunstancias enumeradas por la norma.

[8] MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", en *IDP: Revista de Internet, Derecho y Política* (St. Quirze del Vallès), 5 (2007) 49.

protección de este derecho, diferenciando entre una vertiente negativa y una positiva. En cuanto a la primera, afirma el Alto Tribunal que *"el uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos"*. Este mandato constitucional se completa con el contenido del art. 20.4 CE, de acuerdo con el cual la libertad de uso de la informática tiene su límite en *"el respeto a los derechos reconocidos en este Título (…) y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen"*. Por tanto, el derecho a la intimidad reconocido en el art. 18.1 CE representa un límite constitucional al uso de las tecnologías emergentes, en base al cual instituye un derecho fundamental de la persona a la protección de sus datos de carácter personal.

Su contenido positivo, por otra parte, se manifiesta en forma de un derecho de control sobre los datos relativos a la propia persona[9]; que denomina -en su Sentencia 292/2000[10]- como "libertad informática", esto es, el "*derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención*"[11]. Siguiendo este tenor literal, y de acuerdo con MURILLO DE LA CUEVA, se entiende que *"El bien jurídico subyacente es la libertad informática o -en fórmula menos estética pero más precisa- la autodeterminación informativa"*[12].

Respecto a su naturaleza jurídica, el Tribunal Constitucional reconoce en su Sentencia 94/1998, de 4 de mayo, que el art. 18.4 de la Constitución *"consagra un derecho fundamental autónomo[13] a controlar el flujo de informaciones que conciernen a cada persona (…), pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos*

[9] STC 254/1993, de 20 de julio, FJ 7º.

[10] Esta sentencia constituye un hito para los iusconstitucionalistas en materia de protección de datos, pues es la argumentación jurídica del Tribunal la que concreta y, definitivamente, reconoce el derecho constitucional a la protección de datos de carácter personal, o derecho a la autodeterminación informativa.

[11] STC 292/2000, de 30 de noviembre, FJ 5º.

[12] MURILLO DE LA CUEVA, P. L., "La protección de los datos personales ante el uso de la informática en el derecho español (1ª parte)", en *Estudios de Jurisprudencia* (A Coruña), 3 (1992) 17. Cabe hacer referencia a la sentencia del Tribunal Constitucional Federal alemán, de 15 de diciembre de 1983, sobre la Ley del Censo de Población; un pronunciamiento que se considera clave en la positivización del derecho a la autodeterminación informativa en Europa.

[13] En este sentido, afirma PÉREZ LUÑO que "*la garantía de la protección de la libertad informática sólo podrá consolidarse si la concebimos como un derecho autónomo"*. Vid., PÉREZ LUÑO, A. E., "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", en *Anuario de Derecho Público y Estudios Públicos* (Santiago de Chile), 2 (1989/90) 187.

discriminatorios"[14]. Se trata, por tanto, de un verdadero derecho constitucional subjetivo, distinto en carácter y contenido del propio derecho a la intimidad personal y familiar (art. 18.1 CE). En efecto, como pone de manifiesto la STC 292/2000, de 30 de noviembre, en su FJ 5º:

> "Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con el cual comparte el objetivo de ofrecer una protección constitucional eficaz de la vida privada personal y familiar, atribuye al titular una serie de facultades que consiste, en la mayor parte, en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos la regulación concreta de los cuales tiene que establecer la Ley, aquella que, de acuerdo con el art. 18.4 CE, tiene que limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando el ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín cómo es el de la intimidad radica, así pues, en la distinta función que hacen, cosa que implica, por consiguiente, que también el objeto y el contenido difieran".

A diferencia del derecho a la intimidad (art. 18.1 CE) cuyo propósito radica en proteger el ámbito más personal de la intimidad del individuo[15], el derecho a la protección de datos personales tiene por objeto amparar la dignidad de la persona en el tratamiento de sus datos de carácter personal. Es decir, no protege sus datos personales *per se*, sino únicamente cuando estos se ven sometidos a algún tipo de tratamiento, pues *"estos tratamientos son vistos como un riesgo evidente para los derechos y libertades fundamentales de las personas que viene derivado del progreso tecnológico"*[16]. Sobre esta cuestión, se pronuncia el Alto Tribunal: "*De ahí la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, (…) no se limita sólo a los datos íntimos de la persona, sino a cualquier tipo de*

[14] STC 94/1998, de 4 de mayo, FJ 6º.

[15] *"La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. (…) El art. 18.1 CE no garantiza sin más ni más la 'intimidad', sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea qué sea el contenido de aquello que se quiere mantener lejos del conocimiento público".* Vid., STC 144/1999, de 22 de julio, FJ 8º.

[16] TRONCOSO REIGADA, A., "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", en *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada* (Leioa), 49 (2018) 199.

dato personal, sea o no íntima, el conocimiento o el uso de la cual por parte de terceros pueda afectar sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para lo cual está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal"[17].

Finalmente, conviene hacer un último apunte en lo que concierne al contenido esencial del derecho de protección de datos. A estos efectos, resulta indispensable citar la STC 292/2000, de 30 de noviembre, FJ 7º:

> "De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. (...) En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele".

III. BREVE REFERENCIA AL MARCO JURÍDICO DE APLICACIÓN

3.1. Legislación relevante en materia de protección de datos

3.1.1. *Reglamento General de Protección de Datos de 2016*

Tras escuchar a varios sectores que abogaban por una modificación legislativa en materia de protección de datos, la Comisión Europea finalmente planteó la reforma en enero de 2012. Sin embargo, no fue hasta cuatro años más tarde, caracterizados por un sinfín de negociaciones, que los Estados miembros y los órganos institucionales de la Unión lograron *"un consenso político sobre la necesidad de reformar la legislación vigente en materia de protección de datos*

[17] STC 292/2000, de 30 de noviembre, FJ 6º.

a través del RGPD"[18]. Así, en 2016 entró en vigor el Reglamento General de Protección de Datos (RGPD)[19], derogando la 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos, en su art. 94, cuyo ámbito de aplicación comprende el tratamiento total o parcialmente automatizado y el tratamiento no automatizado de datos personales contenidos o destinados a incluirse en ficheros[20].

El considerando 7 RGPD enuncia el claro objetivo que se perseguía en el tiempo de su aprobación: erigir *"un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta"*. Y señala, "*Las personas físicas deben tener el control de sus propios datos personales"*, de modo que el propósito de esta nueva norma reside en que el interesado disponga de un control más elevado de sus datos; lo cual lleva a cabo a través del reforzamiento de los preceptos de la Directiva 95/46/CE que ahora cuentan con mayores efectos jurídicos, al tratarse de un reglamento de aplicación directa. En este sentido, cabe destacar la configuración de un "nuevo catálogo ampliado de dimensiones de derechos específicos", entre los que se incluyen el derecho al olvido (art. 17 RGPD), el derecho a la limitación del tratamiento (art. 18 RGPD) y el derecho a la portabilidad de los datos (art. 20 RGPD)[21].

Como indica PIÑAR MAÑAS, *"el Reglamento introduce, a veces directamente, a veces de forma algo soterrada, un nuevo modelo de protección de datos para Europa. Un nuevo modelo que podemos decir que pasa de la gestión de los datos al uso responsable de la información"*[22]. En consonancia con esta afirmación, se sostiene que la adopción del RGPD ha supuesto un "auténtico cambio de paradigma" en cuanto a cómo se gestionan los datos personales. JIMÉNEZ ASENSIO enfatiza:

---

[18] CRISTEA UIVARU, L., *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud*, Barcelona 2018, p. 237.

[19] 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.

[20] MARTÍNEZ LÓPEZ-SÁEZ, M., *Una revisión del derecho fundamental a la protección de datos de carácter personal. Un reto en clave de diálogo judicial y constitucionalismo multinivel en la Unión Europea*, Valencia 2018, p. 79.

[21] JIMÉNEZ ASENSIO, R., "El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales", en *Anuario Aragonés del Gobierno Local* (Zaragoza), 10 (2018) 324.

[22] PIÑAR MAÑAS, J. L., "Introducción: hacia un nuevo modelo europeo de protección de datos", en *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Madrid 2016, p. 16.

> "Se puede afirmar, sin riesgo a equivocarse que el RGPD es una disposición normativa que afronta una regulación con vistas a resolver problemas inmediatos, pero que se dota de los instrumentos necesarios para enfrentarse a los innumerables retos e incertidumbres que se abren en el futuro, también en el sector público"[23].

3.1.2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Al igual que ocurrió con la Directiva 95/46/CE, una vez entró en vigor el RGPD se inició el periodo previsto para trasladar a la normativa nacional de los Estados miembros las disposiciones de esta nueva legislación. Esta vez sí, con una diferencia. La Directiva permitía cierto margen de apreciación a los Estados para que, en función de sus necesidades y aspectos culturales, adaptasen el contenido de la misma a su marco legislativo. No obstante, en el presente supuesto, y es por ello que hablábamos de un fortalecimiento del régimen jurídico de la Unión en materia de protección de datos, el Reglamento se incorporase incorpora directamente al ordenamiento jurídico de los Estados, sin necesidad de materializarse en un texto normativo doméstico.

En nuestro caso, la introducción de lo establecido por el RGPD en la normativa española tuvo lugar a través de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), con entrada en vigor en diciembre de 2018, consecuentemente derogando la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que regía la protección de datos hasta el momento. Respecto a su contenido, entonces, no dista significativamente de aquel del RGPD, precisamente debido al principio de aplicación directa que caracteriza a los reglamentos de la Unión.

Aun así, cabe señalar un aspecto concreto que diferencia a la LOPDGDD del RGPD, y este es el reconocimiento entre sus líneas de los denominados "derechos digitales"[24], como ya nos avanzaba su propio título, y sobre los cuales RALLO LOMBARTE ha emitido la siguiente opinión:

---

[23] Vid., JIMÉNEZ ASENSIO, R., "El nuevo marco", o.c., p. 323.

[24] Regulados en su Título X, algunos de estos "derechos digitales" incluyen el derecho a la neutralidad de Internet (art. 80), el derecho de acceso universal a Internet (art. 81), el derecho a la seguridad digital (art. 82), el derecho a la educación digital (art. 83), el derecho a la desconexión digital en el ámbito laboral (art. 88) y el derecho al testamento digital (art. 96). Cabe destacar que estos derechos se ven desarrollados en la recientemente aprobada Carta de Derechos Digitales (2021), si bien esta constituye un instrumento de "*soft-law"* que carece de naturaleza jurídicamente

> "La LO 3/2018 constituye un salto cualitativo en la necesidad de garantizar en la sociedad digital contemporánea derechos que garanticen la subordinación de la tecnología al individuo y que preserven su dignidad en la totalidad de ámbitos en que las personas actúan en sociedad. Los nuevos derechos digitales incluidos en su título X permiten verificar la necesidad de trasladar la garantía efectiva de los derechos constitucionales al mundo virtual, adaptándolos a las singularidades de la realidad *online"*[25].

3.2. Legislación relevante en materia de investigación biomédica: Ley 14/2007, de 3 de julio, de Investigación biomédica

La Ley de Investigación biomédica (LIB), que data de 2007, constituye la primera normativa en tratar las cuestiones y problemáticas que emanan de la investigación científica en el campo de la biomedicina[26] -a pesar de la presencia de algunos textos reguladores de aspectos más concretos como la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud (Capítulo IV relativo a la investigación en salud)[27]. Esta normativa se adopta en base al art.

---

vinculante. Como se indica en sus consideraciones previas, *"la Carta de derechos digitales que se presenta no trata de crear nuevos derechos fundamentales sino de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros"*.

[25] RALLO LOMBARTE, A., "Una nueva generación de derechos digitales", en *Revista de Estudios Políticos* (Madrid), 187 (2020) 131.

[26] ARANDA JURADO determina que la aprobación de la LIB tuvo la intención de *"dar respuesta al agigantado avance de la investigación y a los nuevos métodos y técnicas aplicados en la evolución de la biomedicina, que reivindicaban un necesario avance también en el ámbito legislativo"*. Vid., ARANDA JURADO, M., "Evolución de la normativa de la investigación biomédica en España", en *Actualidad Jurídica Iberoamericana* (Valencia), 9 (2018) 256. En este sentido, cabe destacar que el preámbulo de la LIB alude a los dos principales textos internacionales que toma como referencia para el desarrollo de su contenido, dirigido a *"asegurar el respeto y la protección de los derechos fundamentales y las libertades públicas del ser humano y de otros bienes jurídicos relacionados con ellos a los que ha dado cabida nuestro ordenamiento jurídico, de forma destacada la Constitución Española y el Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina, suscrito en Oviedo el día 4 de abril de 1997, y que entró en vigor en España el 1 de enero de 2000* [mayormente conocido como "Convenio de Oviedo"]*"*. Así, más concretamente, GÓMEZ SÁNCHEZ señala que el primer artículo de esta Ley "*está claramente inspirado en el también artículo 1.1 del Convenio sobre Biomedicina y Derechos Humanos, en lo que se refiere a la mención de la dignidad e identidad del ser humano aunque el Convenio añade que garantizará a toda persona, sin discriminación alguna, el respeto a su integridad y a los demás derechos y libertades fundamentales, expresión que la Ley de Investigación Biomédica incluye en otro precepto, en concreto en el artículo 2. a)."* Vid., GÓMEZ SÁNCHEZ, Y., "La libertad de creación y producción científica: especial referencia a la Ley de Investigación biomédica", en *Revista de Derecho Político* (Madrid), 75-76 (2009) 492 y 493. Por tanto, la importancia del Convenio de Oviedo como referente para el impulso y la redacción de la LIB es indiscutible.

[27] *Ibid.*, pp. 500 y 501.

149.1.15ª CE, que reconoce que *"El Estado tiene competencia exclusiva sobre las siguientes materias: 15.ª Fomento y coordinación general de la investigación científica y técnica"*[28].

A partir del contenido de su art. 1 referente al objeto y ámbito de aplicación de la Ley, se infiere que esta se redacta con el propósito de *"cubrir una necesidad de regulación en materias muy sensibles por su vinculación e implicaciones en los derechos fundamentales y, especialmente, reúne en una norma jurídica los aspectos esenciales de la investigación en Biomedicina"*[29]. En relación con este primer precepto, GÓMEZ SÁNCHEZ reflexiona acerca de la decisión que ha tomado el legislador de utilizar el término "derechos inherentes a la persona" en lugar de "derechos fundamentales y libertades públicas", como se referencia en el Capítulo segundo de la Constitución, pues este pequeño matiz puede tener repercusiones en el alcance jurídico de la normativa. Sus consideraciones se leen a continuación:

> "En una interpretación estricta, estos derechos inherentes de la persona serían aquellos mencionado[s] -junto a la dignidad- en el artículo 10.1 de la Constitución (fuera de la sección 1ª, del capítulo II, del título I), que, sin embargo, la Constitución no relaciona. Estimo que los derechos inherentes citados en el artículo 10.1 CE no son otros sino los que la propia Constitución consagra a lo largo del Título I. Es decir, que no hay derechos inherentes fuera de la Constitución ni hay derechos constitucionales que no sean inherentes a la persona, especialmente en relación con el estándar europeo actual de derechos y libertades. Cabría otra interpretación conforme a la cual los derechos inherentes serían aquéllos directamente relacionados con el ser humano (vida, integridad,….), si bien esta tesis no es fácilmente deducible de la Constitución y no aporta mayores garantías a la persona. Por todo ello, creo que debe hacerse una interpretación integrada de los artículos 1.1 y 2 a) y entender que el objeto de la ley no desconoce el respeto a los derechos fundamentales sino que los mismos están incluidos entre los derechos inherentes a los que se alude en el artículo 1.1 de la Ley"[30].

[28] En cuanto a las Comunidades Autónomas, sobre aquellas cuyos Estatutos de Autonomía así lo dispongan (art. 148.1.17 CE) recae también el principio rector del art. 44.2 CE, que impone a los poderes públicos el cometido de promover la ciencia y la investigación científica y técnica a fin de obtener un provecho general. Vid., ARANDA JURADO, M., "Evolución de la…", o.c., p. 257.

[29] Vid., GÓMEZ SÁNCHEZ, Y., "La libertad de…", o.c., p. 493.

[30] *Ibid.*, p. 501. Esta interpretación va en línea con lo dispuesto en el preámbulo de la LIB, según el cual *"esta Ley tiene como uno de sus ejes prioritarios asegurar el respeto y la protección de los derechos fundamentales y las libertades públicas del ser humano y de otros bienes jurídicos relacionados con ellos a los que ha dado cabida nuestro ordenamiento jurídico"*.

Si continuamos indagando en el tenor literal de este artículo, podemos apreciar el desarrollo que realiza la LIB del contenido esencial del derecho fundamental, en la medida en que hace alusión al derecho a la producción científica, consagrado en el art. 20.1.b) CE: *"Se reconocen y protegen los derechos: b) A la producción y creación literaria, artística, científica y técnica"*. Así, la Ley regula detalladamente, por un lado, los derechos de los sujetos participantes en una investigación biomédica y, por otro, los derechos y obligaciones que se imponen a los profesionales; siendo esta segunda vertiente la que, precisamente, desarrolla de forma directa el contenido del art. 20.1.b) CE[31]. Asimismo, el art. 10 LIB preceptúa, para obedecer a este mandato constitucional, que *"La promoción de la investigación biomédica se atendrá a criterios de calidad, eficacia e igualdad de oportunidades"*.

Esta idea nos lleva a acudir al art. 2 LIB, que recoge los principios y garantías de la investigación biomédica: la protección de la dignidad e identidad del ser humano, la prevalencia de la salud, el interés y el bienestar del ser humano por encima del interés de la sociedad o de la ciencia, la confidencialidad en el tratamiento de los datos personales, la libertad de investigación y de producción científica, el carácter obligatorio de aportar un informe favorable del Comité de Ética de la Investigación para iniciar los proyectos, el principio de precaución y la evaluación de la investigación[32]. A este respecto, GÓMEZ SÁNCHEZ apunta que *"algunos de los principios contenidos en este precepto de la LIB son verdaderos derechos fundamentales que, sin embargo, adoptan aquí la forma de principios aun sin perder su naturaleza de derechos (tal es el caso de la confidencialidad, la protección de datos o de la prohibición de discriminación)"*[33].

Un tercer aspecto a destacar, como una de las novedades que incorpora la LIB, es el referente a la creación de tres órganos colegiados con competencias en materia de gestión y evaluación de las investigaciones biomédicas, que se explican a continuación[34].

- Los Comités de Ética de la Investigación. Se encuentran regulados en el art. 12 LIB, donde se aporta una definición y se establecen sus funciones básicas. Además, de acuerdo con la norma, será necesaria para su acreditación *"la independencia e imparcialidad de sus miembros respecto de los promotores e investigadores de los proyectos de investigación biomédica, así como su composición interdisciplinar"*.

[31] *Ibid.*, p. 498.

[32] Para un mayor detalle sobre las directrices básicas que guían la actuación en investigación biomédica, vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica de la persona en el ámbito de la Biotecnología y del Big Data*, Madrid 2022, pp. 28-32.

[33] Vid., GÓMEZ SÁNCHEZ, Y., "La libertad de…", o.c., pp. 503 y 504.

[34] Vid., ARANDA JURADO, M., "Evolución de la…", o.c., pp. 258-260.

- La Comisión de Garantías para la Donación y Utilización de Células y Tejidos Humanos. Fue fundada en 2012 -relevando a su antecesora, la Comisión de Seguimiento y Control de Donación y Utilización de Células y Tejidos Humanos, en funcionamiento desde 2004-, y se trata de un órgano de naturaleza permanente y consultiva, que está adscrito al Instituto de Salud Carlos III. Entre las garantías legales que debe avalar como parte de sus funciones, llama la atención el requisito de presentar un informe previo favorable de la Comisión para la aprobación de los proyectos de investigación que versen sobre las materias tasadas (art. 35 LIB). Cabe añadir que esta Comisión fue desarrollada reglamentariamente, haciendo uso de la Disposición final tercera.c) de la LIB[35], por el Real Decreto 1527/2010, de 15 de noviembre, por el que se regulan la Comisión de Garantías para la Donación y Utilización de Células y Tejidos Humanos y el Registro de Proyectos de Investigación.

- El Comité de Bioética de España. Explica el preámbulo de la LIB que *"el Comité de Bioética de España se crea como el órgano* [colegiado, independiente y de carácter consultivo] *competente para la consulta de todos aquellos aspectos con implicaciones éticas y sociales del ámbito de la Medicina y la Biología y está llamado a fijar las directrices y principios generales para la elaboración de códigos de buenas prácticas de investigación científica que desarrollen los Comités de Ética de la Investigación"*. Su importancia en el ámbito de la investigación biomédica es tal que consta de un Título propio en el texto (Título VII). El Comité se constituyó el 22 de octubre de 2008 y se encuentra adscrito al Ministerio de Sanidad, Consumo y Bienestar Social.

IV. LAS CATEGORÍAS ESPECIALES DE DATOS PERSONALES EN EL RGPD Y LA LOPDGDD: LOS DATOS RELATIVOS A LA SALUD

4.1. Las bases legítimas del tratamiento de datos: el consentimiento del interesado

De acuerdo con el principio de licitud[36] que impregna el RGPD, el inicio de actividades que implican un tratamiento de datos de carácter personal

[35] *"Se faculta al Gobierno para dictar cuantas disposiciones resulten necesarias para el desarrollo y ejecución de esta Ley, y en particular para establecer: c) El funcionamiento y desarrollo de la Comisión de Garantías para la Donación y Utilización de Células y Tejidos Humanos, que sustituirá a la vigente Comisión de Seguimiento y Control de Donación y Utilización de Células y Tejidos Humanos".*

[36] *"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de*

requiere que el denominado "responsable del tratamiento"[37] determine, en cualquier caso, la base jurídica aplicable para dicho tratamiento[38]. El consentimiento del interesado constituye el primero de los seis elementos de licitud del tratamiento de datos personales que recoge el RGPD, y así lo manifiesta en su considerando 40:

> "Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato".

De igual modo lo recoge el art. 8, párrafo segundo, de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE), al consagrar que los datos de carácter personal se tratarán "*sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley"*. A este respecto, cabe realizar dos consideraciones: en primer lugar, se reconoce expresamente el papel del consentimiento como elemento esencial del derecho fundamental a la protección de datos personales; y, en segundo lugar, el tratamiento que le otorga la CDFUE en calidad de criterio de licitud para el tratamiento de estos datos, dirimiendo de forma simultánea que se pueden establecer otros criterios alternativos por ley[39].

---

otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados". Vid., Reglamento General de Protección de Datos, considerando (39).

[37] El art. 4.7 RGPD define ampliamente al "responsable del tratamiento" o "responsable" como *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"*; pues su finalidad reside en consolidar, por medio de una definición amplia de la noción de "responsable", una protección integral y eficaz de los interesados. Vid., en este sentido, SSTJUE de 13 de mayo de 2014, Google Spain y Google, C-131/12, EU: C:2014:317, § 34; de 5 de junio de 2018, Wirtschaftsakademie Schleswig-Holstein, C-210/16, EU:C:2018:388, § 28; y de 29 de julio de 2019, Verbraucherzentrale NRW eV, C-40/17, EU:C:2019:629, § 66. A este respecto, el TJUE ha concretado que "*una persona física o jurídica que, atendiendo a sus propios objetivos, influye en el tratamiento de datos personales y participa, por ello, en la determinación de los fines y los medios de dicho tratamiento puede ser considerada responsable del tratamiento"*. Vid., SSTJUE de 10 de julio de 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, § 68; y de 29 de julio de 2019, Verbraucherzentrale NRW eV, C-40/17, EU:C:2019:629, § 68.

[38] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, 2020, p. 5.

[39] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 15/2011 sobre la definición del consentimiento*, 2011, p. 6.

El RGPD adopta la misma postura al equiparar, en su art. 6, todos los supuestos de legitimación del tratamiento, prescindiendo de primacías entre ellos[40]. Reza el precepto que *"el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones"*, a saber: la existencia de una relación contractual, de intereses vitales del interesado u otras personas, el cumplimiento de una obligación legal para el responsable del tratamiento, el interés público o ejercicio de poderes públicos, y el interés legítimo prevalente del responsable o de terceros a los que se comunican los datos en cuestión. Impone así la obligación de cumplir imperativamente con, al menos, una de estas bases legítimas, sea el consentimiento u otra, para que el tratamiento de datos se considere ajustado a Derecho.

Define el RGPD en su art. 4.11 -y de igual modo el art. 6 LOPDGDD, siguiendo su tenor literal- el "consentimiento del interesado" como "*toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen"*[41]. Por tanto, el consentimiento requiere de cuatro elementos para que se considere válido:

---

[40] Vid., TRONCOSO REIGADA, A., "Investigación, salud pública*...",* o.c., p. 218. Como indica el propio autor, esta previsión sigue el tenor del art. 7 de la Directiva 95/46/CE, precedente del actual Reglamento, que establecía lo siguiente: *"Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:*

a) el interesado ha dado su consentimiento de forma inequívoca, o

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva".

[41] De la misma manera, el RGPD, en su considerando 32, establece que el consentimiento debe otorgarse *"mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal"*. Así, se utilizan como ejemplos el marcar una casilla de un sitio web en Internet o escoger parámetros técnicos para la utilización de servicios informáticos; aunque el primero no queda exento de duda, pues como aclara el Tribunal de Justicia de la Unión Europea: *"en tales supuestos, parece prácticamente imposible determinar de manera objetiva si el usuario de un sitio de Internet ha dado efectivamente su consentimiento para el tratamiento de sus datos personales al no quitar la marca de una casilla marcada por defecto y si dicho consentimiento ha sido dado, en todo caso, de manera informada. En efecto, no puede descartarse que dicho*

- Que sea libre. El término "libre" entraña un verdadero ejercicio de albedrío, así como un control o dominio real por parte del interesado[42]; esto es, no debe existir un desequilibrio entre el afectado y el responsable del tratamiento[43]. Dicha alteración puede venir dada por varios motivos, entre ellos, que al interesado no se le permita el rechazo o la retirada de su consentimiento sin verse obligado a soportar algún tipo de menoscabo[44] o que se vea forzado a otorgar el mismo[45]. En definitiva, "*el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado (que puede manifestarse de formas muy distintas) que impida que este ejerza su libre voluntad"*[46], de modo que sólo se considera que el interesado actúa libremente cuando ocupa un papel protagonista en el proceso de toma de decisión relativo a si accede o no a que sus datos personales sean tratados en el contexto en cuestión[47].

---

usuario no haya leído la información que acompaña a la casilla marcada por defecto, o que ni tan siquiera la haya visto, antes de proseguir con su actividad en el sitio de Internet que visita". Vid., SSTJUE, de 11 de noviembre de 2020, Orange România, C-61/19, EU: C:2020:901, § 37; y de 1 de octubre de 2019, Planet49, C-673/17, EU:C:2019:801, § 55.

[42] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, 2018, p. 6.

[43] Vid., TRONCOSO REIGADA, A., "Investigación, salud pública...", o.c., p. 222. El RGPD, en su considerando 42, introduce un matiz: *"en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento"*.

[44] Reglamento General de Protección de Datos, considerando (42). Son relevantes en este sentido el art. 7.3 (*"El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo"*), el art. 13.2.c) (*"el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada"*), y el art. 14.2.d) ("*el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado: d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada"*) del Reglamento.

[45] Vid., GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el…*, o.c., p. 6.

[46] *Ibid.*

[47] GIL GONZÁLEZ, E., *El interés legítimo en el tratamiento de datos personales*, Madrid 2022, p. 64.

- Que sea específico. Este requisito, estrechamente relacionado con aquel que demanda el consentimiento "informado" del afectado, pretende garantizar un cierto grado de control y transparencia para este último[48]. Cabe poner en relación esta característica con el deber de información del responsable sobre los fines del tratamiento y la base jurídica (arts. 13.1.c) y 14.1.c) RGPD) y con el principio de limitación de la finalidad (art. 5.1.b) RGPD); que trataremos en epígrafes posteriores. En síntesis, se traduce en la condición necesaria de que el consentimiento se preste para una o varias finalidades específicas[49], y así lo determina el considerando 32 RGPD: *"El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos"*. Es más, en caso de querer añadir o modificar la información, se requiere la obtención de un nuevo consentimiento, ya que, al no haber podido ser "razonablemente previstos" en el momento de otorgar el consentimiento inicial, se entiende que estamos ante un cambio del propósito original para el que se prestó el consentimiento[50].

- Que sea informado. En palabras del RGPD, *"para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales"*[51], lo que incluye cuáles son los datos y los motivos que justifican el tratamiento. Asimismo, la información debe ser comprensible, siendo necesario que se describa con precisión y claridad el alcance y las consecuencias del tratamiento[52], y que esté disponible para el interesado de manera inequívoca y en un lugar destacado[53].

- Que sea inequívoco. Dispone el considerando 32 RGPD que ni el silencio ni la inacción deben constituir consentimiento, sino únicamente aquella *"declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales"*. Por tanto, debe haber una certeza absoluta de que el interesado aceptó

[48] Vid., GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el…*, o.c., p. 13.
[49] *Ibid.*, p. 67.
[50] MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 78. El propósito es evitar el fenómeno conocido como "desviación del uso", que *"supone un riesgo para los interesados ya que puede dar lugar a un uso imprevisto de los datos personales por parte del responsable del tratamiento o de terceras partes y a la pérdida de control por parte del interesado"*. Vid., GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el…,* o.c., p. 13.
[51] *Ibid.*
[52] Vid., GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el…*, o.c., p. 19.
[53] Vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 77.

dar su consentimiento para el tratamiento de los datos[54]. Además, *"cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento"*[55].

4.2. Los datos de salud como categoría especial de datos. Análisis desde el ámbito de la investigación científica

Las denominadas "categorías especiales de datos" se encuentran reguladas en el art. 9 del RGPD[56], precepto que las define como *"datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física"*[57].

Utilizan el adjetivo "especiales" debido a que se trata de *"datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales"*; derechos y libertades que pueden estar sujetos a riesgos significativos en el contexto de su tratamiento[58], ya que el catálogo de datos que se enumeran bajo el término de "categorías especiales de datos" constituyen un "*conjunto de informaciones personales especialmente próximas al núcleo de la intimidad del individuo (art. 7 CDFUE y 18.1 CE) y de la libertad ideológica (art. 10 CDFUE y 16.2 CE), cuyo conocimiento fuera de los supuestos legales y sin las garantías adecuadas*

[54] *Ibid.*, p. 79.

[55] Reglamento General de Protección de Datos, considerando (42).

[56] La LOPDGDD también consta de un artículo noveno dedicado a las categorías especiales de datos, en el que alude al art. 9 RGPD y afirma, en su primer párrafo, que: *"A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico. Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda"*.

[57] El Convenio 108 fue el primer instrumento jurídicamente vinculante en calificar a un tipo específico de datos como "categorías particulares de datos", pues de acuerdo con su art. 6, *"Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas"*. Como podemos observar por el tenor literal del art. 9 RGPD, este último toma la definición del Convenio 108 como base para formular la suya propia y, además, la actualiza incorporando nuevos tipos de datos.

[58] Reglamento General de Protección de Datos, considerando (51).

puede acarrear un daño severo en los derechos de los ciudadanos, e influir en la adopción de decisiones por parte de terceras personas, que pueden entrañar un perjuicio para aquellos"[59]. Es por ello que, como se plasma en el propio Reglamento, esta categoría de datos merece una protección específica.

En su apartado primero el RGPD erige, como regla general, la prohibición de tratamiento como consecuencia, precisamente, de su naturaleza de carácter especial. No obstante, se recogen a continuación una serie de excepciones[60] *numerus clausus* a estas primeras líneas que justifican el tratamiento de los datos considerados "sensibles". Cabe enfatizar que, al tratarse de datos de categoría especial, es necesaria tanto la concurrencia de una de las bases de legitimación generales del art. 6 RGPD como la aplicación de una de las circunstancias del segundo párrafo del art. 9 RGPD para considerar lícito su tratamiento[61]. Es decir, con esgrimir una de las excepciones contenidas en el art. 9.2 no basta para que el tratamiento de los datos se estime ajustado a Derecho, pues es indispensable el cumplimiento de ambos preceptos.

Son varias las circunstancias del art. 9.2 RGPD para el tratamiento de datos de categoría sensible (consentimiento explícito del interesado[62], cumplimiento de obligaciones y ejercicio de derechos concretos del responsable o del interesado,

[59] SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales", en *Estudios de Deusto. Revista de Derecho Público* (Bilbao), 68 (2) (2020) 265.

[60] En este sentido, el considerando 51 señala que: *"Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento"*. Así, varias de estas habilitaciones requieren de un "sustento normativo" que recae en el derecho doméstico de los Estados miembros o en el Derecho de la Unión. Vid., CÁTEDRA DE DERECHO Y GENOMA HUMANO, *Informe sobre implicaciones legales para el desarrollo de un modelo de gestión de datos genéticos*, Universidad del País Vasco (2021), p. 18.

[61] Vid., *ibid*.

[62] En la normativa de protección de datos, el consentimiento constituye tanto un fundamento general de licitud (art. 6 RGPD) como un criterio específico en determinados contextos (art. 9.2.a) RGPD). Si queremos legitimar un tratamiento de datos considerados "especiales" en la base del consentimiento, la obtención del mismo deviene más exigente que la norma general, pues se prevé que para este tipo de casos el consentimiento debe ser "explícito". A modo de ejemplo, la Disposición Final 11ª LOPDGDD modifica el art. 15.1 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en el sentido de que *"Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos (...), el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley"*.

protección de intereses vitales del interesado u otra persona física…). Sin embargo, a los efectos del presente estudio, vamos a profundizar únicamente en el último apartado, según el cual se levanta la prohibición de tratamiento cuando:

> "el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado".

Específicamente, nos resulta de gran interés lo relativo al uso de datos de salud con fines de investigación científica[63]. Cuando hablamos del tratamiento de datos personales con fines de investigación científica, es necesario hacer alusión al art. 5 RGPD que establece los distintos principios referentes al tratamiento. En su apartado primero, letra b, se prevé que los datos de carácter personal serán *"recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales"*. Así, esta previsión nos remite al art. 89.1 del Reglamento relativo a las garantías y excepciones aplicables al tratamiento de datos con fines de investigación científica -entre otros-, sobre las que, en el presente supuesto, se establece que se tratarán de *"medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines.*

[63] Por "investigación científica" se entiende "*un proyecto de investigación establecido con arreglo a las correspondientes normas metodológicas y éticas relacionadas con el sector, de conformidad con prácticas adecuadas"*. Vid., COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Directrices 5/2020 sobre…*, o.c., p. 29. La única referencia a aquello que comprende la noción de "investigación científica" en el propio RGPD figura en el considerando 159, al subrayar que *"El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia (…)"*. Afirma SERRANO PÉREZ que esta delimitación del concepto es: (i) amplia, respecto a los campos científicos que engloba (*"que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado"*), y (ii) solidaria, en lo relativo a la concepción del interés social. Vid., SERRANO PÉREZ, M. M., "El marco jurídico…", p. 271. Sin embargo, el CEPD deja claro que este término *"no debe ampliarse más allá de su significado común"*, y aporta la definición *ut supra* referenciada. En lo que respecta a la definición del término acotado de "investigación biomédica" (que se estima parte de la investigación científica), según el preámbulo de la LIB, "*abarca la investigación básica y la clínica con exclusión de los ensayos clínicos con medicamentos y el implante de órganos, tejidos y células"*.

Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo".

Se infiere de la redacción de la norma que todo tratamiento de datos con este propósito queda sujeto a la adopción de una serie de garantías específicas recogidas en el Reglamento en forma de medidas técnicas y organizativas -que deben ser enfatizadas por el riesgo que suponen para los derechos de los interesados en este ámbito[64]-, entre las que destaca la minimización y la seudonimización de los datos; siendo esta última una de las más notables en el contexto de la investigación biomédica. RECUERO LINARES remarca que también existen otras modalidades que no se han visto reflejadas en este artículo, pero que, sin embargo, aparecen en el texto legal europeo. Algunos ejemplos son las evaluaciones de impacto, la intervención de delegados de protección de datos, los códigos de conducta, el "soft-law"[65], la revisión de la investigación por parte de Comités de Ética de la Investigación acreditados, la supervisión de las cesiones de datos y la firma de acuerdos de cesión[66]. No obstante, recae sobre los Estados miembros la decisión de elegir las garantías que estimen oportunas para asegurar que el tratamiento de datos personales con fines de investigación científica se ajusta a la normativa presente[67].

En lo que respecta a nuestro país, la única referencia que contiene la LOPDGDD en cuanto al tratamiento de categorías especiales de datos personales es lo dispuesto en el art. 9, que regula la necesidad de que se preste un consentimiento explícito[68]; es por ello que debemos recurrir a los criterios de licitud que consagra el RGPD a fin de legitimar el tratamiento de estos datos sensibles[69].

---

[64] Vid., SERRANO PÉREZ, M. M., "El marco jurídico…", o.c., p. 272.

[65] RECUERO LINARES, M., *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado*, Accésit del Premio de Investigación en Protección de Datos Personales Emilio Aced de la Agencia Española de Protección de Datos 2019, p. 36. Por otra parte, el autor califica esta exigencia de proporcionar garantías "como una suerte de contrapartida" por lo que denomina el régimen "privilegiado" que recae sobre este tipo de tratamientos a lo largo de todo el texto normativo.

[66] Vid., CÁTEDRA DE DERECHO Y GENOMA HUMANO, *Informe sobre implicaciones…*, o.c., p. 23. Incluso se propone, como manifestación de este principio, la institución tanto de un comité encargado de controlar el acceso a los datos -el conocido como *Data Access Committee* (DACO)-, como de un comité de seguimiento de los aspectos éticos y jurídicos.

[67] Vid., SERRANO PÉREZ, M. M., "El marco jurídico…", o.c., p. 272.

[68] En su primer párrafo, establece: *"A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico".*

[69] Vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 84.

4.3. Los principios de minimización de datos y limitación de la finalidad

La minimización de datos se manifiesta como principio vertebrador del tratamiento de datos de carácter personal en el art. 5.1.c) RGPD, de acuerdo con el cual los datos personales deben ser *"adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"*. Su objetivo consiste en garantizar que no se recojan y almacenen más datos personales de los estrictamente necesarios para cumplir con los fines establecidos[70]. El propio RGPD lo recoge como un principio a aplicar de forma explícita en los tratamientos de datos con fines de investigación científica:

> "El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos"[71].

En esta línea, complementa el considerando 39 RGPD la definición dada por el art. 5.1.c), afirmando que, para que los datos personales sean adecuados, pertinentes y limitados a lo necesario para los fines para los que son tratados, se debe "*garantizar que se limite a un mínimo estricto su plazo de conservación. (…) Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica"*.

De la redacción de estos preceptos, se pueden realizar las siguientes consideraciones.

---

[70] GRUPO DE TRABAJO INTERNACIONAL SOBRE PROTECCIÓN DE DATOS EN LAS TELECOMUNICACIONES, *Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics*, 55th Meeting, 5-6 May 2014, Skopje, Macedonia, p. 6.

[71] Reglamento General de Protección de Datos, considerando (156). Asimismo, el art. 25.2 RGPD, que regula la protección de datos por defecto, establece que *"El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas"*.

1º. El principio de minimización requiere que, previo al tratamiento, se conozca claramente cuál es la finalidad para tratar los datos, pues, de lo contrario, no es posible determinar si se cumple con lo dispuesto en el art. 5.1.c) RGPD.

2º. Se puede observar un elemento temporal que precisa la eliminación de los datos una vez dejen de ser necesarios para cumplir con la finalidad del tratamiento. De igual manera, cuando se trate de una finalidad que englobe varias etapas, aquellos datos que no se consideren indispensables para las etapas posteriores, deberán suprimirse. Este factor hace que el principio de minimización de datos se encuentre estrechamente relacionado con el principio de "limitación del plazo de conservación", recogido en el art. 5.1.e) RGPD: *"Los datos personales serán: e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales"*. Si estamos ante un tratamiento con fines de investigación científica, entre otros, la norma establece que los datos podrán conservarse durante períodos de tiempo más extensos, siempre y cuando esta sea su única finalidad y se apliquen las medidas técnicas y organizativas apropiadas del art. 89.1 del Reglamento.

3º. Los adjetivos "adecuados" y "pertinentes" aluden a la necesaria idoneidad de los datos respecto a los fines para los cuales van a ser utilizados.

4º. En cuanto a la noción de "limitados a lo necesario en relación a los fines", el precepto hace referencia al principio de limitación de la finalidad del art. 5.1.b) RGPD, donde se establece que los datos personales serán *"recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines"*. De forma complementaria, el RGPD dispone que *"El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial"*[72]. Este principio, por tanto, se basa en la premisa de que los datos de carácter personal deben ser únicamente recabados cuando se hayan establecido *a priori* los objetivos lícitos y concretos que regirán su posterior tratamiento[73].

Sin embargo, existen dos excepciones a este principio en el ámbito de la investigación biomédica, para las cuales la base legítima del consentimiento

[72] Reglamento General de Protección de Datos, considerando (50).

[73] VARIOS, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Barcelona 2015, Grupo de Opinión del Observatorio de Bioética y Derecho de la Universitat de Barcelona, p. 39.

se entiende normativamente de forma amplia. Se consideran las dos caras de una misma moneda: mientras el consentimiento por línea o área de investigación facilita la obtención del consentimiento para el uso de datos dentro de una misma línea o área de investigación, la reutilización (o uso secundario) de datos permite que se utilicen los datos recogidos en base a un consentimiento específico para otros proyectos que integran esa misma línea o área de investigación[74].

4.3.1. El consentimiento por línea o área de investigación

El RGPD, en su considerando 39, establece que *"los fines específicos del tratamiento de los datos personales (…) deben determinarse en el momento de su recogida"*, pues tradicionalmente siempre se ha precisado que el consentimiento se debía otorgar para un proyecto de investigación en concreto, siendo inadmisible la concesión de un consentimiento abierto para proyectos de finalidades similares o pertenecientes a una misma área de investigación por no cumplir con el tenor de lo que se entiende por "consentimiento explícito"[75].

No obstante, como señala su anterior considerando 33: *"Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida"*, de modo que el Reglamento se posiciona a favor de un uso más flexible del consentimiento[76] y admite la posibilidad de prestar consentimiento por área de investigación[77]. Cabe poner esta previsión en relación con el art. 6.2

[74] MÉNDEZ GARCÍA, M. y ALFONSO FARNÓS, I., "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada* (Leioa), Núm. Extraord. (2019) 215.

[75] *Ibid.*, p. 212.

[76] *"Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida"*. Vid., Reglamento General de Protección de Datos, considerando (33).

[77] En calidad de intérprete del considerando 33 RGPD, la AEPD concluye que *"De todo ello se derivaría que los requisitos de especificidad y carácter inequívoco para la prestación del consentimiento no deben ser interpretados en el ámbito de la investigación científica de un modo restrictivo, limitado a una concreta investigación de la que se facilite toda la información disponible, sino que cabe considerar que concurren en los supuestos en los que el consentimiento se presta en relación con un determinado campo de investigación, pudiendo extenderse en el futro ese consentimiento, sin que ello lo vicie en modo alguno, incluso a "finalidades" o áreas de investigación que ni siquiera hubieran podido determinarse en el momento en que se prestó sin que sea necesario recabar un nuevo consentimiento del sujeto fuente, teniendo en cuenta los beneficios para los individuos y la sociedad en su conjunto que pueden derivarse de tal*

LOPDGDD, que establece que *"Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas"*. La AEPD se ha pronunciado a este respecto para aclarar que:

> "no sería preciso, para garantizar el carácter inequívoco y específico del consentimiento [requisitos a los que alude el art. 6.2 LOPDGDD], que el mismo fuese prestado para la realización de una investigación concreta; ni siquiera para la realización de investigaciones en una rama muy delimitada, (…) sino que, teniendo en cuenta la interpretación derivada directamente del propio Reglamento, será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación"[78].

A la vista de lo dispuesto, el Grupo de Trabajo del Artículo 29 sugiere al responsable del tratamiento de los datos que *"Cuando no puedan especificarse totalmente los fines de la investigación, (...) debe buscar otras maneras de garantizar que se protege la esencia de los requisitos de consentimiento, por ejemplo, permitir que los interesados den su consentimiento a un fin de investigación en términos más generales y a fases concretas de un proyecto de investigación que ya se conozcan desde el inicio"*[79].

De igual modo, la Disposición Adicional 17ª LOPDGDD, relativa al tratamiento de datos para fines de investigación en salud, consolida en su apartado segundo, letra a) la noción amplia de consentimiento del considerando 33 RGPD[80]: *"El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora"*. Este precepto reconoce las distintas modalidades de amplitud que puede abarcar el consentimiento del interesado, idea que se contrapone a la regla general de que el afectado debe otorgar su consentimiento para cada uno de los fines predeterminados. En consecuencia, *"se puede ir de lo más general a lo más específico, con fines de investigación biomédica o para áreas pertenecientes a una especialidad de investigación"*, aclara MARTÍNEZ VELENCOSO[81].

---

investigación no prevista". Vid., AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Informe 073667/2018, Gabinete Jurídico, p. 8.

[78] *Ibid*.

[79] Vid., GRUPO DE TRABAJO DEL ARTÍCULO 29, "Directrices sobre el…", o.c., p. 30.

[80] Vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 88.

[81] *Ibid*.

4.3.2. La reutilización de datos de salud con fines de investigación biomédica

La LOPDGDD también reproduce la posibilidad de reutilizar los datos relativos a la salud cuando tenga por objeto una investigación biomédica, diferenciando entre el uso de aquellos datos obtenidos con anterioridad a la entrada en vigor de la LOPDGDD y aquellos recogidos posteriormente. Por una parte, la reutilización de los datos recabados *a priori* se encuentra regulada en la Disposición Transitoria 6ª, que dice así:

> "Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:
>
> a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.
>
> b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial".

De acuerdo con lo expuesto, se habilita el uso de estos datos -obtenidos con el propósito de realizar un determinado estudio- para ulteriores proyectos de investigación de naturaleza similar o que se desarrollen en áreas de investigación relacionadas. Resulta notable que la única condición que se impone es la necesidad de que los estudios para los que se va a hacer uso de dichos datos se encuentren dentro de la misma área de investigación o de una que se encuentre vinculada a la misma, a diferencia de lo dispuesto para los datos de salud recopilados después de la entrada en vigor de la citada Ley[82]. En relación con estos últimos, cabe hacer referencia a la Disposición Adicional 17ª LOPDGDD, segundo apartado, y en este caso, a su letra c):

> "Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

[82] Vid., MÉNDEZ GARCÍA, M. y ALFONSO FARNÓS, I., *La legitimación para…*, o.c., p. 215.

> En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del 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 sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.
>
> Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación".

Así, para que la utilización de los datos recogidos con posterioridad sea legítima, además de los requisitos prescritos en la Disposición Transitoria 6ª, se requiere que se cumplan, de forma complementaria, dos condiciones. En primer lugar, un dictamen favorable del Comité de Ética de la Investigación es indispensable, como supervisor del buen funcionamiento del tratamiento de datos, pues dos de sus funciones clave son ponderar *"los aspectos metodológicos, éticos y legales del proyecto de investigación"*[83] y *"el balance de riesgos y beneficios anticipados dimanantes del estudio"*[84]. Por consiguiente, su intervención consistirá en comprobar que, efectivamente, el tratamiento se ajusta a los requisitos del RGPD; aunque, como percibe SERRANO PÉREZ, también es cierto que sería oportuno *"establecer pautas de actuación consensuadas para orientar las decisiones de los comités de ética de la investigación en lo que a protección de datos se refiere"*, a fin de que su actuación no se limite únicamente a lo dispuesto en el art. 12 LIB[85].

En segundo lugar, la información relativa al estudio en concreto debe ser publicada y facilitada al interesado, para dar cumplimiento al deber de información del responsable del tratamiento de datos como exige el art. 13.3 RGPD: *"Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior,*

[83] Ley 14/2007, de 3 de julio, de Investigación biomédica, art. 12.2.b).

[84] *Ibid.*, art. 12.2.c).

[85] Vid., SERRANO PÉREZ, M. M., "El marco jurídico…", o.c., p. 280. Sobre la aplicación del principio de transparencia (art. 5.1.a) RGPD) en las funciones del Comité de Ética de la Investigación en relación con la reutilización de datos de carácter personal, propone la autora el *"mostrar un borrador de la página web lo más explícito posible, así como la forma alternativa de comunicar la información a los interesados en caso de no disponer de medios electrónicos para conocerla"* como la vía más apropiada para garantizar este principio durante el procedimiento.

información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2"[86]. Cabe añadir que este requisito, asimismo, está en consonancia con el principio de transparencia (art. 5.1.a) RGPD) que rige todo tratamiento de datos, de suerte que resulta más sencillo comprobar la compatibilidad de las distintas finalidades[87]. Sin embargo, MÉNDEZ GARCÍA y ALFONSO FARNÓS apuntan a que este segundo requisito se presenta arduo en su puesta en práctica, especialmente respecto a su grado de cumplimiento real y al modo de llevarlo a cabo. Como solución, articulan, será necesario que las entidades a cargo de las investigaciones biomédicas establezcan las garantías y mecanismos pertinentes para que la reutilización de datos sea lícita; a la par que destacan la función crucial que desempeña el Delegado de Protección de Datos como asesor de los investigadores a estos efectos[88].

En otro orden de cosas, es necesario mencionar que cabe la posibilidad de que el afectado manifieste su oposición al uso secundario de sus datos personales con fines de investigación que no constituyen los iniciales. Es por ello que resulta de suma importancia que conste de forma pública, clara y visible, ya sea en la página web del centro o en la información enviada por correo electrónico, cómo pueden los titulares de los datos que no estén de acuerdo con la reutilización de los mismos ejercer su derecho de oposición al tratamiento[89].

V. ASPECTOS ÉTICO-LEGALES DE LA UTILIZACIÓN DE SISTEMAS *BIG DATA* CON FINES DE INVESTIGACIÓN BIOMÉDICA

5.1. Concepto y características principales del Big Data. Las "*seis uves*"

El término *"Big Data"* fue acuñado por primera vez por el científico informático y ex jefe de *Silicon Graphics* (SGI), John R. Mashey, a finales de los noventa[90],

[86] Este artículo demuestra la posición del legislador europeo, al permitir la posibilidad de utilizar datos personales con fines diferentes para los que se autorizó, mediante consentimiento, su recogida en un primer momento.

[87] Vid., SERRANO PÉREZ, M. M., "El marco jurídico…", o.c., p. 279. En este sentido, el COMITÉ EUROPEO DE PROTECCIÓN DE DATOS arguye que *"La transparencia constituye una garantía adicional cuando las circunstancias de la investigación no permiten obtener un consentimiento específico. Los responsables del tratamiento pueden compensar la falta de concreción del fin facilitando información periódica sobre el desarrollo del fin a medida que avanza el proyecto de investigación de manera que, con el tiempo, el consentimiento sea lo más específico posible. De esta manera, el interesado tiene, al menos, una noción básica de la situación, lo que le permite valorar si utilizar o no, por ejemplo, el derecho a retirar el consentimiento con arreglo al artículo 7, apartado 3".* Vid., COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Directrices 5/2020 sobre…*, o.c., p. 30.

[88] Vid., MÉNDEZ GARCÍA, M., y ALFONSO FARNÓS, I., *La legitimación para…*, o. c., pp. 217 y 218.

[89] Vid., SERRANO PÉREZ, M. M., "El marco jurídico…", o.c., p. 281.

[90] DIEBOLD, F. X., "On the Origin(s) and Development of "Big Data": The Phenomenon, the Term, and the Discipline", University of Pennsylvania (2019) 3.

con la elaboración de una presentación de diapositivas propia de SGI que llevaba por título *"Big Data and the Next Wave of InfraStress"*[91]. Estas diapositivas sirvieron de base para la posterior publicación de un artículo, con idéntico rótulo, en el que MASHEY reflexionaba acerca del considerable estrés y fatiga de los que estaban a punto de adolecer las infraestructuras físicas y humanas de la informática como consecuencia del "imparable tsunami de datos" que se vislumbraba en el horizonte, una cantidad que calificaba de inmanejable para los instrumentos de gestión que existían en el momento.

Otros autores de la época, como WEISS E INDURKHYA (1998)[92], empezaron a hacer uso del término al señalar que ya en aquel entonces se estaba iniciando una recopilación de colecciones muy grandes de datos en almacenes de datos centralizados, permitiendo, de este modo, a los analistas utilizar métodos eficaces de análisis para examinar dichas cantidades de datos más exhaustivamente. En esta línea, a pesar de la existente variedad de definiciones provenientes de fuentes dispares, la AEPD define el *"Big Data"* como el *"conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo"*[93]. Por otra parte, LANEY (2001)[94] desarrolló lo que se concibe como una primitiva determinación de las características propias de *Big Data*: las "tres uves"; esto es, volumen, variedad y velocidad.

- Volumen. A diferencia de la estadística tradicional que lleva a término sus estudios a partir de muestras, el *Big Data*, como su propio nombre indica, conlleva la recogida, el almacenamiento y el tratamiento de enormes cantidades de datos y metadatos[95].

- Velocidad. Tanto la obtención como el movimiento y el proceso de los datos se desarrolla a una gran velocidad, hasta el punto de suceder, en algunas ocasiones, en tiempo real[96]. Así, una de las grandes ventajas del *Big Data* es que

[91] Accesible en el siguiente link: https://static.usenix.org/event/usenix99/invited_talks/mashey.pdf.

[92] WEISS, S. M. e INDURKHYA, N., *Predictive Data Mining: A Practical Guide*, Burlington 1998.

[93] VARIOS, *Código de buenas prácticas en protección de datos para proyectos de Big Data*, elaborado para la Agencia Española de Protección de Datos (AEPD) y la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain), p. 3.

[94] LANEY, D., *3-D Data Management: Controlling Data Volume, Velocity and Variety*, META Group Research Note, 6 February 2001.

[95] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, Accésit en la XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, Madrid 2016, p. 21.

[96] Vid., VARIOS, *Código de buenas…*, o.c., p. 3.

hace posible la transferencia de datos de una forma eficiente y económica, de modo que permite que se analicen no sólo los datos dinámicos que continuamente son creados, sino también aquellos datos estáticos o históricos que han sido previamente almacenados[97].

- Variedad. Los datos que se utilizan para extraer información emanan de tres tipos de fuentes, según la clasificación de datos de JOYANES AGUILAR[98], y en consecuencia pueden ser: datos estructurados[99], semiestructurados[100] y no estructurados[101]; un factor que presenta dificultades por la heterogeneidad de las distintas fuentes[102]. Sin embargo, los sistemas *Big Data* están diseñados de forma tal que es posible combinar datos sin necesidad de que estén recopilados en ficheros que mantengan la misma estructura[103].

Adicionalmente, autores como GIL GONZÁLEZ indican que estas tres particularidades pueden complementarse, a fin de precisar la definición del concepto de *Big Data*, con la formulación de tres nuevas 'v': veracidad, visualización y valor de los datos[104].

- Veracidad. Tiene relación con el nivel de fiabilidad o calidad de los datos.

- Visualización. La visualización de los datos es clave para su comprensión y posterior toma de decisiones respecto a los mismos.

- Valor. El procesamiento de datos mediante sistemas *Big Data* tiene como propósito final crear valor, en forma de oportunidades económicas o de innovación.

---

[97] Vid., GIL GONZÁLEZ, E., *Big data, privacidad y…*, o.c., p. 21.

[98] Vid., JOYANES AGUILAR, L., *Big data: análisis de grandes volúmenes de datos en organizaciones*, Ciudad de México 2013.

[99] Se considera "datos estructurados" a *"aquellos que se presentan en un formato o esquema bien definido y que poseen campos fijos. Son hojas de cálculo, archivos, bases de datos tradicionales provenientes de CRM, ERP, etc., que han sido recolectados por profesionales del marketing en algún momento."* Vid., ARGANZA SALCEDO, R., y ARROYO LÓPEZ, M., "Big data: Aplicaciones de la gestión del dato en las distintas etapas del *funnel* de conversión", en *Revista de Marketing y Publicidad* (Madrid), 1 (2019) 49.

[100] En cuanto a los "datos semiestructurados", se dice que estos "*no tienen formato definido, pero sí contienen etiquetas u otros marcadores con el fin de clasificar los elementos de los mismos. En esta categoría encontramos textos con etiquetas XML y HTML".* Vid., *ibid*.

[101] Los "datos no estructurados" son "*datos de tipo indefinido, almacenados principalmente como documentos u objetos sin estructura fija ni bajo ningún patrón concreto. Pueden ser generados por máquinas y personas. Son archivos de audio, vídeo, fotografía y formatos de texto libre como emails, SMS, artículos, WhatsApp, etc."* Vid., *ibid*.

[102] Vid., *ibid*, p. 49.

[103] *Ibid*.

[104] Vid., GIL GONZÁLEZ, E., *Big data, privacidad y…*, o.c., p. 23 y 24.

Por su parte, el Instituto de Ingeniería del Conocimiento (IIC), ubicado en la Universidad Autónoma de Madrid, añade una séptima: la viabilidad[105]. En este caso, se refiere a la capacidad de utilizar de forma eficiente el enorme volumen de datos que manejan las empresas. Frente a esta definición tradicional del *Big Data*, donde se habla de "seis uves" -o más, dependiendo de la fuente-, GALLO SALLENT plantea que habría que agregar a la definición jurídica de *Big Data* lo que él denomina las "tres íes": identificables, interrelacionados y que infieran sobre las personas[106].

5.2. Retos jurídicos del *Big Data* en el ámbito de la protección de datos. Especial referencia a su aplicación en un contexto de investigación biomédica

5.2.1. La problemática de la desanonimización y la reidentificación de datos personales mediante el uso de *Big Data*

5.2.1.1. Anonimización vs. seudonimización de datos: ¿un mismo concepto jurídico?

El RGPD introduce, como uno de los mecanismos de garantía en el tratamiento de datos personales, la técnica de la "seudonimización". Este método permite *"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"*[107], y constituye una vía para armonizar la protección de los datos de carácter personal con el avance científico -reconocido en el art. 44 CE[108].

---

[105] Véase la entrada de blog aquí: https://www.iic.uam.es/innovacion/big-data-caracteristicas-mas-importantes-7-v/#viabilidad. No obstante, cabe señalar, además, que existen otros blogs donde afirman que son más las características propias del *Big Data*, llegando a incluir como tales la variabilidad (entendida, por un lado, como "*el número de inconsistencias en los datos [que] (…) deben ser encontrados por métodos de detección de anomalías y valores atípicos para que ocurra cualquier análisis significativo"* y, por otro, como "*la multitud de dimensiones de datos que resultan de múltiples tipos y fuentes de datos dispares"*; aunque, se añade, *"la variabilidad también puede referirse a la velocidad inconsistente a la que se cargan grandes datos en bases de datos"*), la validez (hace alusión a *"la limpieza que tienen los datos, a cuán precisos y correctos son para su uso"*) y la vulnerabilidad (es decir, *"toda preocupación de seguridad respecto a los datos"*). Al respecto, véase el siguiente link: https://www.datahack.es/10-vs-del-big-data/.

[106] GALLO SALLENT, J. A., *El big data. Implicaciones jurídicas para un cambio de paradigma: El derecho al olvido y el consentimiento* [Tesis doctoral, Universitat Internacional de Catalunya], Tesis Doctorals en Xarxa 2020, https://www.tdx.cat/handle/10803/670038#page=1, p. 401.

[107] Reglamento General de Protección de Datos, considerando (28).

[108] Vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 85.

Resulta de suma importancia puntualizar que no se deben confundir los términos "seudonimización" y "anonimización". Si bien es cierto que, como apunta GIL GONZÁLEZ, tradicionalmente la seudonimización se entendía comprendida entre los distintos métodos de la anonimización[109], hoy en día se conciben como procedimientos completamente distintos que encuentran, a su vez, diferencias de trato por parte de la legislación misma.

Si nos dirigimos al art. 4.5 RGPD, la "seudonimización" se define 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* [contempladas en el art. 89.1] *destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"*[110]. Por su parte, la LIB recoge el concepto de "anonimización", siendo este *"el proceso por el cual deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere".* Así pues, encontramos dos diferencias sustanciales.

En primer lugar, el considerando 26 RGPD establece que *"Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable"*, y aclara: *"Los datos personales seudonimizados (…) deben considerarse información sobre una persona física identificable*[111]*".* Por consiguiente, los principios y obligaciones de la normativa de protección de datos deben aplicarse a los datos seudonimizados, pues mantienen su estatus de dato de carácter personal. Sin embargo, no ocurre lo mismo con los datos anonimizados -o irreversiblemente disociados-[112], para los cuales dispone la norma que dichos principios de protección de datos no son aplicables, pues se trata de datos que *"no puede[n] asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionados"*[113]. Así, el considerando 26 RGPD *in fine* pone de manifiesto esta postura:

[109] Vid., GIL GONZÁLEZ, E., *El interés legítimo…*, o.c., p. 64.

[110] En relación con este precepto, cabe señalar que, interpretando su tenor literal, se permite el tratamiento de datos personales seudonimizados con fines de investigación, a condición de que la legislación interna de los Estados miembros así lo autorice.

[111] De acuerdo con el Tribunal de Justicia de la Unión Europea, *"se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".* Vid. STJUE de 19 de octubre de 2016, Breyer, C-582/14, EU: C:2016:779, § 32.

[112] Vid., VARIOS, *Documento sobre bioética…*, o.c., p. 33.

[113] Vid., Ley 14/2007, de 3 de julio, de Investigación biomédica, art. 3.i).

> "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

En segundo lugar, en relación con la calificación del dato seudonimizado como dato personal, es relevante destacar que la Disposición Adicional 17ª.d) LOPDGDD prevé la opción de reidentificar al titular de los datos, como excepción, *"cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria"*; de modo que, aunque por regla general se garantiza la confidencialidad, es posible reidentificar al titular de los datos en los supuestos tasados legalmente, pues se conserva cierta información adicional sujeta a las medidas técnicas y organizativas pertinentes que autorizan esta dispensa. Por el contrario, en el caso del tratamiento anonimizado de datos, no es presumible -o, en principio, no debería- que se pueda llevar a cabo.

Cabe señalar que la Disposición Adicional 17ª, párrafo segundo, letra d) considera *"lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica"*. Sin embargo, para que este uso de datos seudonimizados se ajuste a Derecho, es necesario que cumpla con una serie de requisitos mínimos que se enumeran a continuación:

> 1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.
>
> 2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:
>
> i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.
>
> ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Resulta indispensable poner en relación estas condiciones con la letra g) de la misma norma, de acuerdo con la cual *"El uso de datos personales seudonimizados*

con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial. En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679". Y si recordamos lo dispuesto para el uso secundario de datos de salud en la Disposición Adicional 17ª.2.c), se solicita, en este caso también, el visto bueno del Comité de Ética para la Investigación.

5.2.1.2. Riesgos de las técnicas de anonimización de datos para el afectado

A pesar de la indudable relevancia que se les otorga a los métodos de anonimización en el ámbito de la investigación científica, como hemos podido observar en el considerando 26 RGPD[114], expertos afirman que, en la actualidad, se ha demostrado que este procedimiento ya no puede garantizar la privacidad de los datos de carácter personal, debido a que se han desarrollado técnicas de ingeniería informática que posibilitan la trazabilidad de los datos hasta su titular[115]. En este sentido, la *Federal Trade Commission* de Estados Unidos ha puesto de manifiesto que: *"Hay evidencias suficientes que demuestran que los avances tecnológicos y la posibilidad de combinar diferentes datos puede conllevar la identificación de un consumidor, ordenador o dispositivo, incluso si estos datos por sí mismos no constituyen datos de identificación personal. Es más, no solo es posible reidentificar datos que no son identificadores personales a través de medios diversos, sino que las empresas tienen fuertes incentivos para hacerlo"*[116].

Estas "técnicas" hacen alusión a los sistemas *Big Data*, que son capaces de analizar grandes cantidades de datos hasta conseguir reidentificar a los afectados; y lo que es más preocupante, lo llevan a cabo utilizando datos que no están catalogados como de identificación personal e, incluso, a partir de datos anónimos o irreversiblemente disociados[117]. Esto se debe a que el riesgo de reidentificación de los sujetos aumenta con la recopilación y cruce de datos de fuentes de naturaleza diversa -que *a priori* se presentan como anónimos- con otras bases de datos disponibles, lo que demuestra que la anonimización como método de protección de datos carece de efectividad[118].

---

[114] Vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 84.

[115] Vid., VARIOS, *Documento sobre bioética…*, o.c., p. 33.

[116] FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for businesses and policymakers*, Informe, 2012, p. 20.

[117] Vid., GIL GONZÁLEZ, E., *Big data, privacidad y…*, o.c., p. 88.

[118] Vid., GRUPO DE TRABAJO INTERNACIONAL SOBRE PROTECCIÓN DE DATOS EN LAS TELECOMUNICACIONES, *Working Paper on…*, o.c., p. 7.

A diferencia del procedimiento de seudonimización para el cual está prevista la posibilidad de reidentificar los datos en su origen *"cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria"*[119], en el caso de la anonimización esta opción no se contempla, dado que las técnicas de anonimización están diseñadas para que no sea posible singularizar a los afectados, desvinculando los datos de su persona a fin de evitar el riesgo de desanonimización. Por esta misma razón, el tratamiento de los datos anonimizados o irreversiblemente disociados no está amparado bajo la normativa de protección de datos; aunque ello no quiere decir que no esté sujeto a garantías tasadas por el legislador[120].

El El Grupo de Trabajo Internacional sobre Protección de Datos en las Telecomunicaciones -conocido como "Grupo de Berlín"- ha calificado la posible reidentificación del titular de los datos personales como uno de los principales riesgos asociados al análisis de *Big Data*, que evidencian las limitaciones de la que se presentaba como la solución óptima para tratar los datos protegiendo la privacidad de los sujetos: queda patente la disminución de los efectos de la anonimización como medida para asegurar la protección íntegra de la privacidad y la confidencialidad de los datos, especialmente en la era del *Big Data*.

En conclusión, *"Es unánime entre los expertos en protección de datos, la advertencia sobre la necesidad que existe de que mecanismos seguros, fiables y consistentes permitan la total anonimización de los datos de los pacientes, y que*

[119] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, Disposición Adicional 17ª.2.d). Sin embargo, esta permisión también tiene su "contra", pues al igual que es posible reidentificar los datos en los supuestos mencionados, en caso de hacerlo en situaciones distintas a las legalmente previstas, se considerará una de las infracciones catalogadas como "muy graves" por el art. 72 LOPDGDD: *"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes: p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados".*

[120] A modo de ejemplo, el art. 5.3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), establece que: *"Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento".*

estos mecanismos impidan la identificación del sujeto mediante la vuelta atrás del proceso y su reidentificación"[121]. Asimismo, se requiere que estos métodos se ejecuten junto a la implementación de garantías que prevengan los riesgos que se generan como resultado del uso del *Big Data*[122].

5.2.2. ¿Sigue siendo el consentimiento la base legal para el tratamiento de datos más adecuada a la luz de los nuevos avances tecnológicos?

Tras haber analizado las disposiciones que regulan las bases legitimadoras del tratamiento de datos de salud en el marco de una investigación científica, cabe dilucidar si, efectivamente, el actual modelo de consentimiento -que constituye el criterio "predilecto" para tratar este tipo de datos- continúa siendo el más adecuado desde la implantación de las tecnologías *Big Data* en este contexto.

Partiendo de la magnitud del volumen de datos personales que manejan los sistemas *Big Data*, resulta lógico llegar a la conclusión de que su uso lleva aparejado el riesgo de realizar nuevos tratamientos de estos datos sin el consentimiento explícito del afectado, debido a la evidente complejidad que supone el recabar tal consentimiento de una gran cantidad de personas. Y es que, como indica el "Informe Sobre Big data en salud" (2017), dirigido por José María SAN SEGUNDO ENCINAR, en relación con las opiniones proporcionadas por varios expertos[123]:

> "Big data precisa almacenar una enorme cantidad de datos procedentes, en su mayoría, de los pacientes. Estos datos personales son extremadamente sensibles y será preciso que la normativa que garantice los derechos en este ámbito consiga asegurar la confidencialidad de la información sin que ello suponga un freno para su propio desarrollo. En este sentido, la mayoría de los profesionales consultados muestran una cierta insatisfacción con el actual marco normativo, hasta el punto que para muchos de ellos, es la principal barrera a superar"[124].

Así, a pesar de la tradicional preferencia por el consentimiento como base legitimadora, hoy en día se pronuncian cada vez más voces que se manifiestan a

[121] Vid., CRISTEA UIVARU, L., "La protección de…", o.c., p. 304.

[122] Vid., MARTÍNEZ VELENCOSO, L. M., *La protección jurídica…*, o.c., p. 85.

[123] Entre los que se incluye MARTÍNEZ MARTÍNEZ, como así lo manifiesta en MARTÍNEZ MARTÍNEZ, R., "Big data, investigación en salud y protección de datos personales. ¿Un falso debate?", en *Revista Valenciana d'Estudis Autonòmics* (Valencia), 62 (2017) 254.

[124] SAN SEGUNDO ENCINAR, J. M., *Big data en salud digital*, Madrid 2017, p. 9.

favor del uso de garantías alternativas para garantizar el derecho fundamental a la protección de datos de carácter personal[125]. Mientras BROWNSWORD afirma que el consentimiento *"se reduce a un proceso burocrático, en el que la obtención del consentimiento informado se lleva a cabo de forma casual, y en el que sucumbimos a la tentación de hacer uso del consentimiento como una perezosa justificación"*[126], KOSTA refuerza esta idea argumentando que "*el papel del consentimiento en esta era se reduce, pues el control del individuo sobre su información personal se supera mediante la agilización de las actividades cotidianas en las comunicaciones electrónicas y especialmente en internet, en la medida en que no se infrinja la privacidad del individuo"*[127].

En consecuencia, como apunta ZANFIR-FORTUNA, si el rol del consentimiento se ve reducido, será necesario un marco de garantías alternativas para la protección de sus datos personales. Esta autora, más concretamente, pone el foco en la importancia de revestir a los ciudadanos con estas garantías (*"suitable safeguards"*, como ella lo conceptualiza), a fin de que los afectados estén amparados bajo un sistema que les proteja de forma eficaz ante las limitaciones del consentimiento como fundamento legitimador[128]. Así, la propuesta de EDWARDS se centra en dejar de lado el requisito de otorgar el consentimiento en el momento de obtener los datos, y poner el foco en su concesión para usos concretos de *Big Data*; otra aportación que se añade a la doctrina ya existente que propugna la supresión total del consentimiento como noción central[129].

En base a estas posturas y al marco regulatorio en materia de protección de datos, es interesante la interpretación que realizan MÉNDEZ GARCÍA y ALFONSO FARNÓS de la Disposición Adicional 17ª, segundo párrafo, letra d) LOPDGDD, como "desarrollo" o "concreción" del contenido del art. 89 RGPD. Las autoras argumentan que, a fin de evitar que la seudonimización de datos de carácter personal con un propósito investigador se convierta en un "cheque en blanco", es preciso que se haga uso de esta salvaguarda junto a una habilitación legal, pues, de lo contrario, podría perjudicar al interesado. Así, citan el art. 16.3 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información

[125] Vid., GIL GONZÁLEZ, E., *El interés legítimo…,* o.c., p. 100.

[126] BROWNSWORD, R., "The cult of consent: fixation and fallacy", en *King's Law Journal*, 15 (2004) 224.

[127] KOSTA, E., *Consent in European Data Protection Law*, Leiden 2013, p. 318.

[128] Vid., ZANFIR-FORTUNA., "Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law", en *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges*, Nueva York 2014, pp. 237-257.

[129] Vid., EDWARDS, L., "Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling", en *Law, Policy and the Internet*, Londres 2018, pp. 119-164.

y documentación clínica (también conocida como "LAP")[130], razonando que la base jurídica para tratar los datos contenidos en la historia clínica de un centro con fines de investigación, por ejemplo, sería la habilitación legal del art. 16.3 LAP más la garantía de la seudonimización de los datos en cuestión -y no el consentimiento[131].

Si bien esta parece una alternativa razonable y coherente para el tratamiento de datos de salud con una base jurídica distinta al controvertido consentimiento informado del titular de los datos, encontramos un grave problema. Como analizábamos anteriormente, en el caso de los datos seudonimizados, la reidentificación del sujeto es posible, ya que dichos datos nunca dejan de estar asociados a una información concreta que permite la determinación de su titular. Es por ello que, en un contexto de *Big Data*, donde el riesgo de la desanonimización crece exponencialmente, no parece la opción más adecuada de cara a tratar este tipo de datos sensibles.

Entre las distintas alternativas que la doctrina ha planteado, cabe destacar, por una parte, las propuestas realizadas por los expertos que forman parte del proyecto "*BigDatius"*, llevado a cabo por el Grupo de Investigación de la Cátedra de Derecho y Genoma Humano de la Universidad del País Vasco (UPV). La investigadora principal del proyecto y jurista, Pilar NICOLÁS JIMÉNEZ, ha

---

130 *"El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos".

131 Vid., MÉNDEZ GARCÍA, M. y ALFONSO FARNÓS, I., "La legitimación para…", o.c., p. 222.

señalado la posibilidad de hacer uso de una suerte de herramienta informática que pueda acceder a las distintas bases de datos, de tal forma que *"los datos no se comparten, el investigador hace una pregunta y la herramienta entra en las bases y analiza esos datos para dar una respuesta"*[132]. También, aseguran, pueden tener un papel preponderante en la investigación con tecnología *Big Data* los Comités de Ética de la Investigación en materia de investigación con datos de salud[133], encargados de velar por el respeto y la observancia de los derechos de las personas que participan en la investigación y de carácter obligatorio en España desde 2018, con la entrada en vigor de la LOPDGDD, a través de:

- La comprobación de que, efectivamente, se están aplicando las medidas técnicas necesarias para garantizar el carácter íntimo y reservado de los datos tratados.

- La valoración de los distintos aspectos metodológicos, éticos y jurídicos que sientan las bases del proyecto de investigación, con especial hincapié en controlar el tratamiento de los datos.

- El seguimiento de los proyectos de investigación y el requerimiento de que esté disponible para la ciudadanía la información íntegra que sea considerada oportuna.

- El desempeño de un rol "proactivo" en la diseminación de conocimientos acerca de la ética en investigación con tecnologías *Big Data* en el campo de la salud, con el propósito de promover una cultura de respeto basada en la privacidad y la confidencialidad de los datos personales.

En relación con el reforzamiento del papel de los Comités de Ética de la Investigación, MARTÍNEZ MARTÍNEZ añade que "*No es por tanto concebible un futuro adecuado para la investigación en Big data y salud sin la integración de la figura del delegado de protección de datos en los comités de ética"*[134], de modo que, además de consolidar el papel de estos órganos en el ámbito de la investigación biomédica, se plantea la posibilidad de incluir a un Delegado de Protección de Datos entre sus miembros con la principal función de velar por el respeto de los derechos fundamentales en el transcurso del tratamiento de datos.

[132] "Expertos demandan un marco jurídico y ético apropiado para afrontar los retos y oportunidades del Big Data en salud", *Gaceta Médica*, entrada de 31 de enero de 2018, accesible en: https://gacetamedica.com/politica/expertos-demandan-un-marco-juridico-y-etico-apropiado-para-afrontar-los-retos-y-oportunidades-del-big-data-en-salud-ek1378996/

[133] Respecto al uso secundario de datos de salud, los Comités de Ética de la Investigación deberían tomar en consideración el Informe de 28 de abril de 2020 del Comité de Bioética de España, sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, a la hora de orientar el ejercicio de sus funciones.

[134] Vid., MARTÍNEZ MARTÍNEZ, R., "Big data, investigación…", o.c., p. 266.

Por otra parte, es relevante citar de nuevo a MARTÍNEZ MARTÍNEZ[135] que, a la par que otros autores, como RECIO GAYO, defienden el impulso del principio de responsabilidad proactiva o rendición de cuentas (en su denominación original, "*principle of accountability"*) como solución a este marco regulatorio deficitario. A este respecto, RECIO GAYO advierte:

> "En definitiva, si aplicásemos el actual marco regulatorio de la protección de datos personales y privacidad a los datos masivos y su tratamiento analítico alrededor del mundo, el resultado del análisis nos llevaría a poder afirmar que es necesario un cambio de aproximación, y que en lugar de complejas regulaciones nacionales, por ser en unos casos excesivamente prolijas y en otros demasiado prescriptivas, o incluso ambas a la vez, se impulse decidida y definitivamente, a nivel internacional, el principio de responsabilidad, a través de normas robustas y adaptables que sean capaces, por una parte, de responder a la evolución social, tecnológica, económica y jurídica, lo que pasa por impulsar también la autorregulación, y, por otra parte, que faciliten también la innovación"[136].

Este principio, que se recoge en el art. 5.2 RGPD, es una de las grandes novedades introducidas por el RGPD en la normativa de protección de datos. Establece el precepto que "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo"*; es decir, la responsabilidad proactiva exige, en primer lugar, que las organizaciones pongan en marcha medidas técnicas y organizativas adecuadas y, en segundo lugar, que sean capaces de probar que las implementaron de forma eficaz cuando se les solicite[137]. No obstante, a razón de esta pauta, MARTÍNEZ MARTÍNEZ matiza que:

> "Este principio no sólo debe aplicarse por los responsables de los tratamientos en investigación, también le corresponde a la autoridad de protección de datos personales ofreciendo criterios y soluciones, razonables, viables y ajustadas a la realidad material de la investigación. Si el regulador no es *"accountable"* en su ejercicio cotidiano, si opera desde el autismo o el desconocimiento de la realidad, si no baja a la arena a ofrecer soluciones viables estará cercenando la investigación y con ello todas las oportunidades que para el país y los pacientes pudieran surgir"[138].

[135] Vid., MARTÍNEZ MARTÍNEZ, R., "Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos", en *Dilemata* (Madrid), 24 (2017) 160.

[136] RECIO GAYO, M., "*Big Data*: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* (Bogotá), 17 (2017) 23.

[137] Vid., SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, *Accountability*, disponible en: https://edps.europa.eu/data-protection/our-work/subjects/accountability_en.

[138] Vid., MARTÍNEZ MARTÍNEZ, R., "Big data, investigación…", o.c., pp. 266 y 267.

VI. CONCLUSIONES

La Constitución española consagra, en su artículo 44, párrafo segundo, que "*Los poderes públicos promoverán la ciencia y la investigación científica y técnica en beneficio del interés general"* como principio rector de las Administraciones públicas. En esta línea, el considerando 4 RGPD sostiene que "*El tratamiento de datos personales debe estar concebido para servir a la humanidad"*. De ambos preceptos, deriva la idea de que es necesario que exista un equilibrio entre el progreso científico y tecnológico y los derechos fundamentales y libertades públicas de las personas, de modo que estos últimos no se vean menoscabados por el creciente desarrollo de aquellos.

Es evidente que los beneficios que aportan las tecnologías *Big Data*, especialmente en el ámbito de la salud, son inconmensurables y el uso del consentimiento como base legitimadora no sólo limita sus capacidades, sino que, además, entorpece su eficacia. Ante este escenario, queda evidenciado que la normativa que actualmente rige las actuaciones de los responsables del tratamiento no es la idónea, y por tanto resulta indispensable la formulación de alternativas que garanticen una protección eficaz y completa de los derechos y libertades personales.

A título personal, me gustaría hacer una aportación en clave de reflexión. En base al análisis que se ha llevado a término y la problemática que dimana de la utilización de estas nuevas tecnologías en el ámbito de la investigación científica en salud, cabe decir que, a mi juicio, aun existiendo varias opciones sobre la mesa, como las mencionadas, no considero que sea necesario ir más allá de lo que ya consta regulado en la normativa europea a este respecto. Es decir, no se busca una solución "mágica" que, de la noche a la mañana, elimine todos los potenciales riesgos que la utilización de tecnologías *Big Data* entraña, como la desanonimización y reidentificación del titular de los datos, sino que el objetivo es diseñar una fórmula que permita aprovechar las ventajas tecnológicas de estos sistemas y que, al mismo tiempo, ello no represente una amenaza para el derecho constitucional a la protección de nuestros datos personales.

Por tanto, los artículos 6 y 9 del Reglamento deberían ser el foco de atención, pues son los que habilitan el tratamiento de este tipo de datos, para examinar si, en lugar del consentimiento como criterio de licitud, sería más conveniente esgrimir otra base jurídica entre las nombradas como, por ejemplo, el interés legítimo del responsable del tratamiento (art. 6.1.f) RGPD)[139].

[139] "*El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del*

Esta cuestión no es baladí. Si queremos garantizar un desarrollo "sostenible" de la investigación biomédica, a causa de los numerosos beneficios que aporta a la sociedad en su conjunto, es absolutamente indispensable que esta se lleve a cabo con las debidas garantías para la protección del derecho fundamental reconocido en el art. 18.4 CE. Y ha quedado constatado que el actual marco jurídico basado en el consentimiento como base legitimadora por antonomasia no cumple con esta exigencia.

VII. BIBLIOGRAFÍA

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Informe 073667/2018, Gabinete Jurídico.

- AGUILERA VAQUÉS, M. y SERRA CRISTÓBAL, R., *Rights and Freedoms in the Spanish Constitution*, Valencia 2015.

- ARANDA JURADO, M., "Evolución de la normativa de la investigación biomédica en España", en *Actualidad Jurídica Iberoamericana* (Valencia), 9 (2018) 254-275.

- ARGANZA SALCEDO, R. y ARROYO LÓPEZ, M., "Big data: Aplicaciones de la gestión del dato en las distintas etapas del *funnel* de conversión", en *Revista de Marketing y Publicidad* (Madrid), 1 (2019) 39-68.

- BROWNSWORD, R., "The cult of consent: fixation and fallacy", en *King's Law Journal*, 15 (2004) 223-251.

- CÁTEDRA DE DERECHO Y GENOMA HUMANO, *Informe sobre implicaciones legales para el desarrollo de un modelo de gestión de datos genéticos*, Universidad del País Vasco (2021).

- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, 2020.

- CRISTEA UIVARU, L., *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en salud*, Barcelona 2018.

- CRUZ VILLALÓN, P., "Formación y evolución de los derechos fundamentales", en *Revista Española de Derecho Constitucional* (Madrid), 25 (1989) 35-62.

interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable". Vid., Reglamento General de Protección de Datos, considerando (47).

- DIEBOLD, F. X., "On the Origin(s) and Development of "Big Data": The Phenomenon, the Term, and the Discipline", University of Pennsylvania (2019).

- EDWARDS, L., "Data Protection and e-Privacy: From Spam and Cookies to Big Data, Machine Learning and Profiling", en *Law, Policy and the Internet*, Londres 2018, pp. 119-164.

- FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for businesses and policymakers*, Informe, 2012.

- GALLO SALLENT, J. A., *El big data. Implicaciones jurídicas para un cambio de paradigma: El derecho al olvido y el consentimiento* [Tesis doctoral, Universitat Internacional de Catalunya], Tesis Doctorals en Xarxa 2020: https://www.tdx.cat/handle/10803/670038#page=1.

- GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, Accésit en la XIX Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, Madrid 2016.

- GIL GONZÁLEZ, E., *El interés legítimo en el tratamiento de datos personales*, Madrid 2022.

- GÓMEZ SÁNCHEZ, Y., "La protección de los datos genéticos: el derecho a la autodeterminación informativa", en *DS: Derecho y salud* (Barcelona), 16 (núm. extra. 1) (2008) 59-78.

- GÓMEZ SÁNCHEZ, Y., "La libertad de creación y producción científica: especial referencia a la Ley de Investigación biomédica", en *Revista de Derecho Político* (Madrid), 75-76 (2009) 489-514.

- GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 15/2011 sobre la definición del consentimiento*, 2011.

- GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679*, 2018.

- GRUPO DE TRABAJO INTERNACIONAL SOBRE PROTECCIÓN DE DATOS EN LAS TELECOMUNICACIONES, *Working Paper on Big Data and Privacy. Privacy principles under pressure in the age of Big Data analytics*, 55th Meeting, 5-6 May 2014, Skopje, Macedonia.

- JIMÉNEZ ASENSIO, R., "El nuevo marco normativo de la protección de datos personales: su aplicación a las entidades locales", en *Anuario Aragonés del Gobierno Local* (Zaragoza), 10 (2018) 321-365.

- JOYANES AGUILAR, L., *Big data: análisis de grandes volúmenes de datos en organizaciones*, Ciudad de México 2013.

- KOSTA, E., *Consent in European Data Protection Law*, Leiden 2013.

- LANEY, D., *3-D Data Management: Controlling Data Volume, Velocity and Variety*, META Group Research Note, 6 February 2001.

- LÓPEZ-MUÑIZ GOÑI, M., "La ley de regulación del tratamiento automatizado de los datos de carácter personal", en *Informática y derecho: Revista iberoamericana de derecho informático* (Montevideo), 6-7 (1994) 93-116.

- MARTÍNEZ LÓPEZ-SÁEZ, M., *Una revisión del derecho fundamental a la protección de datos de carácter personal. Un reto en clave de diálogo judicial y constitucionalismo multinivel en la Unión Europea*, Valencia 2018.

- MARTÍNEZ LÓPEZ-SÁEZ, M., "Repensando el derecho constitucional a la protección de datos ante la mutación de la "informática", en *Constitución, política y administración: España 2017, reflexiones para el debate*, Valencia 2020, pp. 161-174.

- MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", en *IDP: Revista de Internet, Derecho y Política* (St. Quirze del Vallès), 5 (2007) 47-61.

- MARTÍNEZ MARTÍNEZ, R., "Big data, investigación en salud y protección de datos personales. ¿Un falso debate?", en *Revista Valenciana d'Estudis Autonòmics* (Valencia), 62 (2017) 235-280.

- MARTÍNEZ MARTÍNEZ, R., "Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos", en *Dilemata* (Madrid), 24 (2017) 151-164.

- MARTÍNEZ VELENCOSO, L. M., *La protección jurídica de la persona en el ámbito de la Biotecnología y del Big Data*, Madrid 2022.

- MÉNDEZ GARCÍA, M., y ALFONSO FARNÓS, I., "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en

Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada (Leioa), Núm. Extraord. (2019) 205-231.

- MURILLO DE LA CUEVA, P. L., "La protección de los datos personales ante el uso de la informática en el derecho español (1ª parte)", en *Estudios de Jurisprudencia* (A Coruña), 3 (1992).

- MURILLO DE LA CUEVA, P. L., *Informática y protección de datos personales (estudio sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal)*, Madrid 1993.

- PÉREZ LUÑO, A. E., "Nuevos derechos fundamentales de la era tecnológica: la libertad informática", en *Anuario de Derecho Público y Estudios Públicos* (Santiago de Chile), 2 (1989/90) 171-195.

- PIÑAR MAÑAS, J. L., "Introducción: hacia un nuevo modelo europeo de protección de datos", en *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Madrid 2016, pp. 15-22.

- RALLO LOMBARTE, A., "Una nueva generación de derechos digitales", en *Revista de Estudios Políticos* (Madrid), 187 (2020) 101-135.

- RECIO GAYO, M., "Big Data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías* (Bogotá), 17 (2017) 4-24.

- RECUERO LINARES, M., *La investigación científica con datos personales genéticos y datos relativos a la salud: perspectiva europea ante el desafío globalizado*, Accésit del Premio de Investigación en Protección de Datos Personales Emilio Aced de la Agencia Española de Protección de Datos 2019.

- SAN SEGUNDO ENCINAR, J. M., *Big data en salud digital*, Madrid 2017.

- SANTAMARÍA IBEAS, J. J., "La LORTAD: breve análisis de sus antecedentes", en *Informática y derecho: Revista iberoamericana de derecho informático* (Montevideo), 4 (1994) 261-276.

- SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y Garantía de los Derechos Digitales", en *Estudios De Deusto. Revista de Derecho Público* (Bilbao), 68 (2) (2020) 257-292.

- TRONCOSO REIGADA, A., "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", en *Revista de Derecho y Genoma Humano: Genética, Biotecnología y Medicina Avanzada* (Leioa), 49 (2018) 187-266.

- VARIOS, *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública*, Barcelona 2015, Grupo de Opinión del Observatorio de Bioética y Derecho de la Universitat de Barcelona.

- VARIOS, *Código de buenas prácticas en protección de datos para proyectos de Big Data*, elaborado para la Agencia Española de Protección de Datos (AEPD) y la Asociación Española para el Fomento de la Seguridad de la Información (ISMS Forum Spain) 2017.

- WEISS, S. M. e INDURKHYA, N., *Predictive Data Mining: A Practical Guide*, Burlington 1998.

- ZANFIR-FORTUNA, ZANFIR, "Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law", en *Reloading Data Protection. Multidisciplinary Insights and Contemporary Challenges*, Nueva York 2014, pp. 237-257.