UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

EL FUTURO DEL *BIG DATA* EN EL ÁMBITO SANITARIO. LAS CLAVES JURÍDICAS DEL TRATAMIENTO DE LOS DATOS DE SALUD

LETICIA LATORRE LUNA

2021

UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

EL FUTURO DEL *BIG DATA* EN EL ÁMBITO SANITARIO. LAS CLAVES JURÍDICAS DEL TRATAMIENTO DE LOS DATOS DE SALUD

Tesis doctoral realizada bajo la tutela y dirección de

Profesor Dr. D. Julián Valero Torrijos

Profesora Dra. Dª María Magnolia Pardo López

LETICIA LATORRE LUNA

2021

A mi destino.

A mi familia.

(Con todo mi amor incondicional).

"Sólo es posible avanzar cuando se mira lejos.
Sólo cabe progresar cuando se piensa en grande."

- J. Ortega y Gasset -

Índice

ABREVIATURAS

ADMIRE	*Alzheimer´s Disease Medical Images Research Environment*
AEPD	Agencia Española de Protección de Datos
AO	Aprendizaje Organizacional
AP	Análisis Predictivo
Art.	Artículo
Arts.	Artículos
BD	*Big data*
BI	*Business intelligence* (Inteligencia de Negocios)
BOE	Boletín Oficial del Estado
BSC	*Balanced Scorecard*
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CI	Capital Intelectual
CISNS	Consejo Internacional del Sistema Nacional de Salud
CMI	Cuadros de Mando Integral
CP	Código Penal
DIGNA	*Degenerative Neural Intelligent Alerts*
DM	*Data Mining* (Minería de Datos)
DPO	Data Protection Officer (Delegado de Protección de Datos)
DS	*Data Science* (Ciencia de Datos)
DSS	Sistemas de Soporte a la Decisión
DW	*Data Warehouse*
EA	Enfermedad de Alzheimer
EIPD	Evaluación de Impacto en la Protección de Datos (PIA, en inglés)
EIS	*Executive Information Systems* (Sistemas de Información Ejecutiva)
ERP	*Enterprise Resource Planning* (Planificación de Recursos Empresariales)
ETL	*Extraction, Transformation and Loading* (Extracción, Transformación y Carga)
FD	Fundamento de Derecho
FJ	Fundamento Jurídico
GC	Gestión del Conocimiento

GT29	Grupo de Trabajo del Artículo 29
HCDSNS	Historia Clínica Digital del Sistema Nacional de Salud
HCE	Historia Clínica Electrónica
HCR	Historia Clínica Resumida
HES	Historia Electrónica de Salud
IA	Inteligencia Artificial
IaaS	Infraestructura como Servicio
IBM	*International Business Machines*
IIC	Instituto de Ingeniería del Conocimiento
IoT	*Internet of Things* (Internet de las Cosas)
IT	*Information Technologies* (Tecnologías de la Información)
KDD	*Knowledge Discovery in Databases* (Extracción de Conocimiento en Bases de Datos)
LECr.	Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal
LGT	Ley 58/2003, de 17 de diciembre, General Tributaria
LIB	Ley 14/2007, de 3 de julio, de Investigación biomédica.
LOPDGDD	Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
LORTAD	Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal
LPAP	Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas
MGI	*Mckinsey Global Institute*
MPP	Procesamiento Paralelo Masivo
MRP	*Material Requirements Planning* (Planificación de Requerimientos Materiales)
MRP II	Sistema de planeamiento y control de la producción totalmente integrado
NN	*Neural Networks* (Redes neuronales)
PaaS	Plataforma como Servicio
PWC	PriceWaterhouseCoopers
RD	Real Decreto
RDSI	Red Digital de Servicios Integrados
RGPD	Reglamento General de Protección de Datos
RWD	*Real World Data* (Datos del mundo real)

SaaS	*Software as a Service* (*Software* como servicio)
SEE	Sociedad Española de Epidemología
SEIS	Sociedad Española de Informática de la Salud
SEPAS	Sociedad Española de Salud Pública y Administración Sanitaria
SIIA	*Software & Information Industry* (*Software* e Industria de la información)
SNA	*Social Network Analysis* (Análisis de redes sociales)
SNS	Sistema Nacional de Salud
SQL	*Structure Query Language* (Lenguaje de consulta de estructuras)
SVM	*Support Vector Machines* (Máquinas de vectores de soporte)
TC	Tribunal Constitucional
TCE	Tratado Constitutivo de la Comunidad Europea
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y la Comunicaciones
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
TSI	Tarjeta Sanitaria Individual
WCG	*World Community Grid* (Red Comunitaria Mundial)
XML	*Extensible Markup Language* (Lenguaje del mercado extensible)

AGRADECIMIENTOS

De antemano, he de agradecer a Dios por darme la fortaleza, energía y tiempo que he necesitado para iniciar, desarrollar y culminar este trabajo y, sobre todo, por darme la oportunidad de convertir mis sueños en realidad.

En el ámbito académico, agradecer a mis compañeros del Centro de Estudios de Bioderecho, Ética y Salud (C.E.B.E.S.) la oportunidad de formar parte de un excelente equipo, cada uno de vosotros me habéis transmitido los verdaderos valores de la Facultad de Derecho de la Universidad de Murcia, sois unos excelentes profesores y profesionales. También, agradecer a todos los profesores de los que he sido alumna durante mi trayectoria académica, especialmente, a los profesores de la Licenciatura en Derecho, así como en la de Filosofía y en el Máster de la Universidad de Salamanca, quienes me han enseñado y transmitido conocimientos y actitudes de gran utilidad en la práctica del Derecho.

En el ámbito personal, mi más sincero agradecimiento a mi familia por su apoyo incondicional, comprensión, amor y paciencia, especialmente a mis padres, Vicente y Carmen, por ofrecerme la oportunidad de estudiar y por creer en mí desde el primer día que viene a este mundo, sobre todo, por transmitirme los valores más importantes de la vida, sois un gran ejemplo de superación, sacrificio y amor, me siento muy afortunada.

Igualmente, agradecer a mis amigas y amigos su apoyo incondicional y energía, sobre todo, a mis amigas de la infancia y a las personas que la vida me ha regalado este año 2021, sin duda, una amistad que me ha ayudado incondicionalmente en los últimos soplos de este trabajo.

Por último, en el ámbito profesional, estoy enormemente agradecida a quienes habéis confiado en mí como profesional haciendo posible que pueda poner en práctica mi vocación como jurista y docente.

Muchas gracias a todos los que habéis fomentado la ilusión de hacer este sueño realidad.

INTRODUCCIÓN

Desde el surgimiento del derecho de protección de datos hasta la actualidad se puede apreciar una evolución en el marco normativo jurídico tanto europeo como nacional, generándose una evidente tensión con la propia evolución de las tecnologías al convertirse estas en fuentes relevantes de datos personales de los ciudadanos. En este contexto donde la tecnología se convierte en generadora de grandes volúmenes de datos aparece el *big data* como herramienta que analiza los datos masivos y sustrae de los mismos a través de la aplicación de algoritmos información y conocimiento con el que se puede predecir y prevenir, entre otros y en gran medida, situaciones y hechos en cualquier sector de la sociedad. En el momento en el que las tecnologías conquistan el sector sanitario (e-Salud), así como aparecen otras fuentes de datos externas a los ficheros sanitarios que igualmente generan datos relativos a la salud de los ciudadanos, se producen en tiempo real grandes volúmenes de diversa variedad de datos de salud que tras la aplicación de herramientas *big data*, aportan conocimiento e información veraz y de gran valor, pues, entre otros, se adelanta a la enfermedad, ayuda a la toma de decisiones más idóneas a los profesionales sanitarios, así como proporciona al paciente una asistencia sanitaria y tratamiento más personalizado y eficiente, entre otros beneficios que se pueden destacar de interés general para la humanidad y, especialmente, en el ámbito de investigación biomédica y de la asistencia sanitaria y, por consiguiente, de la mejora y bienestar de la humanidad, pues es obvio que vivimos en una economía de datos donde a través de la aplicación de herramientas *big data* accedemos a un nuevo modo de generar conocimiento, información y, por supuesto, de hacer ciencia.

En este sentido, el *big data* sanitario en la actualidad es fuente de información y conocimiento en la medicina, habiendo sido la escritura hasta la llegada de las tecnológicas, la fuente tradicional y principal. Tal es así que posiblemente en un futuro no es de extrañar que los datos personales relativos a la salud a través de la aplicación de las tecnologías *big data* y, más recientemente con la Inteligencia Artificial, se conviertan en lo que podrían ser los "libros" del mañana sobre todo para los profesionales del ámbito sanitario.

¿Qué habría sido de la evolución del conocimiento humano y de la ciencia en general si no hubiéramos podido acceder a los textos clásicos y a las investigaciones halladas en los años, décadas y siglos anteriores? Si la escritura no hubiera existido y, por ende, los libros ¿qué habría sido del conocimiento? ¿qué habría sido de la evolución humana? Si hubiésemos limitado el acceso a las bibliotecas, ¿cómo hubiera evolucionado la humanidad? Por ejemplo, desde la Filosofía y la creación del conocimiento, si los grandes pensadores y científicos no hubieran escrito nada sobre sus investigaciones y pensamiento, poco habríamos evolucionado a lo largo de la Historia.

Por ende, la presente tesis doctoral pretende llevar a cabo un estudio general que ofrezca, en la medida de lo posible, una visión global de la información y conocimiento de gran valor que se puede sustraer de los datos personales relativos a la salud a través de la aplicación de herramientas de *big data*, poniendo de relieve las cuestiones más interesantes que el derecho de protección de datos suscita.

Lo anterior se traduce en este trabajo, por un lado, en el estudio de las herramientas *big data* en general y, de manera particular, en el ámbito sanitario y, por otro lado, en el análisis del marco normativo de protección de datos tanto europeo como nacional desde sus inicios con el objeto de plasmar esa continua tensión entre el derecho de protección de datos y la evolución de las tecnologías, así como acreditar la insuficiencia y deficiencias del actual marco normativos europeo y español en lo que respecta al tratamiento de los datos relativos de salud*,* a los efectos de asentar las bases jurídicas esenciales que deberían ser reguladas por una ley específica de protección de datos de salud y aplicación de herramientas *big data.* No obstante, la generalidad buscada en la ley sectorial de protección de datos de salud y *big data* en el sector sanitario impide que se agoten de forma exhaustiva toda y cada una de las cuestiones tratadas, tanto del contenido esencial de la propia ley, como de las medidas y garantías que deben recoger los proyectos que apliquen técnicas de *big data*, así como de aquellas materias conexas.

Previamente a la publicación del Reglamento (UE) 2016/679 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, los profesionales sanitarios e investigadores científicos no autorizados por el paciente, desde un punto de vista legal no podían tratar los datos de salud registrados en los ficheros sin el consentimiento del paciente, ya que según la normativa vigente en aquel entonces en todo caso primaba el derecho de protección de datos y el derecho a la privacidad del mismo. Así pues, desde esta premisa, con este trabajo en su día se cuestionó sobre el hecho de que si se limita el tratamiento de los datos de salud a terceros que desarrollaban proyectos de salud pública e investigación biomédica y farmacéutica de interés general y, que por consiguiente, necesitan de los mismos a fin de recopilar información y conocimiento por medio de la aplicación de tecnológicas de *big data*, es como si se estuviera poniendo límites al progreso y a la evolución de la medicina y de la ciencia, algo que sin duda resulta de interés general para la población del presente y para las futuras generaciones.

En suma, la normativa jurídica de protección de datos existente antes a la entrada en vigor del RGPD era una normativa que necesitaba ser adaptada a los continuos avances tecnológicos, fundamentalmente debido a que en determinados supuestos de hecho iba en contra del interés general de la población, del bienestar de la humanidad y de la evolución de la medicina, ya que el ciudadano disponía de la potestad absoluta para decidir sobre del destino de sus datos de salud.

Posteriormente, con la publicación del RGPD, resultó de satisfacción que el legislador europeo tomara conciencia del valor de los datos de salud, permitiendo, por un lado, la libre circulación de los datos personales y, por otro lado, salvaguardando el derecho de protección de datos personales de los ciudadanos, otorgándole un tratamiento especial a los datos personales relativos a la salud, permitiéndose un tratamiento lícito de los mismos sin el consentimiento del interesado ante aquellas situaciones en las que se considera que debe primar el interés general, es decir, cuando sea necesario por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica, histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

En la actualidad, parece ser que las nuevas tecnologías y el Internet de las Cosas han generado un cambio de paradigma social, cultural y económico, donde los juristas tenemos la responsabilidad de asegurar desde la eficacia y la eficiencia de la norma jurídica, por un lado, la evolución de la humanidad a través de los innumerables beneficios y ventajas que nos aporta la era digital y, a su vez, salvaguardar los derechos fundamentales de las personas, sin que en ningún caso se dé lugar a la pérdida de la esencia de los derechos fundamentales y ni de los valores éticos y morales propios de nuestra sociedad y de nuestro Estado de Derecho.

Lógicamente, el estudio profundiza en las cuestiones más importantes, controvertidas o necesitadas de regulación, partiendo de una concepción genérica del *big data*, en especial, del *big data* sanitario que permite una perspectiva jurídica sistemática y de conjunto imprescindible para la coherencia e imparcialidad de las decisiones adoptadas.

Por último, se ha de indicar que para el desarrollo del presente trabajo se ha tenido en cuenta la confrontación de las opiniones de la doctrina más autorizada con las necesidades prácticas evidenciadas en las distintas resoluciones jurisprudenciales y, de la influencia de las tecnologías en la nueva era digital, lo que ha generado ineludiblemente una constante tensión entre el cambio tecnológico y la normativa jurídica de protección de datos personales.

CAPÍTULO PRIMERO

CONTEXTUALIZACIÓN DEL *BIG DATA*

I. CUESTIONES PREVIAS

Previamente a entrar en el contenido del trabajo, por cuestiones puramente pragmáticas se han de tener en consideración las siguientes indicaciones genéricas a fin de garantizar una mayor comprensión del contenido debido a la particularidad de las herramientas *big data* en el ámbito de la sanidad.

Por un lado, hablaremos en general de los principales "actores del *big data* en salud" o "actores de la sanidad" haciéndose referencia en concreto a los siguientes[1]: (1) Los organismos sanitarios públicos o privados (centros de salud, hospitales, centros de investigación, entidades farmacéuticas y cualquier otra entidad que trate de manera directa con datos relacionados con la salud); (2) Los profesionales o facultativos

[1] *Vid.* GUBBIOLI BELLECQ, J., "El valor de la información y el Big Data", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, p. 41.

sanitarios dirigidos por los datos (médicos, enfermeros, investigadores y cualquier otro profesional que trata de manera directa con datos relacionados con la salud); (3) Los usuarios del sistema sanitario (pacientes); (4) El ciudadano; (5) Cualquier otro organismo público o privado que sea fuente generadora de datos de salud.

Por consiguiente, cuando se utilice en este trabajo la expresión "diferentes actores de la sanidad" englobará en su conjunto a todos y cada uno de los anteriores mencionados. Igualmente, cada uno de los actores abarcará de manera genérica a cada uno de los referenciados de manera específica, así pues, por ejemplo, cuando se hable en general de los organismos sanitarios públicos o privados, nos estaremos refiriendo a los centros de salud, hospitales, centros de investigación, entidades farmacéuticas y cualquier otra entidad que trate de manera directa con datos relacionados con la salud y, así para el resto de los actores sanitarios.

Por otro lado, cuando se utilice la expresión "investigación científica" nos estaremos refiriendo de manera exclusiva y excluyente a la "investigación biomédica" (incluyéndose la investigación clínica y epistemológica) y a la "investigación farmacéutica" cuyos proyectos de desarrollo sean de interés general.

En tercer lugar, los datos relacionados con la salud abarcarán los datos genéticos, los datos relativos a la salud y los datos biométricos, no obstante, en este trabajo, se hablará en general y de manera indistinta bien, de datos relativos a la salud o, bien de datos sanitarios.

Por último, el término "asistencia sanitaria" se utilizará para hacer referencia a la salud pública que se entenderá implícitamente en todo caso de interés general.

II. ANTECEDENTES HISTÓRICOS DEL *BIG DATA*

Previamente al estudio de los orígenes de la tecnología *big data*, resulta de interés reflexionar acerca de la relevancia del conocimiento en la humanidad, pues es indudable tratar este punto en el sentido de que la presente tesis defiende el gran valor y

potencial de los datos de salud como fuente de conocimiento e información para la medicina, la ciencia y, en consecuencia, para la evolución de la humanidad.

Posteriormente, se efectuará un repaso de las etapas más importantes del contexto histórico de la figura que nos ocupa, pues como sucede en la mayoría de las ramas del Derecho, es necesario entender la sistemática y funcionamiento del *big data* como tecnología que surge en la era digital a los efectos de promulgar una ley que se adapte a las nuevas exigencias y necesidades de la actual sociedad tecnológica y de tomar conciencia de los métodos y técnicas empleadas para sustraer conocimiento de los datos sanitarios. Por este motivo, los primeros epígrafes del presente capítulo se dedican a los antecedentes históricos del *big data* y a la influencia de la gestión del conocimiento como aspecto fundamental para su desarrollo.

Para finalizar, en los últimos epígrafes de este capítulo introductorio y, no menos importante, se tratará de diferenciar el *big data* de otras tecnologías previas a su surgimiento, tales como el *business intelligence, data mining y data science*, así como de otros conceptos influyentes posteriores, tales como, *open data* y *smart data*, entre otros.

1. LA RELEVANCIA DEL CONOCIMIENTO Y LA INFORMACIÓN EN LA HUMANIDAD

Las razones que ponen de manifiesto la necesidad de realizar un estudio sobre la presente materia desde una perspectiva jurídica son diversas como se podrá apreciar a lo largo del trabajo.

No obstante, igualmente, cabe tener presente que desde un punto de vista filosófico el tema que nos ocupa también tiene una gran relevancia, pues no cabe duda que desde los inicios de la humanidad la creación del conocimiento e información, su divulgación, así como poder acceder al mismo en cada periodo histórico ha resultado fundamental para la evolución humana, de ahí dimana el inestimable valor de los textos clásicos, los libros y artículos científicos, entre otros, desde su surgimiento hasta la actualidad, pues resulta indudable que sin estos la evolución del ser humano desde

cualquier aspecto y materia de la vida hubiera sido prácticamente imposible[2]. Uno de los primeros pensadores conscientes de este hecho fue el filósofo Platón (428/427- 347 a.C.) cuando se vio en la necesidad de escribir el pensamiento filosófico que su maestro Sócrates (470/469-399 a.C.) divulgó a los ciudadanos atenienses, pues como es sabido, todo lo que conocemos de quien es considerado en la Historia de la Filosofía como el fundador de la filosofía moral occidental[3], es sobre todo por su discípulo Platón (sin tenerse en cuenta los textos de Jenofonte, Aristóteles y Aristófanes) pues Sócrates dialogar, dialogó hasta el último instante de su vida, pero, sin embargo, escribir, nada escribió[4].

Otros de los grandes personajes de la Historia que valoraron los libros fueron los faraones de Egipto, Ptolomeo II y Ptolomeo III, pues gracias al primero, la Biblioteca de Alejandría[5] que contaba con un archivo de quinientos mil manuscritos (que equivalen a cien mil libros impresos de hoy), llegó a alcanzar la cifra de setecientos mil manuscritos procedentes de los barcos que llegaban a la ciudad y que eran revisados uno a uno, cuando se encontraba un libro, se llevaba a la Biblioteca donde era copiado y posteriormente devuelto a su dueño. Igualmente, Ptolomeo III fue consciente de la gran importancia y valor de los libros, hasta el extremo de escribir una carta a los soberanos

[2] Al respecto PONCE DE LEÓN, A., "La evolución humana. Un conocimiento integrador", *Innovación educativa,* vol. 18, núm. 77, 2018, p. 67, señala que: "Se ha atribuido en este texto un valor especial al conocimiento sobre la evolución humana como parte de un conjunto importante de conocimientos que funcionan como andamios para situar nuevos conocimientos y para ampliar horizontes de comprensión en estudiantes de diversos niveles, desde preescolar hasta universitario. Se recuperaron ideas de pensadoras como Marguerite Yourcenar y María Montessori, quienes atribuyen al educando la necesidad de una educación universal, que contemple al ser humano como parte del universo o cosmos, que lo posibilite así a comprender su lugar en el mundo y en el gran concierto de la vida y de los recursos o bienes del planeta. Se enfatizó que el tema de la evolución humana contiene conocimientos útiles para apoyar una comprensión de las dimensiones temporal, animal, cultural y ecológica de nuestra especie, que brinda con ello al estudiante y al público en general elementos para una mayor inteligibilidad sobre la historia natural de nuestra especie".

[3]REALE, G. y ANTISERI, D., *La Historia del Pensamiento Filosófico y Científico. Tomo I,* Editorial Herder, Barcelona, 1988, p.85.

[4]SILVANI, L., *Historia de la Filosofía,* Editorial Optima, Barcelona, 2003, p. 32-33, señala que: "La dificultad a la hora de aproximarse al hombre y a su filosofía reside en que Sócrates no dejó nada escrito, y lo que se sabe de él procede básicamente de cuatro fuentes, que además resultan contradictorias entre sí: Jenofonte, Platón, Aristófanes y Aristóteles".

[5] La Biblioteca y el Museo de Alejandría que alcanzaron su máximo esplendor durante el reinado de Filadelfo entre el año 285 – 246 a.C., en Egipto. El Museo ofrecía todo tipo de artefactos para las investigaciones en Medicina, Biología o Astronomía, de hecho, durante esa época se invitó a estudiosos a llevar a cabo observaciones y deducciones en Matemáticas, Medicina, Astronomía, y Geometría, naciendo así nuevas disciplinas como la Filología, la Trigonometría, la Gramática y la Preservación de Manuscritos.

de todo el mundo solicitando prestados sus libros para copiarlos. De hecho, un antecedente curioso es que cuando Atenas le prestó a Ptolomeo III los textos de Eurípides, Esquilo y Sófocles, copió los mismos y, con astucia devolvió las copias y guardó los originales, lo que ha permitido que hoy día podamos conservar libros y textos de gran valor pues, no cabe duda que si no hubiera sido por la Biblioteca de Alejandría y por la labor de Ptolomeo III, hubieran desaparecido, causando en consecuencia una gran pérdida de conocimiento en la humanidad[6], a pesar de que la mayoría de los libros fueran perdidos, robados y quemados.

Así sucede con la mayoría del conocimiento de la humanidad, pues es sabido que lo que actualmente conocemos y sabemos es debido esencialmente a lo que otros con anterioridad a nosotros han investigado y escrito e igualmente, lo que ahora se está investigando y escribiendo, será de gran utilidad para las generaciones futuras y, por consiguiente, para la mejorar del bienestar social y la evolución de la humanidad, hechos que resultan en sí mismos de interés general. No obstante, en la actual era digital, hemos de ser conscientes que el paradigma parece ser que ha cambiado, en el sentido, de que ya no sólo tenemos libros, artículos científicos y textos clásicos para investigar y continuar evolucionando, sino que también poseemos una gran herramienta: los datos[7] y, en concreto, por el interés que nos ocupa en el presente trabajo, los datos relativos a la salud[8], datos de los que se puede sustraer tras la aplicación de herramientas

[6]H. ELÍA, R., "El incendio de la biblioteca de Alejandría por los árabes: una historia falsificada", *Byzantion Nea Hellán,* núm. 32, 2013, pp. 37-69. Documento disponible en: https://scielo.conicyt.cl/pdf/byzantion/n32/art02.pdf (última consulta 15/08/18).

[7] En este sentido en MONLEÓN GETINO, A., "El impacto del *Big Data* en la información. Significado y utilidad", *Historia y comunicación social,* vol. 20, núm. 2, 2015, pp. 430-431, afirma que: "No sólo son importantes los datos y el conocimiento que nos aportan los mismos (Monleón, 2010), sino que están cambiando la economía mundial. En nuestro entorno, la Unión Europea concentra gran parte de sus actividades de investigación. e innovación en el denominado Programa Marco que en esta edición se denominará Horizonte 2020 (H2020). En el período 2014-2020 y mediante la implantación de tres pilares, contribuye a abordar los principales retos sociales, promover el liderazgo industrial en Europa y reforzar la excelencia de su base científica. H2020 promueve la generación de una economía basada en el conocimiento, así uno de los objetivos que ha fijado dentro del H2020 es el de desarrollar tecnologías y sus aplicaciones para mejorar la competitividad europea, contando y promocionando inversiones en tecnologías clave para la industria, como Tecnologías de la Información y Comunicación (TIC) (Ministerio de Economía y Competitividad, 2014)."

[8] Uno de los campos más prometedores es el campo de la medicina, así el análisis de los Big-data está contribuyendo a reducir los elevados costes de la investigación clínica, proporcionando medidas reales del desempeño de nuestro sistema sanitario y ayudando a los médicos y pacientes a tomar mejores decisiones (Science Spain, 2014). Pablo Serrano, director médico del Hospital de Fuenlabrada (Madrid), durante el 59º Congreso de la Sociedad Española de Farmacia Hospitalaria (SEFH) celebrado el pasado octubre de 2014 señaló nuevos retos en el uso de estos datos, así "en el ámbito de la farmacia hospitalaria, la tecnología Big-data ayudaría a comprender mejor la utilización de los medicamentos y los integrarían

de *big data*, información y conocimiento de gran utilidad e interés para la sociedad actual y del mañana[9], como se verá más adelante.

Debe tenerse en cuenta, sin embargo, que a pesar de que el concepto de "dato" es uno de los más utilizados desde finales de los años 90, debemos remontarnos a los inicios de la humanidad, a fin de analizar los primeros métodos empleados para la recopilación de datos con el objetivo de almacenar información para poder así transmitir un conocimiento exacto sobre algo concreto. A pesar de que el concepto de "dato" es relativamente contemporáneo, sin embargo, previamente a su creación y de emplease contextualmente como en la actualidad viene a significar, cabría pensar que desde los inicios de la humanidad podría haber sido empleado como un sinónimo de información. En este sentido, a modo de curiosidad se ha de destacar que en la época del Paleolítico Superior, sobre el año 18000 a.C., se empleaban diversos métodos de almacenamiento de datos mediante la utilización de palillos o muescas de huesos que le permitían al hombre llevar una contabilidad de provisiones, un control de la actividad comercial, realizar cálculos, predecir necesidades de comida y un registro de inventarios. En este momento, es donde aparecen los primeros documentos de interés por el hecho de recopilar, contar y guardar datos a efectos de poder acceder a una información que divulgaba un conocimiento exacto.

En concreto, en el año 2400 a.C., en Babilonia es desarrollado el «ábaco», un sistema destinado al cálculo de datos, surgiendo además las primeras bibliotecas de Babilonia como lugares destinados al archivo de información y consulta de conocimiento. Durante los años 300 a. C. y 48 d.C. con la construcción de la Biblioteca de Alejandría aparece el centro principal de almacenamiento de datos en toda la

---

en el conjunto del hospital. Otro ejemplo sanitario comentado por Esteban (2014) en el artículo "Cinco ejemplos de cómo el 'Big-data' puede mejorar la sociedad" sería el de las pandemias, como el ébola que recientemente se ha convertido en un problema mundial. Así mediante el Big-data se puede descubrir el riesgo de una pandemia en tiempo real a través de las tendencias que se registran en un buscador de internet como Google u otros". En MONLEÓN GETINO, "El impacto del *Big Data*…", *op. cit.,* pp. 432-433.

[9] Asimismo, MONLEÓN GETINO, "El impacto del *Big Data*…", *op. cit.,* pp. 431-432, destaca que: "La Comisión Europea (2014b) cita algunos ejemplos de cómo el análisis y tratamiento de datos, sobre todo de Big-data, cambiarán la sociedad: Transformaran las industrias de servicios de Europa mediante la generación de una amplia gama de productos y servicios de información innovadores; Aumentaran la productividad de todos los sectores de la economía; Mejorarán la investigación y acelerar la innovación; Lograrán reducciones de costos a través de servicios más personalizados; Aumentarán la eficiencia en el sector público".

humanidad, hasta que finalmente, en el año 48 d.C. con la invasión de los romanos en Alejandría se destruye la biblioteca, teniendo que ser trasladados parte de los fondos rescatados a otros lugares, a pesar de ello la mayoría de los libros fueron quemados, perdidos o robados. Por otro lado, en Grecia, durante los años 100 y 200 a.C., se desarrolló la primera computadora mecánica de la humanidad con el mecanismo de Anticitera, diseñada a fin de predecir posiciones astronómicas y marcar el calendario, sobre todo las fechas concretas de los Juegos Olímpicos[10].

Comentado lo anterior y, tras una breve introducción histórica sobre la relevancia del conocimiento y de la información en la humanidad, a continuación, se expondrá de manera detallada el contexto histórico del *big data* partiendo de la Edad Moderna hasta nuestros días.

2. CONTEXTO HISTÓRICO DEL *BIG DATA*

Es en el siglo XVII cuando es instaurado el almacenamiento de datos estructurado con el surgimiento de la estadística en el año 1663 por el científico Graunt, quien promovió los pilares de una estadística científica, realizando la primera tabla de mortalidad de la ciudad de Londres mediante la recopilación de datos sanitarios en relación con las defunciones, hecho que le permitió - tras analizar los mismos - elaborar un sistema de alerta para la peste bubónica en Europa[11].

Es en el siglo XVIII, en concreto, en el año 1792 cuando la estadística comienza a ser considerada una ciencia, a pesar de que el análisis de datos estadísticos surgiera en las Guerras del Peloponeso y, el concepto "estadística" se creara unos años antes en Alemania, va a ser a finales del siglo XVIII cuando aparecen términos relevantes dentro de esta rama del conocimiento, tales como "colección de datos" y "clasificación de datos". En 1865 es publicada la obra *Enciclopedia de anécdotas en los negocios y el*

[10] Acerca del origen del *Big Data*, *Vid.* MARR, B., "A Brief History of *Big Data* Everyone Should Read", *World Economic Forum,* Febrero 2015, [Documento sin paginación]. Disponible en: https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/ (última consulta 03/01/18).

[11] Gacetilla Matemáticas, *John Graunt,* 2001, [Documento sin paginación]. Disponible en http://mcj.arrakis.es/graunt.htm (última consulta 12/11/17).

comercio[12] por el autor Miller Devens, donde aparece por primera vez el término *business intelligence*, un concepto esencial en la analítica dentro de la historia del *big data*. En la citada obra, el autor narra el éxito financiero del banquero Furneses, quien a través de recopilar, estructurar y analizar datos esenciales de su actividad logra una relevante ventaja competitiva. Posteriormente, con la creación de la máquina tabuladora, en 1880, por el ingeniero fundador de la compañía IBM, Herman Hollerith, mediante la utilización de tarjetas perforadas consigue reducir notablemente el volumen de trabajo en el censo de los Estados Unidos, puesto que a través de las tarjetas perforadas se pudo analizar la masiva cantidad de información en un año, cuando se estima que se habría tardado al menos diez años sin la invención de las mismas[13].

Años después, en el año 1926, Tesla con la tecnología inalámbrica predice que la humanidad en algún momento podrá acceder, almacenar y analizar datos desde un dispositivo tan pequeño que podrá llevar en el bolsillo. Dos años después, en 1928, surge el primer sistema magnético de almacenamiento de datos, creación del ingeniero alemán Fritz Pfleumer, método que actualmente se continúa empleando (aunque cada vez menos) en el almacenamiento de datos mediante discos duros de los ordenadores.

Son destacables también dos de los acontecimientos que surgieron en 1932 en Estados Unidos por generar la necesidad urgente de un registro preciso y organizado de la información: de un lado, el notable aumento de la población estadounidense en poco tiempo, lo que provocó una masiva emisión de números de la seguridad social; de otro lado, el mundo de la investigación y el conocimiento también creció en abundancia, debido a ello, en 1940 las bibliotecas se convirtieron en el lugar idóneo donde organizar y almacenar los datos, de hecho, muchas de las bibliotecas tuvieron que readaptar sus instalaciones y métodos de almacenamiento a fin de dar una respuesta más rápida y eficaz al aumento de la demanda de nuevas publicaciones e investigaciones.

---

[12] DEVENS MILLER, R., *Cyclopaedia of Commercial and Business Anecdotes*. *Comprising Interesting Reminiscences and Facts, Remarkable Traits and Humors of Merchants, Traders, Bankers Etc. in All Ages and Countries*, D. Appleton and Company, London, 1865, p. 210.

[13] DA CRUZ, F., "Columbia University Computing History", *German Hollerith,* 2011, [Documento sin paginación]. Disponible en: http://www.columbia.edu/cu/computinghistory/hollerith.html (última consulta 04/11/17).

Con la aparición del periódico *Lawton Constitution,* en el año 1941, se empieza hablar de la «explosión de la información» como motivo del fenómeno de la expansión de la información. El citado término se acuñó en un artículo del "New Statesman" en marzo de 1964, donde se menciona el problema de la gestión de los masivos volúmenes de información disponible[14]. A lo anterior habría que añadir otro acontecimiento[15], el estudio que realizó Rider a fin de conocer la cantidad de información que se genera, donde ya en el año 1944 el bibliotecario de la Universidad Wesleyana, pronostica que la Biblioteca de la Universidad de Yale contendrá aproximadamente 200 millones de libros almacenados en 6.000 millas (9.656 km) de estanterías en el año 2040, por lo que se necesitaría un personal de catalogado de más de seis mil personas, lo que supuso un primer aviso al problema del almacenamiento y la recuperación de datos como consecuencia del crecimiento del conocimiento[16].

Paralelamente, en 1936 el matemático inglés Alan Mathison Turing publicó un artículo "Sobre los números computables, con una aplicación al Entscheidungsproblem", en el que desarrolla el teorema de Gödel por el que se considera oficialmente el origen de la informática teórica. En el citado artículo el matemático hizo referencia a la máquina de Turing a efectos de demostrar la existencia de problemas irresolubles, tales que ninguna máquina de Turing podría solucionar, motivo por el que se le consideró el padre de la teoría de la computabilidad, pues la máquina de Turing era una entidad matemática abstracta que formalizó el concepto de algoritmo, convirtiéndose en la precursora de los ordenadores[17].

Por otro lado, en 1948 el matemático e ingeniero Shannon con la publicación de la "Teoría matemática de la comunicación", establece un sistema de trabajo a efectos de determinar los requisitos de datos mínimos para transmitir la información a través de canales imperfectos afectados por el ruido[18], de hecho, cabe resaltar que con esta teoría se ha conseguido disminuir el volumen de datos hasta nuestros días. Posteriormente, el

[14] MARR, "A Brief History of *Big Data*...", *op. cit.,* [Documento sin paginación].

[15] MARR, "A Brief History of *Big Data*...", *op. cit.,* [Documento sin paginación].

[16] *Vid.* PRESS, G., *A Very Short History Of Big Data,* Forbes, 2013, [Documento sin paginación]. Disponible en: https://www.forbes.com (última consulta 08/01/18).

[17] ALFONSECA MORENO, M., "La máquina de Turing", *Revista de didáctica de las matemáticas,* núm. 43-44, 2000, p. 165.

[18] MARR, "A Brief History of *Big Data*...", *op. cit.,* [Documento sin paginación].

físico Rudolf Güntsch, en 1956 desarrolla el concepto de "memoria virtual", su idea se fundamenta en tratar el almacenamiento de datos finito como infinito, es decir, un almacenamiento administrado por un *hardware* integrado y *software* a fin de no desvelar detalles al usuario, entre otros, su investigación ha permitido procesar los datos sin las limitaciones de memoria de *hardware*. Asimismo, diez años más tarde, el matemático Luhn[19] crea el concepto de Inteligencia de Negocios o, lo que comúnmente se conoce como *business intelligence.*

En consecuencia, a partir del concepto *business intelligence* (BI) surgen los primeros análisis de datos en la esfera de los negocios. Durante este periodo, la ciencia y el pensamiento científico continúa aumentando, según el científico Price, la revolución científica era el motor de la comunicación agilizada de ideas nuevas como la información científica, debido a ello y al rápido crecimiento, se tomó la medida de duplicar cada quince años los nuevos registros que se iban creando[20]. En concreto, en la Expo de 1962 es presentada la máquina *IBM Shoebox* creada por el ingeniero Dersch, un proyecto cuyo objetivo era el de registrar palabras en inglés en formato digital mediante el reconocimiento de voz, siendo la primera máquina que consiguió entender dieciséis palabras y diez dígitos en inglés hablado por medio de uso de datos disponibles, capaz de procesarlos correctamente[21].

Igualmente cabe destacar que, en esta época empieza a emerger lo que más tarde supondría un cambio de paradigma a consecuencia del colapso de información masiva desordenada dimanante del gran volumen de datos existente en la investigación científica, lo que supuso un sobreesfuerzo para los científicos a la hora de investigar, hasta la fecha, el método de organización del conocimiento llevado a cabo era mediante resúmenes documentales creado a finales de la década de 1800, pero conforme se avanzaba en el tiempo, en el mundo de la investigación y la ciencia cada vez se generaban más documentos, lo que supuso que el método de resúmenes documentales aplicado dejase de resultar suficiente. En consecuencia, a principios de la década de

[19] LUHN, H.P., "A *business intelligence* System", *IBM Journal*, Vol. 2-4, Octubre 1958, pp. 314-319. Disponible en http://altaplana.com/ibmrd0204H.pdf (última consulta 15/01/18).

[20] PRESS, "*A Very Short History Of Big Data…", op. cit.,* [Documento sin paginación].

[21] IBM 100, *Pioneering Speech Recognition,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/speechreco/ (última consulta 21/12/17).

1960 nace la necesidad de buscar una solución a la organización de la información almacenada[22], lo que generó que el Gobierno de los Estados Unidos en 1965 construyera un centro con la finalidad de recopilar y almacenar la ingente cantidad de datos existente a fin de solventar la problemática del almacenamiento de datos, proyectándose así el primer *data center* del mundo destinado a guardar mediante una cinta magnética documentación sobre los impuestos y los juegos de huellas dactilares.

En este sentido, se empiezan a desarrollar, a diseñar e implantar sistemas informáticos que permiten a las organizaciones científicas y del mundo de los negocios acceder de manera digital a los sistemas de inventario. En concreto, el matemático y científico inglés, Codd[23], colaborador en IBM Research Lab, publica en el año 1970 un artículo[24] sobre el desarrollo del modelo relacional de base de datos*,* un sistema de archivos jerárquico cuya finalidad principal consiste en que además de los científicos de la computación, cualquier persona pueda utilizar bases de datos accediendo a los registros mediante un sistema de índice simple, donde se desconoce la forma en la que se encuentra estructurada la información o el lugar dónde se encuentra registrada dentro de la base de datos, lo que supuso la posibilidad de que cualquier persona sin conocimientos informáticos cualificados ni específicos pudiera recuperar información, por ello, es utilizado desde su surgimiento hasta la actualidad en la mayoría de las transacciones de datos cotidianas - como acceder a cuentas bancarias, utilizar tarjetas de crédito, compra de acciones, compras en internet, entre otros - estructuras basadas en la teoría de la base de datos relacional[25].

Más tarde, surge el fenómeno del crecimiento de la comunicación bidireccional en Japón, donde el Ministerio de Correos y Telecomunicaciones realiza el Censo de Flujo de la Información con la finalidad de controlar el volumen de información en el país. Para ello, como unidad de medición, el gobierno japonés hace uso del número de palabras utilizadas en los medios de comunicación. Así pues, con el citado estudio, se

---

[22] PRESS, "*A Very Short History Of Big...*", *op. cit.,* [Documento sin paginación].

[23] Al respecto, hay que aclarar que Edgar F. Codd, es un científico inglés promotor de las doce leyes del procedimiento analítico informático y autor del término OLAP.

[24] IBM 100, *Relational Database,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com (última consulta 21/12/17).

[25] IBM 100, *Relational Database,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com (última consulta 21/12/17).

pudo comprobar que el volumen de palabras era mucho más elevado que el volumen de información, así como una deficiencia notoria en la demanda de comunicación unidireccional, siendo la tendencia demandada la comunicación bidireccional, una comunicación más personalizada en respuesta a las necesidades de los ciudadanos[26].

De igual modo, a consecuencia de la popularización en el uso común de los negocios de los sistemas de Planeación de Requerimientos Materiales (MRP)[27] utilizados por las empresas para organizar y planificar su información en el año 1976, se genera una mejora de la eficiencia de las operaciones en la empresa, surgiendo así los primeros usos comerciales de los ordenadores, donde la informática, el almacenamiento y la distribución de datos fueron la base para la organización de tareas de rutina diaria. Este acontecimiento generó un cambio en los procesos de negocio y las funcionalidades de contabilidad, tal es así que se fundan empresas como Oracle[28], JD Edwards y SAP[29].

A comienzos de los años 80, la información es generada con mayor velocidad y cantidad, y a su vez, las posibilidades de almacenamiento y de organización de los datos es menor, puesto que se almacena todo tipo de datos ante la imposibilidad de sustraer aquellos datos relevantes y útiles. El anterior fenómeno es definido por Tjomsland como la Ley de los Datos de Parkinson, afirmando en la conferencia "Where Do We Go From Here?*"* dada en *Fourth IEEE Symposium on Mass Storage Systems*[30], que:

"Los datos se expanden para llenar el espacio disponible [...] las grandes cantidades de datos se guardan porque los usuarios no tienen forma de identificar los

[26] DUFF, A.S., *Information Society Studies,* Ed. Routledge, London, 2000, p.37.

[27] Se trata de un *software* de gestión de materiales antecedentes de los ERP actuales.

[28] En concreto, destacar que la empresa Oracle comercializó el *Structure Query Language* (SQL) que "es un lenguaje declarativo estándar internacional de comunicación dentro de las bases de datos que nos permite a todos el acceso y manipulación de datos en una base de datos, y además se puede integrar a lenguajes de programación, por ejemplo, ASP o PHP, y en combinación con cualquier base de datos específica, por ejemplo, MySQL, SQL Server, MS Access, entre otras". Fuente: https://devcode.la/blog/que-es-sql/ [Documento sin paginación].

[29] HOPP, W. J. and SPEARMAN, M. L., "To Pull or Not to Pull: What is the Question?", *Manufacturing & Service Operations Management (M&SOM)*, vol. 6, núm. 2, 2004, pp. 133-148. Documento disponible en: https://pubsonline.informs.org/doi/pdf/10.1287/msom.1030.0028 (última consulta 11/11/18).

[30] TJOMSLAND, I.A., "To Digest of Papers: The Gap between MSS Products and User Requirements*",* *Fourth IEEE Symposium on Mass Storage System*s, abril 1980, pp. 15-17.

datos obsoletos; las penalizaciones derivadas de almacenar datos obsoletos tienen una importancia inferior a las que conlleva eliminar datos potencialmente útiles".

Paralelamente, surgen nuevos métodos de organización, almacenamiento y creación de datos a consecuencia del avance tecnológico, comienzan a tomarse las primeras decisiones de negocio mediante el uso de los datos. Otro acontecimiento importante en este contexto es la publicación del artículo "Tracking the Flow of Information*"* por Ithiel de Sola Pool en la revista *Sciencie,* donde analiza el aumento de la información en 17 medios de comunicación desde el año 1960 hasta 1977, concluyendo que el crecimiento de la información es una consecuencia derivada de la expansión del sector de las comunicaciones[31]. Igualmente, nace la necesidad de almacenar de manera homogénea los datos y de analizar aquellos datos de alta calidad, completos y exactos, por lo que Devlyn y Murphy desarrollan una arquitectura para los informes y análisis de negocio en IBM, convirtiéndose en la base del almacenamiento de datos[32].

En concreto, en 1985 se crea la Planificación de Recursos de Fabricación (MRP II), a fin de optimizar la gestión del área de producción y la distribución, la gestión de proyectos, las finanzas, los recursos humanos y la ingeniería. Por otro lado, durante esta década se incrementan los sistemas de Planificación de Recursos Empresariales (ERP), siendo cada vez más sofisticados y coordinados entre los distintos departamentos de las empresas, lo que en consecuencia provoca que mediante las bases de los sistemas de MRP, MRP II y ERP, los datos se clasifiquen en los distintos sectores dentro de una misma empresa (producción, distribución, contabilidad, finanzas, recursos humanos, gestión de proyectos, gestión del inventario, gestión del transporte y, gestión del servicio y mantenimiento, entre otros) ofreciendo mayor accesibilidad, visibilidad y homogeneidad en toda la empresa[33]. Un año después, se amplía el concepto de *business intelligence*[34] por Howard Dresner, quien considera que la BI se materializa en sistemas

[31] DE SOLA POOL, I., "Tracking the Flow of Information", *Science,* vol. 221, agosto 1983, pp. 609-613.

[32] DEVLIN, B.A. and MURPHY, P.T., "An architecture for a business and information system", *IBM Systems Journal,* vol. 27, núm. 1, febrero 1998, pp. 60-80. Documento disponible en: http://www.9sight.com/pdfs/EBIS_Devlin_&_Murphy_1988.pdf (última consulta 02/02/18).

[33] HOSSAIN, L., PATRICK, J.D. and RASHID, M.A., *Enterprise Resource Planning: Global Opportunities and Challenges,* Ed. Idea Group Publishing, Estados Unidos, 2002.

[34] El concepto *business intelligence* es creado en 1958 por Hans Peter Luhn.

software que por medio de la recopilación de datos ayudan a la toma de decisiones eficientes de negocio, puesto que los datos históricos permiten obtener una mayor perspectiva de lo que ha sucedido y está sucediendo en la empresa. A raíz de todo lo anterior y, a consecuencia de la necesidad de mejorar la BI, empresas como Business Objects, Actuate, Crystal Reports[35] y MicroStrategy, comienzan a presentar sus propios informes y análisis de datos[36].

Por último, como hecho relevante que surge a finales de los años 80, es la primera aparición del término de *big data* en un artículo[37] escrito por Larson para la revista *Harper´s Magazine*, donde realiza una crítica del correo basura que recibe y de la manera en la que los anunciantes usan los datos para dirigirse a los clientes. Asimismo, en este año comienza a usarse con más frecuencia herramientas de *business intelligence* a fin de analizar la actividad comercial y el rendimiento de las operaciones. A finales de la década de los 80 aparece también como novedad, por un lado, el concepto *data mining* (minería de datos)[38] como técnica de análisis con la que se extrae el conocimiento a partir de bancos de datos y, por otro lado, aparece la expresión *knowledge discovery in databases* (KDD).

No obstante, hasta ese momento todavía no asistimos a una conectividad global en red que produzca grandes volúmenes de datos masivos en poco tiempo, pues el cambio de paradigma vendrá determinado a través del acceso a internet y a su vez con la implantación de las nuevas tecnologías que, actualmente, se encuentran presentes en la mayoría de los sectores de la sociedad[39].

---

[35] En 1992, la empresa "*Crystal Reports"* junto con "*Windows"* crea el primer informe de base de datos. La creación de estos informes sencillos a partir de datos iniciales con escasa programación de código genera una notoria reducción a la presión existente sobre el panorama saturado de datos y, permite asimismo que las empresas puedan emplear la inteligencia empresarial de un modo asequible.

[36] POWER, D.J., "A Brief History of Decision Support Systems"*, DSSResources.COM*, 2007, [DOCUMENTO SIN PAGINACIÓN]. Disponible en: http://dssresources.com/history/dsshistory.html (última consulta 18/02/18).

[37] BRUECKNER, R., "Where Dig *Big Data* Come From", *InsideBIGDATA*, núm. 3, febrero 2013, [Documento sin paginación]. Disponible en: https://insidebigdata.com/2013/02/03/where-did-big-data-come-from/ (última consulta 02/07/18).

[38] MITCHELL, "*Machine Learning…*", *op. cit.,* p. 432, afirma que debemos de tener presente que la técnica en la que se emplea en *data mining* (minería de datos) para crear modelos predictivos es el *Machine Learning* (aprendizaje automático), sobre todo se aplica en el sector financiero y de seguros, a fin de tomar decisiones acertadas en la creación de productos financieros eficaces y exitosos.

[39] BRENT, D.R., "En la era de la información: información, tecnología y estudio del comportamiento", *Documentación De Las Ciencias De La Información*, vol. 13, 1980, p. 55, afirma que: "Las nuevas

3. LA INTERCONEXIÓN Y CONECTIVIDAD GLOBAL

A principios de la década de los ´90 con las nuevas tecnologías de la información y el nacimiento de internet, surge la comunicación a través del ordenador y con ello la conectividad global en red[40], lo que en consecuencia generó una mayor producción, almacenamiento, recuperación y análisis de datos a gran velocidad[41].

De hecho, Berners - Lee, ingeniero de telecomunicaciones, desarrolla un sistema de red con interconexiones a nivel mundial accesible para todos en cualquier lugar, lo que en consecuencia generó una notable y masiva producción de datos a gran escala y velocidad. Dos años más tarde, es fundada QlikTech (actualmente Qlik), creándose un sistema revolucionario de BI, lo que en el 2012 sería el análisis *business discovery* del

---

tecnologías están presentes en casi todas las facetas de la actividad social y profesional contemporáneas. Un área donde sus consecuencias son especialmente evidentes es la del ocio, en el que el sistema por cable, las telecomunicaciones, los distintos grabadores de video y los aparatos de reproducción, han aumentado en gran manera el número de salidas útiles para el entretenimiento. Los vídeos y receptores portátiles proporcionan una mayor flexibilidad en cuanto al cuándo, al dónde, y a cómo deseamos entretenemos".

[40] Al respecto, en relación con la conectividad general en el sector del a salud BARRERA, L., GONZÁLEZ F., VALENZUELA, J. y CEDEÑO, M., *Impacto de las TICS en la Salud,* [Documento sin paginación] señalan que: "El fenómeno de la globalización estos últimos años ha alcanzado en estos últimos años características que lo diferencian, un espacio físico que se dilata en lo geográfico y se aproxima en el tiempo, un aumento exponencial en la capacidad de intercambiar bienes y servicios y sobre todo una mayor interdependencia entre las personas, las organizaciones y las tecnologías. Los nuevos instrumentos como internet, las comunicaciones móviles y las redes de medios de comunicación, están promoviendo la interconexión más amplia que jamás ha existido entre unas personas y otras y entre estas y todo tipo de organismos e instituciones. Ello ha dado lugar a un acceso cada vez más fácil a la información y a un intercambio mucho más rápido de conocimiento. Como ocurre en otros campos, las TIC se están haciendo presentes cada vez más en el ámbito de la salud. La práctica clínica gira alrededor de datos, información y conocimiento. Internet se ha convertido en la mayor fuente de información sanitaria no solo para los profesionales sino también para los pacientes. Además, han surgido y siguen surgiendo multitud de iniciativas de aplicaciones médicas y sanitarias que, aparte de los servicios de información, contemplan la posibilidad de consulta a médicos: La segunda opinión, los grupos de apoyo entre pacientes, servicios de telemedicina y una amplia gama de posibilidades. El desarrollo de infraestructuras de redes digitales de comunicaciones de tipo corporativo y el acceso generalizado a Internet están permitiendo el flujo de información entre todos los actores, usando historiales clínicos electrónicos en un entorno seguro, mejorando la calidad de los servicios y facilitando una gestión más eficiente y cómoda para los ciudadanos". Disponible en: http://www.neopuertomontt.com/InformaticaMedica/lasticsenelsectorsalud.pdf (última consulta 02/15/18)

[41] "Las nuevas tecnologías de la información están integrando al mundo en redes globales de instrumentalidad. La comunicación a través del ordenador engendra un vasto despliegue de comunidades virtuales. No obstante, la tendencia social y política característica de la década de 1990 fue la construcción de la acción social y la política en tomo a identidades primarias, ya estuvieran adscritas o arraigadas en la historia y la geografía o de génesis reciente en una ansiosa búsqueda de significado y espiritualidad. Los primeros pasos históricos de las sociedades informacionales parecen caracterizarse por la preeminencia de la identidad como principio organizativo", en CASTELLS M., *La Sociedad Red. Volumen I. La era de la información: economía, Sociedad y cultura*, Alianza Editorial, Madrid, 1997, p.46.

que hace referencia la compañía Gartner[42]. Igualmente, a modo curiosidad hay que destacar que, transcurridos cinco años desde el surgimiento de internet, en concreto, en 1996, los precios del almacenamiento de datos digital comienzan a ser accesibles, hasta el extremo de resultar más rentables que el papel a efectos de almacenar datos[43]. A consecuencia de lo anterior, comienzan a surgir las plataformas de *business intelligence 2.0*, lo que genera una gran revolución en la historia del *big data*. De igual modo, en la década de los años ´90 debido a la interconexión en red los datos aumentan desmesuradamente y a gran velocidad, lo que provoca la necesidad de tener que diseñar y actualizar los productos ERP, generando una ruptura de los límites de titularidad y de personación, obligando a los proveedores a abandonar intranet y optar por un método de negocio corporativo.

En 1997, Google pone a disposición del usuario un motor de búsqueda en internet, lugar de la red que se convertirá en el más popular y usado por los navegantes para la búsqueda de información. Por otro lado, el autor Lesk, publica su estudio "¿Cuánta información hay en el mundo?"[44], donde concluye que una de las graves consecuencias del motivo por el que se genera gran cantidad de información en poco tiempo es que parte de esta información no será nunca procesada por nadie, pues el universo digital irá aumentando diez veces su tamaño cada año.

En ese mismo año, el concepto de *big data* es empleado por segunda vez en un estudio académico realizado por los investigadores de la NASA, Michael Cox y David Ellsworth, con el título "Application controlled demand paging for out of core visualization"[45], siendo este el primer artículo publicado por la *ACM digital library* que emplea el término *big data*. De igual modo, en el mundo de la Inteligencia Empresarial, a finales de los años 90 aparece el problema de acceso a los datos y a la información,

---

[42] Visítese sitio web oficial de la compañía Gartner: https://www.gartner.com/technology/home.jsp [Documento sin paginación].

[43] MORRIS, R.J.T. and TRUSKOWSKI, B.J., "The Evolution of Storage Systems", *IBM Systems Journal,* núm. 1, julio 2003, pp. 205-217.

[44] LESK, M., "How much information is there in the world?", *Tenopi,* 1997, [Documento sin paginación]. Disponible en: http://www.lesk.com/mlesk/ksg97/ksg.html (última consulta 23/11/17).

[45] COX, M. and ELLSWORTH, D., "Application controlled demand paging for out of core visualization", *ProceedinGC of the 8th IEEE Visualization ´97 Conference*, 1997, pp. 235 - 244. Documento disponible en https://www.evl.uic.edu/cavern/rg/20040525_renambot/Viz/parallel_volviz/paging_outofcore_viz97.pdf (última consulta febrero 2018).

donde únicamente pueden acceder a los mismos los departamentos informáticos, se genera así una gran dependencia a los citados departamentos por parte del resto de personal y empleados de las empresas, puesto que los informáticos se responsabilizaban del 80% del acceso a la BI[46].

A finales de los años 90, surge el primer uso del concepto *Internet of Things* (IoT) en la presentación de negocios que realiza el empresario Ashton cofundador del Auto-ID Center del MIT, para *Procter and Gamble*[47]. Igualmente, en ese mismo año, surge el fenómeno en el que se cuantifica el volumen total de información nueva generada en el mundo durante un año, en concreto, el estudio se realiza sobre el año 1999, en el que se concluye la producción mundial de 1,5 exabytes[48] de información en todo el año[49]. Asimismo, en ese mismo momento *ComputerWeekly* publica el artículo "Choosing and Installing the Right ERP Solution" por Preston, donde se explica el método de elección e instalación correcto de la solución ERP y se establece el uso de pronósticos de análisis predictivo como cambio eficaz y productivo en el método de trabajo organizativo[50].

Es destacable, también, que a principios del siglo XXI, Doug Laney, analista de Gartner, define en un artículo titulado "3D *data management*: Controlling Data Volume, Velocity, and Variety"[51], las 3 V´s del *big data*: *Volumen, Velocity, Variety*, resultando ser los tres conceptos fundamentales del término y, que actualmente resultan ser las

---

[46] SMITH, N., "History of *business intelligence* ", *SlideShare,* 1 abril 2009. Video disponible en: https://www.slideshare.net/nicsmith/history-of-business-intelligence-1236862 (última consulta 12/01/18).

[47] ASHTON, K., "That `Internet of ThinGC´ Thing", *RFID Journal,* 2009*,* [Documento sin paginación]. Documento disponible en: http://www.rfidjournal.com/articles/view?4986 (última consulta 12/03/18).

[48] Un exabyte es una unidad de medida de almacenamiento de datos cuyo símbolo es el EB. Equivale a 10^{18} bytes. El prefijo exa-, adoptado en 1991, procede del griego έξι , que significa «seis» (como *hexa*-), pues equivale a 1024^6 1 EB = 10^3 PB = 10^6 TB = 10^9 GB = 10^{12} MB = 10^{15} KB = 10^{18} bytes. 1024 exbibytes equivalen a un zebibyte (Información proporcionada desde la enciclopedia libre Wikipedia). [Documento sin paginación].

[49] LIMAN, P. and VARIAN, H.R., "How much information?", *Regents of the University of California,* 18 de octubre de 2000, [Documento sin paginación]. Documento disponible en: http://www2.sims.berkeley.edu/research/projects/how-much-info/ (última consulta 10/10/17).

[50] PRESTON, P., "Choosing and installing the right ERP solution", *TechTarget,* 1999, [Documento sin paginación]. Documento disponible en: http://www.computerweekly.com/feature/Choosing-and-installing-the-right-ERP-solution (última consulta 10/10/17).

[51] LANEY, D., "3D *data management*: Controlling Data Volume, Velocity, and Variety", *Application Delivery Strategies, Meta Group Inc*., 6 de febrero 2001, [Documento sin paginación]. Documento disponible en: https://bloGC.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (última consulta 11/10/17).

dimensiones que lo definen, junto con veracidad y valor. Otros de los fenómenos relevantes es la popularización del concepto «SaaS» (*software as a service),* base principal de las aplicaciones basadas en la nube. Por otro lado, también es cuando en un artículo sobre la división de comercio electrónico de *Software & Information Industry* (SIIA) aparecen por primera vez las siglas "SaaS" (*Software* como servicio). A comienzos del milenio, aparece el concepto *data science* (ciencia de datos) como herramienta y técnica que integra principios y fundamentos de diversas disciplinas científicas – estadística, matemáticas, informática, computación, entre otras – a fin de guiar la extracción de conocimiento mediante la técnica de *data mining* aplicada en los análisis de datos.

Posteriormente, a consecuencia de la ampliación de complementos y módulos básicos en los sistemas ERP durante los años 90, aparecen los denominados ERP extendidos o ampliados, siendo aumentado a su vez el número de *software* y *hardware*, fundándose empresas especializadas en *software* ERP, como Oracle, PeopleSoft, JD Edwards y SAP[52], que facilitan a sus clientes creaciones de aplicaciones nuevas a partir de datos de otras aplicaciones mediante la utilización del *Extensive Marketing Lenguage* (XML)[53].

En el año 2005, el número de datos comienza a aumentar en la era digital y nace la Web 2.0, siendo en la actualidad la mayoría del contenido web creado por los usuarios[54]. En ese mismo año, se constituye la empresa Workday Inc., que ofrece un *software* más intuitivo, económico y de fácil uso para el usuario final, que el de las empresas Oracle y SAP. Un año después, en 2006, es creado HADOOP, un entorno de trabajo *big data* de *software* libre y descarga gratuita, como respuesta a la necesidad de

[52]RASHID, M.A., HOSSAIN, L. and PATRICK, J.D., "The Evolution of ERP Systems: A Historical Perspective", *Idea Group Publishing,* 2002, pp. 1-16. Documento disponible en: https://faculty.biu.ac.il/~shnaidh/zooloo/nihul/evolution.pdf (última consulta 15/10/17).

[53] El Extensible Markup Language, traducido como "Lenguaje de Marcado Extensible" o "Lenguaje de Marcas Extensible", es un metalenguaje que permite definir lenguajes de marcas desarrollado por el World Wide Web Consortium utilizado para almacenar datos en forma legible. Información rescatada de: https://es.wikipedia.org/wiki/Extensible_Markup_Language (último acceso 22/04/21).

[54] O´REILLY, T., "What is Web 2.0?", *O´Reilly Media*, 2005, [Documento sin paginación]. Documento disponible en: http://www.oreilly.com/pub/a//web2/archive/what-is-web-20.html (última consulta 01/01/18).

sistemas nuevos para gestionar los datos en internet[55], siendo, por tanto, un código abierto de almacenamiento y procesamiento de datos.

En esta época, la revista *Wired* publica un artículo[56] en el que analiza la perspectiva positiva y negativa de la masividad de los datos mediante el concepto *big data a las masas,* resurgiendo así el uso del término *big data*. De otro lado, ese mismo año, se publica el artículo "Big Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science, and Society" [57] por un grupo de investigadores informáticos. Un año después, los directores de tecnologías de la información le otorgan prioridad y absoluta credibilidad a la Inteligencia Empresarial (BI)[58]. Paralelamente, aparece por primera vez el concepto *linked data*, empleado por Berners - Lee en el congreso TED de 2009, a fin de describir un método de publicación de datos estructurados, basado en protocolos web estándar, interconectados con otros ordenadores y enlazados con otros datos externos[59]. Al respecto un dato curioso es aportado por Schmidt, presidente ejecutivo de Google, en una conferencia que dio en el año 2010, donde señaló que "los datos que se generan en dos días equivalen a la cantidad de datos generados desde el inicio de la civilización hasta 2003"[60].

---

[55] OLSON, M., "HADOOP: Scalable, Flexible Data Storage and Analysis", *Connecting Innovation and Intelligence IQT QUARTERLY,* Vol. 1, núm. 3, 2010, pp. 14-18. Documento disponible en: https://blog.cloudera.com/wp-content/uploads/2010/05/Olson_IQT_Quarterly_Spring_2010.pdf (última consulta 01/10/18).

[56] ANDERSON, CH., "The end of theory: the data deluge makes the scientific metohd obsolete", *Wired,* 2008 [Documento sin paginación]. Documento disponible en: https://www.wired.com/2008/06/pb-theory/ (última consulta 17/01/18).

[57] BRYANT, R.E., KATZ, R.H. and LAZOWSKA, E.D., "Big-Data Computing: Creating revolutionary breakthroughs in commerce, science, and society: A white paper prepared for the Computing Community Consortium committee of the Computing Research Association", *CCC-Led White Papers,* 2008, [Documento sin paginación]. Documento disponible en: http://cra.org/ccc/resources/ccc-led-whitepapers/ (última consulta 16/01/18).

[58] STAMFORD, C., "Gartner EXP Worldwide Survey of More than 1,500 CIOs Shows IT Spending to Be Flat in 2009, *Gartner,* enero 2009, [Documento sin paginación]. Documento disponible en: Available from: https://www.gartner.com/newsroom/id/855612 (última consulta 21/01/18).

[59] BIZER, CH., HEATH, T. and BERNERS-LEE,T., "Linked Data - The Story So Far", *Tomheath,* 2009, [Documento sin paginación]. Documento disponible en: http://tomheath.com/papers/bizer-heath-berners-lee-ijswis-linked-data.pdf (última consulta 22/01/18).

[60] SCHMIDT, E., "Eric Schmidt at Techonomy", *Techonomy,* 2010, [DOCUMENTO SIN PAGINACIÓN]. Documento disponible en http://www.techonomy.com/. Acceso video Eric Schmidt speaks on a panel with Debby Hopkins, Kevin Kelly and Lisa Randall, moderated by David Kirkpatrick, at the Techonomy conference in Lake Tahoe, Calif., de fecha 4 de agosto 2010 en: https://www.youtube.com/watch?v=UAcCIsrAq70.

Asimismo, *The Economist,* ese mismo año, publica un informe bajo el título *Data, Data Everywhere* donde se afirma que: "[...] el mundo contiene una cantidad de información digital de una magnitud inimaginable, cuyo ritmo de crecimiento es frenético […] El efecto es patente en todos los ámbitos de nuestra vida, desde los negocios hasta la ciencia, los gobiernos o el arte"[61]. Igualmente, en el 2010, aparecen las tecnologías de nube para los sistemas ERP, siendo pioneras de las mismas las empresas Netsuite y Lawson *Software*, quienes ofrecen a empresas medianas y otras organizaciones sistemas ERP asequibles y sencillos[62]. De otro lado, es destacable también, tal y como pone de manifiesto Bernard Marr en su artículo[63] que, en el año 2011, el informe *McKinsey Global Institute* estimó que en 2018 Estados Unidos tendría un déficit de entre 140.000 y 190.000 científicos profesionales de datos, apercibiendo que problemas como la privacidad, la seguridad y la propiedad intelectual necesitaran de resolución jurídica previa ante la alarma del valor del *big data*[64]. En ese mismo año, dentro del mundo de la Inteligencia Empresarial, priman los servicios de la nube, la visualización de datos, el análisis predictivo y el *big data*[65].

Posteriormente, en el año 2012 se define el *big data* como "un fenómeno cultural, tecnológico e intelectual que aparece por la interconexión de los siguientes elementos: tecnología, análisis y mitología", en el artículo "Critical Questions for Big Data"[66] publicado por *Information, Communications, and Society Journal.*

---

[61] CUKIER, K., "Data, data everywhere", *The Economist,* febrero 2010, [Documento sin paginación]. Documento disponible en: http://www.economist.com/node/15557443 (última consulta 17/01/18).

[62] SARAN, C., "Putting ERP in the cloud", *Computer Weekly*, 2010, [Documento sin paginación]. Documento disponible en: http://www.computerweekly.com/news/1280092536/Putting-ERP-in-the-cloud (última consulta 17/01/18).

[63] MARR, "A Brief History of *Big Data*...", *op. cit.,* [Documento sin paginación].

[64] MANYIKA, J., BROWN, B., DOBBS, R., ROXBURGH, CH. and BYERS, A. H., "*Big Data*: The next frontier for innovation, competition, and productivity", *McKinsey Global Institute*, junio 2001, [Documento sin paginación]. Documento disponible en: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation (última consulta 15/11/17).

[65] ROGERS, S., "Top 10 Trends in *business intelligence* and Analytics for 2011", *Enterprise Management EMA BloGC,* 2011 [Documento sin paginación]. Documento disponible en: http://bloGC.enterprisemanagement.com/shawnrogers/2011/01/11/top-10-trends-in-business-intelligence-and-analytics-for-2011/ (última consulta 10/01/18).

[66] BOYD, D., "Critical questions for *Big Data*", *Journal Information, Communication & Society,* vol. 15, núm. 5, 2012, pp. 663-679. Documento disponible en https://people.cs.kuleuven.be/~bettina.berendt/teaching/ViennaDH15/boyd_crawford_2012.pdf (última consulta 11/01/18).

Finalmente, en los últimos años hemos asistido a varios acontecimientos de notoria relevancia en la esfera de las nuevas tecnologías y del Internet de las Cosas: por un lado, es en el año 2014, cuando por primera vez en la historia de internet el uso del «Internet móvil» supera a los ordenadores, lo que genera un gran volumen de datos y mejora la conectividad con otros dispositivos, convirtiéndose en una prioridad el análisis de grandes volúmenes de datos[67]. En concreto, se implantan en la mayoría de las empresas nuevas tecnologías a fin de analizar y optimizar cantidades de datos masivos, donde los datos ya se perciben como un producto empresarial que forman parte del activo de negocio a efectos de obtener beneficios y ventajas frente a la competencia[68]; por otro lado, en el año 2015 presenciamos al surgimiento de las *Smart Cities* o Ciudades Inteligentes, ciudades que usan el análisis de información contextual en tiempo real a fin de mejorar la calidad y el rendimiento de los servicios urbanos, reducir costes, optimizar recursos e interactuar de forma activa con los ciudadanos. Posteriormente, en el año 2016, el *big data* empieza a ser una tendencia, no sólo en la industria tecnológica sino en otros ámbitos de la espera social, aumentando la oferta de expertos en *big data*, el *Machine Learning* se instala en las fábricas y el Internet de las Cosas (IoT) empieza a abarcar toda la industria tecnológica. Un año después, en el 2017 las masas generan datos, lo que en consecuencia ha provocado que la multitud pueda controlar, acceder, conocer e informarse sobre datos mediante las aplicaciones móviles.

En conclusión, como se puede apreciar, el *big data* no es un fenómeno que ha surgido aisladamente de todo acontecimiento social, sino que procede de una larga evolución de los datos y de su uso[69]. Por ende, este gran acontecimiento que llamamos *big data* ha generado la necesidad social de organizar y almacenar la información, puesto que debido al crecimiento de la industria tecnológica donde se ha generado un gran volumen de datos surge inevitablemente la necesidad de crear sistemas de almacenamiento de datos más eficaces y eficientes a efectos de solventar los problemas

[67] Encuesta internacional realizada por GE donde el 88% de los ejecutivos responden que el análisis de grandes volúmenes de datos es una prioridad.

[68] OLAVSRUD, T., "12 *Big Data* Predictions for 2014", *CIO from IDG,* 2011, [DOCUMENTO SIN PAGINACIÓN]. Documento disponible en: https://www.cio.com/article/2369764/big-data/132163-12-Big-Data-Predictions-for-2014.html (última consulta 19/01/18).

[69]Como señala MARR: *"*es sólo un paso más que traerá cambios en la forma en que manejamos los negocios y la sociedad. Al mismo tiempo que sentará las bases sobre las que se construirán otras evoluciones". *Vid.* MARR, "A Brief History of *Big Data…", op. cit.,* [Documento sin paginación].

generados a causa del caos diamante del desorden de los datos[70]. Por último, sobre la perspectiva de futuro del *big data*, cabría afirmar, como se verá más adelante, que se prevé que en un futuro se genere un rápido aumento de datos a causa del cambio de tecnologías analógicas a digitales tanto por parte de personas físicas como personas jurídicas[71].

III. LA INFLUENCIA DE LA GESTIÓN DEL CONOCIMIENTO COMO ASPECTO FUNDAMENTAL EN EL POSTERIOR DESARROLLO DEL *BIG DATA*: DATO, INFORMACIÓN Y CONOCIMIENTO

Es preciso, en este punto resaltar que en el año 1970 con la aparición de las tecnologías (TIC), el conocimiento adquiere un nuevo y revolucionario valor, donde comienza a ser tratado por la sociedad como un producto y elemento estratégico para toda organización, así como el hecho de que en 1980 con la aparición de la sociedad de la información, el conocimiento se convierte en un elemento substancial para el desarrollo estratégico de las organizaciones, debido a la gran demanda social de productos y servicios basados en el conocimiento, como más adelante se verá. Asimismo, a consecuencia de la aparición de las TIC, del Internet de las Cosas (IoT) y de la Inteligencia Artificial, quedan obsoletos los modelos tradiciones de valoración de conocimiento, debido a la gran velocidad por la que se generan espaciosos volúmenes de datos e información, siendo estimulado el desarrollo de sistemas, modelos e indicadores para la medición del conocimiento en las organizaciones a fin de desarrollar estrategias de formación continua[72].

El ámbito sanitario no desconoce lo anterior y, por ello, sus procesos asistenciales, de gestión e investigación se adaptan cada vez más a la era digital, siendo una de las finalidades principales de los países desarrollados la digitalización total del sistema sanitario, a efectos de que tanto los diferentes actores del sector sanitario como

[70] HERNÁNDEZ MARTÍN, A., "Breve historia del *Big Data", Archivamos*, núm. 97, Marzo, 2015, pp. 41-44.

[71] Si bien, como es sabido, únicamente son titulares del derecho de protección de datos las personas físicas.

[72] RODRÍGUEZ GÓMEZ, D., "Modelos para la creación y gestión del conocimiento: una aproximación teórica", *Educar*, núm. 37, 2006, p. 27.

los propios pacientes dispongan de herramientas electrónicas que permitan gestionar la información médica y acceder a la misma en tiempo real, así como la posibilidad de interactuar de manera digital los facultativos sanitarios entre ellos, así como con sus pacientes, objetivos todos ellos que en los últimos años se han ido alcanzando con mayor facilidad y rapidez gracias a los avances tecnológicos así como a la inversión financiera en las TIC SALUD.

Se ha de tener presente que a causa de la transformación de la digitalización del sistema sanitario, cada vez se acumula más información digital que está siendo de gran utilidad para nuevos proyectos de investigación biomédica y farmacéutica que reutilizan la misma a través de la aplicación de herramientas *big data*, donde se extrae nuevo conocimiento de gran valor para optimizar procedimientos, mejorar la calidad asistencial y abrir nuevas líneas de investigación, entre otras muchas oportunidades que más adelante se detallarán. De igual modo, la información también resulta un pilar relevante pues facilita el proceso de toma de decisiones, donde incluso conocer qué información necesitamos es sumamente importante, e incluso las propias herramientas *big data* nos facilitarán información acerca de dónde invertir para conseguirla, así pues, a través de las mismas es posible generar información de gran utilidad para decidir y planificar.

Debido a lo anterior, si consideramos el *big data* como una herramienta innovadora que crea conocimiento, resulta imprescindible que previamente sean asimilados los conceptos de conocimiento, dato e información en el contexto actual, así como el modelo de gestión del conocimiento, conceptos que serán analizados a continuación.

1. ASPECTOS DIFERENCIALES ENTRE DATO, INFORMACIÓN Y CONOCIMIENTO

En primera instancia, será analizado en este punto el concepto de "conocimiento" desde una perspectiva propiamente tecnológica y científica centrándonos en las doctrinas pronunciadas al respecto en las últimas décadas, todo ello

a fin de adaptar los aspectos diferenciales con conceptos propiamente contemporáneos como es el de dato e información.

Así pues, a modo de ejemplo, cabe citar a los autores Nonaka y Takeuchi[73] quienes sostienen que la inteligencia y el conocimiento son los activos con más valor en una organización. En concreto, para estos autores el conocimiento es un proceso humano y dinámico que se orienta a un fin determinado, con intención y perspectiva, definiendo el conocimiento como una creencia verdadera justificada, esto es, como un proceso humano dinámico que justifica la creencia personal con relación a la verdad. Por consiguiente, según Nonaka y Takeuchi el proceso de generación del conocimiento en la organización denominado el Modelo Espiral del Conocimiento, consiste en la transformación del conocimiento tácito en conocimiento explícito, es decir, cuando el conocimiento que se encuentra en la mente de los individuos es transferido, capturado, clasificado y almacenado en un soporte en papel o electrónico (libros, bases de datos, manuales, entre otros), desarrollándose en un espiral que se inicia en lo individual y se desplaza en una interacción que va creciendo en forma de espiral que únicamente finalizaría con la desaparición de la humanidad.

Por otro lado, nos encontramos con el Proceso de Conversión del Conocimiento en la Organización, donde según Nonaka y Takeuchi el Modelo Espiral del Conocimiento da lugar a cuatro fases en el proceso de creación del conocimiento:

(1) Socialización. Adquisición de conocimiento tácito a partir de conocimiento tácito por medio de la interacción directa entre las personas. El emisor del conocimiento comparte sus experiencias y conocimientos con el receptor, que es la persona interesada en el conocer y aprender;

[73] NONAKA, I. and TAKEUCHI, H., *The knowledge creating company,* Oxford University Press, Nueva York, 1995, p. 3 y p. 21, cuyo conocimiento lo definen como "creencia verdadera justificada para reflejar el conocimiento actual en el que se enmarca la existencia del mismo. Esta creación de conocimiento organizacional se definió como "... la capacidad de una empresa en su conjunto para crear nuevos conocimientos, así como difundirlo en toda la organización y que queden establecidos en productos, servicios y sistemas". (Traducción propia de la obra de referencia).

(2) Exteriorización. Conversión del conocimiento tácito en conocimiento explícito. Por medio del diálogo el individuo exterioriza ideas, imágenes y/o palabras, haciendo tangible el conocimiento mediante el uso de metáfora;

(3) Combinación. Transferir conocimiento explícito en conocimiento explícito. El individuo transfiere conocimiento explícito sobre un determinado campo a partir de los escritos e investigaciones de otras personas que también han transferido conocimiento explícito vinculado a la misma cuestión;

(4) Interiorización. Incorporar conocimiento explícito en conocimiento tácito. El individuo mediante vivencias y experiencias adquiere conocimiento tácito en forma de modelos mentales que posteriormente va a utilizar en otras situaciones de su vida[74].

De igual modo, los autores Davenport y Prusak consideran que el conocimiento funciona a través de cuatro actividades progresivas – acceso, generación, fijación, y transferencia de conocimiento, definiendo el mismo como:

"[…] una mezcla de experiencia, valores, información y "saber hacer" que sirve como marco para la incorporación de nuevas experiencias e información, y es útil para la acción. Se origina y aplica en la mente de los conocedores. En las organizaciones con frecuencia no sólo se encuentra dentro de documentos o almacenes de datos, sino que también está en rutinas organizativas, procesos, prácticas y normas"[75].

En este sentido, Sveiby[76] ante la cuestión "¿Qué es el conocimiento?" señala que el conocimiento puede englobar diferentes significados dependiendo de la lengua y del contexto en el que se aplique. Este autor describe cuatro características fundamentales del conocimiento:

---

[74] MEJÍA ROCHA, M.I. y COLÍN SALGADO, M., "Gestión del conocimiento y su importancia en las organizaciones*", Trilogía. Revista Ciencia, Tecnología y Sociedad,* núm. 9, julio – diciembre, 2013, p.31.

[75] DAVENPORT, T. and PRUSAK, L., "Diferencia Entre Dato, Información y Conocimiento"*, Gestión del conocimiento,* 1999, [Documento sin paginación]. Documento disponible en: http://www.gestiondelconocimiento.com/conceptos_diferenciaentredato.htm (última consulta 12/03/17).

[76] SVEIBY, K., *The new organizatonial wealth: managing and measuring intangible assets,* Ed. Berret – Koelher Publishers, San Francisco,1998.

(1) Tácito: el significado del concepto de conocimiento depende de las experiencias particulares de la persona que lo posee;

(2) Dinámico: el conocimiento a través de la acción genera nuevos conocimientos, transformándose, superando los antiguos y, consiguiendo perfeccionarse;

(3) Ilimitado: el conocimiento se encuentra sustentado por reglas, puesto que atiende a los esquemas o patrones de creación del cerebro humano que lo procesa, permitiéndole actuar ante situaciones extremas de manera rápida, eficaz y automática y;

(4) Movible: el conocimiento permanece en constante cambio, debido a su capacidad de ser transferido entre las personas.

En definitiva, según Sveiby existen tres fuentes que generan conocimiento: en primer lugar, las personas, con su propia experiencia procedente de la formación y de las vivencias con el mundo exterior, en segundo lugar, las organizaciones, mediante su cultura, procesos, know-how y capital intelectual y, en tercer lugar, el entorno, conocimiento generado por los propios clientes, el mercado, gobernanzas e investigaciones científicas.

Así, igualmente, en opinión de algunos autores[77], el conocimiento se ha de clasificar en dos categorías principales: conocimiento tácito y conocimiento explícito:

"Conocimiento tácito es el conocimiento personal resultando de la experiencia, es práctico debido a que se utiliza para actuar, se encuentra incrustado en las personas como resultado de su experiencia adquirida; implica ideales, valores y emociones de cada persona. No se transfiere fácilmente entre las personas. Conocimiento explícito, es el conocimiento consensuado, codificado, sistematizado resultado del procedimiento y la racionalidad. Secuencial y teórico. Puede adaptar la forma de programas informáticos, patentes, diagramas o similares. Transferible entre las personas, por lo

[77] MEJÍA ROCHA y COLÍN SALGADO, "Gestión del conocimiento…", *op. cit.,* p. 28, entre los que cita a Hayek, Penrise, Polanyi, Winter, Baracco, Blacker, Cook y Yanow.

tanto, es trascendental en la generación del conocimiento"[78]. No en vano, frente a las anteriores opiniones, el autor Tiwana describe tres categorías del conocimiento:

1) Conocimiento fundamental *(core knowledge).* Es esencial en la organización, pero sin aportar nada a nivel competitivo.
2) Conocimiento avanzado *(advanced knowledge).* Es aquel conocimiento que en determinadas áreas representa un mayor nivel de la sociedad frente a sus competidores.
3) Conocimiento innovador *(innovative knowledge)*. Es el conocimiento que le otorga éxito a la compañía haciéndola destacar como líder en un determinado sector[79].

En este sentido, debido a que el conocimiento se deriva de la información, así como la información se deriva de los datos, cabe diferenciar entre datos, información y conocimiento. Por otro lado, en relación con los datos, según Davenport y Prusak "un dato es un conjunto discreto, de factores objetivos sobre un hecho real. Dentro de un contexto empresarial, el concepto de dato es definido como un registro de transacciones. Un dato no dice nada sobre el porqué de las cosas, y por sí mismo tiene poca o ninguna relevancia o propósito"[80]. Así pues, se puede afirmar que los datos son la materia prima para generar información, su función se limita en describir parte de la realidad, sin aportar ningún tipo de juicio de valor o interpretaciones a fin de orientar nuestras acciones e indicarnos lo que debemos o no hacer. A pesar de lo anterior, los datos son fundamentales a fin de tomar decisiones eficaces, predictivas y preventivas que supongan un beneficio para la organización, de lo que se precisa de una correcta gestión y almacenamiento de los mismos.

Para terminar, sobre la "información" hemos de destacar, como afirman los autores Davenport y Prusak que:

---

[78] MEJÍA ROCHA y COLÍN SALGADO, "Gestión del conocimiento y su…", *op. cit.,* p.28.

[79] TIWANA, A., *The Knowledge Management Toolkit,* Ed. Prentice Hall, Upper Saddle River, 2002, pp.129-130.

[80] DAVENPORT and PRUSAK, "Diferencia Entre Dato, Inf... *", op. cit.,* [Documento sin paginación].

«La palabra "informar" significa originalmente "dar forma a" y la información es capaz de formar a la persona que la consigue, proporcionando ciertas diferencias en su interior o exterior. Por lo tanto, es el receptor y no el emisor, quien decide si el mensaje que ha recibido es realmente información, es decir, si realmente le informa. Un informe lleno de tablas incoherentes puede ser considerado información por el que lo escribe, pero a su vez puede ser juzgado como algo sin sentido por el que lo recibe. A diferencia de los datos, la información tiene significado (relevancia y propósito). No sólo puede formar potencialmente al que la recibe, sino que está organizada para algún propósito. Los datos se convierten en información cuando su creador les añade significado. Transformamos datos en información añadiéndoles valor en varios sentidos»[81].

En este sentido, la información es un conjunto de datos que una vez procesados obtienen una relevancia y propósito, en definitiva, un significado. Cuando añadimos un valor a los datos (contexto) y una utilidad (disminuir la incertidumbre), éstos se transforman en información. Así pues, es el individuo quien transforma los datos en conocimiento en el momento que les otorga relevancia y valor a los datos para la generación de información.

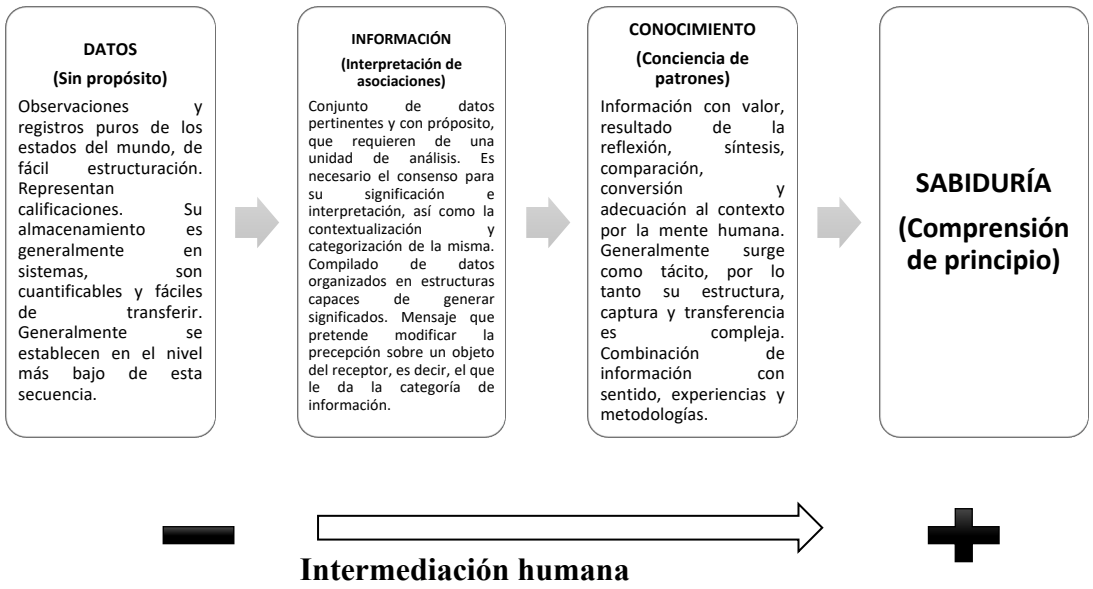

Imagen 1. De los datos a la sabiduría [82]

[81] DAVENPORT and PRUSAK, "Diferencia Entre Dato, Inf... *", op. cit.,* [Documento sin paginación].

[82] Esquema elaborado [a partir de Davenport y Prusak (1999)] por MEJÍA ROCHA y COLÍN SALGADO, "Gestión del... *", op. cit.,* p.30.

En conclusión, sobre los aspectos diferenciales entre el conocimiento, dato e información, se ha de concretar que, los datos se encuentran localizados en el mundo exterior y el conocimiento reside bien en las personas o en las organizaciones, mientras que la información adopta un papel mediador entre los datos y el conocimiento[83]. De igual modo, según mantienen algunos autores, el conocimiento *know – how*[84], es aquel conocimiento especifico que posee una persona sobre un determinado campo, que le permite desarrollar con pericia, agilidad y de manera eficiente una determinada actividad, resultando ser un "experto" en la misma, generando a su vez nuevas experiencias e información. Por último, la sabiduría es la acción orientada a lo eficiente, mejorando la toma de decisiones a través de un alto nivel de conocimiento sobre una determinada materia o cuestión específica[85].

2. GESTIÓN DEL CONOCIMIENTO

Además, una vez que hemos comprendido las principales diferencias entre conocimiento, dato e información, es necesario que nos cuestionemos sobre el modo de gestionar ese conocimiento o, lo que es lo mismo, ¿cómo es gestionado el conocimiento a través de los datos para aportar información eficiente a la organización? Todo ello con la finalidad de indagar en profundidad en la gestión del conocimiento (GC) – en el sector de la ciencia y, más concretamente, de la medicina – que se adquiere de los datos de salud tras la aplicación de las herramientas *big data*, como se comprobará más adelante.

Para ello, resulta meridianamente necesario asentar una concepción general de la GC pese a la variedad de definiciones existentes actualmente sobre la misma. Si bien es cierto que algunos autores sostienen que la GC supone gestionar el conocimiento de los empleados que trabajan en una organización, otros autores, sin embargo, defienden la idea de que la GC es el resultado de una combinación de sinergias entre datos, información e innovación. De igual modo, otra parte de la doctrina considera la GC

---

[83] MEJÍA ROCHA y COLÍN SALGADO, "Gestión del conocimiento y su…", *op. cit.,* pp. 28-29.

[84]Acerca del concepto *know – how*, *Vid.* LIEBOWITZ, J. and BECKMAN, T., *Knowledge Organizationes: What every manager should know,* CRC Press, Estados Unidos, 1998, p.155.

[85] MEJÍA ROCHA y COLÍN SALGADO, "Gestión del*...", op. cit.,* p.30.

como un proceso y sistema de gestión de las capacidades más eficientes de resolución de problemas en el menor tiempo a efectos de generar ventajas competitivas[86].

Asimismo, cabe citar a fin de completar esta breve exposición sobre la GC, los factores principales de éxito para la GC establecidos por algunos autores[87]: así pues, en primer lugar – según mantienen Sallis y Jones – el éxito para la GC conlleva situar el cambio en el contexto cultural, confianza de los de los miembros de su organización, liderato del personal directivo, considerar escenarios alternativos y producir estrategias coherentes; por otro lado, para Rivero el éxito de la GC conlleva partir de un modelo común sobre GC; crear una cultura común de conocimiento; asegurar la existencia de suficiente base cultural; disponer de un suporte tecnológico común y evitar caer en la tentación de limitarse a la cosmética.

De igual modo, Alavi y Leidner consideran que se ha de procurar que los datos sean utilizables, actuales, correctos u pertinentes; asegurar la confidencialidad del cliente; actualizar la información; fomentar una cultura del conocimiento; establecer responsabilidades en la GC y determinar los requisitos de la infraestructura (actualizada, seguridad). Igualmente, cabe destacar que, según algunos autores, las condiciones y el entorno en las que se genera, conserva, utiliza, transforma y transmite el conocimiento son los factores que realmente gestionan el mismo. Por lo que el GC se vincula de manera directa con el Aprendizaje Organizacional (AO) y, por consiguiente, con el

[86] Al respecto, TITO HUAMANÍ, P.L., "Gestión del conocimiento: un nuevo paradigma organizacional", *Gest. Terc. Milen*, núm. 9, octubre, 2002, [Documento sin paginación]. Documento disponible en: https://sisbib.unmsm.edu.pe/bibvirtual/Publicaciones/administracion/v05_n9/gestion_conocimiento.htm# (última consulta 19/03/17) afirma que: «Existen una variedad de posiciones en el mundo académico para argumentar que se entiende por Gestión del Conocimiento. Veamos algunas de ellos: "La gestión del conocimiento implica gestionar el conocimiento de la gente que directa o indirectamente, tiene relación con la empresa. Dicha gestión se desarrolla sobre lo que las personas piensan y desean que se haga en la empresa para la cual trabajan, obteniendo una optimización de sus productos o servicios)) (Flores, 2001). "La gestión del conocimiento es la combinación de sinergias entre datos, información, sistemas de información y la capacidad creativa e innovadora de seres humanos)) (Malhotra, 1997). "La gestión del conocimiento es el conjunto de procesos y sistemas que permiten que el capital intelectual de una organización aumente de forma significativa, mediante la gestión de sus capacidades de resolución de problemas de forma eficiente (en el menor tiempo posible), con el objetivo final de generar ventajas competitivas sostenibles en el tiempo)) (Carrión, 2001). A nuestro entender la gestión del conocimiento, es la gestión de los activos intangibles que tiene una organización para afiadirle valor. Tales activos intangibles lo conforman: El capital humano representado por el conjunto de conocimientos y capacidades de sus trabajadores; por aquellos conocimientos acumulados por la empresa en el tiempo de su existencia, manifestándose en su *knowhow*, patentes, marcas, etc.; y por el conjunto de relaciones que mantienen con el exterior, principalmente, clientes, proveedores, otros actores económicos, etc.».

[87] RODRÍGUEZ GÓMEZ, "Modelos para la…", *op. cit.,* p. 37.

Capital Intelectual (CI) de la organización[88]. Por otro lado, otros autores afirman que la GC se refiere a la obtención del conocimiento necesario para la solución de problemas y la mejora constante de métodos de trabajo con la intención de incrementar los niveles de productividad de la organización[89].

Para terminar, cabe destacar que la GC se verifica en todos y cada uno de los departamentos de una organización que necesita tener habilitado el acceso a la totalidad de su infraestructura a fin de realizar búsquedas distribuidas, controlar los agentes inteligentes, así como poder distribuir y almacenar documentos y materiales multimedia creados conjuntamente por la organización.

En definitiva, a partir de lo anterior, cabría afirmar que la GC consiste en una serie de procesos sistemáticos – identificación y captación del capital intelectual; tratamiento, desarrollo y comportamiento del conocimiento; y su utilización – destinados al desarrollo de una organización a fin de generar una ventaja competitiva para la misma frente a otras organizaciones.

Por adelantarnos a lo que más adelante se expondrá, cabría tener presente en este punto como modelo de organización los centros sanitarios, públicos o privados, así como los centros de investigación científica y, otros organismos del sector sanitario, que a través de la aplicación de las herramientas *big data* podría conseguir una GC óptima con mejores resultados sanitarios a través de tratamientos más eficientes, así como la posibilidad de prevenir enfermedades, entre otras muchas previsiones que se estudiaran más adelante en el presente trabajo.

[88] RODRÍGUEZ GÓMEZ, "Modelos para la…", *op. cit.,* p. 37.

[89] MÁS, B., ACOSTA, Y. y BATISTA, M., "Visualización de la gestión del conocimiento en diferentes objetos de estudio: ayuda para la investigación-acción. Primera Parte", *Ciencias de la Información,* Vol. 40, núm. 3, 2009, pp. 3-12.

3. *BIG DATA*: UNA HERRAMIENTA DE INNOVACIÓN TECNOLÓGICA

Por último, se estima oportuno tratar en este apartado una breve reflexión sobre la posibilidad de considerar el *big data* como una herramienta de innovación tecnológica, en el sentido de que tras su aparición se ha podido apreciar un cambio sustancial en el sistema social, económico, tecnológico y, para el caso que nos ocupa, sanitario y jurídico, a consecuencia de que a través de las técnicas *biga data,* por un lado, son creados nuevos conocimientos e información y, por otro lado, asimilados los conocimientos previos permitiendo una aplicación eficiente de los mismos en el contexto (sanitario) actual, entendiéndose así por innovación "el proceso que consiste en crear o asimilar conocimientos y aplicarlos para generar riqueza o bienestar social de una forma nueva. Por lo tanto, podemos considerar la innovación como un tipo específico de actividad creativa: la que tiene por objeto la creación de riqueza o bienestar social"[90]. En este sentido, como herramienta innovadora, el *big data* accede a los datos y los transforma en conocimiento e información y, en consecuencia, en la mayoría de los casos se podría afirmar que aumenta la riqueza intelectual y el bienestar social[91].

En consecuencia de lo anterior, el *big data* puede tener dos aspectos diferenciadores, puesto que puede ser considerado, por un lado, como una innovación tecnológica, en el sentido de ser una innovación "que consiste en la generación de riqueza o bienestar social, mediante la introducción en el sistema económico de nuevos productos, servicios o procesos de producción basados en la aplicación de conocimiento tecnológico"[92] y, por otro lado, como conocimiento técnico, al entenderse por este como un "conjunto de habilidades y saberes operacionales que, en forma sistemática, permiten conseguir algo que se considera valioso o resolver determinados problemas prácticos en lo que estamos interesados"[93], siendo en todo caso, los flujos de información y de datos una gran influencia causal en la innovación tecnológica y en el conocimiento técnico[94].

---

[90] QUINTANILLA, M.A., *Tecnología: un enfoque filosófico y otros ensayos de filosofía de la tecnología.* Fondo de Cultura Económica, México, 2005, pp.250-251.

[91] QUINTANILLA, *Tecnología: un enfoque filosófico…, op. cit.,* p.251.

[92] QUINTANILLA, *Tecnología: un enfoque filosófico…, op. cit.,* p.252.

[93] QUINTANILLA, *Tecnología: un enfoque filosófico…, op. cit.,* p.252.

[94] QUINTANILLA, *Tecnología: un enfoque filosófico…, op. cit.,* p.252.

IV. CONTEXTUALIZACIÓN DE LAS RELACIONES ENTRE LOS SISTEMAS DE ANÁLISIS DE DATOS PREVIOS AL *BIG DATA*: *BUSINESS INTELLIGENCE*, *DATA MINING* Y *DATA SCIENCE*

No en vano, a pesar de que el *big data* pueda ser considerado como una innovación tecnológica y como conocimiento técnico, como se ha podido observar, no es una herramienta propiamente novedosa en el sentido de ser creada sin antecedentes algunos, sino todo lo contrario, es el resultado de otras figuras tecnológicas generadoras igualmente de conocimiento e información. Por ello, en los siguientes epígrafes se analizarán las mismas, así como las herramientas creadas posteriormente al *big data* a efectos de delimitar su contexto y, profundizar en la razón de ser de la citada herramienta, pues no obviemos que como juristas debemos ser conocedores de la realidad tecnológica a efectos de poder dar una respuesta a los distintos supuestos de hecho a través de una regulación jurídica que se adapte a la realidad, como se verá más adelante en el capítulo correspondiente.

Bien, uno de los fenómenos más relevantes de la evolución de las nuevas tecnologías (TIC) y de Internet de las cosas (IoT) desde mediados del siglo XX, son los diferentes conceptos que surgen dentro de este proceso de modernización tecnológica. Así pues, previo al término *big data*, se desarrolla un marco conceptual compuesto por distintas herramientas tecnológicas (o, si se prefiere conceptos tecnológicos) que dan respuesta a los diferentes cambios y etapas del desarrollo de la era tecnológica, así como de las fuentes de información procedentes de la misma.

En este sentido, conceptos como *business intelligence* (BI)*, data mining* (DM) *y data sciencie* (DS), son previos al *big data* que emergen dentro del cambio tecnológico, marcando cada uno de ellos una diferente etapa dentro de la propia evolución de la información tecnológica. Para ello, resulta imprescindible partir de un análisis histórico de estos conceptos que nos permita analizar en perspectiva la evolución de las fuentes de los datos dentro del paradigma tecnológico, a fin de tener una visión de conjunto sobre cómo se ha ido configurando el propio concepto de *big data*.

1. LA INFLUENCIA DEL *BUSINESS INTELLIGENCE* EN EL SURGIMIENTO DEL *BIG DATA*

El término *business intelligence* surge a consecuencia de la progresiva informatización de los procesos de selección de datos. El origen del citado concepto se remonta al año 1958, cuando el investigador de IBM, Hans Peter Luhn, hace mención por vez primera del mismo, definiendo la inteligencia de negocios como "la capacidad de aprehender las interrelaciones de los hechos presentados, de tal forma, que permiten orientar la acción hacía una meta deseada" [95]. En concreto, Luhn hace referencia al *business intelligence,* para definir un nuevo método de selección de documentos que surgen dentro del marco de tipo de negocio concreto a fin de seleccionar aquellos datos que aporten una información valiosa que nos permita organizar y restructurar de manera eficaz la propia empresa. Por consiguiente, nos encontramos, según Luhn, ante una manera inteligente de negocio que deriva de la selección de aquellos datos recopilados en los propios archivos internos del negocio que aportan una información valiosa acerca del mismo. En definitiva, se trata de tomar decisiones inteligentes y eficaces en el mundo de los negocios desde dentro del propio negocio u organización, es decir, desde un análisis interno de la propia información recopilada desde los inicios de la empresa.

Posteriormente, a partir del año 1980, se aprecia una evolución en el concepto *business intelligence,* donde la idea de negocio inteligente se afianza con el proyecto desarrollado por Howard Dresner en 1989, analista entonces de la firma de investigación Gartner Inc., quien en el año 2006 redefine el *business intelligence,* como:

"[…] formas de entregar información a los usuarios finales sin necesidad de que sean expertos en investigación operativa. Al principio, algunas compañías intentaron hacer que el término fuera aún más amplio que la "información cuantitativa" para incluir contenido no estructurado. Pero quedó claro que era un problema simple que debía resolverse con contenido estructurado. Eso proporciona mucho más valor a los

[95] LUHN, "A business intelligence …", *op. cit.,* p. 315.

negocios que tratar de hervir todo el océano. BI está en el medio, [con] información estructurada en un extremo y el usuario en el otro extremo"[96].

En concreto, Dresner ingenia un conjunto de sistemas de *software* cuya función es la de recopilar y analizar datos antiguos y presentes sobre un determinado negocio a efectos de obtener una mayor rentabilidad de este, todo ello gracias a la información procedente del análisis de los propios datos de la organización. El objetivo final es obtener una información que ayuda a que la toma de decisiones por parte de los órganos de dirección y administración de la empresa sea más eficaz y productiva, en definitiva, más inteligente, resultando ser por tanto una herramienta esencial en la empresa que se ha de tener en cuenta previamente a la toma de una decisión determinada.

De manera general, el *business intelligence* se basa en un análisis descriptivo de los propios datos empresariales, siendo relacionados y entrecruzados unos con otros, a fin de obtener una respuesta más próxima y veraz acerca de las causas de los problemas acaecidos en relación con la propia organización, así como para solventar posibles errores presentes y predecir el surgimiento de muchos otros.

1.1. Análisis de la metodología *data warehouse*

El método que se emplea en el *business intelligence* se basa fundamentalmente en agrupar en un servidor central un conjunto de datos empresariales, donde los mismos son analizados en modo off-line tras haber sido almacenados en un fichero denominado *data warehouse.* Posteriormente, una vez analizados los datos, los mismos son estructurados en una base de datos relacional convencional formada, por un lado, por una serie adicional de índices y, por otro lado, por las distintas formas de acceso a las tablas donde permanecen organizados.

[96] MARTENS, CH., "BI at age 17", *Computerworld,* octubre 2006, [Documento sin paginación]. Documento disponible en: https://www.computerworld.com/article/2554088/business-intelligence/bi-at-age-17.html (última consulta 22/02/18).

El *data warehouse,* traducido literalmente como almacén de datos, consiste en un archivo de soporte electrónico que almacena de forma segura y fiable información acerca de los datos de una empresa u organización, de fácil recuperación y administración[97]. En concreto, se trata de una base de datos corporativa caracterizada principalmente por integrar y ordenar información procedente de una misma fuente o de fuentes diferentes a fin de procesar la misma mediante un análisis que abarca multitud de perspectivas proporcionando respuestas a gran velocidad, pincipalmente, su creación se debe a la necesidad de dar una solución plena, completa y fiable de *business intelligence*.

El término *data warehouse* nace en 1988 dentro del contexto del *business intelligence*, su origen procede de los investigadores de IBM, Devlin y Murphy, aunque es Inmon el padre del citado concepto por otorgar una definición del mismo, en concreto lo define como "un almacén de datos orientado a un tema, integrado, no volátil y variante en el tiempo, que soporta decisiones de administración"[98]. Según Inmon, un *data warehouse* se caracteriza por los siguientes elementos:

(1) Integridad. Implica la necesidad de que la estructura donde son integrados los datos almacenados en *data warehouse* sea consistente. Igualmente, la propia información es estructurada en distintos niveles de detalle a fin de dar respuesta a las diferentes necesidades de los usuarios;

(2) Temático. Los datos son organizados por temas a efectos de facilitar el acceso y el entendimiento de la información a los usuarios finales. De igual modo, hemos de tener presente que únicamente los datos necesarios para el proceso de generar conocimiento del negocio son integrados desde un contexto operacional;

---

[97] BALAGUERÓ, T., "Del Dataware House al *data lake*", *Deusto Formación. Planeta Formación Universitaria,* enero 2018, [Documento sin paginación]. Documento disponible en: https://www.deustoformacion.com/blog/gestion-empresas/dataware-house-data-lake (última consulta 25/02/18).

[98] INMON, W. H., *Building the data warehouse,* Ed. John Wiley and Sons, Nueva York, 1993, p. 31. Documento disponible en: http://fit.hcmute.edu.vn/Resources/Docs/SubDomain/fit/ThayTuan/DataWH/Bulding%20the%20Data%20Warehouse%204%20Edition.pdf (última consulta 24/02/18).

(3) Histórico. Una de la información más valiosa del *data warehouse* es el tiempo, de ahí su gran utilidad a fin de analizar tendencias, ya que a través de distintos valores en una determinada variable de tiempo se pueden realizar comparaciones y deducir tendencias. Por el contrario, en los sistemas operacionales, los datos siempre reflejan el estado presente de la actividad del negocio;

(4) No volátil. Almacenamiento de datos permanente y fijo, cuya información no se puede modificar, simplemente leer. Por consiguiente, una actualización de un *data warehouse* consiste en la incorporación de los últimos y nuevos valores procedentes de las diferentes variables contenido en el mismo, sin efectuarse modificación alguna en lo anterior.

Por otro lado, otra de las características relevantes del *data warehouse*, son los metadatos, que son datos sobre datos que informan sobre todo acerca del origen de la información, de su fiabilidad, periodicidad de refresco y forma de cálculo. Los metadatos simplifican y automatizan la obtención de la información desde los sistemas operacionales a los sistemas informacionales. La finalidad de los metadatos es, por un lado, dar respuesta al usuario final facilitando las diferentes clases de información que compone el *data warehouse*, así como el significado de esta, a fin de que el acceso sea más sencillo y pueda elaborar consultas, informes y análisis mediante herramientas de BI como: Sistemas de Soporte a la Decisión[99] (DSS), Sistemas de Información Ejecutiva[100] (EIS) o Cuadro de Mando Integral[101] (CMI). Así como, dar soporte a los

[99] Un Sistema de Soporte a la Decisión (DSS) es una herramienta de *business intelligence* enfocada al análisis de los datos de una organización. El principal objetivo de los Sistemas de Soporte a Decisiones es, a diferencia de otras herramientas como los Cuadros de Mando Integral (CMI) o los Sistemas de Información Ejecutiva (EIS), explotar al máximo la información residente en una base de datos corporativa (*datawarehouse o datamart*), mostrando informes muy dinámicos y con gran potencial de navegación, pero siempre con una interfaz gráfica amigable, vistosa y sencilla. Fuente: http://www.sinnexus.com/business_intelligence/sistemas_soporte_decisiones.aspx [Documento sin paginación].

[100] Un Sistema de Información para Ejecutivos o Sistema de Información Ejecutiva es una herramienta *software*, basada en un DSS, que provee a los gerentes de un acceso sencillo a información interna y externa de su compañía, y que es relevante para sus factores clave de éxito. La finalidad principal es que el ejecutivo tenga a su disposición un panorama completo del estado de los indicadores de negocio que le afectan al instante, manteniendo también la posibilidad de analizar con detalle aquellos que no estén cumpliendo con las expectativas establecidas, para determinar el plan de acción más adecuado. De forma más pragmática, se puede definir un EIS como una aplicación informática que muestra informes y listados *(query & reporting*) de las diferentes áreas de negocio, de forma consolidada, para facilitar la monitorización de la empresa o de una unidad de la misma.

El EIS se caracteriza por ofrecer al ejecutivo un acceso rápido y efectivo a la información compartida, utilizando interfaces gráficas visuales e intuitivas. Suele incluir alertas e informes basados en excepción,

responsables técnicos del *data warehouse,* entre otros, en aspectos de auditoría, gestión de la información, administración y elaboración de programas de análisis de información. El proceso de construcción del *data warehouse*, denominado ETL – Extracción, Transformación y Carga – parte de estas tres funciones principales: en primer lugar, extrae la información de las distintas fuentes internas y externas, en segundo lugar, transforma la información filtrando, limpiando, depurando, homogeneizando y agrupando la misma, por último, carga los datos y los metadatos en la base de datos organizándolos y actualizándolos[102].

En síntesis, un *data warehouse* presenta una arquitectura dividida en tres estructuras simplificadas diferentes: por un lado, una estructura básica, compuesta por datos en bruto procedentes de sistemas operativos y archivos planos que se almacenan junto con metadatos; por otro lado, a esa estructura básica se le puede añadir un área de ensayo entre las fuentes de datos y el almacén, cuya finalidad es la limpiar los datos antes de entrar en el almacén. En tercer lugar, se puede efectuar agregando *data marts*, que son sistemas diseñados para una actividad de negocio concreta, nos podemos

---

así como históricos y análisis de tendencias. También es frecuente que permita la domiciliación por correo de los informes más relevantes.

A través de esta solución se puede contar con un resumen del comportamiento de una organización o área específica, y poder compararla a través del tiempo. Es posible, además, ajustar la visión de la información a la teoría de Balanced Scorecard o Cuadro de Mando Integral impulsada por Norton y Kaplan, o bien a cualquier modelo estratégico de indicadores que maneje la compañía. Fuente: http://www.sinnexus.com/business_intelligence/sistemas_informacion_ejecutiva.aspx [Documento sin paginación].

[101] El Cuadro de Mando Integral (CMI), también conocido como *Balanced Scorecard* (BSC) o *dashboard,* es una herramienta de control empresarial que permite establecer y monitorizar los objetivos de una empresa y de sus diferentes áreas o unidades.

También se puede considerar como una aplicación que ayuda a una compañía a expresar los objetivos e iniciativas necesarias para cumplir con su estrategia, mostrando de forma continuada cuándo la empresa y los empleados alcanzan los resultados definidos en su plan estratégico. El Cuadro de Mando Integral se diferencia de otras herramientas de *business intelligence* , como los Sistemas de Soporte a la Decisión (DSS) o los Sistemas de Información Ejecutiva (EIS), en que está más orientados al seguimiento de indicadores que al análisis minucioso de información. Por otro lado, es muy común que un CMI sea controlado por la dirección general de una compañía, frente a otras herramientas de *business intelligence* más enfocadas a a la dirección departamental. El CMI requiere, por tanto, que los directivos analicen el mercado y la estrategia para construir un modelo de negocio que refleje las interrelaciones entre los diferentes componentes de la empresa (plan estratégico). Una vez que lo han construido, los responsables de la organización utilizan este modelo como mapa para seleccionar los indicadores del CMI. Fuente: http://www.sinnexus.com/business_intelligence/cuadro_mando_integral.aspx [Documento sin paginación].

[102] Sinnexus. Business Intelligence e Informática Estratégica, *Datawarehouse*, 2016, [Documento sin paginación]. Documento disponible en: http://www.sinnexus.com/business_intelligence/datawarehouse.aspx (última consulta 27/02/18).

encontrar un departamento divido por diferentes *data marts* separados, donde el usuario puede acceder a datos de uno o de la totalidad[103].

Por último, hay que destacar que entre sus aportaciones se encuentra la de proporcionar una herramienta esencial para la toma de decisiones en cualquier departamento del negocio y, la de proporcionar aprendizaje basado en los datos del pasado y capacidad de predicción de posibles situaciones futuras en desiguales contextos. En concreto, el *data warehouse* es un conjunto de procesos y acciones, vinculados a una determinada cuestión, integrados y no volátiles cuya utilidad es la de ayudar y colaborar en la toma de decisiones de la empresa. A pesar de suponer un alto coso en el negocio, actualmente es una herramienta de gran eficacia cuyo funcionamiento brinda veracidad a la información de acceso a los usuarios.

1.2. Descripción de la técnica *data mart*

El *data mart* es un almacén de datos específico sobre un tema concreto, integrado volátil y variante en el tiempo a fin de orientar sobre un subconjunto específico de decisiones de administración. Asimismo, la diferencia entre un *data mart* y un *data warehouse*, principalmente se basa en que el primero es especializado y volátil[104]. Por consiguiente, el *data warehouse* va a contener todos los datos de un negocio, mientras que el *data mart* únicamente va a almacenar un subconjunto de los datos en relación con un área específica del negocio. La finalidad del *data mart* es cubrir las necesidades de un determinado departamento dentro de la empresa, por lo que es definido como un almacén de datos departamental.

Una de sus características específicas es la de disponer de una estructura óptima de datos que analiza la información de manera detallada abarcando cada una de las perspectivas afectas a los diferentes procesos del departamento. El *data mart* se puede

---

[103] Power data. Especialistas en Gestión de datos, *Data warehouse: todo lo que necesitas saber sobre el almacenamiento de datos*, [Documento sin paginación]. Documento disponible en: https://www.powerdata.es/data-warehouse (última consulta 27/02/18).

[104] PÉREZ, S.C. y FERNÁNDEZ. N., "Apoyo para la toma de decisiones", *Cátedra de gestión de datos UTN-F.R.M.* 3er. Año, 2006, [Documento sin paginación]. Documento disponible en http://www.edutecne.utn.edu.ar/sistemas-informacion/sist-info.htm (última consulta 01/03/18).

alimentar, bien, desde los datos de un *data warehouse*, bien, integrando por sí misma un extracto de las distintas fuentes de información[105].

1.3. Breve análisis descriptivo de la herramienta *data lake*

El *data lake* (DL) es "un entorno de datos compartidos, en su formato original, que comprende múltiples repositorios y aprovecha las tecnologías de *big data*. Contiene grandes cantidades de datos en bruto, estos datos se mantienen allí almacenados hasta que sean necesarios para cualquier uso en la organización"[106]. En concreto, el DL nace del contexto del *data management* o gestión de datos, englobando esferas más amplias que las del *data warehouse*, complementado los esfuerzos existentes y dando suporte al descubrimiento de nuevas cuestiones. Por consiguiente, en el momento que surgen nuevas preguntas se está optimizando las respuestas, lo que significa que nos movemos fuera del propio contexto del DL para dirigirnos a un *data mart* o un *data warehouse*[107].

En definitiva, los sistemas de análisis de datos que giran en torno al *business intelligence*, son sistemas cuya toma de decisiones de negocio se basa principalmente en la recogida de hechos o datos, enfocándose en un análisis descriptivo de datos históricos

---

[105] Sinnexus. Business Intelligence e Informática Estratégica, *Datamart*, 2016, [Documento sin paginación]. Documento disponible en: http://www.sinnexus.com/business_intelligence/datamart.aspx (último acceso 02/03/18).

[106] BALAGUERÓ, "Del Dataware House al *data…", op. cit.,* [Documento sin paginación].

[107] Diferencias entre *data lake* y *data warehouse:* **"**Datos: Un *data warehouse* sólo almacena datos que han sido modelados o estructurados, mientras que un *data lake* no hace acepción de datos. Lo almacena todo, estructurado, semiestructurado y no estructurado. Procesamiento**:** Antes de que una empresa pueda cargar datos en un *data warehouse*, primero debe darles forma y estructura, es decir, los datos deben ser modelados. Eso se llama *schema-on-write*. Con un *data lake*, sólo se cargan los datos sin procesar, tal y como están, y cuando esté listo para usar los datos, es cuando se le da forma y estructura. Eso se llama *schema-on-read*. Dos enfoques muy diferentes. Almacenamiento**:** Una de las principales características de las tecnologías de *Big Data*, como Hadoop, es que el coste de almacenamiento de datos es relativamente bajo en comparación con el de un *data warehouse*. Hay dos razones principales para esto: en primer lugar, Hadoop es *software* de código abierto, por lo que la concesión de licencias y el soporte de la comunidad es gratuito. Y segundo, Hadoop está diseñado para ser instalado en *hardware* de bajo coste. Agilidad**:** Un almacén de datos es un repositorio altamente estructurado, por definición. No es técnicamente difícil cambiar la estructura, pero puede tomar mucho tiempo dado todos los procesos de negocio que están vinculados a ella. Un *data lake*, por otro lado, carece de la estructura de un *data warehouse*, lo que da a los desarrolladores y a los científicos de datos la capacidad de configurar y reconfigurar fácilmente y en tiempo real sus modelos, consultas y aplicaciones. Seguridad**:** La tecnología del *data warehouse* existe desde hace décadas, mientras que la tecnología de *Big Data* (la base de un *data lake*) es relativamente nueva. Por lo tanto, la capacidad de asegurar datos en un *data warehouse* es mucho más madura que asegurar datos en un *data lake*. Cabe señalar, sin embargo, que se está realizando un importante esfuerzo en materia de seguridad en la actualidad en la industria de *Big Data*". *Vid.* el siguiente enlace web: https://www.powerdata.es/data-warehouse.

a efectos de obtener una perspectiva más eficaz y concisa de la situación anterior y actual del negocio.

2. LA ESPECIAL RELEVANCIA DEL *DATA MINING* Y SU INFLUENCIA EN LOS INICIOS DEL *BIG DATA*

El *data mining* (minería de datos), es un concepto que surge al margen del *business intelligence* debido a la necesidad de determinar una definición concreta referente al citado análisis predictivo, a finales de la década de los ´80 surge la expresión *data mining* (DM). Esta herramienta no se centra en un análisis puramente descriptivo de los datos, sino más bien, en un análisis predictivo, puesto que los mismos son utilizados para la toma de decisiones cuya finalidad es la de extraer información y conocimiento de los datos a modo de patrones a seguir, a efectos de predecir de manera eficiente el resultado de determinadas acciones futuras.

El DM[108] y el proceso de extracción de conocimiento en base de datos (*knowledge discovery in databases* o KDD), son términos utilizados de manera equitativamente, aunque lo cierto es que el DM es un sistema que se encuentra incluido dentro del KDD. En un principio, el DM ha sido definido, como "un proceso no trivial de identificación válida, novedosa, potencialmente útil y entendible de patrones comprensibles que se encuentran ocultos en los datos"[109].

De igual modo, se ha de señalar que las bases de la minería de datos se encuentran en la Inteligencia Artificial, en el Análisis Estadístico, en la Computación Gráfica, en las Bases de Datos y en el Procesamiento Masivo. En concreto, la herramienta principal del DM son las Bases de Datos, las cuales son rastreadas automáticamente por medio de una serie de técnicas y tecnologías con el fin de

[108] MOLINA FÉLIX, L.C., "Data Mining: torturando a los datos hasta que confiesen", 2002, [Documento sin paginación]. Documento disponible en: http://www.uoc.edu/web/esp/art/uoc/molina1102/molina1102.html (última consulta 02/03/18).

[109] FAYYAD, U.M., PIATESKY – SHAPIRO, G., SMYTH, P. and UTHURUSAMY, R., *Advances in knowledge and data mining,* Ed. AA*IA*/MIT Press, Cambridge (Massachussets), 1996. Asimismo, MOLINA FÉLIX, L.C. y RIBERO, S., "Descubrimiento conocimiento para el mejoramiento bovino usando técnicas de *data mining*", *Actas del IV Congreso Catalán de Inteligencia Artificial*, Barcelona, 2001, pp. 123-130, definen el DM como "la integración de un conjunto de áreas que tienen como propósito la identificación de un conocimiento obtenido a partir de las bases de datos que aporten un sesgo hacia la toma de decisión".

encontrar un patrón repetitivo que explique de manera objetiva los motivos del comportamiento de los datos en un determinado contexto[110]. Por otro lado, en el DM los datos son la materia prima bruta, que una vez que adquieren un significado para los usuarios pasan a ser información, una información que alcanzará un valor agregado en el momento que se convierta en conocimiento objetivo, una vez que los especialistas han elaborado un modelo o patrón a través de la misma[111].

En definitiva, entre las ventajas del DM, hemos de destacar que nos encontramos ante una tecnología que, mediante la cooperación entre los investigadores y el personal del negocio, tiene como resultado un producto de gran valor que ayuda a la "toma de decisiones" de una empresa a modo de predicción sobre acciones futuras, lo que genera el ahorro de grandes cantidades de dinero y, su vez, la apertura a nuevas oportunidades de negocio[112].

---

[110] Universia España, *¿Qué es Machine Learning y cómo se usa en Big Data*?, 12 de septiembre de 2017, [Documento sin paginación]. Documento disponible en: http://noticias.universia.es/ciencia-tecnologia/noticia/2017/09/12/1155659/machine-learning-como-usa-big-data.html (última consulta 04/03/18).

[111] MOLINA FÉLIX, "Data Mining: torturando…", *op. cit.,* [Documento sin paginación], establece cuatro etapas principales del proceso de DM: (1) "*Determinación de los objetivos*. Trata de la delimitación de los objetivos que el cliente desea bajo la orientación del especialista en *data mining*; (2) *Pre-procesamiento de los datos*. Se refiere a la selección, la limpieza, el enriquecimiento, la reducción y la transformación de las bases de datos. Esta etapa consume generalmente alrededor del setenta por ciento del tiempo total de un proyecto de *data mining*; (3) *Determinación del modelo*. Se comienza realizando unos análisis estadísticos de los datos, y después se lleva a cabo una visualización gráfica de los mismos para tener una primera aproximación. Según los objetivos planteados y la tarea que debe llevarse a cabo, pueden utilizarse algoritmos desarrollados en diferentes áreas de la Inteligencia Artificial; (4) *Análisis de los resultados*. Verifica si los resultados obtenidos son coherentes y los coteja con los obtenidos por los análisis estadísticos y de visualización gráfica. El cliente determina si son novedosos y si le aportan un nuevo conocimiento que le permita considerar sus decisiones".

[112] Como indica el Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p.68, señalan que: "Básicamente, los algoritmos en Machine Learning se pueden segmentar en función de la intervención humana en 3 tipologías:

-*Aprendizaje supervisado:* estos algoritmos se utilizan sobre todo cuando existen datos etiquetados históricos y se conoce el tipo de resultado que se quiere obtener. Mediante técnicas de clasificación o regresión se puede predecir el comportamiento futuro en función del histórico en el repositorio de datos. Estos algoritmos comparan los resultados obtenidos con los resultados esperables que conoce el sistema y, en función de las diferencias entre ambos, extrae la información que se desea.

-*Aprendizaje no supervisado:* en el aprendizaje no supervisado, el modelo analítico no tiene de entrada resultados etiquetados, ni cuentan con resultados esperables, por lo cual por si mismos han de detectar patrones subyacentes en los datos sin necesidad de soporte alguno. Muchas de las aplicaciones de *text mining* siguen este modelo de aprendizaje.

-*Tipos híbridos de aprendizaje:* los tipos híbridos, como los modelos semiestructurados o los modelos de aprendizaje por refuerzo, se sitúan en un estadio intermedio entre ambos. Se aplican cuando el proceso de etiquetaje no puede ser completo, por las razones que sea, por ejemplo, porque representa un coste no asumible. En el caso de los sistemas por refuerzo también existe la particularidad que el sistema tiene

3. EL *DATA SCIENCE*: ANTECEDENTE DEL *BIG DATA*

El término *data science* (ciencia de datos), es relativamente nuevo, que se utiliza de manera intercambiable con el concepto analítica de negocio. A consecuencia del sistema tecnológico del *data mining,* a principios del año 2000 nace el concepto *data science*[113] a fin de dar nombre al proceso de revisión dentro de las áreas técnicas de la estadística y adaptarse mejor a las prácticas de análisis de datos que venían desarrollándose en la época, fundamentalmente las procedentes del DM.

Precisamente por este motivo, este proceso de revisión es aplicado en los diferentes departamentos de negocio y en la recopilación y análisis tecnológico de los datos. En concreto, la Ciencia de Datos, explora y analiza datos procedentes de diversas fuentes que poseen formatos muy variados, puesto que pueden provenir de múltiples dispositivos electrónicos – móvil, todo tipo de sensores, secuenciadores de genoma, redes sociales, datos médicos, páginas web – influyendo de manera notoria en la investigación científica de muchos sectores, destacando entre otros, la biomédica, el campo de las ciencias biológicas, la informática médica y las ciencias sociales. Por ende, el *data science* responde a las cuestiones planteadas mediante el siguiente proceso[114]:

1) Extracción de datos. Consiste en extraer los datos de manera independiente de la fuente – webs, csv, loGC y apio, entre otros – y del volumen (*big data* o *Small Data*).

2) Limpieza de los datos. Eliminar mediante una limpieza de los datos aquellos datos que puede obstaculizar o distorsionar.

---

marcado un objetivo deseable y, a partir de procesos de análisis iterativos por ensayo y error, va ajustando su modelización hasta obtener el mejor de los resultados posibles".

[113] Según definición aportada por STANTON, J., *An introduction to data science,* Ed. Syracuse University, Nueva York, 2012, p.2, "El *data science* se refiere a una emergente área de trabajo relacionada con la recopilación, elaboración, análisis, visualización, gestión y conservación de grandes colecciones de información. Aunque el nombre de Ciencia de Datos parece conectar más estrechamente con áreas tales como bases de datos y la informática, muchos tipos diferentes de habilidades – incluyendo habilidades no-matemáticas – son necesarias*"*.

[114] OBIOLS, A., "¿Qué es un Data Scientist?", *InLab FIB talent & tech UPC,* 2015, [Documento sin paginación]. Documento disponible en: https://inlab.fib.upc.edu/es/blog/que-es-un-data-scientist (última consulta 05/03/18).

3) Procesamiento de datos. Procesar los datos usando métodos estadísticos (inferencia estadística, modelos de regresión, pruebas de hipótesis…); en cuarto lugar, en caso de que fuera necesario, diseñar test o experimentos a fin de obtener una respuesta más eficaz y objetiva y, por último, visualización y representación gráfica de los datos.

Igualmente, cabe tener presente que el objetivo del *data science* es abordar conjuntamente el proceso de análisis con el proceso de gestión de los datos, siendo necesario que la explotación de los datos sea llevada a cabo analizando y gestionando todos los datos a la vez, debido al gran volumen, variedad y velocidad en la que se generan los mismos. Por consiguiente, la Ciencia de Datos engloba las habilidades asociadas a la extracción de conocimiento de datos, incluyendo *big data*[115].

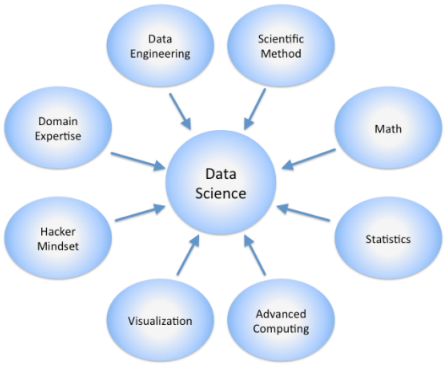

Imagen 2. Data Sciencie[116]

En este sentido, el *data science* extrae información y conocimiento de los datos, creando así productos nuevos, a través de técnicas y teorías procedentes de las matemáticas, estadística, ingeniería de datos, reconocimiento de patrones y aprendizaje, computación avanzada, visualización, modelado de la incertidumbre, almacenamiento de datos y la informática de alto rendimiento.

[115] Soft Computing and Intelligent Information System, *Sistemas Inteligentes para la Gestión de la Empresa,* Universidad de Granada, 2015-2016, [Documento sin paginación]. Documento disponible en: http://sci2s.ugr.es/sites/default/files/files/Teaching/GraduatesCourses/SIGE/Tema01-SIGE-Introduccion%20a%20la%20Ciencia%20de%20Datos%20-%202015-16.pdf (última consulta 06/03/18).

[116]Soft Computing and Intelligent Information System, *Sistemas Inteligentes para la Gestión de la Empresa,* Universidad de Granada, 2015-2016, [Documento sin paginación].

Las personas encargadas de la extracción de conocimiento de los datos científicos deben ser profesionales de las matemáticas y la estadística, con conocimiento de analítica, de lenguajes de programación y de ciencias de la computación[117]. Por ende, un científico de datos debe tener un gran dominio de las matemáticas, la estadística y la informática, debe saber programar y tener un gran conocimiento de Base de Datos, así como poseer agilidades en herramientas de procesamiento y visualización, todo ello a efectos de extraer conocimiento a partir de grandes volúmenes de datos clasificados mediante información estructurada y no estructurada.

V. DEFINICIÓN DEL CONCEPTO DE *BIG DATA* Y DE SUS ELEMENTOS MÁS RELEVANTES

Bien, encontrándonos en este punto del presente capítulo introductorio y a la vez sumamente imprescindible para introducir un algo más de luz en la determinación del tema a tratar – pues como trabajo jurídico debe profundizarse en el estado en cuestión a efectos de ofrecer una perspectiva práctica y real del actual contexto social – y, una vez asentados los diferentes conceptos previos al surgimiento del *big data*, procede en este momento del trabajo adentrarnos en el concepto propio de *big data*, así como en su estructura y en sus aspectos más relevantes.

1. DEFINICIÓN DEL CONCEPTO *BIG DATA*

Debido a que son varias y diversas las definiciones del *big data* dadas desde su creación hasta la actualidad, siendo todas ellas igualmente de ciertas y concisas, a continuación, se destacaran las más relevantes a fin de acotar una concepción general. En el año 2001, el analista Laney de META Group (actualmente Gartner) define el *big*

[117] Según afirma GUERRERO, J.A.: "[…] un científico de datos es una persona con fundamentos en matemáticas, estadística y métodos de optimización, con conocimientos en lenguajes de programación y que además tiene una experiencia práctica en el análisis de datos reales y la elaboración de modelos predictivos. De las tres características quizás la más difícil es la tercera; no en vano la modelización de los datos se ha definido en ocasiones como un arte. Aquí no hay reglas de oro, y cada conjunto de datos es un lienzo en blanco" entrevista realizada en El Confidencial, *Un matemático andaluz desconocido es el mejor cientofco de datos del mundo*, 2013, [Documento sin paginación]. Documento disponible en: https://www.elconfidencial.com/tecnologia/2013-12-19/un-matematico-andaluz-desconocido-es-el-mejor-cientifico-de-datos-del-mundo_67675/ (última consulta 22/03/18).

data como *"*el conjunto de técnicas y tecnologías para el tratamiento de datos, en entorno de gran volumen, variedad de orígenes y en los que la velocidad de respuesta es crítica"[118]. Asimismo, el Diccionario *LID de Inteligencia y Seguridad* señala que el *big data* es un "anglicismo que hace referencia al conjunto de datos cuyo tamaño excede la capacidad de los programas informáticos utilizados habitualmente para capturar, gestionar y procesar información"[119]. Posteriormente, en el año 2012, en el artículo "Critical Questions for big data" se define *big data* como "un fenómeno cultural, tecnológico e intelectual que aparece por la interconexión de los siguientes elementos: (1) Tecnología. Optimización de la capacidad informática y de la precisión de los algoritmos para recopilar, analizar, enlazar y comparar grandes conjuntos de datos: (2) Análisis. Basarse en grandes conjuntos de datos para identificar patrones con el fin de realizar afirmaciones económicas, sociales, técnicas y legales; (3) Mitología. La creencia popular de que los grandes conjuntos de datos ofrecen una forma superior de inteligencia y conocimientos que pueden generar datos que anteriormente no eran posibles, con un aura de verdad, objetividad y exactitud"[120].

En otros términos, el *big data* es el conjunto de datos que, por su volumen y variabilidad y por la velocidad a la que necesitan ser procesados, supera las capacidades de los sistemas informáticos habituales. En concreto, el *big data* engloba una serie de tecnologías, técnicas y herramientas que hacen posible la recogida, procesamiento y análisis de volúmenes masivos de datos, y también la visualización de los resultados. De igual modo, otros autores afirman que *big data* es un término que se ha aculado para referirse a la manipulación de gran cantidad de datos, "es, sin la menor duda, uno de los campos más importantes de trabajo para los profesionales de las TIC. No hay área ni sector que no esté afectado por las implicaciones que este concepto está incorporando; cambian algunas herramientas, se modifican estrategias de análisis y patrones de medida"[121].

---

[118] LANEY, "3D *data management*: Controlling…", *op. cit.,* [Documento sin paginación].

[119] AMAGO, F., *Diccionario LIB Innovación,* Ed. LID, Madrid, 2010, p.55.

[120] BOYD, "Critical questions for…", *op. cit.,* p. 663.

[121] *Vid.* TASCÓN, M., "Introducción: *Big Data*. Pasado, presente y futuro", *Telos: Cuadernos de comunicación e innovación,* núm. 95, 2013 p. 47. Documento disponible en: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articuloTelos&idContenido=2013062110090002&idioma=es

De igual modo, otros autores definen el *big data* como "una nueva generación de tecnologías y arquitecturas diseñadas para extraer valor económico de grandes volúmenes de datos heterogéneos habilitando una captura, identificación y/o análisis a alta velocidad"[122] y también un "conjunto de técnicas y tecnologías de gran volumen, variedad de orígenes y en los que la velocidad de respuesta es crítica"[123].

En este sentido, el *big data*, hace referencia a aquellos datos que una vez analizados mediante nuevas arquitecturas, algoritmos, técnicas y analíticas aportan un valor y conocimiento oculto en los mismos, conduciendo a la toma de mejores decisiones y movimientos estratégicos de un determinado momento[124]. En consecuencia, cabría afirmar que, el *big data* se consiste en datos masivos acumulados que producen conocimiento y aportan en tiempo real un gran volumen de información a efectos de predicción, rentabilidad, eficacia y seguridad de un determinado proyecto o producto en fase de ejecución. Además, el *big data* es el conjunto de datos que, por su volumen y variabilidad y por la velocidad a la que necesitan ser procesados, supera las capacidades de los sistemas informáticos habituales. Asimismo, es el conjunto de tecnologías, técnicas y herramientas que hacen posible la recogida, procesamiento y análisis de volúmenes masivos de datos, y también la visualización de los resultados a fin de detectar patrones, disminuir tiempos muertos y aumentar la eficiencia[125].

En síntesis, una definición incontrastable del *big data* es que "en términos generales podríamos referirnos como a la tendencia en el avance de la tecnología que ha abierto las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, la

---

[122] PUYOL MONTERO, J., *Aproximación jurídica y Económica al Big Data,* Ed. Tirant lo Blanch, Madrid, 2015, p.12, citando a PHILIP CARTER, "Conceptos básicos de *Big Data", TRC Informática S.L.*

[123] Universidad Oberta de Catalunya, "Introducción al *business intelligence* y al *Big Data*, 3ª Edición", curso on-line de *Míriadax*, 2017, disponible en https://miriadax.net/web/introduccion-al-business-intelligence-y-al-big-data-3-edicion-/inicio?timestamp= [Documento sin paginación].

[124] SOCHE LÓPEZ, S., "Metodología para el modelamiento de datos basado en Big Data, enfocados al consumo de tráfico (voz-datos) generado por los clientes"*, Especialización en Gerencia Integral de Proyectos,* Universidad Militar Nueva Granada Bogotá, 2016, p. 5. Documento disponible en: https://core.ac.uk/download/pdf/143452539.pdf

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

cual es utilizada para describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que tomaría demasiado tiempo y sería muy costoso cargarlos a una base de datos relacional para para su análisis. De tal manera que, el concepto de *big data* se aplica para toda aquella información que no pude ser procesada o analizada utilizando procesos o herramientas tradiciones"[126].

Por último, resulta de interés destacar que, según IBM, existen cinco tipos de *big data*, en concreto: (1) *Web and Social Media*; (2) *Machine-to-Machine (M2M)*; (3) *Big Transaction Data;* (4) *Biometrics* y; (5) *Human*, cuya descripción y algunos ejemplos son detallados a continuación en la siguiente tabla:

Datos	Descripción	Ejemplos
Web and Social Media	Contenido web e información que es obtenida de las redes sociales	www, Facebook, Twitter, LinkedIn, blogs
Machine-to-Machine (M2M):	Tecnologías que permiten conectarse a otros dispositivos. M2M utiliza dispositivos como sensores o medidores que capturan algún acontecimiento en particular. Se transmiten a través de redes alámbricas, inalámbricas o híbridas.	Velocidad, temperatura, presión, variables meteorológicas, variables químicas
Big Transaction Data	Incluye datos procedentes de transacciones masivas de los centros de atención telefónica, de banca, finanzas, atención a clientes, etc	Incluye registros de facturación, en telecomunicaciones los llamados registros detallados de las llamadas (Call Detail Record o CDR), etc.
Biometrics	Información biométrica. En el área de seguridad e inteligencia, los datos biométricos son sumamente importantes para los gobiernos, seguridad privada, servicios de inteligencia, policía, etc	Huellas digitales, escaneo de la retina, reconocimiento facial, genética, etc
Human Generated	Datos digitales generados por las personas, en sentido genérico	Notas de voz, correos electrónicos, documentos electrónicos, resultados de estudios médicos, multas, etc

Imagen 3. Tipos de datos del Big-data según IBM (Recopilado a partir de IBM, 2014)[127]

[126] BARRANCO FRAGOSO, R., "¿Qué es Big Data? Todos formamos parte de ese gran crecimiento de datos", *IBM*, junio 2012, [Documento sin paginación]. Documento disponible en: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/ (última consulta 03/06/18). Igualmente, VÁZQUEZ DE CASTRO señala que son tratamientos inteligentes y a gran escala de datos masivos o macrodatos. *Vid.* VÁZQUEZ DE CASTRO, E., "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y nuevas tecnologías,* núm. 46, 2018, p. 52.

[127] MONLEÓN GETINO, "El impacto del *Big Data*…", *op. cit.,* p. 436.

2. ANÁLISIS DE LAS CARACTERÍSTICAS PRINCIPALES DEL *BIG DATA*: VOLUMEN, VARIEDAD, VELOCIDAD, VERACIDAD Y VALOR

En el año 2001, Doug Laney, analista de Gartner, define en un artículo "3D *data management*: Controlling Data Volume, Velocity, and Variety"[128], las 3 V´s del *big data*: *volumen, velocity & variety*. Posteriormente, en el informe ejecutivo desarrollado por *IBM Global Business Services Business Analytics and Optimisation* y la Escuela de Negocios Saïd en la Universidad de Oxford[129] se introducen y añaden la *Veracidad* y el *Valor* como dos nuevas dimensiones del *big data*.

Por ende, aunque no existe unanimidad sobre estas dos últimas características, resulta aceptable confirmar que actualmente las cinco dimensiones que definen al *big data* son: volumen, variedad, velocidad, veracidad y valor.

Imagen 4. Las 5 V´s que componen la tecnología big data[130]

[128] LANEY, "3D *data management*…", *op. cit.,* [Documento sin paginación].

[129] SCHROECK, M., SHOCKLEY, R., ROMERO-MORALES, D. y TUFANO, P., "Analytics: el uso de *Big Data* en el mundo real. Cómo las empresas más innovadoras extraen valor de datos inciertos. Informe Ejecutivo", *IBM Global Business Services Business Analytics and Optimisation y la Escuela de Negocios Saïd en la Universidad de Oxford*, 2012, [Documento sin paginación]. Documento disponible en: ftp://ftp.*software*.ibm.com/la/documents/swg/es/analytics/IBM_Analitica_uso_de_Big_Data_en_mundo_para_sector_servicios_financieros.pdf (última consulta 19/03/18).

[130] SOCHE LÓPEZ, "Metodología para el modelamiento…", *op. cit.,* p. 6.

El *big data* se caracteriza por su volumen de datos masivos de gran tamaño que comprenden información y conocimiento de valor, datos que pueden proceder de múltiples modos, por ejemplo, de dispositivos móviles, audio, video, sistemas GPS, incontables sensores digitales en equipos industriales, automóviles, medidores eléctricos, veletas, anemómetros, etc. Esta contribución a la acumulación masiva de datos la podemos encontrar en diversas industrias, donde las compañías mantienen grandes cantidades de datos transaccionales, reuniendo información acerca de sus clientes, proveedores, operaciones, entre otros. De la misma manera sucede con el sector público, donde en muchos países se administran enormes bases de datos que contienen datos de censo de población, registros médicos, impuestos, entre otros. Además, si a todo lo anterior, añadimos las transacciones financieras realizadas en línea o por dispositivos móviles, análisis de redes sociales[131], ubicación geográfica mediante coordenadas GPS, es decir, todas aquellas actividades que la mayoría de nosotros realizamos varias veces al día con nuestros *Smartphones*, estamos hablando de que se generan alrededor de 2.5 quintillones de bytes diariamente en el mundo[132].

De lo anterior se concluye que el volumen hace referencia al crecimiento exponencial de datos, la cantidad de gigabytes a terabytes de información diaria que se genera y almacena por medio de los seres humanos y la comunicación máquina a máquina (M2M *machine – to – machine*)[133]. Por consiguiente, debido a la existencia de organizaciones creadas por las nuevas tecnologías que se encargan de recoger datos procedentes de las citadas fuentes, incluyendo tanto las transacciones de negocios, redes sociales y la información de los sensores o los datos de sistema a sistema, se ha optimizado el almacenamiento, situación que hubiera conllevado un grave problema en el pasado en caso de haber sido creadas las mismas.

---

[131] Al respecto, anunciar que en Twitter son cerca de 12 Terabytes de tweets creados diariamente y Facebook almacena alrededor de 100 Petabytes de fotos y videos.

[132] BARRANCO FRAGOSO, *¿Qué es Big Data?…*, *op. cit.,* pp.1-2.

[133] BARRANCO FRAGOSO, *¿Qué es Big Data?…*, *op. cit.,* pp. 2-3 establece que: "Los sensores digitales instalados en contenedores para determinar la ruta generada durante una entrega de algún paquete y que esta información sea envidada a las compañías de transportación, sensores en medidores eléctricos para determinar el consumo de energía a intervalos regulares para que sea envía esta información a las compañías del sector energético. Se estima que hay más de 30 millones de sensores interconectados en distintos sectores como automotriz, transportación, industrial, servicios, comercial, etc., y se espera que este número crezca un 30% anualmente".

Por otro lado, en el *big data*, la procedencia de los datos puede darse en diferentes formatos y estructuras de los datos, así pueden tener orígenes de datos estructurados (bases de datos, hojas de cálculo o ficheros CSV), orígenes de datos semi – estructurados (Documentos XML o páginas web) y orígenes de datos no estructurados (documentos de texto, audio, imágenes o video). Así pues, desde el campo sanitario, por ejemplo, "un dato estructurado es un dato que puede ser almacenado, consultado, analizado y manipulado por máquinas. Un dato desestructurado es todo lo contrario. Por ejemplo, datos no estructurados son las recetas de papel, los registros médicos, las notas manuscritas de médicos y enfermeras, las grabaciones de voz, las radiografías, resonancias magnéticas, TAC y otras imágenes. Los datos estructurados y semiestructurados incluyen archivos electrónicos de contabilidad, datos de actuario o datos clínicos. Pero los avances tecnológicos están generando nuevas cascadas de datos (tanto estructurados como no estructurados), son los que provienen de dispositivos para fitness (sensores), de los medios sociales, de Apps en *Smartphones* o de la genética y genómica"[134]. En definitiva, la variedad es una característica del *big data* que se deriva los diversos y variados tipos y fuentes de los que pueden proceder los datos masivos, complejo que engloba tanto los datos estructurados, semi-estructurados y no estructurados. En *big data* el origen mayoritario de los datos procede de datos no semi-estructurados o no estructurados.

Ineludiblemente, los datos en *big data* se generan a una gran velocidad, siendo procesados en un tiempo (casi) real, donde el tiempo de respuesta es crítico. En concreto, pueden darse dos tipos diferentes de velocidad: por un lado, la *velocidad de carga* – procesos ETL – Extracción Transformación de Carga – y, por otro lado, *velocidad de procesamiento*, donde se requiere una respuesta adecuada a su procesamiento y análisis, siendo la misma esencial a fin de dar una respuesta requerida de manera inmediata debido a la rápida capacidad de generación de estos, donde en muchos casos, queda obsoleto lo que era válido con anterioridad. En este aspecto, la labor del analista de datos es esencial a efectos de rentabilizar y optimizar el uso adecuado de los datos y la eficacia de unos resultados de calidad y precisos.

[134] PUYOL MONTERO, *Aproximación jurídica…, op. cit.,* pp. 482-483.

Debido a que en el *big data* se genera una gran variedad de datos de manera masiva y a gran velocidad, ese esencial que los mismos sean veraces, por ello es necesario que sea invertido tiempo a fin de conseguir datos de calidad, para ello deben ser eliminados los datos imprevisibles que obstaculicen la toma de decisiones y afecten a la calidad de los resultados. Por consiguiente, con veracidad nos referimos al grado de confianza que se establecen en aquellos datos que van a ser utilizados. El volumen y variedad de los datos conforme transcurre el tiempo aumenta, lo que conlleva un mayor desafío en la veracidad de los datos. Por ello, es sumamente importante que el analista de datos sea imparcial y objetivo a fin de asegurar en los datos una cierta confianza, autenticad, origen, reputación, disponibilidad y responsabilidad[135].

El valor es el conocimiento e información que se extrae tras previo análisis de los grandes volúmenes de datos, así como la capacidad de usar el valor que aportan los datos en la toma de decisiones, reducción de riesgos, detección de nuevas oportunidades, detectar patrones, disminuir tiempos muertos y aumentar la eficiencia. Cuando los datos se transforman en información y, ésta a su vez se transforma en conocimiento y, el conocimiento se convierte en acción o en decisión, es el momento en el que los datos adquieren un valor, puesto que coopera en que la toma de decisiones sea eficaz y exitosa. En conclusión, las cinco dimensiones que caracterizan al *big data*, son lo que comúnmente se denomina "Las 5 V´s": volumen, variedad, velocidad, veracidad y valor. Igualmente, hemos de tener presente que el Instituto de Ingeniería del

[135] SOCHE LÓPEZ, "Metodología para el modelamiento…", *op. cit.,* p. 11.

Conocimiento añade la viabilidad y la visualización de los datos, como otras características a tener en cuenta del *big data*[136].

Para terminar y, sin ánimo de exhaustividad por no ser el momento apropiado, para posteriormente acercarnos a la concreta figura que nos ocupa, debe destacarse que la estructura principal de un sistema *big data* se divide en cinco sectores fundamentales:

En primer lugar, el sector de la fuente de los datos, que es donde se encuentran recogidos todos los orígenes de la información, desde bases de datos relacionadas hasta datos estructurados o no; en segundo lugar, por la integración, donde se adquieren los datos y se van integrando en conjuntos con los formatos adecuados; en tercer lugar, por el almacenamiento de datos, donde se encuentran los recursos idóneos para almacenar los grandes volúmenes de datos; en cuarto lugar, por el análisis y modelos de computación, donde las herramientas de manejo de datos operan sobre los recursos de almacenamiento e incluyen la gestión de los datos y los modelos de programación; por último, la sección de presentación y aplicación, donde una vez obtenida la información y el conocimiento, es aplicado a los distintos procesos.

[136] A modo de aclaración se ha de tener en consideración las siguientes definiciones: "Viabilidad: La inteligencia empresarial es un componente fundamental para la viabilidad de un proyecto y el éxito empresarial. Se trata de la capacidad que tienen las compañías en generar un uso eficaz del gran volumen de datos que manejan. La inteligencia competitiva también se asocia con la innovación de los equipos de trabajo y el uso de tecnologías empleadas. Una empresa inteligente analiza, selecciona y monitoriza la información con el fin de conocer mejor el mercado en el que opera, a sus clientes y diseñar estrategias eficaces. Es necesario filtrar a través de esta información y seleccionar cuidadosamente los atributos y factores que son capaces de predecir los resultados que más interesan a las empresas. El secreto del éxito es descubrir las relaciones entre las variables ocultas. Una vez que conoces la viabilidad de tu organización, es el momento de detallar el proyecto en una hoja de ruta, y desarrollar el plan de negocio. Visualización de los datos: Cuando hablamos de visualización nos referimos al modo en el que los datos son presentados. Una vez que los datos son procesados (los datos están en tablas y hojas de cálculo), necesitamos representarlos visualmente de manera que sean legibles y accesibles, para encontrar patrones y claves ocultas en el tema a investigar. Para que los datos sean comprendidos existen herramientas de visualización que te ayudarán a comprender los datos gráficamente y en perspectiva contextual", Instituto de Ingeniería del Conocimiento, *Las 7V del Big Data: características más importantes,* 2016, [Documento sin paginación]. Documento disponible en http://www.iic.uam.es/innovacion/big-data-caracteristicas-mas-importantes-7-v/#viabilidad (última consulta 05/03/18).

VI. VINCULACIÓN DE LAS TECNOLOGÍAS PREVIAS AL *BIG DATA* Y SUS PRINCIPALES DIFERENCIAS

No obstante, tras haberse efectuado un estudio exhaustivo sobre los conceptos previos al *big data*, así como del concepto propio de *big data*, su estructura y características, es fundamental delimitar las diferencias principales entre los conceptos tratados anteriormente con el de *big data* a efectos de alcanzar el carácter real del contexto tecnológico en el que se desarrollan las distintas herramientas y figuras.

1. DIFERENCIAS PRINCIPALES ENTRE *BUSINESS INTELLIGENCE* Y *BIG DATA*

Una de las grandes diferencias entre el *business intelligence* (BI) y el *big data*, es que en el caso del *big data*, como detallaremos más adelante, los datos no se agrupan en un servidor central, sino que son almacenados en un sistema de ficheros distribuido, resultando ser éste un método más seguro y flexible, puesto que se adapta a la incorporación de nuevos datos de manera automática, siendo los mismos clasificados por diferentes campos conceptuales lo que genera que la información y conocimiento procedente de su análisis sea más segura y concreta.

Igualmente, otro rasgo diferencial con el BI es que el *big data* analiza datos en diferentes formatos, abarcando tanto datos estructurados en ficheros o bases de datos tradicionales, como datos no estructurados, de hecho, actualmente debido a la velocidad en la que se genera un gran volumen de información, lo frecuente y habitual en la tecnología del *big data* es el análisis de datos no estructurados, lo que le permite tener acceso a un análisis global de distintas fuentes de información.

Por otro lado, a diferencia del BI, el *big data* no sólo analizada datos históricos, sino que, a consecuencia del hecho de trabajar con fuentes de datos en tiempo real, tiene acceso a datos que son procesados al momento, de tal modo, que las empresas puedan tomar decisiones al instante sobre problemas reales y actuales de manera ágil y eficaz.

Por último, otra característica diferenciadora es que la tecnología del *big data* analizada a gran velocidad grandes volúmenes de información dividiendo el análisis de datos sobre un proyecto concreto en varias partes de ejecución paralelo, reunificando cada una de ellas al final del proceso, presentando así resultados globales. Es lo que se denomina la técnica de conceptos de Procesamiento Paralelo Masivo (MPP)[137].

2. DIFERENCIAS ENTRE *DATA MINING* Y *BIG DATA*

En relación con las diferencias a destacar entre el *data mining* y el *big data*[138], cabe resaltar que este último se centra en el almacenamiento de grandes volúmenes de datos, esto es, en la captura, gestión y procesamiento de los datos en un tiempo prudencial y de manera eficiente.

En concreto, como se ha visto, la finalidad del *big data* es la de analizar en el menor tiempo y de la mejor forma la información y conocimiento contenido en los datos. No obstante, el *data mining* consiste en un proceso puramente de identificación de todo tipo de información relevante extraída previamente de los grandes volúmenes de datos, estructurando la misma de manera compresible y ordenada a fin de averiguar patrones y tendencias. Así, pues el proceso de la minería de datos se lleva a cabo en base a las siguientes fases:

1) Identificación del problema a resolver y comprensión de lo buscado;
2) Determinación, captación y limpieza de los datos;
3) Creación de modelos y patrones;
4) Validación y comunicación de los resultados;
5) Integración de los resultados previamente validados y comunicados.

---

[137] GTI, Software & Networking, *5 Diferencias entre Big Data y business intelligence,* 2015 [documento sin paginación]. Documento disponible en: http://noticias.gti.es/productos/5-diferencias-entre-big-data-y-business-intelligence/ (última consulta 25/02/18).

[138] *Vid.* BALAGUERÓ, T., "Qué es la minería de datos en *Big Data*. *Deusto Formación",* noviembre 2017, [Documento sin paginación]. Documento disponible en https://www.deustoformacion.com/blog/gestion-empresas/que-es-mineria-datos-big-data (última consulta 02/04/18). *Vid.*, BIG DATA INTERNATIONAL CAMPUS, "Data Mining vs Big Data", febrero 2017, [Documento sin paginación]. Documento disponible en http://www.campusbigdata.com/big-data-blog/item/82-data-mining-vs-big-data (última consulta 02/04/18).

En definitiva, con el *data mining* nos encontramos ante una serie de técnicas cuya finalidad es la de extraer la información y el conocimiento contenido en los grandes volúmenes de datos, siendo el *big data* la tecnología que captura, gestiona y procesa en tiempo razonable y de manera veraz los datos de los que posteriormente el DM va a extraer la información relevante a fin de que las tomas decisiones resulten eficaces, de calidad y resolutivas.

3. DIFERENCIAS ENTRE *DATA SCIENCE* Y *BIG DATA*

De antemano, a pesar de que en muchas ocasiones *data science* y *big data* podrían ser considerados conceptos con cierta similitud, lo cierto es que entre ambos radican grandes e importantes diferencias a tener en consideración. En concreto, debemos destacar las siguientes[139]:

Así pues, como primera diferencia a tener en cuenta, es que el *big data* involucra datos procedentes de múltiples servidores, sin embargo, el *data science*, involucra conocimientos específicos de uno o varios dominios (por ejemplo, finanzas, medicina o geología).

En segundo lugar, el *big data* entremezcla gestión y procesamiento de datos, por otro lado, el *data science* tiene en cuenta aspectos computacionales.

En tercer lugar, el *big data* únicamente no se limita a las bases de datos relacionales y *data warehouse*, así como que permite resultados diferentes y totalmente novedosos a los enfoques anteriores o que conllevarían más tiempo de ejecución.

Sin embargo, con el *data science* nos encontramos que el mismo lo confortan técnicas científicas como la prueba de hipótesis y la validación de resultados, resultados que a su vez deben ser confiables. Asimismo, involucra más cantidad de matemáticas y

[139]PASCUAL, P., "¿Cuáles son las diferencias entre *Big Data* y *data science*?", *PiperlabK,* diciembre 2017 [Documento sin paginación]. 5 diciembre. Documento disponible en: https://piperlab.es/2017/12/05/diferencias-entre-big-data-data-science/ (última consulta 03/03/18).

estadísticas que los enfoques anteriores. Igualmente, incluye aprendizaje automatizado (*Machine Learning*), Inteligencia Artificial o algoritmos de descubrimiento de conocimiento (*knowledge discovery*), así como una visualización y creación eficiente de prototipos para el desarrollo de *software*, satisfaciendo en nivel perturbador al menos uno de estos deberes.

VII. TECNOLOGÍAS POSTERIORES A LAS HERRAMIENTAS *BIG DATA*: *OPEN DATA* Y *SMART DATA*

Asimismo, resulta imprescindible hacer referencia a aquellos conceptos (tecnologías) influyentes que ha surgido después de las herramientas *big data* a fin obtener una perspectiva más amplia que nos permita delimitar y definir su contexto.

1. EL CONTEXTO DEL *OPEN DATA* Y MARCO CONCEPTUAL

En primer lugar, se ha de señalar que como resultado del valor de la información que aportan los datos procedentes de las nuevas tecnologías y del Internet de las Cosas, en la esfera de la Administración Pública – siendo la misma considerada una gran fuente originaria de datos – nace el concepto *open data*, cuya finalidad principal es la de poner a disposición de los ciudadanos aquellos datos generados y administrados desde los organismos públicos, a fin de que los mismos sean utilizados, reutilizados y retribuidos por la población. En concreto, los datos son accesibles mediante formatos técnicos y legales para todo aquel ciudadano que los necesite para cualquier tipo de finalidad, siempre y cuando la misma sea lícita y conforme a Derecho.

En efecto, con el *open data* se pretende conseguir una política de participación ciudadana cuyo objetivo es el de fortalecer una sociedad democrática, creando un sistema de estatal donde el gobierno y el Estado se fundamente en una cultura de transparencia, colaboración, participación y rendición de cuentas a los ciudadanos, permitiéndoles a los mismos el acceso libre y público a los datos que contienen información con un gran valor administrados y gestionados por las Administraciones

Públicas, todo ello a fin de que la población pueda desarrollar actividades de emprendimiento y generar soluciones a retos públicos.

Por otro lado, hemos de tener presente que mediante el *open data* se les otorga a los datos un valor que es evaluado económicamente, por lo que resultaría beneficioso que existiera la posibilidad de que las Administraciones Públicas puedan adoptar la medida de vender los datos a aquellas entidades privadas que necesiten de los mismos para el desarrollo de un proyecto del que van a obtener un gran beneficio económico. De este modo, lo recaudado por el Estado mediante la venta de los datos de los ciudadanos podría ser invertido en otros proyectos de interés común y general de la población, así como para dar solución a problemas patentes en la sociedad y suplir determinadas necesidades sociales.

Por ende, los datos abiertos *"*son datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen"[140]. De la anterior definición se pueden derivar una serie de características[141] que engloban el significado el concepto de *open data*, en concreto:

(1*)* Disponibilidad y acceso. Toda la información en su conjunto debe quedar a disposición del ciudadano de manera conveniente a un coste mínimo, pudiéndose, por un lado, descargar la mayoría de la información de manera rápida y directa a través de internet, así como ser la misma modificada.

(2) Reutilización y distribución*.* Los datos deben ser regulados bajo condiciones que permitan su reutilización y redistribución, incluyéndose la posibilidad de ser integrados en otros conjuntos de datos.

---

[140] Open Data Charter, *Carta Internacional de los Datos Abiertos. Principios*, octubre 2015 [Documento sin paginación]. Documento disponible en https://opendatacharter.net/principles-es/ (última consulta 14/04/18).

[141] ORTIZ DE ZÁRATE, A., "Open Data el valor de los datos", *Alorza.net*., junio 2016 [Documento sin paginación]. Documento disponible en: https://es.slideshare.net/alorza/open-data-el-valor-de-los-datos (última consulta 12/04/18).

(3) Participación universal. Todo ciudadano debe poder tener acceso a los datos a fin de utilizar, reutilizar y redistribuir la información de estos. Por consiguiente, quedará prohibida toda condición que discrimine en términos de esfuerzo, personas o grupos el acceso a los datos, quedando así prohibida toda restricción "no comercial" o de uso para ciertos fines.

Igualmente, son establecidos una serie de principios que deben regir los datos abiertos, en concreto detalla que los datos deben ser:

"(1) Públicos: se recomienda abrir todos los datos públicos. (2) Detallados: publicar relatos originales con el nivel de granularidad más detallado posible. (3) Actualizados: los datos deben ser puestos a disposición de los usuarios con la frecuencia necesaria para que los datos no pierdan su valor. (4) Accesibles: es necesario hacer accesible los datos al mayor número de usuarios posible. (5) Automatizados: los datos deben ser procesados automáticamente, es decir sin intervención humana manual. (6) Sin registro: los datos deben estar disponibles para todo el mundo, sin necesidad de registro previo. (7) Abiertos: se recomienda la utilización de formatos no propietarios. (8) Libres: los datos deben ser de uso 100 × 100 libre para los usuarios"[142].

De igual modo, en el preámbulo de la Carta Internacional de Datos Abiertos, en el párrafo décimo se cita una serie de principios que establecen las bases de acceso, publicación y uso de los datos abiertos, debiendo ser los mismos (a) abiertos por defecto, (b) oportunos y exhaustivos, (e) accesibles y utilizables, (d) comparables e interoperables, (e) para mejorar la gobernanza y participación ciudadana y, finalmente (f) para el desarrollo incluyente y la innovación. Por ende, de conformidad a lo establecido en el citado preámbulo los datos abiertos proporcionan una información y conocimiento que tanto el Estado como los ciudadanos deben aprovechar, debido a los múltiples beneficios de interés general y común que aportan, puesto que, por un lado el *open data* ayuda a la toma de decisiones informadas, colaborando con los ciudadanos y a los organismos – públicos y privados – en el desarrollo de nuevos proyectos e ideas

[142] ORTIZ DE ZÁRATE, "Open Data el valor de…", *op. cit.,* [Documento sin paginación].

innovadoras cuyo objetivo sea el de producir beneficios sociales, económicos y de mejorar el bienestar social.

De manera similar, el *open data* permite desarrollar avances en programas y servicios públicos mediante la combinación y comparación efectiva de los datos, lo que conlleva la posibilidad de detectar tendencias, desafíos e inequidades económicas y sociales. Asimismo, los datos abiertos colaboran con los gobiernos, ciudadanos y organizaciones públicas y privadas a fin de establecer medidas de mejora en cada uno de los sectores de los servicios públicos (salud, educación, seguridad pública, protección del medio ambientes, derechos humanos y desastres naturales). Además, el *open data* contribuye al crecimiento económico mejorando nuevos mercados, empresas y empleos. De modo semejante, los datos abiertos proporcionan una información del gobierno tanto a los ciudadanos como a otros gobiernos mediante la rendición de cuentas y la buena gobernanza, haciendo así que las decisiones de un determinado gobierno sean más transparentes, enriqueciendo la participación y opinión pública.

Por último, hemos de tener en consideración que los datos abiertos ofrecen oportunidades a fin de dar soluciones innovadoras a problemas políticos y cooperar en el crecimiento económico y el bienestar social[143]. Por consiguiente, a tenor de lo anterior, se podría afirmar que los datos abiertos son un producto público que aporta conocimiento, valor e información de interés social y general, puesto que colaboran en la evolución de la humanidad hacía un mundo mejor.

[143] Al respecto, Open Data Charter, *Carta Internacional de los Datos Abiertos. Principios*, octubre 2015 [Documento sin paginación], señala que: "Los datos abiertos pueden lograr esto mediante, por ejemplo: Apoyando políticas públicas basadas en evidencia: alentando a los gobiernos a usar datos en el desarrollo de políticas y en la toma de decisiones basadas en evidencia, lo cual permite mejores resultados de las políticas públicas y apuntala el desarrollo económico sostenible y el desarrollo; Habilitando la colaboración intersectorial: apoyando la colaboración entre gobiernos, ciudadanos, organizaciones de la sociedad civil y del sector privado en el diseño de políticas y en la implementación de mejores servicios públicos; Siguiendo el uso de recursos públicos: mostrando cómo y dónde se gastan los fondos públicos, lo que incentiva a los gobiernos a demostrar que están usando el dinero público de forma eficaz; Mejorando la gobernanza de los recursos naturales: aumentan la concientización sobre el modo en el que los países utilizan los recursos naturales, cómo se gastan los ingresos extractivos, y cómo se comercializa y administra la tierra; Monitoreando impacto: promoviendo la evaluación del impacto de programas públicos, que a su vez permite que los gobiernos, las organizaciones de la sociedad civil y del sector privado respondan de manera más eficaz a las necesidades específicas de las comunidades locales; Promoviendo el crecimiento equitativo: apoyando el crecimiento sostenible e inclusivo a través de la creación y el fortalecimiento de mercados, empresas y empleos; Geolocalizando datos: proporcionando referencias de observaciones geoespaciales y terrestres, que permiten la comparabilidad, e interoperabilidad y análisis eficaces al permitir que los datos dispongan en capas geográficas; y Mejorando la toma de decisiones: haciendo posible que los ciudadanos tomen decisiones mejor informadas respecto a los servicios que reciben y a la calidad de servicio que deberían esperar".

2. *SMART DATA*: LA NUEVA ERA DE LOS DATOS PROCEDENTES DEL INTERNET DE LAS COSAS Y DE LA INTELIGENCIA ARTIFICIAL

El concepto *smart data* surge a partir del *big data*. En concreto, el *smart data* engloba el resultado de los datos previamente almacenados en listas y bases de datos una vez transformados por medio de algoritmos que procesan *big data* en información con valor. De lo que se deduce que una vez que *big data* almacena a gran velocidad información mediante un gran volumen de datos, procesa y filtra la misma, el *smart data* mediante fórmulas matemáticas convierte la información procesada en datos y los transforma en respuestas "axiomáticas"[144].

En suma, el *smart data* se centra en la transparencia y veracidad de los datos a fin de dar una respuesta real a los problemas que se plantean mediante algoritmos. A consecuencia del creciente volumen de datos que se generan en la era tecnológica y digital, donde gran parte de los datos que son procesados proceden de sistemas no estructurados, convirtiendo el *big data* en *smart data*, esto es, en datos inteligentes y útiles[145]. Por ende, el *smart data* analiza e interpreta los datos teniendo en cuenta su contexto, con el objetivo de que la toma de decisiones y los procesos de negocio sean ciertos y eficaces. Para ello es sumamente relevante y primordial que la información inteligente se encuentre disponible en tiempo real a fin de que la respuesta sea realmente eficiente, así como la conexión de múltiples canales, repositorios de datos y dispositivos, consiguiendo dar una respuesta en la mayor brevedad de tiempo posible, una flexibilidad más eficaz y una capacidad de adaptación real al contexto del negocio.

---

[144] MORAES, R., "Big Data v/s Smart Data. Desde la cantidad a la calidad", *Gerencia*, julio 2014 [Documento sin paginación]. Documento disponible en http://www.emb.cl/gerencia/articulo.mvc?xid=3503&sec=12 (última consulta 28/04/18).

[145] En este sentido, GRAU, J., "Smart Data: el tamaño no siempre importa", *AUSAPE*, marzo 2016 [Documento sin paginación]. Documento disponible en: http://www.scl-consulting.com/wp-content/uploads/2016/03/smart-data.pdf (última consulta 03/05/18) afirma que: "mediante este proceso, se deben primar aspectos como la uniformidad, la facilidad de extracción y el análisis y, por supuesto, la relevancia de la información que albergan. Los datos deben servir a la empresa para tomar mejores decisiones y no sólo para describir procesos. Por eso, no basta con recolectar enormes cantidades de datos, sino que es fundamental contextualizarlos para poder interpretarlos correctamente".

3. LA TÉCNICA DE *MACHINE LEARNING*

Para finalizar, resulta imprescindible mencionar la técnica de *Machine Learning* (aprendizaje automático), al resultar una técnica empleada en distintas herramientas, como por ejemplo en el *data mining,* que utiliza la misma para la construcción de modelos predictivos.

A modo resumen, se ha destacar que el *Machine Learning* es una rama de la Inteligencia Artificial – concepto que será tratado más delante en epígrafe distinto debido a su relevancia e influencia con el *big data* – que, mediante el empleo de una serie de algoritmos[146], denominados «Aprendizaje Automático», otorga autonomía a los ordenadores y sistemas informáticos a fin de que por sí mismos aprendan de sus propios errores e incluso lleguen a optimizar sus aciertos sin que sea necesaria la intervención humana. El objeto fundamental es prescindir de continuas programaciones efectuadas por humanos, consiguiendo a su vez de manera automática resultados que maximicen la eficiencia. De tal modo, que los sistemas de *Machine Learning* a partir de grandes volúmenes de datos identifican patrones complejos que una vez procesados predicen el comportamiento. El hecho de no requerir ningún tipo de ayuda externa permite a su vez que puedan desarrollar sus propios modelos para descubrir tendencias[147].

A continuación, se muestran algunas de las principales técnicas estadísticas empleadas en el análisis de *big data* y como parte del *Machine Learning*:

[146] *Vid.* Anexo: Tabla 1: Algoritmos utilizados en el aprendizaje automático (ML).

[147] Universia España, *¿Qué es Machine Learning y cómo se usa en Big Data?*, septiembre 2017, [Documento sin paginación]. Documento disponible en: http://noticias.universia.es/ciencia-tecnologia/noticia/2017/09/12/1155659/machine-learning-como-usa-big-data.html (última consulta 04/03/18).

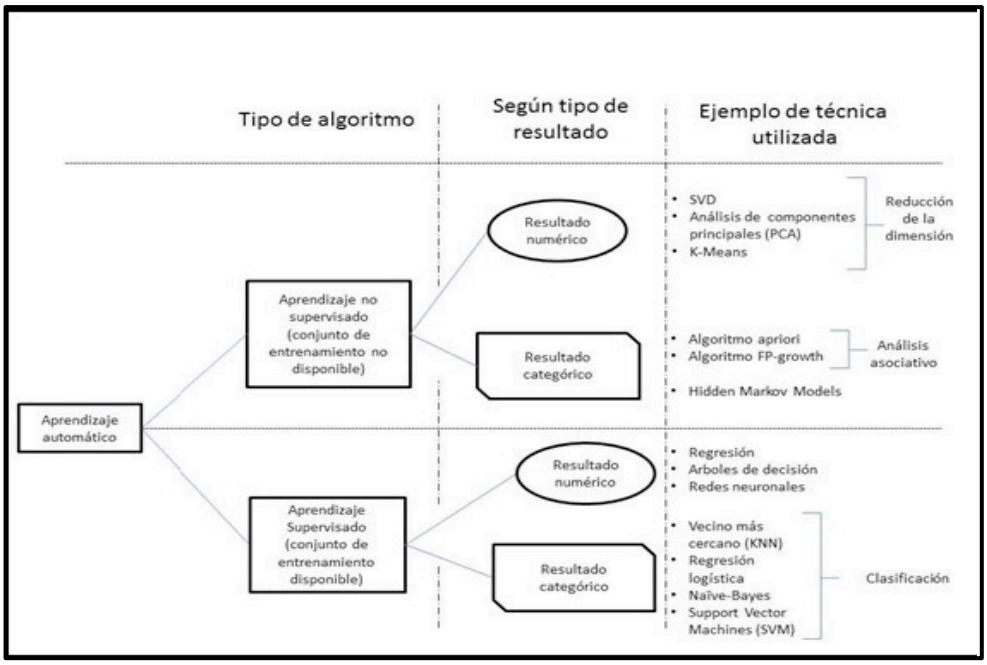

Imagen 5. Esquema de los principales algoritmos ML para el tratamiento de los Big-data clasificados según el tipo de resultado (numérico o categórico), así como ejemplos de técnicas utilizados dentro de los algoritmos[148].

En concreto, del esquema anterior, se ha de aclarar que con la técnica de la clasificación se trata de asignar una clase o categoría a un determinado objeto o individuo, donde en el sistema se le van atribuyendo etiquetas (como "bueno" o "malo", "saludable" o "no saludable" …) conforme se va avanzando en su clasificación, a fin de obtener una clasificación lo más real posible según sus características. Por otro lado, con la técnica de la regresión, lo que se realizada es generalizar el problema de la clasificación a través de la estadística a fin de predecir su impacto en la sociedad. Por último, con el agrupamiento, se organizan (de manera jerárquica o no) los objetos o individuos en grupos que compartan las mismas características y categorías[149].

Por adelantar el contenido de los próximos capítulos, se ha de señalar que hasta hace relativamente poco la técnica que se utilizaba en el *big data* para conseguir las mejoras de la Medicina Personalizada o Medicina de Precisión era el *Machine Learning,* herramienta que por ser esencial para el desarrollo de la Medicina Basada en

[148]MONLEÓN GETINO, "El impacto del *Big Data*…", *op. cit.,* p.440.

[149] MONLEÓN GETINO, "El impacto del *Big Data…"*, *op. cit.,* p.439.

la Evidencia (MBE) continúa empleándose, aunque con menos frecuencia, como se verá en el siguiente capítulo.

Hasta aquí damos por clausurado el mapa conceptual principal que integra el contexto del *big data*, dejándose para más adelante, como se ha comentado, su vinculación con la Inteligencia Artificial debido a su relevancia, así como aquellos conceptos referentes a tecnologías propias del *big data* en el sector sanitario.

CAPÍTULO SEGUNDO

LAS TECNOLOGÍAS *BIG DATA* EN EL SECTOR SANITARIO

I. DEFINICIÓN DEL *BIG DATA* EN EL SECTOR SANITARIO

Debido a que las nuevas tecnologías elementales de la información y de la comunicación analizadas en el capítulo anterior también son, como veremos, aplicadas en el sector de la medicina[150], así como a la relevancia y especial trato de las tecnológicas *big data* en el citado sector, comúnmente en la sociedad se emplea la expresión *big data* sanitario, lo que nos lleva en el presente capítulo a desarrollar una definición aproximada de la misma, adentrándonos a su vez en el estudio de la implantación de la e-Salud en el sector de la sanidad donde se analizaran las principales fuentes de datos sanitarios procedentes de las TIC y el IoT en los servicios sanitarios,

[150] BRENT, "En la era de la información: información, tecnología y estudio del…", *op. cit.,* pp. 55-56.

ofreciendo especial relevancia a la historia clínica electrónica, figura ésta estudiada tanto desde la práctica sanitaria, como desde una perspectiva jurídica.

Así pues, teniendo en cuenta el concepto genérico del *big data* analizado en el capítulo anterior, de manera general podría afirmarse que el *big data* sanitario consiste en transformar los datos de salud en información y conocimiento sanitario tras el almacenamiento y análisis efectuado a través de la aplicación de las herramientas *big data*, organizando de forma efectiva "la información de los datos estructurados ya existentes (fichas personales de los pacientes, etc.) aquellos que permanecen ocultos al sistema actual de almacenamiento y sólo existen de forma analógica en poder de los pacientes (recetas de papel, registros médicos o resultados de pruebas médicas)"[151].

En este sentido, cabe indicar que los datos de salud pueden encontrarse estructurados, semi-estructurados o no estructurados y a través de la aplicación de herramientas *big data* sanitario son almacenados y analizados transformándose a su vez en información y conocimiento. Por un lado, los datos estructurados o semiestructurados pueden ser fácilmente almacenados, consultados, analizados y manipulados por medio de ordenadores, en general, son los datos recogidos en los historiales médicos electrónicos, receta electrónica y en las lecturas de los dispositivos.

Por otro lado, los datos no estructurados o desestructurados son lo que de manera general se encuentran fuera de los datos estructurados o semiestructurados, como notas manuscritas, registros médicos en papel, recetas de papel, ingresos en el hospital, registros de altas, ensayos clínicos, datos a nivel genético, las secuencias genómicas de datos de población radiografías e imágenes médicas.

[151] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, p. 77. Documento disponible en: https://es.slideshare.net/AndresMacario2015/informe-big-data-y-salud?from_action=save (última consulta 02/02/20).

Imagen 6. Tipos de datos y Fuentes de datos[152]

En la actualidad, a causa de la implantación de las TIC y del IoT, existe un gran volumen de datos sanitarios no estructurados generados por dispositivos móviles, la genética, la genómica y las redes sociales, entre otros, por lo que a través del *big data* se pretende que mediante técnicas y herramientas eficientes se puedan adquirir, almacenar, organizar, combinar y convertir en datos estructurados, para un posterior análisis de los mismos a fin de transformar los datos sanitarios en información y conocimiento. Por tanto, el potencial del *big data* sanitario es de combinar datos tradicionales con las nuevas formas de datos procedentes de las TIC y del IoT, tanto de forma individual (paciente) como general (población)[153].

[152] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, p. 77. Documento disponible en: https://es.slideshare.net/AndresMacario2015/informe-big-data-y-salud?from_action=save (última consulta 02/02/20).

[153] En este sentido, OLIVER MORA, M. y IÑIGUEZ RUEDA, L., "El uso de las tecnologías de la información y la comunicación (TIC) en los centros de salud: la visión de los profesionales en Cataluña, España", *Interface (Botucatu)*, Vol. 21, núm. 63, 2007, p. 953, aclaran que: "Concretamente, la introducción de las TIC en el sistema sanitario puede contribuir a mejorar diferentes aspectos, entre los cuales nos gustaría resaltar: a) la relación de confianza entre los pacientes y los profesionales de la atención primaria; b) la formación de los pacientes entorno a su estado de salud; c) la constitución de redes de apoyo entre pacientes; d) la autonomía y la capacidad decisoria de los pacientes; e) una atención sanitaria más personalizada; f) la colaboración entre los profesionales sanitarios; y g) la calidad de las derivaciones de la atención primaria a la atención secundaria".

De igual modo, en el sector sanitario, el valor de los datos sanitarios va a depender de su calidad, puesto que nos encontramos ante un fenómeno que no sólo aporta información, sino también conocimiento, todo ello con la finalidad de obtener una información precisa que ayude al facultativo sanitario a tomar una decisión eficaz y correcta, así como a efectos futuros poder evolucionar hacia una medicina predictiva.

En el mismo sentido, cabe precisar que dentro del *big data* sanitario se encuentran los *Real World Data* (RWD), que son aquellos estudios fuera de los ensayos clínicos aleatorizados que complementan la información de estos en la práctica clínica real. Entre los RWD, se incluyen estudios observacionales de registro, datos provenientes de historias clínicas electrónicas, encuestas de salud y ensayos clínicos pragmáticos. Por tanto, los *Real World Data*, reflejan la atención real que reciben los pacientes en cada contexto concreto y los resultados clínicos que realmente obtienen. En este sentido, permiten identificar pacientes crónicos en riesgo de descompensación, ayudar a la toma de decisiones clínicas en tiempo real, trasladar información directamente a los pacientes, comparar distintos tratamientos para una misma condición estableciendo la función de cada uno según el paciente e igualmente, permiten el desarrollo de indicadores sofisticados desarrollando estrategias de mejora en un centro sanitario determinado. No en vano, en nuestro país, podemos apreciar la existencia de diversos problemas técnicos, en relación con la fragmentación de los sistemas y servicios autonómicos en las diferentes Comunidades Autónomas, lo que genera a su vez una limitada interoperabilidad, de calidad de la información, de desarrollo de diseño y métodos de análisis, junto con la carencia de profesionales TIC especializados en salud. De igual modo, en el Sistema Nacional de Salud (SNS), nos encontramos con problemas procedentes de la precariedad y debilidad de las estructuras investigadoras en servicios de salud y atención sanitaria, necesidad de mayor transparencia en la información y de accesibilidad a los datos de las organizaciones sanitarias, en definitiva con los límites de la evaluación independiente de las políticas sanitarias públicas desde la perspectiva de la protección de la privacidad de los pacientes[154].

Sin embargo, debido a que el *big data* sanitario supone una notoria mejora y evolución en la esfera de la salud, tanto en la calidad de la atención de los pacientes, así

[154]GOST GARDE, J., "Gestión sanitaria y tecnológica de la información", 2001, pp. 37 -57. Disponible en: http://www.conganat.org/SEIS/informes/2001/PDF/2Gost.pdf (última consulta 03/03/20).

como en la prevención, tratamiento y diagnósticos de enfermedades y, toma de decisiones, suponiendo a su vez una considerable reducción de costes sanitarios, resulta imprescindible integrar todos los datos procedentes de las diferentes fuentes, así como desarrollar nuevas herramientas y tecnologías encargadas de almacenar, procesar y analizar la totalidad de los datos a fin de sustraer de los mismos la información y conocimiento relevante de interés común para la humanidad.

Para ello, igualmente, es factor esencial que tanto las Administraciones Públicas, entidades privadas, hospitales y centros sanitarios, facultativos sanitarios, centros de investigación, universidades y demás agentes implicados, se comprometan a apoyar y defender la aplicación de la herramienta *big data* en proyectos sanitarios, que resulten de interés general, siempre y cuando se respeten las medidas y garantías esenciales, como más adelante se detallará.

II. LAS FUENTES PRINCIPALES DE DATOS DE SALUD

Tal vez cabría pensar que las tecnologías de la información y comunicación (TIC), especialmente la conectividad global e internet, han generado un cambio revolucionario en las sociedades industrializadas[155], así como que desde su implantación en el sector sanitario se han convertido en herramientas primordiales y esenciales de interés social debido a las grandes oportunidades que ofrecen tanto a los profesionales sanitarios como a los pacientes[156].

[155]CASTELLS, *La Sociedad Red. Volumen I. La era de la información: economía…, op. cit.,* p.26, señala que: "Una revolución tecnológica, centrada en torno a las tecnologías de la información, empezó a reconfigurar la base material de la sociedad a un ritmo acelerado. Las economías de todo el mundo se han hecho interdependientes a escala global, introduciendo una nueva forma de relación entre economía, Estado y sociedad en un sistema de geometría variable".

[156]Al respecto GOST GARDE, "Gestión sanitaria y tecnológica…", *op. cit*., p.53, señala que: «La tercera gran revolución de la humanidad está poniendo de manifiesto las contradicciones de muchos de nuestros valores. Como gestores debemos responder ante los pacientes del cumplimiento de sus cinco derechos fundamentales: "a través de unos datos clínicos correctos, disponibles en tiempo y forma, adoptaremos – conjuntamente con el paciente– las decisiones pertinentes que, mediante un proceso adecuadamente desarrollado, posibilitarán la obtención de los mejores resultados". En esta responsabilidad, las tecnologías de la información y comunicación se han convertido en una parte muy importante de nuestra estrategia, pero plantean también repercusiones importantes para los pacientes. Podrán perdonársenos muchos errores, pero nunca que vivamos de espaldas a un futuro que ya es presente».

Es indudable que previamente a la conectividad en el sistema de salud, los diferentes sectores sanitarios operaban de manera independiente y aislada, sin tener acceso a la información y a los datos registrados en otro lugar o entidad, e incluso dentro de una determinada institución sanitaria resultaba de gran complejidad el acceso a los datos e información de los pacientes debido a que los mismos se encontraba en soporte papel y de difícil localización, puesto que en ocasiones se hallaban bajo la custodia del propio profesional sanitario o archivados en depósitos ubicados en las instalaciones propiedad de la entidad sanitaria. Todo ello dificultaba la relación entre el personal clínico, los hospitales, las entidades farmacéuticas, los centros de investigación universitarios y las empresas de tecnológica sanitaria, lo que generaba un sistema de salud ineficaz, inicuo y una asistencia sanitaria lenta y costosa. Sin embargo, tras la implantación de las TIC se ha ido avanzado hacia una homogenización de los servicios y procesos sanitarios, permitiendo una interactuación automática e inmediata entre los diferentes sectores y agentes sanitarios tanto dentro de una misma institución o entre diferentes organismos sanitarios ya sean de índole privada o pública.

Por consiguiente, tanto la incorporación de las TIC al sistema sanitario, como la estandarización e interoperabilidad de los sistemas pertenecientes al Sistema Nacional de Salud (SNS), ha provocado en los últimos años una evolución progresiva – aunque inacabada – en la gestión sanitaria, hasta el extremo de conseguir un sistema propiamente integrado y centrado en el paciente y en el cuidado de su salud[157]. Actualmente, debido a la implantación de los sistemas e-Salud[158] el paciente está mejor

[157] BEBEA GONZÁLEZ, I., MARTÍNEZ FERNÁNDEZ, A. y REY MORENO, C., *Guía de la Cooperación Española para la incorporación de las TIC en las intervenciones de Salud en la Cooperación para el Desarrollo*, Agencia Española de Cooperación Internacional para el Desarrollo, Departamento de Cooperación Sectorial y de Género, Área de Salud, 2012, pp. 2-9. Disponible en: https://www.aecid.es/galerias/que-hacemos/descargas/GUIA_TICs_SALUD.pdf (última consulta 23/02/20).

[158] En este sentido, DÍAZ DE LEÓN CASTAÑEDA, CH., "¿Qué es la salud electrónica ("e-Salud")?", *Infotec.* [Documento sin paginación], señala que: "La salud electrónica ("e-Salud") (o en inglés "e-Health"), es un concepto muy amplio que se ha relacionado con la aplicación de las tecnologías de la información y comunicación (TIC) en el campo de la salud. La Organización Mundial de la Salud (OMS) ha definido e-Salud como "el uso costeefectivo y seguro de las Tecnologías de la Información y Comunicación) en apoyo de la salud y de los ámbitos relacionados con ella, incluyendo los servicios de atención sanitaria, vigilancia de la salud, literatura y educación, conocimiento e investigación", sin embargo, ha surgido un debate sobre la precisión del concepto. La salud electrónica implica el uso de las TIC en ámbitos de los sistemas de salud, desde los sistemas de vigilancia epidemológica hasta la provisión de servicios de salud en sus diversos niveles y especialidades, implicando su uso tanto por la población en general como por profesionales o técnicos de la salud (médicos, enfermeras, farmacéuticos, estomatólogos, técnicos en radiología, rehabilitación, etc.). Esto es, la e-Salud tiene implicaciones en la toda la cadena de actividades de salud pública: vigilancia, prevención, promoción y atención de la salud", [Documento sin paginación].

informado y cuenta con un mayor número de profesionales sanitarios que interactúan entre ellos acerca de su salud y cuidado.

Por tanto, la e-Salud supone una mejora significativa en la eficiencia del sistema sanitario, en la medicina preventiva, generando así un perfil de paciente más concienciado y responsable con el cuidado de su salud. De hecho, precisamente se ha producido un cambio de paradigma en el funcionamiento de los centros sanitarios, especialmente con los profesionales sanitarios, donde la conectividad y la implantación de las TIC ha provocado una mayor interacción y cooperación tanto nacional como internacional entre ellos[159], así pues, por medio de plataformas virtuales y aplicaciones, médicos especializados de todo el mundo intercambian conocimientos, resultados de investigaciones y formación avanzada sobre sus especialidades[160].

Asimismo, mediante la incorporación de la e-Salud en el sistema sanitario, se han creado centros sanitarios virtuales desde donde se gestionan y administran los diferentes servicios, proporcionando una información más amplia y una mayor atención al ciudadano.

En concreto, por medio de la Telemedicina los pacientes dependientes o crónicos son identificados a través de Etiquetas de Radiofrecuencia (RFID) que una vez implantados en el paciente mediante brazaletes o adheridas al mismo, transmiten mediante red inalámbrica datos clínicos del paciente a efectos de que en caso de riesgo

---

Asimismo, BARRERA, L.; GONZÁLEZ F.; VALENZUELA, J.; CEDEÑO, M.: *Impacto de las TICS en la Salud.* [on line] Disponible en: http://www.neopuertomontt.com/InformaticaMedica/lasticsenelsectorsalud.pdf [Documento sin paginación] señalan que "La eSalud se define como la aplicación de las Tecnologías de Información y Comunicación (TIC) en el amplio rango de aspectos que afectan el cuidado de la salud, desde el diagnóstico hasta el seguimiento de los pacientes, pasando por la gestión de las organizaciones implicadas en estas actividades. En el caso concreto de los ciudadanos, la eSalud les proporciona considerables ventajas en materia de información e incluso favorece la obtención de diagnósticos alternativos. En general, para los profesionales, la eSalud se relaciona con una mejora en el acceso a información relevante, asociada a las principales revistas y asociaciones médicas, con la prescripción electrónica asistida y, finalmente, con la accesibilidad global a los datos médicos personales a través de la historia clínica informatizada (HCI)". Disponible en https://www.infotec.mx/es_mx/infotec/que_es_salud_electronica_esalud, (última consulta 25/02/20)

[159] BEBEA GONZÁLEZ, MARTÍNEZ FERNÁNDEZ y REY MORENO, *Guía de la Cooperación Española para la incorporación…*", *op. cit.,* pp. 1-2.

[160] A los efectos, a modo de ejemplo se cita el eCIE10ES Edición electrónica de la *CIE-10-ES Diagnósticos,* 3ª Edición, enero 2020. Clasificación internacional de enfermedades 10.ª revisión, modificación clínica. Edición española, Ministerio de Sanidad, Consumo y Bienestar Social. Dirección General de Salud Pública, Calidad e Innovación. Subdirección General de Información Sanitaria: https://eciemaps.mscbs.gob.es/ecieMaps/browser/index_10_mc.html

se pueda asistir al mismo de manera inmediata, además permiten una localización en tiempo real del enfermo[161]. De igual modo, los biosensores son otra tecnología que, tras ser implantados en el enfermo, permiten detectar, analizar y transmitir en tiempo real datos sobre su estado de salud. Ambos sistemas, son los más utilizados actualmente en la sanidad a efectos de generar notificaciones de alertas en situaciones de urgencia, proporcionado una rápida e instantánea asistencia al enfermo por parte de los equipos sanitarios móviles.

Por último, debe tenerse en cuenta que en la actualidad el sistema informático de gestión de la historia clínica implantado en nuestro país es el Selene*,* a efectos de orientar al paciente en el dominio de la salud y de permitir una red integrada de salud, en el que todos los actores del sector sanitario estén interconectados y sea el paciente la base principal conductora de la relación entre los diferentes facultativos médicos independientemente del lugar de la asistencia sanitaria efectuada y del lugar de residencia común del paciente.

A continuación, se diferenciará, por un lado, entre las fuentes de datos sanitarios almacenados internamente en los ficheros de los organismos públicos y/o privados, centrándonos fundamentalmente en la historia clínica electrónica como fuente principal de datos de salud, destacándose a su vez entre otros, la historia clínica de salud, la receta electrónica y las imágenes médicas y, por otro lado, entre las fuentes de datos externas a los ficheros de los centros sanitarios (públicos y privados) como son los registrados en las redes sociales.

[161] Centro Nacional de Excelencia Tecnológica en salud, *¿Qué es la Telesalud y la Telemedicina?,* 2017, [Documento sin paginación]. Disponible en: https://www.gob.mx/salud/cenetec/acciones-y-programas/que-es-la-telesalud-y-la-telemedicina (última consulta 02/03/20).

1. LAS PRINCIPALES FUENTES DE DATOS SANITARIOS ALMACENADOS INTERNAMENTE EN LOS FICHEROS DE LOS ORGANISMOS SANITARIOS PÚBLICOS Y/O PRIVADOS

La digitalización e informatización en los procesos de gestión y administración tanto en los organismos públicos como en las entidades privadas, ha venido provocando a lo largo de los últimos años un gran volumen de recopilación de datos en ambos sectores. En consecuencia, surge la necesidad de gestionar, analizar y extraer la información y el conocimiento de aquellos datos que debido a su complejidad resultan de gran interés por el valor que aportan. Evidentemente, ni los servicios sanitarios ni la investigación en medicina han quedado al margen de estos avances, siendo el sector sanitario uno de los más afectados puesto que mediante la implantación de las TIC se han creado nuevos modelos de organización y gestión de la salud, generándose a su vez, nuevos conceptos de globalidad e interoperabilidad[162]. De lo anterior, se desprenden dos consecuencias: por un lado, que dispongamos en tiempo real de mayor cantidad de información al generarse grandes volúmenes de datos a altas velocidades, a consecuencia de la implantación de la historia clínica electrónica, de las recetas electrónicas, de las imágenes médicas en 3D, de las secuencias genómicas de datos de población, de los lectores de los sensores biométricos o los dispositivos *wereables*, de los datos generados por los dispositivos móviles y sus aplicaciones y, de los medios sociales en general; por otro lado, la necesidad de gestionar y analizar el conocimiento y la información clínica procedente de los datos depositados en las TIC y en el IoT.

En este contexto cabe diferenciar entre información clínica e información sanitaria, donde la información clínica engloba aquellos datos (independientemente de su forma, clase o tipo) que proporcionan o amplían conocimientos acerca del estado de salud de un ciudadano, o la manera de preservar, cuidar, mejorar o recuperar la salud y; la información sanitaria que es la información procedente de la atención sanitaria que recibe una persona, ya sea en atención primaria, especializada o sociosanitaria, generándose a su vez información sobre su estado de salud. Por consiguiente, cuando un profesional sanitario recoge debidamente en un documento información acerca del

[162] WORLD HEALTH ORGANIZATION, "Essential health technologies", *Geneva: WHO*, 2011 [Documento sin paginación]. Documento disponible en: http://www.who.intaspx (última consulta 17/06/18).

estado de salud de un ciudadano, se está generando a su vez información clínica sobre el mismo.

Tradicionalmente, la fuente de información clínica más relevante hasta la fecha ha sido y es la historia clínica, compuesta por una serie de documentos, ya sean escritos o gráficos, que recogen datos, valoraciones e información acerca de los procesos de salud y enfermedad de los pacientes, así como las acciones de índole sanitaria efectuadas en relación con los mismos. Por otro lado, la historia clínica cumple con diferentes funciones, pues además de su función puramente asistencial destinada a la protección de la información petrográfica con objetivo de proporcionar una atención eficaz, es un instrumento de gran utilidad en la docencia, en la investigación biomédica (destacándose la clínica y la epidemiológica), en la gestión clínica y planificación de recursos asistenciales, en el marco jurídico legal (puesto que de por sí es un testimonio documental de la asistencia prestada) y, en el control de calidad asistencial[163].

A pesar de lo anterior, la historia clínica convencional planteaba diversas dificultades, como las deficiencias de gestión debido al desorden documental, información ilegible, difícil acceso a la información por otros facultativos sanitarios, errores en el archivo, altos riesgos de confidencialidad y seguridad – debido a que la historia circulaba libremente por todo el centro sanitario – fácil deterioro y extravío del soporte documental y, dificultad de separación de los datos de filiación con los clínicos. No obstante, las anteriores dificultades fueron subsanadas fácilmente con la entrada de la historia clínica electrónica a consecuencia de la incorporación de las TIC el núcleo de la actividad sanitaria, suponiendo además la creación de un sistema integrado de información y, siendo igualmente, una herramienta de análisis tanto de los profesionales como de la organización de los centros sanitarios.

Por ende, tras la implantación de las TIC en el sistema sanitario, éstas se han convertido en herramientas clínicas fundamentales mediante las cuales los servicios de salud procesan gran cantidad de información, “este fenómeno, se observa en todas las

[163] Previamente a la existencia de las TIC en el sistema sanitario, las fuentes tradicionales de los datos sanitarios eran principalmente los registros médicos personales, la historia clínica convencional, las imágenes médicas, los ensayos clínicos y pruebas de laboratorio, los informes de altas, los datos a nivel genético y los datos procedentes de los Rayos X.

facetas de la actividad, como las de prevención y promoción, las puramente asistenciales, las de evaluación y las de gestión de calidad. Todas han incorporado las TIC a su quehacer diario"[164]. De este modo, las TIC han innovado una mejora de la eficiencia en la gestión en las organizaciones sanitarias, facilitando la comunicación e intercambio de información entre los profesionales médicos independientemente del centro sanitario al que pertenezcan. Por otro lado, las TIC han tenido una significativa repercusión en la calidad de vida de los ciudadanos, puesto que, gracias a las mismas, se han desarrollado estrategias, herramientas y otros servicios sanitarios de interés social en el ámbito de la sanidad[165].

Debido a lo anterior, resulta imprescindible partir de un análisis de las principales fuentes de datos sanitarios de las TIC y el IoT en los servicios sanitarios, como en los siguientes apartados se detallará.

1.1. Previo estudio de la historia clínica electrónica del Sistema Nacional de Salud y su regulación jurídica

No parece que exista duda, como se ha puesto de manifiesto, que una de las fuentes principales de datos sanitarios son las historias clínicas, en papel (cada vez menos) y, electrónicas (cada vez más), a pesar de que actualmente siguen existiendo ambas, es objetivo que en el futuro la historia clínica electrónica suplante por completo a la de papel. Por ello, a continuación, se realizará un estudio exhaustivo de la historia clínica electrónica tanto de una perspectiva sanitaria, como jurídica.

En el año 2006 fue delimitado en España el *Proyecto de Historia Clínica Digital en el Sistema Nacional de Salud* con la finalidad principal de que el pudiera ser atendido en cualquier lugar y servicio del Sistema Nacional de Salud teniendo acceso cualquier facultativo sanitario a su información clínica previa. Las principales garantías y objetivos del citado proyecto, consistían en: (1) garantizar el acceso a los datos de salud mediante vía telemática al ciudadano disponibles en formato digital en cualquiera de los

[164] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2017, [Documento sin paginación]. Documento disponible en: http://seis.es/indice-2017/ (última consulta 10/07/18).

[165] BARRERA, GONZÁLEZ , VALENZUELA y CEDEÑO, "Impacto de las TICS en*... ", op. cit.,* [Documento sin paginación].

Servicios de Salud del SNS, bajo la protección de sus datos ante aquellos terceros no autorizados al acceso; (2) garantizar a los facultativos sanitarios de un determinado centro sanitario del SNS el acceso de los datos sanitarios de aquellos ciudadanos que requirieran sus servicios profesionales residentes en otras Comunidades Autónomas y; (3) propiciar la seguridad de acceso a los datos sanitarios en el SNS a fin de garantizar al ciudadano la confidencialidad de los datos de carácter personal relativos a su salud y, generar un acceso ágil y sencillo a los datos sanitarios en el servicio común del SNS[166].

Por tanto, hasta ese momento cada Comunidad Autónoma contaba con sistemas automatizados de recogida y gestión de los datos individuales de salud, lo que proporcionaba un acceso directo a la información, mejorando la calidad de los procesos asistenciales. El desarrollo del citado proyecto se debe al hecho de que cada vez era más frecuente la movilidad de los ciudadanos dentro del territorio español, lo que conllevó a la necesidad de que cualquier facultativo sanitario pudiera acceder a la información sanitaria de cualquier ciudadano español independientemente del su lugar de residencia. De esta manera, el acceso a la información sanitaria proporcionada mediante las TIC se ampliaba a todo el territorio nacional, lo que conllevaba que cada paciente fuera acompañado en todo momento y en cualquier lugar de su información sanitaria.

En síntesis, otros de los objetivos del proyecto por parte de los actores implicados en el mismo fue el desarrollo de un diseño trascendental donde quedaran aglutinados aquellos datos sanitarios relevantes y esenciales del paciente, no en tanto en cuanto, permitir el acceso indiscriminado por parte del profesional de un centro sanitario de otra comunidad autónoma a toda la información clínica disponible, sino más bien el acceso a aquellos datos sanitarios de relevante interés. De ahí la creación de un sistema que permitiera el acceso libre de los datos relevantes de salud del paciente a fin de mejorar la calidad de la asistencia sanitaria y, a su vez salvaguardar el derecho de los ciudadanos a la intimidad de los datos relativos a su salud, finalidad que se pudo conseguir mediante un buen uso de las tecnologías de la información y las comunicaciones (TIC)[167].

---

[166] *Vid.* enlace web del Ministerio de Sanidad, Consumo y Bienestar Social sobre el contexto general de la Historia Clínica Digital en el Sistema de Salud (SNS): https://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/Antec_e_historial.htm

[167] PÉREZ SANTONJA, T., GÓMEZ PAREDES, L., ÁLVAREZ MONTERO, S., CABELLO BALLESTEROS, L. y MOMBIELA MURUZABAL, M.T., "Historia clínica electrónica: evolución de la relación médico-paciente en

Así pues, gracias a la incorporación de las tecnológicas en el SNS el citado proyecto se pudo llevar a cabo, así pues, en la actualidad mediante la Historia Clínica Digital en el Sistema Nacional de Salud (HCDSNS) los ciudadanos tienen acceso a una serie de datos personales sobre su salud, así como conocer del Registro de Accesos a los mismos y, seleccionar/elegir voluntariamente aquellos datos a los que no desea que acceda un profesional sanitario de otra Comunidad Autónoma.

Adicionalmente, cabe señalar que el proyecto fue elaborando, siguiendo una estrategia de seguridad y una estrategia tecnológica: (1) por un lado, en relación con la seguridad, al tratarse de datos sanitarios que requieren de una protección especial debido su carácter propiamente personal[168], toda persona que acceda a los mismos debe previamente identificarse electrónicamente. Igualmente, no todos los profesionales sanitarios tienen acceso a los mismos datos, sino que el acceso estará restringido según la función que desempeñen y la certificación externa del sistema de gestión de seguridad de la información de todo el sistema de acuerdo con la norma internacional *ISO 27001*. Asimismo, los propios ciudadanos van a ser auditores externos del seguimiento de los accesos realizados a sus datos de salud; (2) por otro lado, en relación con la medida tecnológica, el proyecto se elaboró en base al principio de neutralidad tecnológica, a fin de agilizar interoperabilidad entre los sistemas de las Comunidades Autónomas, de tal modo, que se facilite el intercambio de información entre las Comunidades Autónomas, así como el acceso a la misma, procediéndose a su vez a las comunicaciones independientes entre los sistemas de la plataforma tecnológica utilizada para el intercambio de información entre aplicaciones se emplea la mensajería XML y, el protocolo de comunicación HTTPS.

Finalmente, la implantación generalizada del Proyecto se inició a partir del año 2010, siendo recogido el acuerdo sobre el *Conjunto Mínimo de Datos de Informes Clínicos* por medio del Real Decreto 1093/2010, de 3 de septiembre, por el que se

---

la consulta de Atención Primaria", *Semergen,* vol. 43, núm. 3, 2016 pp. 175-181. Documento disponible en: http://dx.doi.org/10.1016/j.semerg.2016.03.022 (última consulta 12/03/20).

[168] GÓMEZ SÁNCHEZ, Y., "Datos de salud como datos especialmente protegidos", en AA.VV., *Comentario a la Ley Orgánica de Protección de datos de carácter personal* (Dir. A. Troncoso Reigada), Ed. Civitas, Madrid, 2010, p. 647.

aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud. Asimismo, el Ministerio de Sanidad, Servicios Sociales e Igualdad señaló que:

"[…] ha venido suscribiendo, desde el año 2006, una serie de convenios marco con el Ministerio de Energía, Turismo y Agenda Digital y con la entidad pública empresarial Red.es para la agregación de fondos económicos y el desarrollo operativo de los proyectos de interoperabilidad en el Sistema de Salud […] Amparados en dichos convenios marco se han suscrito, a su vez, convenios específicos con cada comunidad autónoma con el fin de cofinanciar las actuaciones de interoperabilidad en el SNS, tanto de la historia clínica, como de la tarjeta sanitaria y de la receta electrónica"[169].

Por consiguiente, la HCDSNS tiene como finalidad principal la de proporcionar el acceso de los datos sanitarios desde cualquier lugar del Sistema Nacional de Salud a los ciudadanos y a los profesionales sanitarios se crea la historia clínica digital, según establece el *Informe de Situación del Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud* emitido por el Ministerio de Sanidad, Consumo y Bienestar Social en julio de 2018:

"El objetivo principal de este servicio es permitir que los pacientes puedan ser atendidos en cualquier dispositivo asistencial del Sistema Nacional de Salud con la garantía de disponer de su información clínica preexistente. Para ello, pone a disposición de los profesionales sanitarios autorizados por cada Comunidad Autónoma[170], una serie de informes clínicos del paciente con información relevante para su atención"[171].

[169] GÓMEZ SÁNCHEZ, "Datos de salud como datos especialmente…", *op. cit.,* p. 647.

[170] "Baleares, Comunidad Valenciana y La Rioja fueron las primeras comunidades en incorporarse a este servicio a través de un proyecto piloto el año 2009; tras ellas se produjo una adhesión gradual del resto, quedando únicamente pendiente en este momento la incorporación de Cataluña" (Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud, Julio 2018).

[171] Ministerio de Sanidad, Consumo y Bienestar Social, *Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud,* 2018. Documento disponible en: https://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/WEB_Informe_de_Situacion_HCDSNS_Julio_2018.pdf (Consultado 21/07/18).

Además, el sistema permite que cada ciudadano pueda acceder por vía telemática a los conjuntos definidos de datos acerca de su salud que se encuentren a su disposición digitalmente en los Servicios de Salud del SNS, siempre y cuando el ciudadano disponga de identificación electrónica.

De un lado, el informe detalla que, de los dieciocho Servicios de Salud existentes en España, diecisiete han activado el perfil emisor, donde la base de datos central de referencias de pacientes que cuentan con contenidos interoperables disponibles es cargada y actualizada por los Servicios de Salud, igualmente, "el servicio de alta de referencias se monitoriza de forma continuada con el fin de detectar y resolver incidencias en su funcionamiento"[172].

De otro lado, según el citado *Informe de Situación* de 2018, en fecha 1 de julio se registró una cobertura de población con referencias HCDSNS, en cifras absolutas de 36.100.087 ciudadanos[173] y, una cobertura del 77,36 % en relación con la población de Tarjeta Sanitaria Individual (TSI)[174]. De modo semejante, en relación con la historia clínica resumida (HCR), la emisión de la HCR se encuentra activada desde un total de quince Servicios de Salud y, "la cobertura estimada de disponibilidad de este documento, en relación con la población que dispone el TSI, es del 62,69% en el conjunto del SNS"[175].

Por último, sobre el *Anillo de Intercambio*, el citado informe detalla que es una infografía que viene a reflejar con gran detalle la situación de cada Servicio de Salud, sin dejar de lado la perspectiva general de la situación propia en el Sistema Nacional de Salud[176].

---

[172] Ministerio de Sanidad, Consumo y Bienestar Social, *Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud,* 2018, p.5.

[173] Según el Instituto Nacional de Estadística la población española en julio de 2018 ascendía a la suma total de 46.659.302 habitantes.

[174] Ministerio de Sanidad, Consumo y Bienestar Social, *Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud,* 2018, p. 5.

[175] Ministerio de Sanidad, Consumo y Bienestar Social, *Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud,* 2018, p. 9.

[176] Ministerio de Sanidad, Consumo y Bienestar Social, *Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud,* 2018, p. 10.

A) Datos esenciales procedentes de los informes clínicos que conforman el contenido de la historia clínica digital en el Sistema Nacional de Salud

La HCDSNS engloba todos aquellos datos clínicos que aportan información relevante del paciente para una atención sanitaria de calidad en cualquier territorio español fuera de su residencia habitual. En concreto, la historia clínica digital se encuentra conformada por siguientes documentos de información sanitaria: el informe clínico de alta, el informe clínico de consulta externa, el informe clínico de urgencias, el informe clínico de atención primaria, el informe de cuidados de enfermería, el informe de resultados de pruebas de imagen, el informe de resultados de pruebas de laboratorio, el informe de resultados de otras pruebas diagnósticas y la historia clínica resumida.

En consecuencia, el registro de información con carácter personal en la HCDSNS es propiamente estructurado al seguir una plantilla de recogida de estos mediante formularios preestablecidos de contestación libre, donde se combina el texto libre con los datos estructurados. A continuación, se desglosa el conjunto mínimo de datos de los citados informes clínicos incluidos en la HCDSNS de conformidad con el Proyecto promovido por la Agencia de Calidad del Sistema Nacional de Salud e Instituto de Información Sanitaria del Ministerio de Sanidad, Consumo y Bienestar Social (en adelante Proyecto del IIS)[177].

De manera general, en cada uno de los informes clínicos constan los siguientes datos: (a) Datos del Documento: tipo de documento; fecha de firma; fecha de ingreso; fecha de alta; nombre y apellidos del responsable 1; categoría profesional 1[178]; nombre y apellidos responsable 2; categoría profesional 2[179]; servicio y unidad; (b) Datos de la Institución Emisora: denominación del Servicio de Salud; denominación del provisor de servicios; denominación del centro y dirección del centro; (c) Datos del Paciente: nombre; apellidos; fecha de nacimiento; sexo; DNI/T. Residencia/Pasaporte; NASS;

[177] Para el desarrollo del presente epígrafe se ha tomado como base el *Informe Historia Clínica Digital en el Sistema Nacional de Salud. Conjunto mínimo de datos de Informes Cínico* de la Agencia de Calidad del Sistema Nacional de Salud. Instituto de Información Sanitaria, Gobierno de España, Ministerio de Sanidad y Consumo y Bienestar Social. Documento disponible en: http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/CMDIC.pdf (Última consulta 27/07/18).

[178] A elegir entre: Médico Residente, Facultativo Especialista de Área, Jefe de Sección, Jefe de Servicio.

[179] A elegir entre: Facultativo Especialista de Área, Jefe de Sección, Jefe de Servicio.

CIP de C. Autónoma; código SNS; CIP Europeo; N.º historia clínica; domicilio y teléfono.

Particularmente, cada informe recoge diferentes datos sanitarios según su tipología, existiendo así una gran diversidad de informes: (1) Informe de Alta de Hospitalización[180]; (2) Informe de Consulta Externa de Especialidades[181]; (3) Informe de Urgencias[182]; (4) Historia Clínica Resumida (HCR)[183]; (5) Informe Clínico de

[180] En relación a los datos del *proceso asistencial*, resulta relevante la siguiente información sanitaria: motivo de alta (traslado a domicilio, traslado de servicio, traslado a otro centro hospitalario, traslado a un centro sociosanitario, alta voluntaria, fallecimiento, otros); motivo de ingreso; tipo de ingreso (urgente/programado); antecedentes (enfermedades familiares hereditarias, enfermedades preventivas, antecedentes neonatales, obstétricos y quirúrgicos, alergias, hábitos tóxicos, actuaciones preventivas, medicación previa, situación funcional; antecedentes sociales y profesionales); historia actual, exploración física; resumen de pruebas complementarias (laboratorio, imagen y otras pruebas); evolución y comentarios; diagnostico principal; otros diagnósticos; procedimientos; otros procedimientos; tratamiento (recomendaciones/fármacos); otras recomendaciones.

[181]Resultan de interés los datos en relación al motivo de consulta; antecedentes (enfermedades familiares hereditarias, enfermedades preventivas, antecedentes neonatales, obstétricos y quirúrgicos, alergias, hábitos tóxicos, actuaciones preventivas, medicación previa, situación funcional; antecedentes sociales y profesionales); historia actual, exploración física; resumen de pruebas complementarias (laboratorio, imagen y otras pruebas); evolución y comentarios; diagnostico principal; otros diagnósticos; procedimientos; otros procedimientos; tratamiento (recomendaciones/fármacos); otras recomendaciones.

[182] Acerca de los datos de la institución emisora además de los datos generales anteriormente referenciados, se incluye como novedad un apartado sobre la dirección Web/Correo Electrónico. Asimismo, en los datos del paciente se incorpora además de los datos generales, nombre y apellidos de la persona de referencia y su teléfono. Sobre los datos de proceso asistencia, en el informe de urgencia, resultan de interés aquellos datos referentes a la procedencia; tipo de consulta (enfermedad, accidente de tráfico, accidente laboral, otros accidentes); motivo de alta (traslado a domicilio, traslado de servicio, traslado a otro centro hospitalario, traslado a un centro sociosanitario, alta voluntaria, fallecimiento, otros); motivo de consulta; antecedentes (enfermedades previas, antecedentes neonatales, obstétricos y quirúrgicos, medicación previa, alergias, situación funcional, antecedentes sociales y profesionales); historia actual; exploración física (TA, FC, FR, temp., Saturación O_2, Glucemia capilar, Resumen exploración); resumen pruebas complementarias (laboratorio, imagen y otras pruebas); evolución y comentarios[182]; diagnóstico principal; otros diagnósticos; procedimientos; otros procedimientos; tratamiento (recomendaciones/fármacos); otras recomendaciones.

[183] La historia clínica resumida (HCR) es el documento más relevante, puesto que le proporciona tanto a los profesionales como a los pacientes los principales datos clínicos desde diversas fuentes de información primaria. Actualmente, se encuentra activada su emisión a un total de 15 Servicios de Salud, lo que supone, una cobertura de disponibilidad en relación con la población que dispone de TSI, de un 62,69% (Datos aportados por el *Informe de Situación del Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud* emitido por el Ministerio de Sanidad, Consumo y Bienestar Social de julio de 2018). En relación con los datos del paciente se incorpora además de los datos generales, nombre y apellidos de la persona de referencia, su teléfono, así como nombre y apellidos del cuidador principal. En concreto, sobre los *datos de salud*, en la HCR resulta de interés conocer los siguientes extremos: si existe o no información reservada por decisión del paciente; si existe o no documento de instrucciones previas; si está o no incluido en protocolo de investigación clínica; alergias; vacunaciones; problemas resueltos, cerrados o inactivos; problemas y episodios activos; tratamiento (Recomendaciones y Fármacos activos en la fecha de actualización); diagnóstico enfermeros activos; resultados de enfermería; intervenciones de enfermería; alertas; observaciones subjetivas del profesional.

Atención Primaria[184]: (6) Informe de Resultados de Pruebas de Laboratorio[185]; (7) Informe de Resultados de Pruebas de Imagen[186]; (8) Informe de Cuidados de Enfermería[187].

En definitiva, se podría afirmar que mediante la HCDSNS se genera de manera constante a gran velocidad un gran volumen de datos variables, verídicos y de inestimable valor. En concreto, según datos sobre Tecnologías de la Información y Comunicación (TIC) en Sanidad aportados por el *Informe ÍNDICE SEIS*, en el año 2017

[184] En el caso del *Informe Clínico de Atención Primaria* también resultan de interés los datos de la persona referencia (nombre, apellidos y teléfono). Por su parte, en relación a los datos de salud es de suma relevancia conocer si el paciente tiene antecedentes (enfermedades familiares hereditarias, enfermedades previas, antecedentes neonatales, obstétricos y quirúrgicos, alergias, hábitos tóxicos, actuaciones preventivas, medicación previa, situación funcional, antecedentes sociales y profesionales; resumen de pruebas complementarias (laboratorio, imagen y otras pruebas); resumen de episodios atendidos; evolución y comentarios; diagnósticos; procedimientos; tratamiento (recomendaciones/fármacos) y otras recomendaciones en relación a planes de actuación previstos que no son propiamente medidas terapéuticas.

[185] En relación al *Informe de Resultado de Pruebas de Laboratorio*, los datos sanitarios relevantes son los referentes a los del proceso asistencial, donde por un lado quedan detallados los datos de la muestra (fecha de toma de muestras, número de muestras, tipo de muestra, grupo de determinación) y, por otro lado, los datos de resultados, que se subdividen a su vez en: *Modelo de TIPO A*, son resultados de pruebas diagnósticas expresados en cifras que hacen referencia a unidades de medida utilizadas y un rango de valores de referencia que se toman como estándar de normalidad y, *Modelo de TIPO B*, que son resultados de pruebas diagnósticas que requieren de una descripción y una conclusión en texto libre.

[186] Con relación a los datos del paciente en el Informe de Resultados de Pruebas de Imagen, se incluye además de los datos generales, el dato referente al número de cama o número de consulta. En concreto, en el citado informe son datos relevantes los datos del proceso asistencial, donde consta la información clínica (justificación de la realización de la prueba y sospechas diagnosticas), exploración, fecha de exploración, descripción detallada de la exploración (prioridad, medios de contraste, reacciones adversas, otros incidentes y abordaje de los mismos, limitaciones técnicas, exploración con la que se compara y fecha de la misma), hallazgos (descripción detallada de los hallazgos, donde se destacan los hallazgos negativos, comparación con estudios previos y limitaciones diagnósticas), diagnóstico y recomendaciones (cuidados o tratamientos que se deben seguir después de la realización de la exploración diagnóstica o intervencionista) e indicación de otras exploraciones que se deben realizar para completar el estudio del paciente o el plazo en el que se debe realizar un control de la exploración.

[187] Los datos que resultan relevantes en el documento son los de las enfermeras responsables (1 y 2) que han atendido al paciente, los cuales son sustituidos por los del responsable profesional. Igualmente, en relación a los datos del proceso asistencial, son de interés: las causas que generan la actuación enfermera; el motivo de alta/derivación enfermera (ingreso, traslado a domicilio, traslado de servicio, traslado a centro hospitalario, traslado a un centro sociosanitario, alta voluntaria, fallecimiento, otros); antecedentes y entorno (enfermedades previas, intervenciones quirúrgicas, tratamientos farmacológicos, alergias, actuaciones preventivas, factores personales, familiares, sociales culturales y laborables, destacables); diagnósticos enfermeros resueltos; protocolos asistenciales en los que está incluido; valoración activa (modelo de referencia utilizado, resultados destacables); diagnósticos enfermeros activos (aquellos diagnósticos presentes en el momento de la elaboración del informe, tanto reales como potenciales); resultados de enfermería (aquellos resultados seleccionados para identificar la evolución del paciente, como resultado de las intervenciones planificadas); intervenciones de enfermería (las intervenciones que se están llevando a cabo en el momento de elaboración del informe); cuidador principal (donde deberá indicarse tanto el nombre como la relación – familiar, cuidador externo…- que tiene con él) e información complementaria/observaciones.

se generaron 2.047.624 Giga Bytes en las exploraciones médicas (imágenes), lo que conlleva una variación del 55,19% respecto al año 2016. Asimismo, según consta en el citado informe, en el año 2017 fueron inscritas entre Atención Primaria y Atención Especializada más de 49.300 historias clínicas electrónicas en España, lo que supone un crecimiento del 5 % de las personas que pueden acceder a sus datos de HCE a través de internet, lo que acredita a su vez, una tendencia continuada en la implantación de la HCE por parte de los centros hospitalarios.

B) Regulación jurídica y aspectos legales de la historia clínica electrónica

La HCE actualmente se encuentra regulada, por un lado, por la legislación sanitaria, mediante la Ley General de Sanidad, de 25 de abril de 1986, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, asimismo, diversas Comunidades Autónomas han dictado normas con rango de Ley sobre la materia, como la Ley 21/2000 de Cataluña, la Ley 3/2001 de Galicia, la Ley Foral 11/2002 de Navarra y el Decreto 45/1998 del País Vasco.

En concreto, el artículo 5 d la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, y la Disposición Adicional Tercera, de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente, de manera imperativa, regulan el deber del Ministerio de Sanidad, Servicios Sociales e Igualdad, de coordinar los mecanismos de intercambio electrónico de información clínica y salud individual para permitir el acceso a profesionales y usuarios, en los términos estrictamente necesarios para garantizar la calidad de la asistencia y la confidencialidad e integridad de la información. De ahí que se adoptaran entre todos los Servicios de Salud elementos de interoperabilidad, como el de aplicar criterios de normalización de la información y el desarrollo de una Intranet sanitaria del Sistema Nacional de Salud, facilitando a su vez la protección de la salud de los ciudadanos, independientemente de que cualquier médico u otro facultativo de servicio de salud del lugar donde un ciudadano precise atención sanitaria pueda acceder a su información sanitaria.

En este sentido, la normativa sobre protección de datos de carácter personal también ha estatuido preceptos sobre la HCE. En concreto, la Ley Orgánica 15/1999, de 13 de diciembre y las normas dictadas en su desarrollo, entre las que resultan relevantes el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

Desde un punto de vista jurídico, se derivan algunos aspectos en relación con la historia clínica electrónica: (a) Obligatoriedad de informar al interesado de la existencia de la HCE (el fichero) y de la identidad y dirección de su responsable, según la normativa de protección de datos; (b) No se exige el consentimiento del interesado para el tratamiento informatizado de los datos contenidos en la HCE; (c) Por medio de regulación legal, se admite expresamente la HCE, como soporte de la información de salud de las personas. El citado soporte puede sustituir a los informes en papel, teniendo los datos el mismo valor legal que los contenidos en la historia clínica en soporte de papel; (d) Derecho del paciente de acceder a los datos de su historia clínica, a excepción de los datos confidenciales que pudieran afectar a terceras personas y que han sido recabados en interés terapéutico del paciente, de las anotaciones subjetivas del profesional y de los datos cuyo acceso deba limitarse al paciente por razones justificadas de necesidad terapéutica. De igual modo, previo consentimiento del paciente, en caso de fallecimiento, los familiares y allegados pueden acceder a los datos clínicos siendo de aplicación las excepciones anteriormente mencionadas; (e) Actualmente, existe una laguna legal en relación con la conservación de la historia clínica y a las condiciones de cancelación de los datos contenidos en la misma; (f) Acceso exclusivo a los datos sanitarios por parte de aquellos profesionales que participen en el tratamiento y diagnóstico del paciente, siempre y cuando quede constancia previamente de la identificación del profesional en el documento de seguridad, en los procedimientos de identificación y autentificación y, en el registro de accesos; (g) Autorización de la cesión o comunicación de los datos sanitarios contenidos en la HCD, sin necesidad de que exista previo consentimiento del interesado, en los supuestos de: (1) cesión a Jueces y Tribunales, el Defensor del Pueblo, el Ministerio Fiscal y el Tribunal de Cuentas; (2) de situación de urgencia; (3) estudios epidemiológicos, actuaciones en materia de salud pública, investigación y docencia, si bien previa anonimización de los datos; (4) para el ejercicio de funciones de

inspecciones, evaluación, acreditación y planificación sanitarias; (h) Desde el ámbito penal, se regula como delito el simple acceso no autorizado a datos reservados de carácter personal; (i) En materia civil, la vulneración de la confidencialidad constituye un daño moral indemnizable; (j) Desde la vía administrativa, se garantiza la reserva y confidencialidad de la información clínica, mediante el régimen de infracciones y sanciones dispuesto por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Lo anterior nos conduce a la conclusión de que la HCD presenta en comparación con la historia clínica tradicional, un mayor grado de exigencias y de garantías, cuya perspectiva legal será desarrolla más adelante, donde se tratará sobre todo el derecho de confidencialidad del paciente[188].

En definitiva, la HCD es una herramienta de gran potencial e interés común, tanto para los servicios sanitarios como para el ciudadano, puesto que permite un acceso rápido, casi inmediato, al conocimiento y, poder disponer de mayor cantidad de información, permitiendo al profesional y al centro sanitario conocer con detalle la historia clínica de un paciente en cualquier momento y en cualquier lugar. Tales son los beneficios de la HCD que mediante el proyecto *Smart Open Services for European Patients* (epSOS) promovido por doce países de la UE que tienen implantada la HCD, se pretende que un profesional que asista a un paciente de otro país de UE pueda acceder a su historia clínica resumida y, que un medicamento pueda dispersarse en un país distinto al que fue prescrito[189].

---

[188] En este sentido, MEDRANO, J. y PACHECO, L., "Historia clínica electrónica y confidencialidad", *Rev. Asoc. Esp. Neuropsiq*., vol. 35, núm. 126, 2015, p. 249. Documento disponible en: doi: 10.4321/S0211-57352015000200001 (última consulta 03/04/19) señalan que: "Uno de los más notables acontecimientos recientes de nuestra realidad sanitaria es la progresiva importancia que ha adquirido la confidencialidad (clásica y corporativamente englobada en el llamado secreto médico) y, en paralelo, los temores de que la historia clínica electrónica (HCE) se convierta en una especie de libro abierto al que pueda acceder cualquier persona, comprometiendo el derecho del paciente a que sus confidencias queden exclusivamente en el marco de la relación asistencial".

[189] Smart open services for european patients, *Stockholm: epSOS,* [Documento sin paginación]. Documento disponible en: https://www.itu.int/net4/wsis/stocktaking/projects/Project/Details?projectId=1399467257 (Última consulta 11/06/18).

C) La tarjeta sanitaria: sistema de identificación esencial de los pacientes

En síntesis, como se ha podido observar en el apartado anterior, la historia clínica electrónica engloba toda la información sanitaria de un ciudadano, independientemente del momento y el lugar en que se haya generado. Igualmente, resulta imprescindible que este sistema clínico se encuentre incluido en un sistema de información del servicio de salud vinculado y relacionado con los sistemas de gestión financiera, planificación estratégica y control de gestión, por lo que se requiere de manera imprescindible que previamente cada ciudadano sea identificado unívocamente.

Por consiguiente, debido a que los sistemas de identificación tradicionales en nuestro país, esto es, el Registro Civil, el Documento Nacional de Identidad y, el Documento de Afiliación a la Seguridad Social, resultaban insuficientes para englobar la información sanitaria de un ciudadano, puesto que carecían de la precisión que exigía la información clínica, además de no comprender la totalidad de la población a la que se le prestaba una atención sanitaria, a finales de la década de los ´80 y a principios de los años ´90 se incorpora en los servicios de salud españoles la identificación clínica de cada ciudadano mediante la asignación de una tarjeta sanitaria. De este modo, mediante la tarjeta sanitaria se accede a información electrónica acerca de un paciente con certeza de su identificación, así como de la identificación del profesional sanitario que produce esa información y del centro sanitario donde se ha atendido al mismo en un determinado momento.

Al respecto, también mediante los códigos nacionales o regionales de uso exclusivo sanitario de identificación personal de cada paciente, es creada una base de datos a disposición de los centros sanitarios que, por un lado, recopila la filiación de todos los ciudadanos con derecho a una asistencia sanitaria pública, por otro lado, identifica de manera unívoca a cada usuario del sistema sanitario y, finalmente acredita el derecho a las prestaciones de manera personal, trámite que hasta ese momento era responsable la administración de la Seguridad Social[190].

[190] Lo que ha generado el problema de confusión entre la identificación del usuario y la acreditación del derecho a las prestaciones por parte de algunos servicios de salud, debido a que únicamente a aquellos ciudadanos que tienen derecho a las prestaciones del sistema público, no siendo identificadas o teniendo graves dificultades de identificación aquellas otras personas que acceden al sistema sanitario por otras vías.

La creación y existencia de una base de datos a disposición de los centros sanitarios, genera la ventaja de que los datos sanitarios sean recopilados automáticamente y de manera estructurada mediante tablas, con sus atributos y relaciones entre las entidades básicas que participan en el desarrollo del sistema. Para ello, es imprescindible una identificación de cada usuario de utilización exclusiva para el sistema sanitario, por lo que se generan números secuenciales como clave de identificación de cada usuario de cuya asignación corresponde a cada comunidad autónoma. Por último, la tarjeta sanitaria permite un acceso seguro y confidencial a la información clínica en red, un almacenamiento de la información sanitaria de cada ciudadano y una automatización de tareas, para lo que se requiere previamente un cumplimiento de los procesos de seguridad, estándares de intercambio de información y tarjetas con chip.

En definitiva, la tarjeta sanitaria supone una herramienta fundamental que además de identificar de manera unívoca al paciente, profesional que lo ha atendido y centro de salud, almacena y trasporta la información sanitaria permitiendo a su vez un acceso seguro a la HCD.

1.2. Análisis de otras fuentes relevantes de datos sanitarios

Tras efectuarse un análisis exhaustivo de la historia clínica electrónica, como la fuente principal de datos sanitarios (en sustitución del papel), a continuación, se examinarán otras fuentes relevantes de datos sanitarios donde igualmente son aplicadas las herramientas *big data* para su análisis y posterior sustracción de conocimiento e información.

A) Historia electrónica de salud

La historia electrónica de salud (HES), está formada por un conjunto de datos registrados de manera heterogénea y manejables gracias a las TIC, puesto que mediante las TIC los datos son recopilados e integrados de manera dinámica independientemente de la forma en la que hayan sido registrados.

Tradicionalmente, los datos eran recogidos y presentados en informes en papel, pero mediante la implantación de las TIC los datos sanitarios son recogidos y presentados de manera electrónica en la HES mediante una pantalla o método de proyección (vista). Asimismo, la presentación puede ser referente a los datos de un ciudadano o de un colectivo mediante presentación agregada. Igualmente, los usuarios fundamentales de la HES son los servicios sanitarios, los servicios sociales, la salud pública, los gestores, los servicios administrativos y el ciudadano mediante una participación activa.

De igual modo, la HES supone que en el Servicio de Salud de una Comunidad Autónoma existe un sistema que permite el acceso "a los procesos de los pacientes de forma agregada y longitudinal con independencia del centro sanitario o ámbito asistencial dentro de la red sanitaria de utilización pública de la Comunidad Autónoma"[191]. Según el *Informe ÍNDICE SEIS 2017*, en España un total de dieciséis Comunidades Autónomas disponen de sistemas que soportan una HES única para cada ciudadano, lo que supone que el 92,84 % de la población protegida tienen una HES única y agregada, con independencia del centro de la red sanitaria pública de su comunidad de residencia. De las dieciséis Comunidades Autónomas, en catorce de ellas los ciudadanos pueden acceder a datos de sus HES a través de internet, en seis los ciudadanos pueden acceder a datos de sus HES a través de una APP específica para dispositivos móviles y en cinco Comunidades Autónomas, los ciudadanos pueden incorporar datos a sus HES a través de internet[192].

A todo ello, habría que añadir que actualmente gracias a la evolución de las TIC se están elaborando proyectos de incorporación de nuevos dispositivos a efectos de presentar los datos sanitarios, como los *tables PC* y de reconocimiento de voz y de escritura manual.

[191] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2018, p. 34. Documento disponible en: http://seis.es/indice-2017/ (Última consulta 10/07/18).

[192] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2018, p. 34.

B) La implantación de la receta electrónica

Indudable influencia para este desarrollo tendrá la implantación de la receta electrónica, pues como es sabido la prescripción de un medicamento por medio de un profesional sanitario mediante receta ya sea convencional o electrónica, es el tratamiento para seguir por parte del paciente fuera del centro de salud atendido por medio de suministro de un medicamento a consciencia de una enfermedad padecida y de un diagnóstico. Por consiguiente, el envase recetado es una fuente de información y de datos sanitarios de un ciudadano, puesto que permite disponer de información clínica, farmacológica y fármaco-económica completa y actualizada en el mismo momento de la prescripción, permitiendo a su vez realizar un seguimiento de la adherencia de las prescripciones a los tratamientos y del cumplimiento del mismo por parte del paciente, posibilitando al farmacéutico que pueda comunicar al profesional sanitario aquellas cuestiones relevantes para la salud del paciente acerca del tratamiento, de igual modo, el sistema informa del momento y lugar en el que el paciente ha retirado la medicación recetada.

Por medio del el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y ordenes de dispensación se implantó en España el Servicio de Receta Electrónica, a fin de que el ciudadano obtenga su medicación, por medios electrónicos, en cualquier oficina de farmacia de España independientemente del lugar donde se haya tramitado la prescripción sin necesidad de que presente una receta en papel, evitar tareas administrativas al profesional médico prescriptor en desplazamientos de pacientes fuera de la Comunidad Autónoma, avanzar en los sistemas de información permitiendo que las Comunidades Autónomas tengan acceso a las transacciones que se realizan entre ellas y que el SNS disponga de un sistema único e integrado de receta electrónica[193]. El ciudadano únicamente debe presentar en una oficina de farmacia para recoger un producto farmacéutico prescrito en otra comunidad autónoma la tarjeta sanitaria individual e indicar la comunidad autónoma donde le han realizado la prescripción a

[193] Subdirección General de Información Sanitaria e Innovación. Área de receta Electrónica del SNS (Coord. Subdirección General de Tecnologías de la Información), *Interoperabilidad de receta electrónica en el Sistema Nacional de Salud*, Dirección General de Salud Pública, Calidad e Innovación. Ministerio de Sanidad, Servicios Sociales e Igualdad. Documento disponible en: https://www.msssi.gob.es/profesionales/recetaElectronicaSNS/Doc_Bas_Proyect_Interop_RESNS_v2.1.pdf (Última consulta 1/08/18).

efectos de que el farmacéutico pueda acceder a su listado de productos dispensables[194]. De manera automática, una vez dispensado el producto, el sistema informa a la Comunidad Autónoma de prescripción de los productos y envases retirados, descontando los mismos de futuras dispensaciones.

Según establece el citado Proyecto de interoperabilidad de receta electrónica del SNS "la receta médica electrónica es una modalidad de servicio digital de apoyo a la asistencia sanitaria que permite al facultativo emitir y transmitir prescripciones por medios electrónicos, basados en las tecnologías de la información y comunicaciones, que posteriormente pueden ser objeto de dispensación."[195].

De conformidad a datos facilitados por el *Informe ÍNDICE SEIS 2017*, en el año 2017 se dispensaron un total de 937.016 envases por medio de receta, de los cuales 838.804 envases fueron dispensados mediante el sistema de receta electrónica por importe total de 10.638.409 (en miles de euros) suponiendo el 89,52% del total y, los restantes 98.212 por el sistema convencional, por la suma de 1.593.303 (en miles de euros) lo que supone tan sólo el 13,03% del total.

Asimismo, desde el año 2016, el Servicio de Receta Electrónica está operativo en el 100% de los 3.259 centros de salud españoles y en las 22.151 oficinas de farmacia que había es España. Por otro lado, tal y como establece el *Informe ÍNDICE SEIS 2017*, "según el Ministerio de Sanidad, Servicios Sociales e Igualdad, en enero de 2018, son catorce las comunidades autónomas que están en condiciones de intercambiar recetas (prescritas en una CA y dispensas en otra) a través del sistema de receta electrónica"[196]. De lo anterior, se deduce una evidente tendencia de intercambio de información y datos

[194] Los productos dispensables es la relación de productos farmacéuticos junto con el número de envases dispensables para cada uno de ellos que pueden ser dispensados por la oficina de farmacia. Actualmente, se pueden dispensar medicamentos autorizados e incluidos en las bases de datos del SNS, efectos y accesorios y, productos dietéticos contemplados en la cartera de servicios comunes del SNS.

[195] Subdirección General de Información Sanitaria e Innovación. Área de receta Electrónica del SNS (Coord. Subdirección General de Tecnologías de la Información), *Interoperabilidad de receta electrónica en el Sistema Nacional de Salud*, Dirección General de Salud Pública, Calidad e Innovación. Ministerio de Sanidad, Servicios Sociales e Igualdad, p. 2. Documento disponible en: https://www.msssi.gob.es/profesionales/recetaElectronicaSNS/Doc_Bas_Proyect_Interop_RESNS_v2.1.pdf (Última consulta 1/08/18).

[196] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2018, p. 37. Documento disponible en: http://seis.es/indice-2017/ (Última consulta 10/07/18).

relevantes a la salud de un paciente entre las distintas Comunidades Autónomas por medio del Servicio de Receta Electrónica.

Con relación a la regulación jurídica específica de la receta electrónica, la misma se encuentra recogida, por un lado, en la Ley 16/2003 de mayo, de cohesión y calidad del SNS, regula algunos aspectos en relación con la receta electrónica. Por otro lado, la Ley 29/ 2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios, hace referencia a normativa que regula la receta médica electrónica. Igualmente, el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y ordenes de dispensación, dedica el capítulo IV a la "Recta médica electrónica oficial del SNS", donde regula los criterios para su desarrollo, la coordinación en el SNS y otros aspectos. Por último, Real Decreto – ley 16/2012, de 20 de abril, de medidas urgentes para garantizar la sostenibilidad del SNS y mejorar la calidad y seguridad de las prestaciones, realiza modificaciones al Real Decreto 1718/2010 de receta médica y órdenes de dispensación.

C) Las tecnologías de imagen médica

De igual modo, las tecnologías de imagen médica son fuente relevante de datos sanitarios, resultando ser cada vez más esenciales para el diagnóstico médico y terapéutico, así como para detectar diferentes enfermedades[197].

En la actualidad, el sistema sanitario avanza hacía un cambio donde los sistemas convencionales como los rayos-X genéricos y ultrasonidos están siendo sustituidos por la miniaturización y portabilidad de equipamiento, la digitalización óptima de valores medidos, sistemas de imagen híbridos, el uso de modalidades de imagen no ionizantes o el procesamiento de imágenes médicas 3D, así como la tomografía computarizada, resonancia magnética avanzada, imagen de alta resolución, microscopía o imagen molecular. Por medio de la imagen médica se han desarrollado sistemas que permiten

[197] Para el desarrollo de este epígrafe se ha consultado especialmente la siguiente fuente: Instituto de Salud Carlos III, (Coord. Campus excedencia internacional, Centro de Apoyo a la Innovación Tecnológica (CIAT) y Universidad Politécnica de Madrid), *Imagen médica. Informe de vigilancia tecnológica*, Noviembre 2015. Documento disponible en https://fipse.es/sites/default/files/documentos/documento/2017/04/16/20151130_informe_vtimagenmedica.pdf (última consulta 03/08/18).

detectar enfermedades tempranas, así como el uso de técnicas específicas de diagnóstico.

En concreto, la implantación de las TIC han significado un avance relevante en los métodos de diagnóstico, de prevención de enfermedades y en la organización de pacientes, puesto que por medio de las imágenes digitales de alta resolución, es posible el diagnóstico de una enfermedad temprana y la administración de un tratamiento presintomático, ya que los diferentes centros sanitarios pueden acceder e intercambiar información clínica y genómica procedente de la imagen digital registrada en una base de datos común de los pacientes. Por otro lado, a pesar de que actualmente se utiliza con frecuencia instrumentos híbridos[198] para los estudios preclínicos en fisiopatología del cáncer, neurología, cardiología y estudio de fármacos, se utiliza también la imagen como herramienta tecnológica en la investigación preclínica, así como equipos independientes que relacionan datos diferentes obtenidos por medio de un *software* que los relaciona.

La imagen de espectroscopia por RM es utilizada para estudios preclínicos en aquellas enfermedades prevalentes e incidentes en una determinada población, usándose técnicas de imagen para el desarrollo del procedimiento a seguir y la trazabilidad celular en medicina regenerativa[199]. De igual modo, para el diagnóstico clínico, se utilizan técnicas de PET que permiten diagnosticar enfermedades como el Alzheimer, sistemas de biopsia guiada por imagen, imágenes en 3D y, sistemas que resuelven diagnósticos complejos o de extremada urgencia desde cualquier lugar gracias a las telecomunicaciones, creándose a tales efectos Centros Consultores que dan asistencia sanitaria a distancia en cualquier momento del día[200].

[198] PET-TEC, SPECT/TC, PET, /RM.

[199] Instituto de Salud Carlos III, (Coord. Campus excedencia internacional, Centro de Apoyo a la Innovación Tecnológica (CIAT) y Universidad Politécnica de Madrid), *Imagen médica. Informe de vigilancia tecnológica*, Noviembre 2015, p. 8.

[200] Instituto de Salud Carlos III, (Coord. Campus excedencia internacional, Centro de Apoyo a la Innovación Tecnológica (CIAT) y Universidad Politécnica de Madrid), *Imagen médica. Informe de vigilancia tecnológica*, Noviembre 2015, p. 8.

Asimismo, las técnicas de imagen son empleadas con frecuencia para llevar un seguimiento de las intervenciones, activar fármacos y terapias locales y guiar la destrucción de lesiones de manera no invasivas. En casos de radioterapia, son utilizados los llamados sistemas de conformación de dosis de radioterapia guiados por imagen y modelos de compensación de los movimientos de respiración o latidos de corazón, resultando ser una herramienta relevante para la planificación de las sesiones.

En conclusión, la imagen médica es una de las fuentes de datos sanitarios más relevante, puesto que en la práctica clínica es uno de los instrumentos de diagnósticos más influyentes y esenciales. El interés común de que la tecnología de imagen médica digital continúe evolucionando es evidente, para lo que resulta necesario una inversión en infraestructuras destinadas al desarrollo de proyectos donde participen y cooperen de manera activa o pasiva y vinculada actores profesionales especializados del gobierno, de la universidad y de la empresa. Por medio del *big data* se pretende desarrollar técnicas que sean aplicables a cada tipo de imagen que permitan aplicar algoritmos y metodologías para analizar, procesar e interpretar los datos procedentes de las imágenes médicas a fin de extraer el conocimiento e información sanitaria de las mismas. De tal modo que, tras obtener la información sanitaria de valor procedente de cada modalidad de imagen, el profesional sanitario deberá realizar una anotación semántica automática o semiautomática por medio de un algoritmo de las imágenes donde relacione el conocimiento obtenido con las mismas, a fin de facilitar la búsqueda semántica por conceptos de las imágenes en las bases de datos específicas. El citado desarrollo conlleva la necesidad de instalar grandes bases de datos que sean capaces de detectar el mejor algoritmo aplicable, para ello es necesario que los facultativos sanitarios respeten y sigan un protocolo de validación común a fin de comparar y dar validez a unos algoritmos frente a otros.

Además cabría añadir que, existen otras fuentes relevantes de datos de salud, como puede ser: la genómica (datos registrados en el materia genético para prevenir y tratar enfermedades de origen genéticos); del *business intelligence* (en concreto las técnicas y herramientas destinadas a la administración y creación de conocimiento mediante el análisis de datos generados en los distintos procesos de asistencia sanitaria); de modelos predictivos (diagnósticos y estadísticas de morbilidad y mortalidad procedentes de la minería de datos); del *crowdsourcing* (investigaciones científicas que

usan datos sanitarios procedentes de las redes sociales, financiaciones colectivas y compartimiento voluntario de datos); secuencias genómicas de datos de población; lectores de los sensores biométricos o los dispositivos *wereables*; datos generados por los dispositivos móviles; la genética y; los medios sociales en general.

En definitiva, de todas las fuentes citadas, debido al hecho de que la historia clínica electrónica está implantada en la mayoría de los hospitales, las aplicaciones de *business intelligence* y de modelos predictivos son herramientas esenciales en los resultados de atención médica[201].

2. LAS REDES SOCIALES COMO FUENTE EXTERNA DE DATOS DE SALUD

2.1. El impacto del *crowdsourcing* en la investigación biomédica

El concepto *crowdsourcing* fue empleado por primera vez en 2006 por Jeff Howe, en su artículo "The Rise os Crowdsourcing" publicado en la revista *Wired Magazine,* donde se refiere al mismo como un negocio en la web que aprovecha la "creatividad colectiva" en las redes. Según señala Howe[202], el *crowdsourcing* está formado por cuatro fases:

1. Primera fase: la Administración Pública o una empresa privada solicita a la sociedad que participe por medio de las redes sociales en la producción de contenidos acerca de un proyecto o idea común.

[201] Al respecto DÍAZ DE LEÓN CASTAÑEDA, "¿Qué es la salud electrónica ("e-Salud")?...", *op. cit.,* [Documento sin paginación], señala que: "Más recientemente, con el desarrollo de las TIC, se han incorporado nuevas aplicaciones al campo de la e-Salud, como el análisis de grandes volúmenes de datos ("*Big Data*") en los sistemas de vigilancia epidemiológica, en el monitoreo del desempeño de los servicios de salud y en el apoyo a la toma de decisiones; las técnicas de aprendizaje artificial ("Machine learning") aún en desarrollo como auxiliares para los profesionales sanitarios en la toma de decisiones clínicas; los sistemas de realidad virtual y aumentada ("VR", "AR") en actividades de educación sanitaria y como auxiliares en procedimientos quirúrgicos; así como los sistemas de Internet de las Cosas ("IoT") para el monitoreo hospitalario o a distancia de pacientes (dispositivos acoplados a sistemas de telemedicina)".

[202] HOWE, J., *Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*, Three Rivers Press, Nueva York, 2008.

2. Segunda fase: el desarrollo de la participación de los ciudadanos en un entorno abierto *(open source*), a fin de acceder al conocimiento y a la información útil para la posterior creación de aplicaciones y programas informáticos.

3. Tercera fase: capacidad de acceder a medios y herramientas de producción de contenidos a efectos de generar comunicación e interrelaciones entre los participantes.

4. Cuarta fase: aumentar las partes del proceso con capacidad de autogestión, de tal modo, que cuanto mayor sea el número de organizaciones o comunidades que intercambien información y conocimiento sobre intereses comunes, óptimo será el resultado.

Por otro lado, en el año 2008, Brabham interpreta el *crowdsourcing* de la siguiente manera[203]: "[…] una empresa plantea un problema en la red, un gran número de personas ofrecen su particular solución, la idea o ideas ganadoras reciben algún tipo de recompensa, y la empresa produce en masa la solución para su propio beneficio"[204].

En la actualidad, el *crowdsourcing* se define como "un modelo de producción social puesto que el producto se obtiene gracias a la colaboración social de multitud de individuos que participan vía Red y de forma descentralizada y asincrónica, en la generación de una idea, resolución de un problema, obtención de un producto, etc."[205]. Asimismo, se ha de destacar que generalmente, los participantes en los procesos de *crowdsourcing* a cambio de su participación en el proyecto reciben algún tipo de

[203] Texto orgiginal: *"… a company posts a problem online, a vast number of individuals offer solutions to the problem, the winning ideas are awarded some form of a bounty, and the company mass produces the idea for its own gain".* En BRABHAM, D.C., "Crowdsourcing as a Model for Problem Soving: An Introduction and Cases", *Convergence,* Sage Publications, Vol. 14, núm. 1, 2008, p.76. Documento disponible en: http://sistemas-humano-computacionais.wdfiles.com/local--files/capitulo%3Aredes-sociais/Crowdsourcing-Problem-solving.pdf (última consulta 08/08/18).

[204] BRABHAM, "Crowdsourcing as…",*op. cit.,* p. 76.

[205] ALONSO DE MAGDALENO, M.I. y GARCÍA GARCÍA, J., "Crowdsourcing: la descentralización del conocimiento y su impacto en los modelos productivos y de negocio", *Cuadernos de Gestión,* Vol. 14, núm. 2, 2014, pp. 39. Documento disponible en: http://www.redalyc.org/articulo.oa?id=274332765002 (última consulta 12/08/18).

recompensa, ya sea económica, de reputación, reconocimiento o incluso para reclutar talentos por medio de un contrato de trabajo[206].

Por consiguiente, el *crowdsourcing* en la esfera sanitaria es aplicado como un modelo de producción colaborativa con fines altruistas, puesto que colabora en la investigación biomédica por medio de las redes sociales, plataformas on-line o programas informáticos las diferentes entidades públicas y privadas gracias a las TIC y a una financiación colectiva interactúan con el usuario e intercambian datos sanitarios de manera voluntaria sobre un propósito o proyecto común e innovador en el marco de la salud, de interés tanto para las entidades interrelacionadas, como para la sociedad en su conjunto.

Por ultimo, cabe destacar el proyecto *World Community Grid* (WCG) coordinado por IBM, pues es un ejemplo de *crowdsourcing* en la esfera sanitaria, cuya finalidad es la de cooperar con proyectos científicos de investigación en beneficio de la humanidad. El método a seguir se basa en técnicas de computación distribuida a fin de aprovechar el tiempo inactivo de ordenadores personales, generando un sistema virtual de gran capacidad, donde una vez que la persona o institución se ha registrado en el proyecto, descarga e instala el programa cliente en su ordenador personal, va recibiendo pequeñas porciones de información que, tras análisis, se remiten de nuevo al equipo del investigador responsable.

El primer proyecto de WCG se inició en el año 2004, a fin de agilizar la investigación biomédica centrada en la cura para la viruela, gracias al *crowdsourcing* los investigadores pudieron examinar el efecto de 35 millones de compuestos farmacológicos contra las proteínas de la viruela, obteniéndose finalmente 44 compuestos de gran interés para el tratamiento de la enfermedad. Otro de los proyectos, surgió con la finalidad de conseguir un avance en el tratamiento del síndrome de inmunodeficiencia adquirida (SIDA), encontrando dos prometedores inhibidores. Asimismo, desde el año 2011, se encuentra en vigor el proyecto *GO Figh Against*

[206] Empresas como Pepsi, Heinz, Procter & Gamble, General Motors y Adtriboo.com, son claros ejemplos en el uso del *crowdsourcing* desde una perspectiva propiamente profesional, *Vid.* RAMÓN MORENO, J. R., "*Crowdsourcing* creativo o la democratización del talento", marzo 2012, [Documento sin paginación]. Documento disponible en: http://www.marketingnews.es/varios/opinion/1064265028705/crowdsourcing-creativo-democratizacion-talento.1.html (última consulta 09/09/18).

Malaria, a efectos de descubrir compuestos farmacológicos efectivos contra la malaria probando millones de compuestos en distintos candidatos, seleccionando aquellos que desactiven las proteínas que permiten al parasito de la malaria sobrevivir y reproducirse, siendo posteriormente investigados por el *Scripps Researche Institute* (California) organismo que dirige y coordina el proyecto. Se estima que gracias al proyecto se reduce a un año, el trabajo que supondría más de cien años si se efectuara con los medios tradicionales[207]. Así pues, el *crowdsourcing* en la investigación biomédica, además de cooperar en la mejora y eficiencia de la misma, agiliza el tiempo de resolución del problema y reduce costes, así como la participación activa de personas y organizaciones en un proyecto común facilitando la colaboración e intercambio de conocimiento e información compartida entre todas las personas y entidades interconectadas, consiguiéndose a su vez gracias a las TIC y al IoT un efecto-red on-line de todos los agentes interconectados[208].

2.2. El *big data* en las redes sociales como fuente de información de salud pública y privada

Por medio de las redes sociales, los distintos agentes del ámbito sanitario intercambian información y conocimiento de gran valor e interés[209]. En consecuencia, la finalidad de la red social va a depender de los agentes que intervienen en la misma. Las redes sociales se pueden clasificar en tres tipos:

a) Redes sociales activas: conectan a distintos profesionales de la sanidad (facultativos médicos, investigadores, farmacéuticos, enfermeros…) cuya finalidad es del intercambiar de manera activa conocimiento clínico a través de información científica, criterios y experiencias profesionales, a fin de resolver de manera activa un problema de salud. Ejemplos de redes sociales activas son:

---

[207] *Vid.*: https://www.worldcommunitygrid.org/research/gfam/overview.do

[208] En este sentido, siendo mayor el valor del conocimiento y más descentralizado cuanto mayor sea el número de actores que interactúen y, a su vez consiguiendo un resultado óptimo.

[209] Ministerio de Economía y Empresa, *TIC y Salud: aplicaciones móviles, redes sociales e iniciativas pública*, Red.es, [Documento sin paginación]. Documento disponible en: http://www.red.es/redes/es/magazin-red/reportajes/tic-y-salud-aplicaciones-moviles-redes-sociales-e-iniciativas-publicas (última consulta 22/09/18).

AMN Healthcare, Dosimity, Sermo, Figure, SharePractice, WeMedUp, Doc2Doc, Ippok, Doctor-Dice, MedCenter y *Medicalia*.

b) Redes sociales pasivas: conectan a distintos pacientes y familiares entre sí mismos a efectos de intercambiar y compartir sus propias experiencias, síntomas sufridos, emociones a fin de intercambiar de manera pasiva información sobre una enfermedad o tratamiento, así como para encontrar recomendaciones, apoyo, segundas opiniones y otras alternativas. Por ejemplo, destacar entre otras: PatientsLikeMe*, Tudiabetes.org*, *Stupidcancer, Curetugether* y *Aoranna.*

c) Redes sociales mixtas: son las redes sociales que conectan a médicos con pacientes, como, por ejemplo, *RareShare*.

Por consiguiente, el intercambio de información y conocimiento entre los distintos agentes vinculados a la salud en las redes sociales genera de manera automática y en tiempo real en la red datos sanitarios no estructurados de gran valor y relevante interés[210]. Asimismo, en la actualidad, las redes sociales que conectan a diferentes profesionales sanitarios son las más comunes.

La diferencia principal entre la salud pública y la salud privada viene dada por el número y volumen de pacientes y usuarios inscritos, abarcando la salud pública a la totalidad de la población de un país, puesto que la protección y la mejora de la salud de la población es un derecho humano fundamental que la mayoría de los países tiene regulado en su legislación, aunque, por desgracia, en la actualidad continúa sin ser un derecho recogido y amparado en muchos otros. De acuerdo con el contenido del artículo 25 de la Declaración Universal de Derechos Humanos de 1948 que establece que*:* "Toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia sanitaria y los servicios sociales necesarios". Debido a lo anterior, el *big data* en la esfera de la salud pública adquiere una gran relevancia, puesto que los usuarios y

[210] En este sentido cabe destacar la idea de contraprestación de los datos de salud donde los particulares ceden sus datos sanitarios a cambio del uso gratuito de determinadas aplicaciones móviles o redes sociales, al respecto *vid.* PLANA ARNALDOS, Mª C., "Los datos personales como contraprestación", en AA.VV., *Protección de datos personales,* (Coord. I. González Pacanowska), Asociación de profesores de Derecho Civil, Tirant lo Blanch, Valencia, 2020, pp. 561-618.

pacientes son generadores de datos y, cuanto mayor sea el número de usuarios mayor será el volumen de datos generados. Igualmente, al tratarse de datos que al proceder de la sanidad pública afectan a un gran número de personas o poblaciones, resultado ser de mayor relevancia a efectos estadísticos y de investigación por la información y conocimiento que se puede extraer de los mismos una vez analizados. Por ende, las Administraciones Públicas a través de las redes sociales, son una fuente de información y conocimiento de tipo social, bien en calidad de responsable del archivo y custodia de un gran volumen de datos sanitarios, bien en calidad de promotora de proyectos de desarrollo de las mismas. El programa europeo H20202 del año 2016-2017 "Big Data Supporting Public Health Policies (SC1-PM-18-2016)" es un claro ejemplo de la relevancia existente entre las redes sociales, la salud pública y el *big data*.

En definitiva, las redes sociales generan un alto volumen de datos sanitarios que contienen información y conocimiento de gran valor científico-sanitario, adquiriendo gran relevancia las redes sociales específicas entre profesionales donde se intercambia información y conocimiento entre los distintos especialistas en medicina y/o investigadores sobre determinadas patologías y sus tratamientos, generando datos sanitarios que una vez analizados pueden aportar nueva información y ampliar el conocimiento en la esfera sanitaria, creando nuevos tratamientos, detectando errores reales en la práctica, prevenir reacciones y enfermedades adversas, así como ayudar en la toma de decisiones[211]. Por último y, no menos importe, se ha de destacar que el 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 (en adelante, RGPD) autoriza el tratamiento de los datos personales que el usuario ha hecho públicos, ya que para el legislador europeo la publicidad de los datos equivale a un consentimiento explícito (art. 9.2. e) RGPD). En consecuencia, si un ciudadano hace públicos sus datos relativos a la salud en redes sociales abiertas, podrían ser tratados mediante algoritmos y herramientas *big data*[212].

[211]Ministerio de Economía y Empresa, *TIC y Salud: aplicaciones móviles, redes sociales e iniciativas pública*, Red.es, [Documento sin paginación].

[212]PÉREZ GÓMEZ, J. M., "Especialidades en el sector sanitario" en AA.VV., *La adaptación al nuevo marco de protección de datos tras la RGPD y la LOPDGDD* (Coord. J. López Clavo), Wolters Kluwer, Madrid, 2019, pp. 891-892, señala que: "Sin embargo, las indiscreciones del titular del dato no gozan de tanta protección y así el Reglamento autoriza a realizar el tratamiento de los datos personales que el

III. LAS HERRAMIENTAS Y TÉCNICAS DE DESARROLLO DEL *BIG DATA* EN EL SECTOR SANITARIO

Mientras que parece que cada vez son más las fuentes de datos sanitarios, tanto internas como externas al Sistema de Salud, cabe ahora indagar sobre las herramientas y técnicas de *big data* que se aplican a las mismas a fin de sustraer de los datos sanitarios, conocimiento e información de interés, así como examinar el *modus operandi* en los diferentes procesos de análisis.

1. LA IMPORTANCIA DEL *DATA MINING* EN EL CAMPO DE LA INVESTIGACIÓN BIOMÉDICA

Las herramientas de minería de datos y de análisis del gran volumen de datos sanitarios generador por las distintas fuentes procedentes de las TIC y el IoT, son tecnologías esenciales a fin de extraer de los mismos la información y conocimiento de gran utilidad en la toma de decisiones y en la atención al paciente, suponiendo a su vez un gran ahorro económico en el sector sanitario. Asimismo, a partir de la minería de datos surgen diversos modelos predictivos mediante el diagnóstico y cálculo de probabilidad de morbilidad y mortalidad.

1.1. El modelo de proceso *knowledge discovery in databases*

El proceso de descubrimiento de conocimiento en grandes volúmenes de datos denominado *knowledge discovery in databases* (KDD), surge en la década de los años 80 como un nuevo campo de investigación, en concreto:

---

interesado he hecho manifiestamente públicos, equiparando esa publicación a un consentimiento explícito (art. 9.20 e) Reglamento); lo que abre la posibilidad de aceptar el tratamiento delos datos relativos da la salud publicados por su titular en determinadas redes sociales abiertas como, por ejemplo*, twitter, wordpress* o *blogger*. En principio, esta información puede antojarse inocua, pero su tratamiento mediante algoritmos que busquen patrones o relaciones entre variables aplicados a plataformas big data bien puede tener consecuencias que afecten al derecho del titular del dato, pues cada vez resulta más borrosa la distinción entre datos sanitarios y no sanitarios, pero, como afirma Sarria-Santamera que de manera indirecta pueden revelas información sobre la salud de la persona a la que se refieren".

"[…] es un campo de la inteligencia artificial de rápido crecimiento, que combina técnicas del aprendizaje de máquina, reconocimiento de patrones, estadística, bases de datos, y visualización para automáticamente extraer conocimiento (o información), de un nivel bajo de datos (bases de datos)"[213].

El KDD ayuda y guía al investigador o facultativo médico (agente inteligente) a la toma de decisiones, una vez que el agente inteligente extrae de los datos su significado por medio de las técnicas disponibles en KDD. Por consiguiente, la materia prima del KDD son los datos sanitarios procedentes de las diversas bases de datos y, su objetivo principal es el de extraer de los mismos información, a fin de ser transformada en recursos para la toma de decisiones[214]. Por ende, el proceso del KDD en el sector sanitario se compone por los siguientes niveles[215]:

1. Detectar el problema clínico a resolver y objetivos: crear un algoritmo y especificar si la finalidad es predecir, explicar, clasificar o, agrupar.

2. Selección de datos sanitarios originales procedentes de las bases de datos que pueden ayudarnos a resolver el problema.

3. Limpieza y análisis de los datos, clasificación de la totalidad de los datos originales aquellos que aportan un valor por su alto contenido de información y conocimiento de aquellos que no resultan de interés y relevancia, por ser erróneos, atípicos e incompletos.

4. Reducción de los datos en aquellos que comparten unas mismas características de utilidad según los objetivos marcados.

---

[213] FAYYAD, U., PIATESTSKY-SHAPIRO, G. and SMYTH P., "From Data Mining to Knowledge Discovery in Databases*" Al Mazine.* Vol. 17, núm. 3, 1996, pp. 37-54. Documento disponible en: file:///Users/leticialatorreluna/Downloads/1230-Article%20Text-1227-1-10-20080129.pdf (última consulta 23/09/18).

[214] NIGRO, H.O., XODO, D., CORTI, G. and TERREN, D., "KDD (Knowledge Discovery in Databases): Un proceso centrado en el usuario", *Red de Universidades con Carreras en Informática (RedUNCI*), 2004, p. 55. Documento disponible en: http://sedici.unlp.edu.ar/handle/10915/21220 (última consulta 24/09/18).

[215]NIGRO, XODO, CORTI and TERREN, "KDD (Knowledge Discovery in Databases): Un proceso centrado en el usuario…", *op. cit.,* p. 56.

5. Elección de las herramientas y técnicas de *data mining* que se adapten al problema sanitario (algoritmo) y al objetivo clínico (predecir, explicar, clasificar, agrupar…), así como regulación de los parámetros de las distintas redes usadas.

6. Posteriormente, se procede a la presentación al usuario (investigador/ facultativo sanitario) de los patrones descubiertos y relaciones en los datos mediante gráficos, arboles, reglas, entre otros.

7. Análisis e interpretación de los datos sanitarios por parte del analista.

8. Sustracción de conocimiento e información y aplicación de este en casos clínicos reales. En ocasiones, el conocimiento puede ser directamente aplicable, otras, sin embargo, sirve de guía a fin de resolver otros objetivos y problemas clínicos.

A pesar de que originariamente el proceso fue denominado *knowledge discovery in databases,* posteriormente se le asignó el nombre de *data mining*. En suma, es un proceso de gran utilidad para los investigadores de distintas áreas científicas a fin de crear herramientas y técnicas que cooperen con el análisis de los grandes volúmenes de datos almacenados en las bases de datos para la obtención de una información y conocimiento de interés.

1.2. El método del proceso *cross industry standard process for data mining*

En el año 1999 nace el modelo de proceso *cross industry standard process for data mining* (CRISP-DM), como una guía de referencia creada por un conjunto de empresas europeas[216] a efectos de solventar los problemas y complejidades generados por el proceso de *data mining*. El citado modelo sigue un proceso compuesto por seis fases relacionadas unas con otras, permitiendo que por medio de la fase posterior se puedan revisar niveles anteriores.

[216] NCR (Dinamarca), AG(Alemania), SPSS (Inglaterra), OHRA (Holanda), Teradata, SPSS, y Daimer-Chrysler.

La primera fase es la denominada compresión del negocio, donde se establecen los objetivos del proyecto y requerimientos desde una perspectiva propiamente estratégica, teniéndose en cuenta factores como el contexto inicial y criterios de éxito. Igualmente se realiza una evaluación de la situación por medio de herramientas como inventario de recursos, requerimientos, supuestos diversos y tecnicismos aplicables al proyecto. Asimismo, es relevante que se determinen los objetivos y criterios de éxito de la minería de datos, así como la creación de un plan de proyecto donde conste el propio plan a seguir y, las herramientas, equipo y técnicas aplicables a fin de cumplir los objetivos establecidos. La segunda fase consiste en la comprensión de los datos, donde una vez que constan marcados los objetivos, se procede a una primera recopilación de datos, describiendo, explorando y verificando la calidad de estos. En la tercera fase se procede a una preparación de los datos, donde del conjunto inicial de datos se procede a seleccionar y limpiar aquellos datos que resulten de interés por la información y conocimiento que aportan a fin de conseguir los objetivos, construyéndose un conjunto de datos final donde son integrados y formateados los datos con valor.

En una cuarta fase, con el objeto de obtener los máximos valores de los datos, se procede a la aplicación de la técnica de modelado, donde son aplicadas las técnicas de minería de datos a los *dataset*, para ello, se selecciona la técnica de modelado aplicable, se diseña una evaluación, se construye un modelo a seguir y se realiza una posterior evaluación de este. La quinta fase consiste en la evaluación de los resultados, en concreto, en esta fase se evalúan los modelos de las fases anteriores a fin de determinar si el modelo final es el que realmente se ajusta a los objetivos y necesidades del proyecto. Por último, en una sexta fase, se procede al despliegue, donde se aplican los modelos en la práctica integrando los mismos en los procesos de toma de decisiones clínicas. Para ello resulta esencial que sea efectuada una correcta planificación de despliegue, así como de la monitorización y del mantenimiento. Asimismo, en esta fase se genera el proyecto final y, una posterior revisión de este. Actualmente, el modelo de proceso CRISP-DM es la guía de referencia que más se utilizada en proyectos de *data mining*[217], no obstante, a pesar de los amplios beneficios y positivos resultados

[217] EPB 603 Sistemas de Conocimiento, *Metodología para el Desarrollo de Proyectos en Minería de Datos CRISP-DM,* 2007, pp. 1-12. Documento disponible en: http://www.oldemarrodriguez.com/yahoo_site_admin/assets/docs/Documento_CRISP-DM.2385037.pdf (última consulta 25/09/18).

obtenidos de los proyectos de *data mining* en el sector de la investigación científica, especialmente la biomédica y clínica, según Menasalvas, Consuelo Gonzalo, Rodríguez – González, también se detectan una serie de problemas de índole predictivo y descriptivo[218].

2. EL ANÁLISIS PREDICTIVO APLICADO AL *BIG DATA*

El análisis predictivo como una de las ventajas que ofrece el *big data* tiene una especial relevancia en el sector sanitario, no en vano, se ha de destacar que la analítica predictiva existía en la industria antes de la tecnología de *big data*[219], aunque la misma se ha visto incrementada a consecuencia de la aplicación de técnicas de *big data*, pues resulta evidente que se puede predecir a partir de los datos en el ámbito científico y sanitario, lo que se ha venido denominando aprendizaje automático o, más recientemente analítica predictiva, que como indica ERIC SIEGEL[220] es "una tecnología que aprende de la experiencia (los datos) para predecir el futuro comportamiento de los individuos con el propósito de tomar mejores decisiones".

[218]MENASALVAS, E., GONZALO, C. y RODRÍGUEZ-GONZÁLEZ, A., "*Big Data* en Salud: retos y oportunidades" *Economía Industrial,* núm. 405, 2017, p. 90. Documento disponible en: http://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/MENASALVAS,%20GONZALO%20Y%20RODR%C3%8DGUEZ.pdf, (última consulta 29/09/18), señalan que: "Los problemas predictivos cuyo objetivo es predecir el valor de un atributo en particular basado en los valores de otros atributos. El atributo que se predice se denomina comúnmente como atributo objetivo (o variable dependiente), mientras que los atributos que se utilizan para la predicción son conocidos como atributos explicativos (p variables independientes). Destacan aquí los problemas de clasificación o de estimación de valor y como técnicas podemos destacar los enfoques basados en estadísticas, regresión, arboles de decisión y redes neuronales. Los problemas descriptivos cuyo objetivo es derivar patrones (correlaciones, tendencias, agrupaciones o clústeres, trayectorias y anomalías) que resuman las características inherentes a los datos. Dentro de este grupo, cabe destacar el análisis de reglas de asociación para el que el algoritmo "*A priori"* es el más conocido, así como los problemas de segmentación o *clustering*".

[219] Sobre esta cuestión GUAZZELLI, A., "Predicciones sobre el Futuro. Parte 1: ¿Qué es la Analítica predictiva?", *IBM developerWorks,* noviembre 2012, [documento sin paginación]. Documento disponible en: https://developer.ibm.com/es/technologies/predictive-analytics/articles/ba-predictive-analytics1/ (última consulta 01/10/18), afirma que la analítica predictiva existía ya desde unas décadas antes de su relevancia en la industria, refiriéndose a la misma como la "cantidad de datos que se capturaban de las personas (por ejemplo, de transacciones online y redes sociales) y sensores (por ejemplo, de dispositivos GPD móviles) así como la disponibilidad de poder de procesamiento costeable, ya sea basado en la Nube o en Hadoop".

[220] SIEGEL, E., *Analítica predictiva. Predecir el futuro utilizando Big Data*, Ed. Anaya, Madrid, 2014, pp.35-36.

En concreto, para ERIC SIEGEL la analítica predictiva es "la pionera de la tendencia que existe actualmente para tomar decisiones basadas en datos, confiando menos en el instinto personal y más en una evidencia empírica y palpable"[221]. De igual modo, JOYANES AGUILAR [222] define la analítica predictiva como "una rama de la minería de datos centrada en la predicción de las probabilidades y tendencias futuras […] que trata de analizar hechos actuales o históricos con el propósito de hacer predicciones sobre sucesos futuros". La analística predictiva se lleva a cabo a través de la creación de modelos de conocimiento predictivos[223] que son funciones matemáticas o algoritmos por las que se puede determinar y aprender la similitud entre un conjunto de variables datos de entrada registrados en un soporte y una variable de respuesta o de destino. Sobre esta cuestión GUAZZELLI[224] señala las siguientes técnicas más comunes de

[221] SIEGEL, "*Analítica predictiva. Predecir…", op. cit.,* p.36.

[222] JOYANES AGUILAR, L., *Big Data. Análisis de grandes volúmenes de datos en las organizaciones.* Ed. Marcombo, Barcelona, 2014, p.374. Asimismo, para los autores MAYER-SCHÖNBERGER, V. and CUKIER, K., *Big Data. La revolución de los datos masivos*, Ed. Turner, Madrid, 2013, pp.23-24, la utilización de los datos masivos "no consiste en intentar enseñar a un ordenador a pensar como un ser humano. Más bien consiste en aplicar las matemáticas a enormes cantidades de datos para poder inferir probabilidades". Igualmente, los citados autores ponen de relieve que el buen funcionamiento de estos sistemas radica precisamente en que "están alimentados con montones de datos sobre los que basar sus predicciones. Es más, los sistemas están diseñados para perfeccionarse solo a lo largo del tiempo, al estar pendientes de detectar las mejores señales y pautas cuando se les suministran más datos".

[223] SIEGEL, *Analítica predictiva…, op. cit.,* p.51 define el modelo predictivo como un "mecanismo que predice un comportamiento de un individuo, como un clic, una compra, una muerte, o una mentira. Toma como datos de entrada las características del individuo y genera como salida una puntuación predictiva. Cuanto mayor sea la puntuación, más probable será que el individuo exhiba el comportamiento predictivo".

[224] GUAZZELLI, A., "Predicciones sobre el futuro, parte 2: Técnicas de modelado predictivo", *IBM developerWorks*, diciembre 2012, [Documento sin paginación]. Documento disponible en: https://developer.ibm.com/es/technologies/predictive-analytics/articles/ba-predictive-analytics3/ (última consulta 03/10/18) indica que: "Una SVM realiza una correlación de los datos de entrada sobre los vectores en un espacio con más dimensión, donde se construye un "hiperplano óptimo" que separa los datos. Dos hiperplanos paralelos se construyen a ambos lados de este hiperplano. […]. Las SVM, así como también las NN y los modelos de regresión lógica, son técnicas genéricas poderosas que a pesar de ser matemáticamente diferentes, generan de algún modo resultados comparables. Los árboles de decisión también representan otra técnica general de modelado predictivo que sobresale por su habilidad para explicar la racionalidad detrás del producto de salida. Ya que son fáciles de usar y de entender, los árboles de decisión son los más usados entre las técnicas de modelado predictivo. Las técnicas de agrupación en clúster, por otro lado, son muy populares siempre que la variable de destino o respuesta no sea importante o no esté disponible. Como su nombre lo indica, las técnicas de agrupación en clúster son capaces de agrupar los datos de entrada dependiendo de su similitud […] A pesar de que las técnicas predictivas tienen diferentes fortalezas y debilidades, el modelo de precisión depende en gran medida de los datos primarios de entrada y de las características utilizadas para capacitar a un modelo predictivo. Como hemos mencionado anteriormente, el modelo de desarrollo de datos involucra mucho análisis de datos y mensajes. Por lo general, de cientos de campos de datos primarios disponibles, se selecciona un subconjunto y los campos se procesan antes de ser presentados a una técnica de modelado predictivo. De este modo, el secreto detrás de un buen modelo predictivo usualmente depende de buenos mensajes aún más que de la técnica utilizada para capacitar al modelo. Esto no significa que la técnica predictiva no es importante. Si se utiliza la técnica incorrecta o se selecciona un conjunto de parámetros de entrada

modelado predictivo: (1) máquinas de vectores de soporte (SVM); (2) redes neuronales (NN); (3) árboles de decisión; (4) de agregación o *clustering* y; (5) reglas de asociación. De manera general, el análisis predictivo se aplica en diversos sectores a efectos de dar solución a problemas de riesgo o de predecir oportunidades futuras. Así pues, por medio del análisis predictivo en relación con la asistencia sanitaria se puede conocer: los factores de riesgo de los pacientes para desarrollar problemas crónicos (asma, diabetes, enfermedades cardiovasculares…) a efectos de implantar un control más eficaz en la asistencia ambulatoria, llegando incluso a evitar con esta metida la hospitalización de los pacientes: el riesgo de reingreso antes de dar un alta anticipada; detección de riesgos vinculados con el patrón genético, que permita implantar medidas de prevención y tratamiento personalizados; igualmente se puede identificar patrones de riesgo de infección de pacientes monitorizados y; detectar posibles fraudes y abusos en el cuidado de la salud, entre otros.

IV. LA MEDICINA BASADA EN LA EVIDENCIA A TRAVÉS DE LA APLICACIÓN DE HERRAMIENTAS *BIG DATA*

Llegados a este punto, examinaremos a continuación cómo se aplican estas herramientas *big data* en uno de los campos sanitarios que probablemente sea de los más relevantes e influyentes en la actualidad, como es el de la Medicina Basada en la Evidencia (en adelante, MBE).

---

incorrectos, los buenos datos no van a ser de utilidad. Las NN, por ejemplo, vienen en todas las formas y estructuras. Para desarrollar un buen modelo predictivo es importante seleccionar una estructura de red apropiada […] Las técnicas de agrupación en clúster requieren que se provea el número de grupos antes de la capacitación. En este caso, si el número de grupos es muy pequeño, el modelo podría perder diferencias importantes en los datos de entrada, ya que está siendo forzado a agrupar en forma conjunta datos diferentes Por otro lado, si el número de grupos es demasiado grande, puede que pierda similitudes importantes. Los modelos predictivos pueden también beneficiarse de diferentes técnicas de modelado a la misma vez. Esto sucede porque muchos modelos pueden combinarse juntos en lo que se llama conjunto modelo. De este modo, la salida del conjunto está designada para nivelar las diferentes series de fuerzas inherentes a los diferentes modelos y técnicas".

Las tecnologías *big data* realizan un papel relevante en la MBE, pues tras la formulación de una pregunta precisa (algoritmo), la MBE necesita de información para dar respuesta al problema clínico, resultando ser los datos sanitarios procedentes de las TIC y del IoT una vez analizados, una fuente esencial de información y conocimiento, a fin de tomar una decisión evidente y eficaz sobre el tratamiento y el cuidado a seguir en el paciente. Así pues, la MBE se ha convertido a través de las TIC y el IoT en un mecanismo eficaz que coopera en la mejora de la calidad del tratamiento y cuidado sanitario personalizado del paciente, ayuda a la disminución de errores clínicos y en la variabilidad injustificada de la práctica y atención clínica. En concreto, la MBE, facilita y coopera en la búsqueda, recopilación y análisis crítico de la información recopilada de los datos de salud a través de aplicación de las herramientas *big data*, dando como resultado una información y conocimiento que permite una toma de decisiones clínicas refrendadas y basadas en la mejor información científica disponible y actualizada en tiempo real.

1. ANTECEDENTES HISTÓRICOS DE LA MEDICINA BASADA EN LA EVIDENCIA

En el año 1991, Gordon Guyatt, profesor de Epidemiología clínica de la McMaster University en Ontario (Canadá), por primera vez publicó el término Medicina Basada en la Evidencia (MBE) en su artículo "Evidence-based medicine" para la revista *ACP J Club*. Posteriormente, en el año 1996 la MBE fue definida de manera manifiesta por David Sackett como el "empleo consciente, explícito y juicioso de la mejor evidencia actual en la toma de decisiones sobre el cuidado sanitario de los pacientes"[225]. Igualmente, la MBE se define como "un proceso cuyo objetivo es el de obtener y aplicar la mejor evidencia científica en el ejercicio de la práctica médica cotidiana"[226].

[225] SACKETT, D.L., STRAUS, S.E., RICHARDSON, W. S., GLASZIOU, P. y HAYNES, R. B., *Medicina Basada en la Evidencia: como practicar y enseñar la MBE (3ª Ed.),* Ed. Elsevier España, Madrid, 2005.

[226] JUNQUERA, L.M., BALADRÓN, J., ALBERTOS, J.M. y OLAY, S., "Medicina basada en la evidencia (MBE). Ventajas" *Controversias en Cirugía Oral y Maxilofacial: Parte 1. Revista Española Cirugía Oral y Maxilofacial,* núm. 25, 2013, p. 265.

A pesar de ello, el propio Guyatt reconoce en su artículo que la Medicina Basada en la Evidencia tiene sus antecedentes en una base filosófica. De un lado, la MBE supone un nuevo paradigma promovido a mediados del siglo XIX por escépticos como Bichat y Magendie, que asientan las bases de la medicina teórica en el conocimiento procedente de lo empírico y de la praxis. De otro lado, el escepticismo nace en la Antigua Grecia, su mayor representante fue Pirrón (360-275 a.C.) quien defendió que no es posible conocer nada con certeza y, en consecuencia, el sabio debe abstenerse de emitir un juicio de valor. Por ello, la MBE se considera una medicina basada en el conocimiento empírico, puesto que a través de la experiencia clínica se puede deducir una medicina teórica que resuelva de la mejor manera posible desde la evidencia científica los problemas sanitarios cotidianos. La praxis es la base principal del método seguido por la MBE, donde el médico a través de su propia experiencia y su práctica cotidiana y, la compartida por el resto de los profesionales sanitarios, adquiere un buen criterio sanitario a efectos de realizar un diagnósticos más efectivo y eficiente sobre el paciente individual, lo que le permite a su vez, una mejor capacidad para tomar decisiones clínicas sobre el cuidado del paciente teniendo en cuenta las preferencias y derechos de este.

Desde una perspectiva práctica, los antecedentes de la MBE se remontan, por un lado, a finales de los años sesenta en la Escuela de Medicina de la Universidad MacMaster, donde David Sackett desarrolla un programa educativo cuyo objetivo era resolver problemas individuales, haciendo hincapié en la importancia de la epidemiología y el conocimiento estadístico en la práctica médica. Por otro lado, en la Universidad de Oxford se forma la cuna del Centro Cochrane (1992), donde el epidemiólogo británico Cochrane creó un grupo de trabajo compuesto por investigadores a fin de elaborar una base de datos que recopilara Revisiones Sistemáticas (RRSS) de Ensayos Controlados y Aleatorizados (ECA).

2. DEL PROCESO A SEGUIR POR LA MEDICINA BASADA EN LA EVIDENCIA Y ALGUNAS DE SUS VENTAJAS Y LIMITACIONES

La mayoría de los médicos y científicos reducen el proceso de la MBE en los siguientes pasos: (1) el paciente y la pregunta; (2) la búsqueda de información; (3) la evaluación, validez y aplicabilidad y; (4) el paciente y autoevaluación.

En un primer lugar, a partir del problema clínico del paciente se plantea una pregunta acerca del pronóstico, el tratamiento o una prueba diagnóstica, entre otros. En segundo lugar, a fin de dar una respuesta eficaz a la pregunta se localizan en las bases de datos las pruebas disponibles en las diferentes referencias bibliográficas. En tercer lugar, una vez localizadas las pruebas disponibles se realiza una evaluación crítica de la aplicabilidad y validez de estas. Por último, de esa evaluación crítica se obtiene una conclusión evidente que debe aplicarse a la práctica combinándose a su vez con la experiencia del profesional médico y con las preferencias del paciente, dando como resultado una decisión médica basada en la evidencia que se debe evaluar tras la aplicación del conocimiento obtenido.

Asimismo, las principales ventajas de la MBE las podemos resumir en los siguientes extremos[227]: (1) Disminución de la amplia variabilidad (injustificada) en la atención médica; (2) Reducción de la brecha entre la generación del conocimiento y su aplicación; (3) Superación de modas, propagandas, inducciones y otras formas de imposición; (4) Estimulación de la evaluación crítica del conocimiento establecido; (5) Estimulación para la práctica reflexiva; (6) Facilitación del aprendizaje de las estrategias de búsqueda y recuperación de la información; (7) Promoción de la capacidad de discernir entre información científica y no científica; (8) Promoción del establecimiento de un sistema propio de educación continuada; (9) Promoción de la interconexión entre la atención médica, la educación y la investigación biomédica; (10) Favorece la apreciación del valor de la verdad; (11) Favorece la apreciación del valor de la mejor alternativa y; (12) Eliminación de las alternativas que no representan las mejores opciones para los pacientes de acuerdo con el avance científico y tecnológico.

[227] JUNQUERA, BALADRÓN, ALBERTOS y OLAY, S., "Medicina basada…", *op. cit.,* p. 266.

Por consiguiente, puede comprobarse que, para el desarrollo de la MBE, es necesario contar con profesionales sanitarios con experiencia y con las evidencias deducidas de las investigaciones y experimentos científicos, a fin de poder tomar una decisión sanitaria eficiente en relación con el cuidado y tratamiento del paciente. Por tanto, la MBE exige que el profesional médico junto con sus saberes y habilidades para el desempeño de la medicina posea conocimientos básicos de estadística y de investigación biomédica y epidemiología clínica, a fin de aplicar el método apropiado para llegar a unos datos evidentes, ciertos y válidos a efectos de dar una respuesta al problema sanitario cotidiano que plantea el paciente, teniendo en cuenta a su vez las preferencias y valores de este. De igual modo, el paciente a través de la MBE recibe intervenciones más seguras y eficaces, por lo que el riesgo se disminuye de manera notoria, también permite que el paciente forme parte del propio proceso evolutivo de su enfermedad según sus preferencias, necesidades y derechos. Debido a lo anterior, algunos autores[228], sobre todo facultativos sanitarios, opinan que más que avanzar desde la MBE estamos avanzando hasta una "Medicina Generadora de Evidencia", puesto que con la búsqueda de información se generan nuevos conocimientos que antes no existían.

No obstante, la MBE también tiene algunas limitaciones y barreras[229], tales como, que limitan la libertad de ejercicio clínico, en ocasiones nos llevan a soluciones contradictorias, subestiman la pericia clínica, no puede desarrollarse en aquellos centros donde exista una carencia de tecnología como ordenadores, sistemas informáticos y acceso a una red rápida y automática, requiere de altos recursos económicos que permitan el acceso ilimitado a las bases de datos de información científica y sanitaria, implica que el paciente sea una persona con alto nivel educativo a fin poder transmitir sus preferencias y valores, cuando resultan comunes las facultades de comunicación

[228]Al respecto HERNÁNDEZ MEDRANO, I., "La sanidad ante el mundo del Big Data", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, p. 43, opina que: "Un ejemplo del poder del big data es el que representa cualquier plataforma capaz de analizar, resumir y presentar de forma sencilla la información médica contenida en el conjunto de Historias Clínicas Electrónicas o bien proveniente de la captura de datos de salud mediante tecnología móvil, para su reutilización en la práctica clínica, en tiempo real. Esta información reviste gran valor al presentar el fiel reflejo de la forma de pensar de los clínicos a la hora de enfrentarnos a los problemas de los pacientes, en condiciones reales de incertidumbre ("Real World Evidence"). Una información muy valiosa que no está en los libros ni en las publicaciones científicas. Dicho de otra forma, con ello estamos avanzando desde la Medicina Basada en la Evidencia, hacia un nuevo horizonte que podemos llamar Medicina Generadora de Evidencia, ya que con cada búsqueda literalmente se genera un nuevo conocimiento que previamente no existía".

[229] GARCÍA CAMPOS, J., ORTEGA DÍAZ, E. y HERNÁNDEZ SÁNCHEZ, S., "Ciencias de la salud basadas en le evidencia: hechos y reflexiones para la práctica clínica", *El Peu,* núm. 29, 2009, p. 211.

entre los médicos y los pacientes y, en algunos casos la MBE es aplicada como herramienta de reducción de costes.

3. LA RELEVANCIA DE LA PREGUNTA CLÍNICA

Por último, a modo de cierre del presente capitulo cabe destacar que, uno de los elementos comunes que supone a su vez la unión y vinculación existente entre el *big data* sanitario y la MBE es que ambos procesos se inician con el planteamiento de una pregunta clínica (algoritmo), a fin de obtener en los datos sanitarios información y conocimiento que colabore con el buen criterio y a la experiencia del facultativo médico a una toma de decisión eficiente. Principalmente, existen dos tipos de preguntas clínicas:

Por un lado, las preguntas básicas, compuestas por dos componentes y giran en torno a un tema general de una condición, cuya solución fácilmente se puede localizar en un manual de medicina especializado en el tema. Por otro lado, las preguntas específicas típicas de la MBE, que la componen como mínimo tres elementos (P.I.O. o P.I.C.O.)[230] acerca de conocimientos concretos de del problema y cuya respuesta se obtiene en distintos artículos científicos y bases de datos. Por tanto, estamos ante preguntas que surgen en tiempo real y que repercuten directamente en la toma de decisiones, por ello, es sumamente relevante desde una perspectiva sanitaria y clínica que la pregunta esté bien formulada, puesto que ello facilita la búsqueda de la evidencia mediante los descriptores apropiados.

[230]P: paciente, población o problema; I: intervención; C: comparación; O: outcome (resultado).

			Ejemplo
P	Paciente	¿Cómo describes al paciente que estás tratando? Sé preciso.	Prematuro de 1.850 g y dos semanas de vida con cuadro clínico-radiológico compatible con enterocolitis necrotizante
I	Intervención	¿Cuál es la intervención principal que estás considerando? Maniobra terapéutica, realización de una prueba diagnóstica, pronóstico de una enfermedad.	Terapia: laparotomía exploradora
C	Comparación (si procede)	¿Cuál es la principal alternativa con la que comparar la intervención?	Drenaje peritoneal y actitud expectante
O	*Outcome* (resultado)	¿Qué espero conseguir, medir, mejorar o en qué puede afectar la medida tomada?	Resultado 1: Supervivencia Resultado 2: Morbilidad

Imagen 7. La pregunta clínica[231]

Posteriormente, la pregunta formulada se debe centrar en un aspecto clínico concreto a fin de detectar el tipo de estudio que debemos realizar para obtener la mejor respuesta.

Aspecto clínico	*Estudio*
Tratamiento-Prevención	Ensayo clínico aleatorizado (ECA) o revisión sistemática (metaanálisis) de ECA
Pronóstico	Cohortes incipientes («de inicio») con análisis de supervivencia
Factores de riesgo-Etiología	Cohortes o caso-control con análisis multivariante
Diagnóstico	Transversal: comparación independiente con un patrón oro
Motivación	Cualitativo

Imagen 8. Tipo de estudio en función del aspecto clínico a responder[232]

Asimismo, el tipo de pregunta determinará la elección de la fuente de información o base de datos bibliográfica más apropiada. A fin de que la respuesta obtenida sea lícita y ética, resulta de suma importancia que previamente la pregunta formulada sea conforme a derecho, a la moral y al orden público, de tal forma que, desde una perspectiva jurídica y filosófica, lo importante y primordial no es tanto la respuesta obtenida, sino que lo relevante radica en cómo ha sido planteada la pregunta. Es decir, si la pregunta es conforme al derecho, a los principios generales del ordenamiento jurídico, a la moral y al orden público, por lógica, la respuesta que se deduzca de la misma también lo será.

[231] GARCÍA CAMPOS, ORTEGA DÍAZ y HERNÁNDEZ SÁNCHEZ, "Ciencias de la salud…", *op. cit.*, p. 221.

[232] GARCÍA CAMPOS, ORTEGA DÍAZ y HERNÁNDEZ SÁNCHEZ, "Ciencias de la salud…", *op. cit.*, p. 221.

De igual modo, el interés común podrá ser acreditado y justificado según el número de perjudicados o casos clínicos similares a los que pretenda dar una solución. De tal forma, que cuanto mayor sea el número de interesados, mayor será el interés común y social de poder acceder a los datos sanitarios que posean la información y conocimiento necesario a fin de obtener una solución evidente, válida y viable. Por consiguiente, el *big data* sanitario proporciona a la MBE información seleccionada y relevante, procedente de datos obtenidos a través de la estadística y la epidemiología (evidencia), a fin de que el facultativo médico mediante un juicio crítico obtenga la mejor evidencia científica disponible en la cuestión concreta planteada, evidencia que debe ser integrada y complementada con la propia experiencia clínica del profesional sanitario (pericia) y con las expectativas y preferencias del propio paciente (valores).

En definitiva, la MBE es la intersección entre evidencia, pericia y valores, de lo que se deduce, por un lado, que si el resultado obtenido aparentemente evidente es contradictorio a la experiencia (pericia) del facultativo médico, éste previamente a tomar una decisión al respecto, deberá solicitar una segunda opinión a un compañero especializado en el tema a fin de contrastar su propia experiencia con el resultado aparentemente evidente. Por otro lado, si el resultado evidente se aleja o contradice las preferencias y valores del paciente, el mismo deberá ser quien decida acerca de su aplicación o no, teniéndose en cuenta previamente la influencia de factores éticos, así como el código de deontología médica, puesto que por valores y preferencias se entiende las expectativas y perspectivas que tienen los propios pacientes acerca del cuidado de su salud.

Finalmente, ha de tenerse en consideración que aplicar la MBE requiere de recursos, tiempo, condiciones y motivación de la que no siempre disponen los facultativos sanitarios. Sin embargo, actualmente la MBE es el mejor método de practicar la medicina siendo esencial en la toma de decisiones sobre el cuidado de la salud de los pacientes gracias a las herramientas y técnicas desarrolladas por el *big data* sanitario.

CAPÍTULO TERCERO

ANÁLISIS CONTEXTUAL DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN EL RÉGIMEN JURÍDICO EUROPEO Y ESPAÑOL

I. EL ORIGEN DEL DERECHO DE PROTECCIÓN DE DATOS PERSONALES

Examinada la parte técnica sobre la tecnología *big data* en general y, de manera específica en el ámbito sanitario, a continuación, centraremos nuestra atención en el derecho de protección de datos personales regulado en el régimen jurídico comunitario y estatal realizándose un análisis sistemático y exhaustivo de su evolución histórica desde sus inicios hasta la actualidad, haciendo especial mención a los pronunciamientos más relevantes de la doctrina jurisprudencial europea y española.

1. ANTECEDENTES HISTÓRICOS DEL DERECHO DE PROTECCIÓN DE DATOS: EL ARTÍCULO 18.4 DE LA CONSTITUCIÓN ESPAÑOLA

En el ordenamiento jurídico español la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental al amparo del apartado cuarto del artículo 18 de la Constitución Española (en adelante CE) donde se establece 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".

A pesar de que el artículo 18.4 de la CE expresamente no hace referencia a la protección de datos como tal, ha sido a través de la interpretación jurisprudencial del citado precepto lo que ha dado como resultado una regulación autónoma e independiente del derecho a la protección de datos de carácter personal en España. Así pues, como se apreciará, el Tribunal Constitucional (TC) ha tenido un papel fundamental en la creación del derecho fundamental a la protección de datos de carácter personal. En consecuencia, resulta inevitable hacer referencia a la jurisprudencia constitucional cuando se trata de alguna cuestión jurídica sobre el derecho a la protección de datos de carácter personal. Por ende, desde sus primeras sentencias, el Tribunal Constitucional ha asentado las bases y criterios jurídicos sobre la protección de datos de las personas físicas, adaptando las mismas a la normativa jurídica europea, así como a las exigencias del contexto social del momento, sobre todo en los últimos años debido al cambio de paradigma generado por la era digital y las tecnologías.

En la primera sentencia que el Tribunal Constitucional se pronuncia acerca de la vulneración de los apartados primero y cuarto del artículo 18 CE, es en la STC 254/1993, de 20 de julio, donde procede a identificar en el artículo 18.4 de la Constitución un derecho fundamental de libertad informática[233] con el contenido del

[233] *Vid.* STC 254/1993, de 20 de julio, FJ 6, donde establece que: "Dispone el art. 18.4 C.E. 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". De este modo, nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama "la informática".

Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (Convenio 108) y ratificado por Instrumento de 27 de enero de 1984 (publicado en el B.O.E. de 15 de noviembre de 1985), y en vigor desde el 1 de octubre de 1985, debido a la ausencia de desarrollo legislativo del Art. 18.4 de la Constitución Española.

Por ende, en la referenciada sentencia a criterio de GONZÁLEZ MURUA "el Tribunal realiza el paso de una concepción negativa de este derecho a una positiva gracias a la interpretación del citado Convenio: «… la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaría positiva, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España» (Fundamento Jurídico séptimo)"[234]. Por consiguiente, debido a que en el momento de dictarse la sentencia no existía en el España desarrollo legislativo del artículo 18.4 de la CE, el TC en base a la interpretación realizada del Convenio 108 estimó la vulneración del citado precepto legal, en contra del criterio del Abogado del Estado y del Presidente del Tribunal don Miguel Rodríguez-Piñero y Bravo-Ferrer en su voto particular formulado en citado recurso de amparo, quien consideró que el derecho a la intimidad de las personas no debía obligar abiertamente a la Administración Pública a resolver, pronunciarse o una acción de hacer a consecuencia de una determinada cuestión planteada por un ciudadano, a lo que STC 254/1993 señala que:

"No es ocioso advertir que la reciente aprobación de la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal (L.O. 5/1992, de 29 octubre), no hace más que reforzar las conclusiones alcanzadas con anterioridad. La creación del Registro General de Protección de Datos, y el establecimiento de la Agencia de Protección de Datos, facilitarán y garantizarán el ejercicio de los derechos de información y acceso de los ciudadanos a los ficheros de titularidad pública, y además extienden su alcance a los ficheros de titularidad privada. Pero ello no desvirtúa el fundamento constitucional de tales derechos, en cuanto imprescindibles para proteger

[234]GONZÁLEZ MURUA, A.R., "Comentario a la S.T.C. 254/1993, de 20 de julio. Algunas Reflexiones en torno al Artículo 18.4 de la Constitución y la Protección de Datos Personales", *Revista Vasca de Administración Pública,* núm. 37, 1993, p. 233.

el derecho fundamental a la intimidad en relación con los ficheros automatizados que dependen de los poderes públicos. Ni tampoco exonera a las autoridades administrativas del deber de respetar ese derecho de los ciudadanos, al formar y utilizar los ficheros que albergan datos personales de éstos, ni del deber de satisfacer las peticiones de información deducidas por las personas físicas en el círculo de las competencias propias de tales autoridades" (FJ 9).

Así pues, según algunos autores, el objetivo fundamental del TC con la citada sentencia fue el de delimitar el alcance del artículo 18.4 CE al no existir ley específica aplicable al supuesto de hecho[235]. En concreto, según afirma FERNÁNDEZ SALMERÓN: "la cuestión fundamental se contraía, por tanto, a determinar cuál era el contenido – en definitiva, las facultades o derechos – que integraba el artículo 18.4 CE al margen de que no se hubiera materializado la intervención legislativa a que aludía el propio precepto"[236]. En este mismo sentido, en palabras de CASAS BAAMONDE, el TC concluyó "que el derecho fundamental a la intimidad no agota su contenido en facultades puramente negativas, de exclusión; «que la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)» (FJ7)"[237].

En suma, el TC en la sentencia 254/1993 establece el derecho de acceso a los datos como una dimensión positiva en conexión con el derecho a la intimidad, ya que en ese momento todavía no era concebido el derecho de protección de datos de carácter personal como un derecho autónomo e independiente[238]. Asimismo, en la STC

---

[235] GONZÁLEZ MURUA, "Comentario a la S.T.C. 254/1993, de 20 de julio…", *op. cit.*, pp. 227 y ss.; ARROYO YANES, L.M., "El derecho de Autodeterminación Informativa frente a las Administraciones Públicas (Comentario a la STC 254/1993, de 20 de julio)", *Revista Andaluza de Administración Pública,* núm. 16, 1993, pp. 119 y ss.; VILLAVERDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *Revista Española de Derecho Constitucional,* núm. 41, 1994, pp. 187 y ss.

[236] FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas,* Ed. Civitas Ediciones, Madrid, 2003, p. 72.

[237] CASAS BAAMONDE, M.E., "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional", *20 años de protección de datos en España. Agencia Española de Protección de datos,* 2015, pp. 91-126. Documento disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5156606 (última consulta 12/11/18).

[238]En este sentido, en el Fundamento Jurídico Sexto de la STC 254/1993, de 20 de julio se establece que "Esta constatación elemental de que los datos personales que almacena la Administración son utilizados

143/1994, de 9 de mayo, el Tribunal Constitucional señala que igualmente nos encontraríamos ante una vulneración del derecho a la intimidad a causa de una recogida de datos con fines legítimos y con contenido neutro pero que sin embargo no incluye "garantías adecuadas frente a su uso potencialmente inversor de la vida privada del ciudadano a través de su tratamiento técnico"[239].

A pesar de la novedosa jurisprudencia que relacionaba estrechamente el derecho a la intimidad con el derecho de protección de datos personales, algunos autores opinaron al respecto que "[…] no resulta correcta la utilización del término intimidad para referirse a la protección de los datos personales, lo que desgraciadamente ocurre no sólo en el lenguaje ordinario, sino también en organismos oficiales y en disposiciones normativas, pero que hace ya buen número de ellos, tal identificación es rechazada por la doctrina"[240]. Postura doctrinal que estaba en lo cierto, pues más tarde la propia jurisprudencia tanto europea como española consideraron el derecho de protección de datos como un derecho autónomo del derecho a la intimidad[241], como a continuación se apreciará.

---

por sus autoridades y sus servicios, impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración Pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 C.E., y que dan vida al derecho a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente (STC 11/1981, fundamento jurídico 8° y 101/1991, fundamento jurídico 2°)".

[239] *Vid.* STC 143/1994, de 9 de mayo, FJ7.

[240] Al respecto, VILARIÑO PINTOS, E. "Los derechos de la persona en el ámbito de las tecnologías de la información", en AA.VV., *El derecho a la intimidad y a la privacidad y las Administraciones Públicas,* (Dir. D. Bello Janeiro) Ed. Escola Galega de Administración Pública, Santiago de Compostela, 1999, p. 20.

[241] En este sentido, FERNÁNDEZ SALMERÓN, "La protección*…", op. cit.,* p. 82 afirma que "En efecto, en la STC 292/2000, de 30 de noviembre, a pesar de hacer de nuevo una concesión al derecho a la intimidad, el Alto Tribunal dedica gran parte de su argumentación a distinguir este derecho del que tiene por objeto la protección de los datos personales, lo que puede considerarse como una consolidación de su doctrina que en modo alguno puede desconocerse, tal y como ha sido enfatizado recientemente" citando al respecto a HERRÁN ORTIZ, A.I., "A propósito de la Ley Orgánica de Protección de Datos Personales y los problemas sobre su inconstitucionalidad", en AA.VV., *Quince años de Encuentros sobre Informática y Derecho (1987-2002)* (Coord. M. A. Davara Rodriguez), Tomo II, Ed. Universidad Pontificia de Comillas, Instituto de Informática Jurídica, Madrid, 2002, pp. 695-696.

2. EL DERECHO DE PROTECCIÓN DE DATOS: UN DERECHO FUNDAMENTAL AUTÓNOMO DEL DERECHO A LA INTIMIDAD

En el ámbito sanitario, el derecho de protección de datos de salud se encuentra estrechamente vinculado con el derecho a la intimidad del paciente, pues en gran medida proteger los datos del titular tiene como finalidad principal la de proteger su intimidad. Sin embargo, en las últimas décadas hemos sido testigos de un cambio de paradigma social debido a la influencia de las nuevas tecnologías, revolución que ha provocado que el Derecho y con ello, el ordenamiento jurídico europeo y español se adapte a las nuevas circunstancias a fin de dar una respuesta y solución jurídica a los conflictos que puedan surtir en relación a la protección de datos y la libre circulación de los mismos, apareciendo así una nueva regulación jurídica que permita la libre circulación de los datos garantizando un tratamiento de los mismos por medio de garantías que protejan la intimidad de sus titulares.

Desde una perspectiva del Derecho Sanitario, como se verá más adelante, la intimidad del paciente es un derecho fundamental a proteger por el ordenamiento jurídico debido a que nos encontramos ante datos que resultan especialmente sensibles, situación que en los últimos años ha dado un giro debido a las ventajas que implican para una efectiva asistencia sanitaria y tratamiento médico, entre otros, el hecho de poder acceder a los datos sanitarios y sustraer por medio de técnicas de *big data* conocimiento e información relevante para el progreso del propio enfermo, así como de las Ciencias de la Salud y, en consecuencia, una mejora del bienestar de la humanidad, lo que ha dado lugar al conflicto denominado por la mayoría de la doctrina intimidad del paciente versus interés público, encontrándose latente la tensión jurídica entre el derecho de protección de datos y la progresiva evolución de la tecnología.

2.1. Aspectos conceptuales

A continuación, se analizarán las expresiones “intimidad” y “datos personales” desde una perspectiva propiamente conceptual y jurídica a fin de alcanzar una mayor compresión sobre las argumentaciones dadas por la propia doctrina y jurisprudencia que determinan la autonomía del derecho de protección de datos personales frente al

derecho a la intimidad, fundamentaciones jurídicas que serán analizadas *in fine* a modo de clausura del presente apartado.

A) El concepto de intimidad personal

La protección del derecho a la intimidad personal y familiar aparece en un primer lugar regulada en el artículo 18.1 de la Constitución Española, donde se le reconoce juntamente con el derecho al honor y a la propia imagen, como derechos fundamentales debido a que se refieren a la vida privada de las personas[242] sin que la privacidad sea identificación individual de cada uno de ellos[243], trascendiendo los tres referenciados derechos en una evidente manifestación del derecho a la integridad moral regulado en el artículo 15 de la Constitución[244], siendo a su vez un límite a la libertad de expresión y al derecho a la información según el artículo 20.4 de la Constitución y, que al tratarse de derechos fundamentales están igualmente protegidos por el artículo 53 de la Constitución. En concreto, el Tribunal Constitucional en la Sentencia núm. 231/1988, de 2 de diciembre[245], establece que:

"Los derechos a la imagen y a la intimidad personal y familiar reconocidos en el art. 18 de la C.E. aparecen como derechos fundamentales estrictamente vinculados a la propia personalidad, derivados sin duda de la «dignidad de la persona», que reconoce el art. 10 de la C.E., y que implican la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario - según las pautas de nuestra cultura- para mantener una calidad mínima de la vida humana. Se muestran así esos derechos como personalísimos y ligados a la misma existencia del individuo".

[242] En este sentido el TC señala en el Auto 257/1985, de 17 de abril, FJ 2º, que "el derecho a la intimidad que reconoce el art. 18.1 de la C.E. por su propio contenido y naturaleza, se refiere a la vida privada de las personas individuales, en la que nadie puede inmiscuirse sin estar debidamente autorizado, y sin que en principio las personas jurídicas, como las Sociedades mercantiles, puedan ser titulares del mismo, ya que la reserva acerca de las actividades de estas Entidades, quedarán, en su caso, protegidas por la correspondiente regulación legal, al margen de la intimidad personal y subjetiva constitucionalmente decretada".

[243] REBOLLO DELGADO, L., "Derechos de la personalidad y datos personales", *Revista de Derecho Público,* núm. 44, 1998, p. 158.

[244] ZAVALA DE GONZÁLEZ, M.M., *Derecho a la Intimidad*, Ed. Abeledo-Perrot, Buenos Aires, 1982, p. 29.

[245] STC 231/1988, de 2 de diciembre.

Así pues, debido a que nos encontramos ante derechos estrechamente vinculados con los derechos de la personalidad procedentes de la dignidad humana y destinados a la protección del patrimonio de las personas, el ordenamiento jurídico los protege de manera específica y especial por medio de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Sin embargo, se ha tener en consideración que cada uno de estos derechos posee su propio contenido y específica regulación jurídica, así como sustantividad[246], por ello en el presente apartado nos centraremos exclusivamente en el derecho a la intimidad por su estrecha vinculación al tratamiento de datos sanitarios. Asimismo, hacer mención que el derecho a la intimidad también se encuentra protegido por el Derecho Penal con la tipificación de ciertos delitos contra la intimidad, como pudiera ser, la revelación de secretos y, el delito de calumnias e injurias, entre otros.

De manera general, el derecho a la intimidad subyace vinculado con la vida privada de la persona, lo que supone un reconocimiento al ser humano de una esfera personal, secreta, propia, privada e íntima, así como el reconocimiento de una vida personal exclusiva para la persona y excluyente para el resto de la sociedad. Por tanto, el derecho a la intimidad tiene dos vertientes según el Alto Tribunal: (1) una vertiente negativa, en el sentido de que nos encontramos ante una zona de actividad privada que es propia del individuo respecto a la cual se puede prohibir el acceso a los demás, existiendo un poder de exclusión *erga omnes* de ese derecho y; (2) una vertiente positiva, en cuanto a acción que implica la facultad de su titular de control de los datos y de la información relativos a esta esfera privada, en este sentido, el titular puede controlar y disponer de sus datos como estime oportuno, siendo el contenido de esa esfera privada los datos que el propio titular desea mantener privados y además, puede decidir sobre el conocimiento. Por consiguiente, de conformidad con la doctrina jurisprudencial asentada por el Tribunal Constitucional, la intimidad, se atribuye tanto al

[246] GRIMALT SERVERA, P., "La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y libertades en internet", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica,* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, p. 69, afirma que: "Si bien la protección de la vida privada en general y muy especialmente de la intimidad en particular son esenciales, como se dirá, para el desarrollo de la personalidad, la intimidad no es un derecho absoluto; esto es, en algunas ocasiones los derechos que conforman la vida privada de una persona entrarán en colisión con otros derechos y libertades y éstos prevalecerán sobre la intimidad, o sobre el honor o sobre la propia imagen".

individuo aislado como a su núcleo familiar[247]. De igual modo, según el Tribunal Constitucional se trata "de un derecho personalísimo y ligado a la misma existencia del individuo, aunque en algunas ocasiones los efectos de la intromisión se extienden a otras personas en atención a la especial relación o vinculo existente"[248] y se reconoce incluso "a las personas más expuestas al público"[249].

A los efectos de destacar los caracteres esenciales del derecho a la intimidad, la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, el artículo 1 en su apartado primero establece que "el derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo segundo de esta ley".

En primer lugar, el derecho a la intimidad es un derecho irrenunciable, en el sentido de que toda renuncia a la protección regulada por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, es nula de pleno derecho. Ahora bien, cosa distinta es que la persona titular del derecho a la intimidad decida voluntariamente no ejercitar la acción en caso de vulneración del mismo. Además, el legislador posibilita que el titular consienta esa intromisión, pero en ningún caso viene a suponer una renuncia a su derecho. Igualmente, el supuesto de consentimiento no se opone a la irrenunciabilidad del derecho debido a que el consentimiento es puntual y concreto, es decir, el titular cuando presta su consentimiento no lo está prestando de manera genérica e indefinida, sino para un acto concreto y determinado[250].

---

[247] *Vid.* STC 231/1988, de 2 de diciembre, STC 197/1991 y STC 197/1991, de 17 de octubre.

[248] STC 231/1988, de 2 de diciembre.

[249] STC 134/1999, de 15 de julio, donde en el caso de una persona de alcance público, resulta evidente que su círculo íntimo es más reducido, no tanto por la persona en sí misma considerada, sino por el cargo o puesto que ostenta, aunque si la actividad pública que desarrolla afecta a una generalidad de ciudadanos, estos tienen derecho a acceder a parte de datos que tenga alguna relación con su actividad profesional, pero en ningún caso cabría afirmar que una persona con una proyección pública no tenga vida privada.

[250] Al respecto, el TC señala que: "corresponde, pues, a cada individuo reservar un espacio, más o menos amplio según su voluntad, que quede resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio. Y, en correspondencia, puede excluir que los demás, esto es, las personas que de uno u otro modo han tenido acceso a tal espacio, den a conocer extremos relativos a su esfera de intimidad o prohibir

En segundo lugar, nos encontramos ante un derecho inalienable, en el sentido de que no se puede transmitir *inter vivos* debido principalmente a que no cabe la cesión de este. Asimismo, tampoco es trasmisible por actos *mortis causa* puesto que es un derecho inherente a la persona, esencial a la personalidad, encontrándose íntimamente unido a la persona de su titular, lo que significa que se extinguen con la muerte del titular, no formando parte de su herencia. Lo anterior, no es obstáculo a efectos de que, tras la muerte del titular, la persona que el mismo designe expresamente en su testamento o, en su defecto, su cónyuge, descendientes, ascendientes y sus hermanos o, en defecto de los anteriores, el Ministerio Fiscal, se encuentren legitimadas para ejercer una acción reclamando su protección, lo que no implica en ningún caso la transmisión del derecho, se trata más bien de proteger la memoria del difunto, en cuanto que esa memoria es una prolongación de su personalidad[251].

En tercer lugar, es un derecho imprescriptible, por ende, no se agota con el trascurso del tiempo, aunque no se ejercite, no obstante, se ha de tener presente que las acciones caducan a los cuatro años en caso de vulneración del derecho.

Igualmente, se ha de tener en consideración que el derecho a la privacidad es un derecho inherente, esto es, es un derecho innato a la persona, nace con la persona y se extingue con su muerte, por ello es un derecho intrasmisible, así como su carácter de extrapatrimonialidad, en el sentido de que no tiene contenido patrimonial, aunque en caso de vulneración sí que es susceptible de indemnización por daños y perjuicios a causa de la intromisión e igualmente, la persona es libre de comercializar con su derecho a la intimidad consintiendo esa intromisión ilegítima, pero eso no significa que tenga un carácter patrimonial propiamente dicho. Por lo que se refiere a la intromisión ilegítima del derecho a la intimidad en el artículo 7 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen se establecen conductas que invaden el circulo de la esfera privada de las personas sea cual fuere el método empleado para ello. En concreto, en el artículo 7, apartados 1, 2, 3 y 4 se regulan las siguientes conductas que tendrán consideración de intromisiones ilegítimas en el ámbito de protección del derecho a la intimidad:

---

su difusión no consentida, salvo los límites, obvio es, que se derivan de los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos" (STC 115/2000, de 5 de mayo, FJ 4º).

[251]REBOLLO DELGADO, L., *El Derecho Fundamental a la Intimidad,* Ed. Dykinson, Madrid, 2005, p. 186.

"El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación de contenido de cartas, memorias u otros escritos personales de carácter íntimo. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela".

Así pues, en interpretación del anterior precepto, se ha distinguir entre dos supuestos fundamentales de intromisión a la intimidad; por un lado, intromisión ilegítima a la vida privada por medio de obtención de información perteneciente al ámbito de la intimidad de esa persona y; por otro lado, la divulgación o revelación de esos datos por medio de la publicidad de los mismos[252].

De igual modo, se ha de señalar que el contenido fundamental del derecho a la intimidad engloba: la intimidad corporal, la intimidad personal, la intimidad económica, la relacionada con la salud, la vida sexual (excepto casos de acoso), la genética[253] y la

[252] No en vano, se ha de tener en consideración que la ley regula algunos supuestos en los que a pesar de darse las anteriores conductas del artículo 7 considera que no existe intromisión al delimitar su protección. En concreto, los límites generales son los detallados a continuación: por un lado, la propia delimitación establecida por ley, donde no se apreciará la existencia de intromisión cuando la conducta se encuentre expresamente autorizada por ley. Por otro lado, delimitación asentada por los propios usos sociales o por los propios actos del titular del derecho, en este supuesto se atiende a las costumbres o a la práctica que impere en cada momento determinado, así como a las pautas de comportamiento del propio sujeto, teniéndose en cuenta tanto el entorno social, como los actos propios del sujeto. En tercer lugar, delimitación por autorización o decisión de la autoridad de acuerdo con la ley, fundamentalmente a la autoridad judicial. Por último, delimitación que dimana del consentimiento del titular del derecho, siempre y cuando el consentimiento reúna los requisitos legales, que en el caso de tratamiento de datos de salud serán estudiados más adelante en el presente trabajo.

[253] En relación con el derecho a la intimidad genética se ha de hacer constar que este derecho antes de la normativa vigente de protección de datos ya tenía una serie de limitaciones en el caso de que el interés general se estimara más importante que el particular sobre todo en casos de investigación criminal, *Vid.* al respecto CÓRDOBA GARCÍA, F., "La privacidad genética: Concepto, fundamentos y consecuencias", en AA.VV., *Nuevos conflictos sociales. El papel de la privacidad* (Coords. E. Anarte Borrado, F. Moreno Moreno y C.R. García Ruíz), Ed. Iustel, 2015, Madrid, pp. 22-23 y, también, CALVO GALLEGO, F.J., "Test genéticos y vigilancia de la salud del trabajador", *Revista Digital de Seguridad y Salud en el Trabajo,* núm. 1, 2008, pp. 1-18.

protección de los datos personales ante una divulgación ilícita[254]. Por ello, en el ámbito sanitario el derecho a la intimidad del paciente es sumamente relevante, puesto que es un sector donde la información acerca del mismo resulta esencial a efectos de garantizar una asistencia sanitaria de calidad hasta el extremo de que el paciente deba proporcionar datos acerca de su salud y estado físico, debiendo colaborar, en todo caso, para su obtención en el supuesto de no constar previamente registrados, lo que conlleva que las instituciones sanitarias y los profesionales sean recaudadores de todo tipo de datos especialmente sensibles, no únicamente de datos de salud.

En consecuencia, a pesar de que la Ley Orgánica 1/1982, de 5 de mayo*,* regula de manera específica la protección civil del derecho a la intimidad personal y familiar, sin embargo, ni el citado texto legal, ni la Carta Magna ni otra norma jurídica del ordenamiento jurídico español definen el derecho a la intimidad, siendo la jurisprudencia del Tribunal Constitucional[255] la que ha tenido que configurar un definición acerca del mismo, por lo que se ha se ha apreciado una evolución significativa - a consecuencia de los continuos cambios sociales provocados por las nuevas tecnólogas, así como por el IoT[256]– sobre el concepto de derecho a la intimidad a lo largo de la jurisprudencia: "[…] en la que se abandona la tentativa de una definición sustantiva o material de este derecho, que como ya se ha dicho no ha sido demasiado

[254] MARTÍNEZ MARTÍNEZ, R., "El derecho a la vida privada en España", en AA.VV., *El debate sobre la privacidad y seguridad en la red: Regulación y mercados,* (Coords. J. Pérez Martínez y Badía y Liberal), Ed. Ariel, Barcelona, 2012, p. 126.

[255] STC 134/1999 de 15 de julio, F.J.5ºdonde se señala que: "El art. 18.1 C.E. no garantiza una "intimidad" determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio. Del precepto constitucional se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a la de su familia, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida, lo que ha de encontrar sus límites, como es obvio, en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos".

[256] PARDO LÓPEZ, M.ª M., "No sólo protección de datos personales en internet: de los conceptos jurídicos híbridos, las categorías mutantes y otras evoluciones en curso", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica,* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 92-93.

exitosa, y se opta por un concepto formal en función del cual es el particular, el que, en ejercicio de esta autodeterminación, delimita el ámbito de su intimidad"[257].

Por consiguiente, nos encontramos ante un derecho fundamental de "autodeterminación individual de las personas físicas" [258] cuya finalidad principal es la de garantizar a la persona una esfera privada y reservada de su vida frente a la intromisión y conocimiento de un tercero en particular o, bien, de la sociedad en su conjunto, incluyéndose los poderes públicos, dado que puede ser vulnerado con mayor facilidad en el ámbito informático tras el control que se ejerce sobre los datos personales en los archivos electrónicos registrados sobre todo en la Administración Pública como organismo con mayor datos registrados de los ciudadanos debido a su función gestora y administrativa estatal de interés general[259]. En concreto, como doctrina relevante se ha de destacar a LUCAS MURILLO, quien considera que la autodeterminación informativa:

"[…] en cuanto que posición jurídica subjetiva correspondiente al *status de habeas data*, pretende satisfacer la necesidad, sentida por las personas en las condiciones actuales de la vida social, de preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática y de los peligros que esto supone. El objetivo se consigue por medio de lo que se denomina la técnica de protección de datos, integrada por un conjunto de derechos subjetivos, deberes, procedimientos, instituciones y reglas objetivas […] Es, por tanto, algo más que la esfera negativa de los tradicionales derechos de libertad. Este plus y la naturaleza

[257] DE MIGUEL SÁNCHEZ, N., *Tratamiento de datos personales en el ámbito sanitario: intimidad "versus" interés público,* Ed. Tirant lo blanch, Valencia, 2004, p. 25.

[258] VALERO TORRIJOS J. y LÓPEZ PELLICER, J.A., "Algunas consideraciones sobre el derecho a la protección de datos personales en la actividad administrativa", *RVAP,* núm. 59, 2001, p.274, sostienen que: "en cuanto tipo de libertad, el derecho fundamental de intimidad se inscribe en el ámbito de la autonomía o, se si quiere, de autodeterminación individual de las personas físicas para proteger una zona de su vida privada que queda así reservada frente a interferencias ajenas, incluidas las que provengan de los poderes públicos y no sólo de terceros particulares". En el mismo sentido, CARRILLO LÓPEZ, afirma que el derecho a la intimidad tiene la potestad de controlar la información que circula en la esfera pública, sobre todo en Internet y en las redes sociales, *Vid.* CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación", en AA.VV., *El derecho a la privacidad en el nuevo entorno tecnológico,* XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Ed. Centro de Estudios Políticos y Constitucionales, Madrid, 2016, p. 14; y,

[259] Al respecto, HERRERO TEJEDOR, F., *Honor, intimidad y propia imagen,* Ed. Colex, Madrid, 1990, p. 40 y, ROVIRI VIÑAS, A., "Reflexiones sobre el derecho a la intimidad en relación a la informática, la medicina y los medios de comunicación", *Revista de Estudios Políticos,* núm. 77, 1992, pp. 259 y ss.

compleja de este derecho, con sus aspectos institucionales, funcionales, objetivos, lo integran en el conjunto de las categorías modernas que jalonan la progresiva evolución de los derechos fundamentales al ritmo de los tiempos"[260].

En este sentido, cabría afirmar que la autodeterminación informativa abarca todo lo referente a la técnica de protección de datos (derechos, deberes, procedimientos, instituciones y reglas objetivas), otorgando una serie de facultades y poderes de control a sus titulares correspondiente al *status de habeas data*[261]. En consecuencia, como más adelante se expondrá, estas facultades y poderes de control que los titulares tienen sobre sus datos personales con independencia de su naturaleza, así como la existencia de procedimientos específicos para ejercer los derechos subjetivos dimanantes de la autodeterminación informativa, es lo que caracteriza al derecho de protección de datos como un derecho fundamental e independiente del derecho a la intimidad[262].

B) El concepto de dato de carácter personal

Una vez analizado el concepto de intimidad personal en el epígrafe anterior, otras de las vertientes a analizar son los datos personales a fin de destacar las diferencias y similitudes que ha generado una regulación autónoma y específica del derecho de protección de datos, haciéndose a su vez especial mención al concepto de "tratamiento" como concepto estrechamente vinculado con el mencionado derecho.

a) El concepto de dato de carácter personal en el marco jurídico de la Unión Europea y de la interpretación del TJUE

En concreto, en este apartado se muestra un estudio sobre el concepto de dato de carácter personal existente hasta el momento por las dos normas jurídicas europeas más relevantes en materia de protección de datos personales: la Directiva 95/46 y el vigente RGPD, así como la interpretación y definición dada sobre el citado concepto por parte

[260] LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación,* Tecnos, Temas clave, Madrid, 1990, pp. 173-174.

[261] MARTÍNEZ MARTÍNEZ, R., *Una aproximación crítica a la autodeterminación informativa,* Civitas Ediciones, Madrid, pp.253-254.

[262] MARTÍNEZ MARTÍNEZ, *Una aproximación…, op. cit.,* pp. 254-255.

del Tribunal de Justicia de la Unión Europea (TJUE). De antemano, se ha de destacar que, en relación con el concepto de dato de carácter personal, el artículo 2 apartado a) de la Directiva 95/46/CE, define dato de carácter personal como:

"[…] toda información sobre una persona física identificada o identificable (el interesado)", aclarando en el artículo 2 que "se considera inidentificable 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".

Por consiguiente, dato personal según la Directiva 95/46/CE engloba toda información diversa recopilada mediante por la cual se puede identificar a una persona determinada[263]. Al respecto el TJUE concluye "que el respeto del derecho a la vida privada en lo que atañe al tratamiento de los datos de carácter personal se aplica a toda información sobre una persona física identificada o identificable"[264].

En este sentido, sobre los datos referentes al nombre y apellidos de una persona, así como los datos fiscales, sus ingresos de trabajo y capital, sus funciones en una determinada organización, aficiones, situación familiar y datos de contacto - como pudieran resultar el número de teléfono o dirección de correo electrónico – la jurisprudencia unánime dictada por el TJUE concluye que nos encontramos ante datos de carácter personal que entrarían dentro del artículo 2 a) de la Directiva 95/46, destacando entre otras, lo que establecen las siguientes sentencias:

---

[263] Sobre el concepto de dato de carácter personal aclara VALERO TORRIJOS, J., "Las quiebras en internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesario superación de un modelo desfasado", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica,* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 42-43 que: "Así pues, el concepto de dato de carácter personal se subordina a la posibilidad de identificar de forma directa o indirecta a la persona física vinculada a una determinada información, lo cual nos obliga a plantearnos el alcance de esa identificabilidad, especialmente por lo que se refiere al sujeto activo que la pretende. Este proceso adquiere una singular relevancia en el caso de Internet por lo que se refiere, fundamentalmente, a dos instrumentos cuyo uso resulta imprescindible en dicho ámbito o, cuando menos, se encuentra ciertamente generalizados: es el caso de las llamadas direcciones IP y del correo electrónico respectivamente".

[264] Véanse Sentencias de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, Rec. p. I-11063, apartado 52, y de 24 de noviembre de 2011, ASNEF y FECEMD, C-468/10 y C-469/10, Rec. p. I-12181, apartado 42; STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz), apartado 26.

"El concepto de «datos personales» que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva «toda información sobre una persona física identificada o identificable». Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones […] la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del artículo 3, apartado 1, de la Directiva 95/46" (STJCE de 6 de noviembre de 2003, asunto C-101/01 (caso Lindqvist), §§24,27).

"Procede observar que los datos a los que se refiere dicha cuestión, referentes al apellido y nombre de determinadas personas físicas cuyos ingresos sean superiores a ciertos umbrales y, en particular, con una aproximación de 100 euros, los datos relativos a sus rendimientos del trabajo y del capital, son datos personales en el sentido del artículo 2, letra a), de la Directiva, puesto que se trata de «información sobre una persona física identificada o identificable» (véase igualmente la sentencia de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C-465/00, C-138/01 y C-139/01, Rec. p. I-4989, apartado 64)" (STJCE (Gran Sala) de 16 de diciembre de 2008, asunto C-73/07 (caso Satakunnan Markkinapörssi y Satamedia), §§ 35).

"A este respecto, procede observar, basándose en las indicaciones facilitadas por el órgano jurisdiccional remitente, que los datos fiscales transferidos por la ANAF a la CNAS constituyen datos personales en el sentido del artículo 2, letra a), de dicha Directiva, puesto que se trata de «información sobre una persona física identificada o identificable» (sentencia Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 35). Tanto su transmisión por la ANAF, organismo encargado de la gestión de la base de datos en donde se recopilan, como su tratamiento subsiguiente por la CNAS tienen por lo tanto carácter de «tratamiento de datos personales» en el sentido del artículo 2, letra b), de la propia Directiva" (TJUE (Sala Tercera) de 1 de octubre de 2015, asunto C-201/14, (caso Bara), §§ 29).

"Procede señalar que, en el apartado 104 de la sentencia recurrida, el Tribunal declaró acertadamente, al examinar el artículo 2, letra a), del Reglamento nº 45/2001, es decir, la definición del concepto de «datos personales», que los nombres y apellidos pueden considerarse datos personales" (STJUE (Gran Sala) de 29 de junio de 2010, asunto C-28/08 (caso Comisión/Bavarian Lager), §§ 68).

De la misma forma, la Directiva 95/46/CE en el artículo 3 y en el considerando 12, se establece la exclusión del tratamiento de datos por parte de una persona física en el "ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones", así como el tratamiento de datos cuya finalidad sea la "seguridad púbica, la defensa, la seguridad del Estado y las actividades del Estado en materia penal". Al respecto, el TJUE concluye que:

"En cuanto al concepto de «tratamiento» de dichos datos que utiliza el artículo 3, apartado 1, de la Directiva 95/46, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales». Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole"[265].

De manera general, según estima el TJUE, el concepto de "tratamiento" abarca toda operación u operaciones que faciliten el acceso a los datos personales, indistintamente que se realicen o no por medio de procedimientos automatizados, siendo suficiente que por medio de la misma se acceda a los datos personales[266]. De igual modo, el Grupo de Trabajo del Art. 29 de la Directiva 95/46/CE en el Dictamen 4/2007, de 20 de junio sobre el concepto de datos personales, aclara que el legislador europeo percibe el concepto de información de una manera amplia, incluyendo tanto la

[265] *Vid.* la STJCE de 6 de noviembre de 2003, asunto C-101/01 (caso Lindqvist), §§ 26.

[266] PARDO LÓPEZ, "No sólo protección de datos personales en internet…", *op. cit.,* p. 109, afirma que: "La voluntariedad en la recogida y tratamiento de la información es un elemento esencial del derecho a la protección de datos personales".

información objetiva como subjetiva de una determinada persona física, no siendo necesario que la información sea verídica o esté aprobada a fin de ser protegida.

Al hilo del análisis del concepto de dato personal en el marco jurídico europeo, en el RGPD se aprecia una cierta evolución en relación a la definición del mismo, en concreto, en el artículo 4 del RGPD a modo de aclaración se citan ejemplos de lo que se debe entenderse por datos personales, tales como: el 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 una determinada persona física. Parece claro que en virtud del RGPD, son datos personales el nombre y apellidos de una persona, su domicilio, dirección de correo electrónico de tipología "nombre.apellido@empresa.com/es", número de documento de identidad, datos de localización, dirección de protocolo de internet (IP)[267], identificador de una cookie y datos en motores de búsqueda[268], identificador de la publicidad del teléfono, datos relativos a las personas físicas constituidos por sonido e imagen y, sobre la esfera sanitaria, los datos (incluyendo símbolos) registrados en un centro sanitario o el archivo de un facultativo médico que nos permiten identificar de manera univoca a una determinada persona[269]. En contra, no se considerarán datos personales, *v.gr.,* número de registro mercantil, dirección de correo electrónico de tipología "info@empresa.com/es" o los datos anonimizados, extremo éste último que será analizado más adelante.

En el citado texto legal se aprecia un cambio notorio en relación con la exclusión de su aplicación, donde se concretan aquellos datos que el legislador europeo considera dejar fuera del RGPD. Así pues, no serán considerados datos personales de conformidad con el RGPD: (1) los datos personales procedentes del ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; (2) los datos

[267] Citar al respecto la STJUE (Sala Tercera) de 24 de noviembre de 2011, asunto C-70/10 (caso Scarlet), apartado 51 y STJUE (Sala Segunda) de 19 de octubre de 2016, asunto C-582/14 (caso Breyer), apartado 4.

[268] *Vid.* STJUE (Gran Sala) de 13 de mayo de 2014, asunto C-131/12 (caso Google), apartado 27.

[269] Se ha de tener presente para el caso de datos de localización y de identificador de una cookie, puede existir legislación sectorial específica que regule el uso de los mismos, como la Directiva sobre intimidad y comunicaciones electrónicas (Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 (*Vid.* D.O. L 201 de 31 de julio de 2002, p. 37) y, el Reglamento (CE) N.º 2006/2004 del Parlamento Europeo y del Consejo, de 27 de octubre de 2004 (*Vid.* D.O. L 364 de 9 de diciembre de 2004, p. 4).

personales derivados por parte de los Estados miembros cuando llevan a cabo actividades sobre política exterior y seguridad común[270]; (3) aquellos datos que procedan de actividades efectuadas por una persona física exclusivamente personales o domésticas y; (4) como novedad se excluye del ámbito de aplicación aquellos datos procedentes "por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención".

b) El concepto de dato de carácter personal en la legislación española y la reciente interpretación de la doctrina jurisprudencial del TC y del TS

En el ordenamiento jurídico español se puede apreciar en los diversos cambios legislativos sobre el derecho de protección de datos que el concepto de dato de carácter personal ha ido evolucionando. En un principio, como se ha visto anteriormente, el concepto de dato personal se encontraba estrechamente vinculado con el derecho de la intimidad, por ende, en virtud del artículo 18 de la CE, dato personal era todo dato en relación con la intimidad de una persona. Posteriormente, con la publicación de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), el legislador español definió los datos de carácter personal como "cualquier información concerniente a personas físicas identificadas o identificable", en virtud de lo establecido en el artículo 3 a) del citado texto legal. Esta definición permitió que el TC pudiera ampliar el concepto de dato personal, estableciendo desde un principio una doctrina jurisprudencial al definir el dato personal como toda información que permite identificar a una persona indistintamente de que la misma pertenezca o no a la intimidad del titular, siempre y cuando por medio de esos datos podamos identificar a una persona determinada. A modo de ejemplo, destacar la STS/1998, de 4 de mayo, anteriormente citada, donde el TC señala que el derecho de protección de datos "consagra un derecho fundamental autónomo 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" (FJ6).

[270] Actividades reguladas en el capítulo 2 del título V del TUE.

De igual modo, recordando lo comentado en el apartado anterior, la STC 292/2002 nuevamente establece un nuevo concepto de dato de carácter personal otorgando una concepción amplia del mismo, donde el TC detallada de manera más concreta desde una perspectiva jurídica la definición de dato de carácter personal como aquellos datos que no únicamente engloban los datos íntimos de la persona, sino cualquier dato que permita la identificación de la persona incluyendo los datos públicos, así lo establece en el Fundamento Jurídico Sexto:

"[…] De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 C.E. otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

Es clara la ampliación que realiza el TC sobre el concepto de dato personal, definiendo al mismo como cualquier dato personal indistintamente de que sea íntimo o no, cuyo uso por terceros pueda suponer una vulneración de los derechos – fundamentales o no - del titular y, cuya utilización por terceros pueda suponer una amenaza en determinadas circunstancias para su vida privada o íntima. Por tanto, el TC incluye dentro de los datos personales los datos públicos, en concreto, cualquier dato que identifique o permita identificar a una persona concreta, pudiéndose conocer a través de su uso o acceso más información acerca de su identidad.

Asimismo, en la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se respeta la definición de datos personales estatuida por el legislador europeo en la Directiva 95/46/CE, reiterando la misma en el apartado a) del artículo 3, estableciendo que los datos de carácter personal son "cualquier información concerniente a personas físicas identificadas o identificables". Sin embargo, por medio del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal se detalla en el artículo 5 apartado f) que los datos de carácter personal son "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables", abarcando por tanto, todo tipo de información, donde se incluye la "identidad física, fisiológica, psíquica, económica, cultural o social", de conformidad con lo establecido en el artículo 2 de la Directiva 95/46/CE.

En suma, en el citado R.D. 1720/2007 se identifican tres niveles de medidas de seguridad obligatorias – nivel básico, nivel medio y nivel alto – en función de las distintas tipologías de datos personales de los que se disponga en cada fichero, efectuándose una concepción específica sobre el concepto de dato personal según su tipología. Así pues:

En primer lugar, en el nivel básico se regulan: (1) los datos personales registrados en el fichero que afectan a todos los ficheros o tratamientos de datos de carácter personal; (2) los datos personales sobre ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual cuando la única finalidad es realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o caso de ficheros que de forma accesoria contengan estos datos; (3) los datos de carácter personal en relación al grado de discapacidad o invalidez (salud) únicamente para el cumplimiento de los deberes públicos. Con relación a las medidas de seguridad obligatorias para los datos de carácter personal registrados en el nivel básico, se regulan: el documento de seguridad; el régimen de funciones y obligaciones del personal; registro de incidencias; identificación y autentificación de usuarios; control de acceso; gestión de soportes; copias de respaldo y recuperación, verificación semestral; almacenamiento de ficheros no automatizados o en papel bajo llave; pruebas sin datos reales.

En segundo lugar, en el nivel medio se localizan los datos registrados en ficheros sobre: (1) infracciones administrativas o penales; (2) prestación de servicios de información sobre solvencia patrimonial y crédito. Cumplimiento o incumplimiento de obligaciones dinerarias; (3) los datos de carácter personal en relación con las Administraciones Tributarias; (4) prestación de servicios financieros; (5) Entidades Gestoras y Servicios Comunes de la Seguridad Social, en el ejercicio de sus competencias en materia de recaudación y; (6) los datos de carácter personal procedentes de evaluaciones de comportamiento que definan características o de la personalidad. Así pues, las medidas obligatorias para esta tipología de datos además de las medidas de seguridad de nivel básico son: la figura del responsable de seguridad; la auditaría bienal; medidas adicionales de identificación y autenticación de usuarios (límite reintentos de acceso); control de acceso físico; medidas adicionales de gestión de soportes (registro entrada y salida); registro de incidencias (anotación y autorización para los procedimientos de recuperación).

En última instancia, en el nivel alto constan los datos de carácter personal sobre (1) ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual; (2) fines policiales sin consentimiento; (3) actos de violencia de género; (4) operadores de servicios de comunicaciones electrónicas (datos de tráfico y de localización). Las medidas obligatorias que establece la ley para este tipo de datos, además de las medidas de seguridad de nivel básico y medio anteriormente citadas, se desarrollan: las medidas de seguridad en la distribución de soportes (cifrado); registro de accesos (tanto para ficheros automatizados como en soporte papel); medidas adicionales de copias de respaldo (copia en lugar diferente); cifrado de telecomunicaciones y; almacenamiento de ficheros no automatizados o en papel bajo llave y en áreas de acceso restringido.

En la normativa nacional vigente, esto es, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) se aprecia una omisión a la definición propia del concepto de datos personales, por resultar innecesario una vez que ya consta recogida en el resto de las normativas sobre el derecho de protección de datos. No obstante, autores como MARTÍNEZ MARTÍNEZ vienen a considerar de manera acertada que los conceptos de dato y tratamiento se encuentran estrechamente unidos y conectados, puesto que:

"[…] se proyectan sobre el derecho fundamental a la protección de datos hasta conseguir cerrar una tipología muy definida. Ambos conceptos, desde el punto de vista de la aplicación de la norma ofrecen una ventaja innegable, ya que permiten emplear el mecanismo de la subsunción de modo prácticamente automático: cuando se ha identificado un dato personal que es objeto de tratamiento, el silogismo interpretativo resulta más bien sencillo y la prevalencia de lo dispuesto por la LOPD resulta prácticamente asegurada"[271].

Lo cierto es que, desde una perspectiva jurídica no se puede hacer referencia a los datos personales sin tener en consideración el tratamiento de estos que la ley aplicable le otorga, no siendo de aplicación al tratamiento de aquellos datos personales que la ley excluye. Por consiguiente, sendos conceptos "datos personales" y "tratamiento" se encuentran estrechamente vinculados y conectados puesto que la normativa jurídica específica sobre el derecho de protección de datos tiene como objeto el tratamiento de los datos personales, resultando de notoria relevancia conocer los datos que son materia de protección a causa de su tratamiento, así como aquellos datos personales cuyo tratamiento quedaría excluido del ámbito de aplicación legal.

En concreto, la LOPDGDD excluye de su ámbito de aplicación legal, los datos de carácter personal registrados en ficheros automatizados de titularidad pública cuya finalidad sea la del almacenar los mismos para su publicidad con carácter general; los registrados en los ficheros de personas físicas con fines exclusivamente personales; los pertenecientes a ficheros de información tecnológica o comercial que reiteren datos previamente publicados en boletines oficiales; los datos depositados en ficheros de informática jurídica de acceso público; los datos de asociados o miembros y ex miembros depositados en ficheros de partidos políticos, sindicatos e iglesias, confesiones y comunicaciones religiosas. La derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) excluía de su regulación los datos personales de personas físicas en el ejercicio de actividades

[271] MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", *Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Revista de Internet Derecho y Política.* Núm. 5, 2007, p. 51. Documento disponible en: https://www.researchgate.net/publication/28178556_El_derecho_fundamental_a_la_proteccion_de_datos_perspectivas (última consulta 11/11/18).

exclusivamente personales o domésticas, los datos registrados en ficheros con fines de investigación de terrorismo y de formas graves de delincuencia organizada, así como los datos que han de ser regulados por Ley Orgánica específica, como los de régimen electoral, los datos con fines estadísticos, los datos de informes personales suscritos por las Fuerzas Armadas, los datos del Registro Civil y del Registro Central de penados y rebeldes y, los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con el artículo 2 del citado texto legal. En relación con la vigente LOPDGDD, se ha de destacar que exceptúa de su ámbito de aplicación los tratamientos excluidos del ámbito de aplicación del RGPD[272], los datos de personas fallecidas[273] y los "tratamientos sometidos a la normativa sobre protección de materias clasificadas", como se hace constar en el artículo 2 del citado texto legal.

Finalmente, resulta de relevancia tener presente, como se ha hecho mención anteriormente que, de conformidad a la reciente jurisprudencia del TJUE y del TC, tampoco se considerarán datos personales, *v.gr.,* número de registro mercantil, dirección de correo electrónico de tipología "info@empresa.com/es" o los datos anonimizados. Por último, la Audiencia Nacional ha incluido dentro del concepto de dato personal "el dato de la cuenta corriente incluso sin asociar a otros datos porque permite la identificación de la persona a la que se hace un cargo. Se considera que existe un

[272] En este sentido, el RGPD excluye de su ámbito de aplicación: (1) los datos personales procedentes del ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión, (2) los datos personales derivados por parte de los Estados miembros cuando llevan a cabo actividades sobre política exterior y seguridad común, (3) aquellos datos que procedan de actividades efectuadas por una persona física exclusivamente personales o domésticas y, (4) como novedad se excluye del ámbito de aplicación aquellos datos procedentes "por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención".

[273] Acerca de los datos de personas fallecidas, el art. 3 de la LOPDGDD establece que podrán acceder a los datos registrados en el fichero las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos y las personas o instituciones designadas expresamente por el fallecido, así como solicitar su rectificación o supresión siempre y cuando no exista prohibición expresa por escrito por parte de la persona fallecida o prohibición legal, en todo caso, los herederos podrán acceder a los datos de carácter patrimonial del causante. En caso de fallecimiento de menores y personas con discapacidad, también podrán acceder a sus datos personales y, en su caso, su rectificación o supresión, sus representantes legales y por el Ministerio Fiscal (que puede actuar de oficio o a instancia de persona física o jurídica interesada). Asimismo, en el caso de fallecimiento de personas con discapacidad, también podrán acceder a sus datos las personas designadas para el ejercicio de funciones de apoyo, si entre sus medidas de apoyo se encuentra la de acceso a sus datos personales y, en su caso, su rectificación o supresión.

tratamiento del dato del número de teléfono del afectado cuando se asocia al nombre de otro abonado" como aclara PUENTE ESCOBAR[274].

2.2. Fundamentación jurídica acerca del derecho de protección de datos como un derecho autónomo del derecho a la intimidad

Desde el surgimiento del derecho de protección de datos a través de la amplia interpretación dada por el Tribunal Constitucional del artículo 18.4 de la CE, así como su posterior regulación jurídica específica en el ámbito europeo y en el ordenamiento jurídico español, la doctrina ha defendido diversas teorías acerca de si el derecho de protección de datos personales debe ser considerado como un derecho fundamental independiente y aislado del derecho a la intimidad o, más bien, es un derecho dimanante del mismo[275]. En concreto, las diversas postulaciones doctrinales se pueden clasificar en dos teorías principales:

Por un lado, la que se podría denominar la *teoría del derecho a la autodeterminación informativa*, que defiende que el derecho de protección de datos es un derecho fundamental que debe ser concedido como autodeterminación informativa en la era digital y en el tratamiento informático, en el sentido de que tiene como finalidad "[…] preservar la información individual, sea o no íntima, frente a su utilización incontrolada y actuaría a partir del ámbito en el que termina el entendimiento convencional del derecho a la vida privada"[276].

---

[274]PUENTE ESCOBAR, A., *Informes y sentencias relevantes,* 8ª Sesión Abierta de la AEPD. Gran Auditorio Ramón y Cajal, Junio 2016, p. 30. Documento disponible en: https://docplayer.es/69057697-Informes-y-sentencias-relevantes-agustin-puente-escobar-abogado-del-estado-jefe-del-gabinete-juridico.html (última consulta 12/11/18).

[275]DE MIGUEL SÁNCHEZ, *Tratamiento de datos…, op. cit.*, pp. 27-36. En este sentido, FERNÁNDEZ SALMERÓN, *La protección de los datos personale*s…, *op. cit.*, p. 53, afirma que "en nuestro ordenamiento, el planteamiento acerca de la posible o conveniente existencia de un nuevo derecho fundamental autónomo en relación con la protección de los datos personales ha encontrado en Lucas Murillo de la Cueva un decisivo impulsor. El autor señaló en su día que «la noción de intimidad que predomina en nuestro ordenamiento jurídico responde a una concepción preinformática» en LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación…, op. cit.*, p. 115".

[276] DE MIGUEL SÁNCHEZ, *Tratamiento de datos…, op. cit.*, p. 31.

Por ende, este sector de la doctrina mayoritaria – Lucas Murillo de la Cueva[277], Pérez Luño[278], Herrán Ortiz[279], González Navarro[280], Álvarez-Cienfuegos[281], González García[282], Ordás Alonso[283], entre otros – afirma que el ámbito del derecho de protección de datos es más amplio que el derecho a la intimidad, puesto que protege el tratamiento frente a terceros de toda tipicidad de datos personales sin necesidad de que tengan que ser íntimos, entendiendo como equivalentes los conceptos "libertad informática" y "autodeterminación informativa"[284].

Por otro lado, la que se podría definir como la *teoría de la concepción flexible del derecho a la intimidad*, amparada por una vertiente doctrinal - Ortí Vallejo[285], Ruiz

---

[277] LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales…, op. cit.*, p. 31.

[278] PÉREZ LUÑO, A.E., "Nuevos derechos fundamentales en la era tecnológica: la libertad informática", *Anuario de Derecho Público y Estudios Políticos,* núm. 2, 1989, p. 190.

[279] HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales,* Ed. Dykinson, Madrid, 1999, pp. 109 y ss.

[280] GONZÁLEZ NAVARRO, F., "El derecho de la persona física a disponer de los datos de carácter personal que le conciernen", *Revista Jurídica de Navarra,* núm. 22, 1996, p. 21.

[281] ÁLVAREZ -CIENFUEGOS SUÁREZ, J.M., *La defensa de la Intimidad de los Ciudadanos y la Tecnología Informática,* Aranzadi, Pamplona, 1990, p. 15.

[282] GONZÁLEZ GARCÍA, L., "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos", *Derecho y Salud,* Vol. 24, núm. Extra. 1, 2014, p.274.

[283] ORDÁS ALONSO, M., "Intimidad, secreto médico y protección de datos sanitario", en AA. VV., *Razonar sobre Derechos,* (Coord. J. A. García Amado), Ed. Tirant lo Blanch, Valencia, 2016, pp. 773-834.

[284] LÓPEZ -IBOR MAYOR, V., "Los límites al derecho fundamental a la autodeterminación informativa en la Ley española de protección de datos (LORTAD)", *Actualidad Informática Aranzadi,* núm. 8, 1993, p. 1 y ss. En este sentido, LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales…, op. cit.*, pp. 26-27, aclara que: "[…] si el derecho a la intimidad incluye la facultad de vedar la recogida y utilización de información personal, así como el control sobre esta última, cuando se consienta o se realice por mandato legal, entonces no habrá excesiva dificultad en incluir dentro del contenido de tal derecho la tutela frente al uso de la informática […] Ahora bien, si es evidente que, al menos en parte, coinciden el derecho a la intimidad y el derecho a la autodeterminación informativa, ya no lo es tanto que puedan considerarse incluidas en el primero las exigencias relacionadas con la protección de datos de carácter personal no encuadrables en la noción de intimidad en sentido estricto. Por otra parte, aun en el supuesto de que no hubiese duda alguna sobre la identidad del ámbito material tutelado por ambas categorías de derechos, siempre permanecería como dato diferencial el hecho de que ese aspecto de la intimidad relacionado con el control de la información personal plantea perfiles absolutamente nuevos con la irrupción de las nuevas tecnologías y, especialmente, con el uso generalizado de ordenadores. Así pues, la situación no está clara en absoluto. Si no se trata de dos figuras conceptualmente distintas, puede ocurrir que los problemas específicos que plantea la informática hagan conveniente organizar la defensa jurídica del ciudadano en lo que toca a sus datos personales desde la posición de independencia sistemática respecto de los otros perfiles de la intimidad. En hipótesis, por tanto, razones dogmáticas, en un caso, y prácticas, en el otro, pueden aconsejar la diferenciación".

[285] ORTÍ VALLEJO, A., *Derecho a la intimidad e informática (Tutela de la persona por el uso de los ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada),* Ed. Comares, Granada, 1994, pp.48 y ss.

Miguel[286], Villaverde Menéndez[287], Valero Torrijos y López Pellicer[288], entre otros - que se posiciona fundamentalmente en la defensa del carácter básico de la intimidad como garantía de otros derechos entre los que se encuentra el derecho de protección de datos personales. Así pues, esta teoría mantiene una concepción abierta y flexible del derecho a la intimidad adaptable al contexto social y a la realidad tecnológica del momento subyaciendo la idea de que el derecho a la intimidad tiene capacidad jurídica suficiente a efectos de dar solución a los conflictos jurídicos que puedan proceder del uso de las TIC y del IoT.

A pesar de lo sostenido por ambas teorías, lo cierto es que lo que viene a concretar un tratamiento ilícito de los datos personales depende fundamentalmente de la existencia o no de una vulneración del derecho a la intimidad del titular de los mismos, siendo por consiguiente la intimidad el bien jurídico a proteger en el derecho de protección de datos, o si se prefiere, en el derecho específico a la autodeterminación informativa que resulta igualmente un derecho fundamental constitucional – que como se ha mencionado a lo largo de este capítulo – es correlativo de la dignidad de la persona[289].

No obstante, se ha de tener en consideración que a pesar de que la Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y documentación Clínica (en adelante, LAP), hace una especial referencia al derecho a la intimidad en su artículo 7 estableciendo la prohibición de acceso a los datos sanitarios por parte de terceros excepto en aquellos casos previstos por ley, aunque la tendencia del ordenamiento jurídico europeo[290] y

[286] RUIZ MIGUEL, C., "El derecho a la protección de datos de los datos personales en la Carta de los Derechos Fundamentales de la Unión Europea: análisis crítico", *Revista de Derecho Comunitario Europeo,* núm. 14, 2003, p.32.

[287] VILLAVERDE MENÉNDEZ, "Protección de datos personales…", *op. cit.,* p. 223.

[288] VALERO TORRIJOS, J. y LÓPEZ PELLICER, "Algunas consideraciones sobre el derecho a la protección de datos…", *op. cit.,* p. 274.

[289] SERRANO PÉREZ, M.ª M., "Salud pública, epidemiología y protección de datos" en AA.VV., *Tratado de Derecho sanitario,* (Coord. Larios Risco, et al.), Editorial Aranzadi, Navarra, 2013, p. 1095.

[290] En concreto la Carta de los Derechos Fundamentales de la Unión Europea, adoptada en la Cumbre de Niza de 11 de diciembre de 2000, en el artículo 8 sobre "Protección de datos de carácter personal" establece que: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El

español[291], así como de la jurisprudencia del Tribunal Constitucional[292] y del Tribunal Supremo[293], además de la corriente doctrinal que defiende la teoría del derecho a la autodeterminación informativa – anteriormente citada - entiende que el derecho de protección de datos personales es un derecho autónomo e independiente del derecho a la intimidad, al tratarse de un "derecho de nueva generación que otorgaría a cada ciudadano el control 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" (SSTS núm. 803/2017 de 11 de diciembre).

En síntesis, resulta evidente afirmar que el derecho de protección de datos goza de una regulación específica tanto en el derecho comunitario como en el ordenamiento

---

respeto de estas normas estará sujeto al control de una autoridad independiente.» Asimismo, más recientemente, en el considerando uno del RGPD el legislador europeo señala que "La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental".

[291] En el punto primero del Preámbulo de la LOPDGDD se estatuye que «la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la constitución española […] Por su parte, en la Sentencia 292/200, de 30 de noviembre, los considera como un derecho autónomo e independiente que 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 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». Asimismo, en el art. 1 de la LOPDGDD señala que: "El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución…"

[292] *Vid.* La primera sentencia donde el TC reconoce el derecho de protección de datos como un derecho autónomo es en la SSTC 254/1993, de 20 de julio que establece: «… el art. 18.4 C.E. […] consagra un derecho fundamental autónomo 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 discriminatorios. Y aquí se utilizó un dato sensible, que había sido proporcionado con una determinada finalidad, para otra radicalmente distinta con menoscabo del legítimo ejercicio del derecho a la libertad sindical».

[293] *Vid.* SSTS (Sala de lo Penal, Sección 1ª) núm. 803/2017 de 11 de diciembre señala que: «[…]Sobre este extremo concreto se argumenta en la sentencia 586/2016, de 4 de julio, que «la gravedad de las penas asociadas al art. 197.2 del CP son bien expresivas de la necesidad de una fundada y grave afectación del bien jurídico protegido, que no es la intimidad, entendida en el sentido que proclama el art. 18.1 de la CE (RCL 1978, 2836) , sino la autodeterminación informativa a que se refiere el art. 18.4 del texto constitucional. Se trata de una mutación histórica de innegable trascendencia conceptual, de un derecho de nueva generación que otorgaría a cada ciudadano el control 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 palabras del Tribunal Constitucional, el derecho a la protección de los datos de carácter personal deriva del art. 18.4 CE y consagra «en sí mismo un derecho o libertad fundamental» (SSTC 254/1993, de 20 de julio (RTC 1993, 254) ; y 254/2000, de 30 de noviembre , entre otras), que «excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada libertad informática es así 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» (STC 292/2000, de 30 de noviembre (RTC 2000, 292)).»

jurídico español a efectos de ofrecer al titular de los datos personales garantías de confidencialidad y seguridad – entre otras – así como mecanismos de defensa en el caso de resultar afectado por un tratamiento ilícito de sus datos personales y, a su vez garantizar la libre circulación de los datos personales aplicando medidas a fin de no vulnerar el derecho a la intimidad de los titulares[294].

En consideración de lo analizando a lo largo del presente capítulo, se ha de concluir que el derecho a la intimidad es un derecho autónomo al derecho de protección de datos personales[295], pues este último derecho regula garantías que permiten al titular de los datos personales a negarse a dar ciertos datos de carácter personal, conocer de la existencia de los ficheros donde consten registrados sus datos personales, así como el acceso a los mismos y, la posibilidad de rectificar, cancelar y oponerse al tratamiento de estos a alguna finalidad específica[296], pues como afirma LUCAS MURILLO DE LA CUEVA

[294]Al respecto, FERNÁNDEZ SALMERÓN, *La protección de los datos personale*s…, *op. cit.*, p. 75, señala que "[…] desde nuestro punto de vista la prolongada confusión que doctrinal y jurisprudencial se ha mantenido en torno a la asimilación entre intimidad y protección de datos personales – a cuya consolidación ciertamente el Tribunal Constitucional contribuye de modo decidido. puede encontrar un satisfactorio punto de encuentro. En efecto, puede decirse que la intimidad – o, en su reformulación actual, la que la Exposición de Motivos de la LORTAD llamó *privacidad* – u otros derechos del individuo se encuentran potencialmente más amenazados en función de la fase concreta del proceso de tratamiento de los datos personales en que nos encontremos y de la naturaleza intrínseca de los datos que sean su objeto. Así, las facultades negativas del derecho a la autodeterminación informativa, esto es, la eventual negativa del individuo a proporcionar determinados datos personales (consentimiento informado en la obtención y cesión de los datos), tiende a garantizar esa esfera más personal del sujeto que quiere mantener algunos aspectos de su vida al margen del conocimiento ajeno. Se trata, por lo demás, de una facultad típicamente negativa inherente al clásico concepto de intimidad que opera, lógicamente, en materia de protección de datos. Asimismo, ciertas facultades positivas del derecho, como las relativas a la obtención de información, se encuentran más estrechamente vinculadas a la intimidad, en la medida en que tienden a proporcionar al sujeto la información sobre quién y en qué medida tiene en su poder información acerca de esa persona. Pero ello en nada excluye que en relación con otras fases del proceso de tratamiento de los datos en las que se otorgan al interesado diversas facultades, como las de decisión respecto a la utilización de sus datos y, en suma, el control sobre el destino y uso de la información personal que le concierne se encuentre comprometido únicamente el valor intimidad". Igualmente, GUICHOT REINA, E., *Datos personales y Administración Pública.* Cizur Menor: Editorial Aranzadi, p. 165, afirma que: "En definitiva, creemos que, desde nuestros presupuestos constitucionales, es posible defender que el derecho a la intimidad se extiende hoy a toda la información referida a la vida privada de una persona, y otorga al ciudadano un poder de control sobre la misma que se materializa en su derecho a consentir o no su revelación, salvo que otros derechos o bienes constitucionales la impongan, en cuyo caso, habrán de destinarse exclusivamente al fin amparado por ese derecho o bien constitucional, con las necesarias garantías de secreto y seguridad, conservando el interesado su facultad de acceder a dichos datos, y de rectificarlos y cancelarlos en caso de que no se cumplieran las mencionadas condiciones, salvo que, nuevamente, la necesidad de salvaguardar un derecho o bien constitucional imponga la restricción o privación de estas facultades".

[295] MARTÍNEZ MARTÍNEZ, *Una aproximación…, op. cit.,* pp. 328-333.

[296] APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Ed. Aranzadi, Cizur Menor, 2002, pp. 160-161.

lo que se protege del titular de derecho de protección de datos no es su intimidad, sino su privacidad[297].

3. LA EVOLUCIÓN DE LA NORMATIVA COMUNITARIA Y ESPAÑOLA DEL DERECHO DE PROTECCIÓN DE DATOS

En el contexto tecnológico actual resulta imprescindible girar la vista atrás sobre la evolución jurídica del derecho de protección de datos debido a que en la actual era digital y tecnológica no resultan suficientes los principios generales del consentimiento individual. Por ello, a lo largo de las décadas conforme ha ido evolucionando la tecnología paralelamente ha ido progresando el marco jurídico de protección de datos a efectos de regular el tratamiento de los datos dimanantes de las nuevas tecnologías y el Internet de las Cosas y, con ello, las medidas que se han de cumplir ante situaciones

[297]LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales. Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de datos de carácter personal*, Centro de Estudios Constitucionales, Madrid, 1993, p. 33, se dirige a la privacidad como "la propia identidad, nuestra dignidad y libertad". Al respecto FERNÁNDEZ SALMERÓN, *La protección de los datos personales en las…, op. cit.,* p. 54. Asimismo, cabe tener presente el apartado primero de la Exposición de Motivos de la LORTAD donde se afirma que: "nótese que se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona – el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo –, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado. Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnológicas informáticas de tan reciente desarrollo". Al respecto, añade GUICHOT REINA, *Datos personales y Administración Pública…, op. cit.,* p.157, que: "lo que está en juego cuando hablamos de protección de datos no es sólo el derecho a la intimidad, sino la identidad del hombre y su propia libertad. Por ello, difieren el ámbito protegido (referido a cualesquiera datos personales) y la técnica de la protección (que incluye una serie de facultades que se corresponden con obligaciones de hacer de terceros). Desde un punto de vista práctico, el derecho a la protección de datos personales se va configurando como un sector autónomo y singularizado del ordenamiento. Todo ello aconseja abandonar la referencia a la intimidad y enunciar un nuevo derecho fundamental que comienza donde termina el entendimiento convencional, clásico, o preinformático del derecho a la intimidad o la vida privada". De igual modo, LUCAS MURILLO DE LA CUEVA, *Informática y protección de datos personales…, op. cit.*, pp. 120-121, afirma que: "Por todo ello, si no coinciden los ámbitos materiales que se quieren defender con el derecho a la intimidad y con la protección de datos personales; si aquél responde a una concepción preinformática; si ésta va configurándose como un sector especializado del ordenamiento jurídico cada vez más articulado y denso, tal vez convenga abandonar la referencia de la intimidad y encabezar la exposición de esta problemática con un epígrafe distinto. Como es evidente, no se trata únicamente de un cambio nominal, sino de una consideración sistemática, más acorde con la realidad. Este planteamiento facilitará, además, otra novedad: la enunciación de un nuevo derecho fundamental. Precisamente el que tendría como objeto preservar la información individual – íntima y no íntima – frente a su utilización incontrolada, arrancando, precisamente, donde termina el entendimiento convencional del derecho a la vida privada. A nuestro juicio, éste es un paso que es necesario dar. Las razones que se han venido exponiendo lo justifican sobradamente".

tales como: aplicación de herramientas *big data*, Medicina Predictiva, tecnologías médico paciente, entre otros muchos a destacar.

3.1. Contexto europeo

Con carácter previo, se ha de partir de una análisis del derecho de protección de datos desde una perspectiva jurídica en el marco de la Unión Europea debido a las distintas concepciones acerca del mismo que nos podemos encontrar en la jurisprudencia del Tribunal de Justicia de la Unión Europea (en adelante TJUE) y en la del Tribunal Europeo de Derechos Humanos (en adelante TEDH), así como en los cambios en la legislación europea a efectos de adaptar el derecho de protección de datos a las distintas realidades y contextos sociales de la nueva era digital. En 1948, en el artículo 12 de la Declaración Universal de Derechos Humanos, se regula por vez primera en el plano internacional la importancia de proteger por medio de la ley la vida privada de la persona al establecer que:

"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Posteriormente, en 1950, el Convenio Europeo de Derechos Humanos en el artículo 8 regula por primera vez en el marco jurídico europeo el derecho a la privacidad. Aun así, no será hasta el año 1981 con el Convenio 108 elaborado por el Consejo de Europa cuando se proteja realmente a los individuos del tratamiento automatizado de sus datos de carácter personal a fin de garantizar el derecho a la vida privada de los ciudadanos frente a la libre circulación de datos entre los distintos Estados[298], siendo su finalidad la de "garantizar, en el territorio de cada Parte, a

[298] Al respecto se ha de destacar lo que afirma el Convenio 108 en su Exposición de Motivos: "Los Estados miembros del Consejo de Europa, signatarios del presente Convenio. Considerando que el fin del Consejo de Europa es llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto a la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados; Reafirmando al mismo tiempo su compromiso a favor de la libertad de información sin tener en cuenta las fronteras; Reconociendo la necesidad de conciliar los valores fundamentales del respeto a la vida privada y de la libre circulación de la información entre los pueblos".

cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona" según establece el artículo 1 del mismo[299].

De igual modo, en las sentencias dictadas por el TEDH y por el TJUE se puede apreciar un notorio reconocimiento al derecho a la protección de datos de carácter personal a fin de salvaguardar y garantizar el derecho de privacidad de los ciudadanos, al interpretarse por estos Tribunales que el derecho a la protección de datos de carácter personal es un derecho que forma parte del derecho a la privacidad. De hecho, en los primeros pronunciamientos del TEDH se aprecia una postura extrema, donde a pesar de que no se hace mención expresa a la protección de datos personales, se considera por el Tribunal que un uso lícito de las nuevas tecnologías supone en todo caso un respeto de la vida privada de las personas, sin entrar a mencionar la protección de datos personales.

Así, por ejemplo, en relación a la protección de datos de salud, en la sentencia recaída en el asunto *Z.* contra Finlandia, 25 de febrero de 1997, Demanda N.º 22009/93, donde se alega supuesta vulneración del artículo 8 del CEDH sobre el derecho a la vida privada y familiar, por parte del demandante, un enfermo portador de la enfermedad VIH, condenado por violación y dos intentos de homicidio por exponer a sus víctimas al riesgo de transmisión del VIH hasta el extremo de transmitírselo a una de ellas, tras negativa a declarar en juicio, demanda al médico y al psiquiatría que fueron obligados a difundir datos sobre su estado de salud sin haber transcurrido el plazo de 10 años de confidencialidad. Finalmente, el TEDH desestima la demanda planteada al considerar que prevalece el fin legítimo para prevenir los delitos penales en interés común de una sociedad democrática ante el carácter confidencial de las informaciones sobre la

[299] En este sentido, GUICHOT REINA, *Datos personales y Administración Pública…, op. cit.,* p. 29, afirma que: "El Convenio trató de garantizar un estándar mínimo de protección, ampliable por las legislaciones nacionales, ante el incremento del flujo interfronterizo de datos personales sujetos a procesamiento automático, que se dejaba sentir a principios de los ochenta. El objetivo era compatibilizar la garantía del derecho fundamental al respecto de la vida privada y el libre flujo informativo dentro del territorio de todos ellos, extendiendo su protección a cualquier tratamiento de datos, público o privado, de carácter automatizado, y previendo, a un tiempo, que su ámbito de aplicación pudiera extenderse a cualquier técnica de procesamiento (también a los procedimientos no automatizados) y a los datos de personas jurídicas y entes sin personalidad (art. 3). El resultado previsto sería una armonización de los Derechos de los Estados parte, tanto en lo que hace al contenido del derecho, como en cuanto a sus posibles restricciones".

salud[300]. Por otro lado, en la STEDH de 4 de diciembre de 2008, caso S. y Marper c. Reino Unido[301], el TEDH realiza una interpretación del artículo 8 del CEDH en relación al tratamiento de datos biométricos, muestras celulares y perfiles de ADN en base de datos en una sociedad democrática y el derecho a la vida privada, concluyendo "que la conservación sistemática e indiscriminada por parte de autoridades públicas de huellas dactilares y muestra y perfiles de ADN de personas no condenadas vulnera el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales"[302].

En concreto, en la citada sentencia el TEDH considera que existe vulneración del artículo 8.1 del CEDH cuando nos encontramos, bien ante casos de mera conservación de datos relativos a la vida privada (como pueden ser los datos sensibles relativos a la salud, tales como muestras celulares), o bien, ante casos de mera conservación de datos cuyo tratamiento automatizado vaya más allá de una identificación indefinida (como son los datos procedentes del tratamiento automatizado de perfiles de ADN), así como el registro público de datos que de manera susceptible puedan vulneran el derecho a la vida privada (como son los datos derivados de las huellas dactilares).

En la sentencia Malone contra Reino Unido[303] de 2 de agosto de 1984 es donde por primera vez el TEDH hace mención a los mecanismos especiales para la protección de datos personales desarrollados por parte del Consejo de Europa y de los estados contrayentes, en la citada sentencia el Juez Sr. Pettiti, opina que "la recomendación R (83) 10 del Comité de Ministros del Consejo de Europa destaca que debe garantizarse el respeto de la vida privada de las personas «en cualquier proyecto de investigación que requiera el empleo de datos de naturaleza personal»". Posteriormente, en el caso Rotaru

[300] STEDH de 25 de febrero de 1997, caso Z. c. Finlandia (Rec. Núm. 9/1996).

[301] S. and Marper v. The United Kingdom [GC], n. º 30562/04 y 30566/04, 04.12.2008.

[302] GONZÁLEZ FUSTES, G., "TEDH – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Articulo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas", *Revista de Derecho Comunitario Europeo,* núm. 33, Madrid, mayo/agosto 2009, p. 620. Documento disponible en: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=679&IDA=27523 (última consulta 12/12/18).

[303] STEDH, de 2 agosto 1984. Malone contra Reino Unido. Demanda núm. 8691/1979.

contra Rumanía[304], de 4 de mayo de 2000, el TEDH por primera vez establece que los datos privados sobre la vida del ciudadano (estudios, actividades políticas y expediente penal) "[…]cuando son recogidos y memorizados, de manera sistemática en un fichero mantenido por agentes del Estado, corresponden a la «vida privada», a tenor del artículo 8, párrafo 1, del Convenio". Por ende, el TEDH estima vulneración del artículo 8 del Convenio cuando no exista una ley interna estatal que permita al Estado la memorización de estos datos en un registro, así como su posterior utilización y la potestad de negación al ciudadano solicitante la facultad de rechazo, a pesar de que todo ello sea con fines necesarios en una sociedad democrática, al encontramos antes datos que corresponden a la "vida privada" de conformidad con el citado precepto legal.

Se puede apreciar la evidencia de que todavía en este contexto no se era consciente – desde un punto de vista social, científico y jurídico - de la importancia ni del poder de los datos sanitarios en la esfera de la medicina predictiva y de la salud pública, debido principalmente a que en ese momento no se encontraban desarrolladas ni puestas en marcha las técnicas de análisis *big data* en el sector de la salud, lo que impedía conocer lo que en la actualidad es una gran fuente de información y conocimiento de interés público. En consecuencia, el legislador europeo y los tribunales protegían el derecho de protección de datos de manera extrema siendo el único interés el de proteger y salvaguardar el derecho de privacidad de los ciudadanos, hasta el extremo de equiparar un uso lícito de las nuevas tecnologías – que hasta el momento iban surgiendo – con un respeto absoluto de la vida privada de las personas.

Sin embargo, como se concretará a lo largo de este capítulo poco a poco va surgiendo un cambio de paradigma hacía una perspectiva jurídica más flexible y tolerante con el derecho a la privacidad, encaminada a la defensa de una libre circulación de los datos abriendo, entre otros, una puerta al tratamiento lícito de los datos sanitarios y, por ende, a la legalidad de aplicación tecnologías *big data* en el ámbito sanitario. Así pues, el TEDH a consecuencia de la influencia de las nuevas tecnologías en la sociedad, así como del Internet de las Cosas desde una vertiente positiva, cambia su concepción acerca de la protección de los datos personales,

[304] Sentencia Tribunal Europeo de Derechos Humanos nº2834/95, de 4 mayo 2000, caso Rotaru contra Rumanía.

concluyendo en sus sentencias que consta justificada jurídicamente una injerencia del derecho a la vida privada regulado en el artículo 8.1 del CEDH, cuando se cumplan fundamentalmente tres requisitos: (1) cuando exista una ley interna estatal que permita al Estado memorizar y utilizar los datos personales; (2) que la finalidad de registro y utilización de los datos personales de los ciudadano sea en todo caso legitima y; (3) que sea de necesidad en una sociedad democrática. Es imprescindible que se cumplan los tres requisitos, en caso de no cumplirse uno de ellos, según establece el TEDH se considera contraria al art. 8 del CEDH y, por tanto, estaríamos ante una vulneración del citado precepto legal[305].

Se genera, de este modo, en el marco jurídico de la Unión Europea la necesidad de crear una normativa que regule de manera directa la protección de datos de carácter personal, naciendo en este contexto 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 respecta al tratamiento de datos personales y a la libre circulación de estos datos a efectos, (en adelante Directiva 95/46/CE), a efectos de crear un marco jurídico común a todos los Estados miembros de la Comunidad que establezca lazos de unión y asegure el progreso económico y social de manera globalizada, siendo eliminada, de tal modo, toda barrera dentro de los pueblos europeos.

Debido al nacimiento de internet donde a partir de 1991 cualquier usuario podía tener acceso a la información indistintamente del lugar del mundo en el que se encontrase y, a la vista de que de las TIC y del IoT generaban que los sistemas de tratamiento de datos se encontrasen con mayor facilidad y velocidad a disposición de la humanidad, surge la necesidad en el marco jurídico europeo de crear una normativa acerca del tratamiento de datos personales a fin de proteger el derecho a la intimidad y vida privada de las personas y, a la vez garantizar la libre circulación de estos datos entre los Estados miembros.

Así pues, para el legislador europeo, en ese momento resultaba igual de necesario proteger el derecho fundamental a la intimidad y privacidad de los ciudadanos

[305] *Vid.* GONZÁLEZ FUSTES, "TEDH – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Articulo 8 CEDH – Vida privada – Injerencia en una…", *op. cit.,* p. 626.

europeos, al amparo del artículo 7 y del artículo 8 de la Carta, como fomentar y garantizar la libre circulación de datos.

En este sentido, no parece que exista duda de que los miembros del Parlamento Europeo y del Consejo de la Unión Europea eran conscientes de que la figura de la libre circulación de datos debía ser garantizada por medio de la legislación europea y legislación interna de los Estados miembros, puesto que resultaba de notoria necesidad a efectos de asegurar el progreso económico y social de los Estados miembros emanante del comercio interior como gran generador de flujos transfronterizos de datos personales tanto en las instituciones públicas como privadas.

Por último, debe destacarse que, de igual modo resultaba indispensable garantizar la libre circulación de datos a fin de fortalecer la cooperación científica y técnica, como el establecimiento coordinado transfronterizo de nuevas redes de telecomunicaciones europeas[306].

En suma, el objetivo de la Directiva 95/46 era fundamentalmente eliminar los obstáculos a la circulación de datos personales y, establecer un nivel de protección de los derechos y libertades de las personas equivalente en los Estados miembros en relación con el tratamiento de estos. Todo ello a fin de equiparar las legislaciones internas sin que existan diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, en relación con el tratamiento de datos personales que puedan impedir la transmisión de datos de un Estado miembro a otro[307].

Posteriormente, el legislador europeo decide consolidar el derecho de protección de datos en el año 2001 con el Reglamento (CE) 45/2001, del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos

[306] Al respecto, *Vid.* DAVARA DAVARA, M.A., *La protección de datos en Europa: principios, derechos y procedimientos*, Ed. Universidad de Comillas, Madrid, 1998; HEREDERO HIGUERAS, M., *La directiva comunitaria sobre la protección de datos de carácter personal*, Aranzadi, Pamplona, 1997; SÁNCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Ed. Secretariado de Publicaciones de la Universidad de Sevilla, Sevilla, 1998.

[307] Directiva 95/46/CE, considerando1 a 8 y artículo 1.

comunitarios y a la libre circulación de estos datos (en adelante Reglamento 45/2001), que emana de propuesta presentada por la Comisión al Parlamento Europeo y al Consejo – siguiendo el procedimiento regulado en el artículo 251 del citado texto legal – con la finalidad de: (1) adoptar los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos que serán de aplicación a partir del 1 de enero de 1999 a las instituciones y organismos establecidos por el Tratado constitutivo de la Comunidad Europea; (2) crear un organismo supervisión independiente cuya responsabilidad sea la de controlar la aplicación de los actos comunitarios a las instituciones y organismos comunitarios que sancione a los infractores de los derechos de las personas cuyos datos se trata y del incumplimiento de las obligaciones a las que están sometidos a causa del tratamiento de los datos personales y; (3) adoptar, en caso de ser necesario, cualesquiera otras disposiciones pertinentes[308]. En este sentido, el Reglamento 45/2001 surge de la necesidad de proteger jurídicamente unos derechos de los titulares de los datos que son tratados por los responsables del tratamiento y, a su vez, de la necesidad de crear un marco jurídico que regule las obligaciones de los responsables del tratamiento dentro de las instituciones y los organismos comunitarios, creándose una "autoridad de control independiente" encargada de velar por la correcta aplicación del Reglamento y, de vigilar los tratamientos de los datos personales por parte de las instituciones y los organismos comunitarios[309].

En conclusión, se ha de hacer constar que el Reglamento 45/2001 no limita la potestad que le otorga el artículo 32 de la Directiva 95/46/CE a los Estados miembros para elaborar normativa interna en materia de protección de datos, todo lo contrario, lo que añade el Reglamento 45/2001 en el marco jurídico de la Unión Europea, es la garantía de que en la Comunidad Europea se aplique de manera homogénea y equitativa las normas de protección de los derechos y las libertades fundamentales de las personas sobre el tratamiento de los datos personales, así como la libre circulación de los datos personales entre los Estados miembros y las instituciones y los organismo comunitarios.[310] De igual modo destacar que, el Reglamento respeta la definición

[308] Todo ello en virtud de lo establecido en el artículo 286 Reglamento 45/2001.

[309] Reglamento 45/2001, considerando 5.

[310] Reglamento 45/2001, considerando 12, 13 y 21.

recogida en la Directiva 95/46/CE en relación con el concepto de "datos personales" sin realizar modificación alguna al respecto.

En momento posterior, a causa del surgimiento de nuevas redes digitales públicas de telecomunicaciones, así como debido a la introducción de la red digital de servicios integrados (RDSI) y las redes móviles digitales incluidas la televisión interactiva y el vídeo por pedido, resultó fundamental delimitar y definir medidas específicas de protección de datos personales y de la intimidad de los usuarios en una nueva sociedad de la información caracterizada por estos nuevos servicios de telecomunicaciones (RDSI)[311]. Así pues, a efectos de regular de manera específica el tratamiento de los datos personales y la protección de la intimidad en el sector de las telecomunicaciones, así como la libre circulación de los citados datos y de los equipos y servicios de telecomunicación en Comunidad, se publicó la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (en adelante, Directiva 97/66), cuyas disposiciones completan la Directiva 95/46, además de proteger los intereses de los abonados que sean personas jurídicas, de conformidad con lo establecido en el artículo 1 de la Directiva 97/66. Como aportación a destacar de la citada Directiva 97/66, son las definiciones recogidas en el artículo 2 sobre el concepto de "abonado", "usuario", "red pública de telecomunicación" y "servicio de telecomunicación".

Por último, a continuación se citan las siguientes novedades de la Directiva 97/66: de un lado, subyace la importancia que otorga a la seguridad del servicio público de telecomunicaciones, exigiendo que el proveedor debe garantizar a sus usuarios adoptando medidas técnicas y de gestión adecuadas a fin de evitar todo riesgo de violación de la seguridad en la red; por otro lado, lo relevante y necesario que resulta que los Estados miembros garanticen por medio de normas internas, la confidencialidad de las comunicaciones realizadas a través de las redes públicas de telecomunicaciones y de los servicios de telecomunicación accesibles al público, así como la importancia del consentimiento previo de los interesados en casos de que las escuchas, grabaciones, almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones sean

[311] Directiva 97/66, considerando 3, 4, 5, 6, y 10.

efectuadas por personas distintas de los interesados a fin de proteger la intimidad de los mismos en el sector de las telecomunicaciones[312].

Igualmente, de manera similar al planteamiento que se dio en el sector de las telecomunicaciones, el Parlamento Europeo y el Consejo de la Unión Europea subrayaron la importancia de proteger los datos personales y la intimidad en las comunicaciones electrónicas a causa de la introducción en las redes públicas de comunicación de nuevas tecnologías digitales avanzadas de comunicaciones electrónicas[313], motivo por el que el legislador europeo redactó y publicó 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 probidad y las comunicaciones electrónicas), posteriormente modificada por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 y por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009. Fundamentalmente, a causa de la evolución de las estructuras tradicionales del mercado generada por Internet a través de las comunicaciones electrónicas, produciendo a su vez nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad, el objeto de la Directiva 2002/58 de conformidad con lo establecido en el artículo 1 de la misma, consiste en:

"[…] armonizar disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos y, en particular, del derecho a la intimidad y la confidencialidad en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Unión Europea".

Por consiguiente, nos encontramos ante disposiciones que, en todo caso, especifican y completan la Directiva 95/46, de conformidad con lo establecido en el apartado segundo de dicho precepto legal. Igualmente, la citada Directiva 95/46 regula

[312] Véanse artículos 4 y 5 de la Directiva 97/66.

[313] Directiva 2002/58, considerando 4, 5 y 6.

la confidencialidad de las comunicaciones y de los datos de tráfico como obligación esencial de los proveedores, así como la obligación de borrar o anonimizar los datos cuando no sean necesarios para la transmisión de una comunicación, excepto en caso de facturación y cuando exclusivamente sea necesario.

No obstante, como se ha puesto de manifiesto anteriormente, la Directiva 2002/58 fue modificada por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, cuyo objetivo era el de armonizar las disposiciones de los Estados miembros relativas a la conservación durante un determinado periodo, por parte de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, de determinados datos generados o tratados por los mismos a efectos de garantizar que los datos se encuentren disponibles con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, dentro del respeto de los derechos reconocidos en los artículos 7 y 8 de la CDFUE[314].

Posteriormente, la citada Directiva 2006/24 fue declarada inválida por medio de la sentencia *Digital Rights Ireland* dictada por el TJUE (Gran Sala) de 8 de abril de 2014 en relación con la legalidad de medidas legislativas y administrativas nacionales sobre la conservación de datos relativos a comunicaciones electrónicas[315]. En este sentido se pronuncia el TJUE en la citada sentencia concluyendo que la Directiva 2006/24 supone una grave injerencia a los derechos fundamentales regulados en los artículos 7 y 8 de la CDFUE debido principalmente a:

(1) Conservación y acceso durante un tiempo limitado. La obligación impuesta a los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones de conservar durante un determinado periodo datos relativos a la vida privada de una persona y a sus comunicaciones, así como el acceso a los mismos por parte de las autoridades competentes, supone una injerencia del art. 7 de la Carta, indistintamente de que la información relativa a la vida privada tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes.

[314] Artículo 1 y considerandos 4, 5, 7 a 11, 21 y 22 de la Directiva 2006/24.

[315] Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland.*

(2) Ausencia de información. El hecho de conservar los datos y su posterior utilización sin que el usuario registrado haya sido previamente informado supone una injerencia del art. 8 de la Carta.

(3) Injerencia a la vida privada de toda la población europea. La Directiva 2006/24 afecta a todas las personas, medios de comunicación electrónica y datos relativos al tráfico de toda la población europea sin establecer diferenciación, limitación o excepción, lo que supone una injerencia más grave de los artículos 7 y 8 de la Carta, sin que se pueda justificar la conservación de los datos por el interés general de contribuir a la lucha contra la delincuencia grave y a la seguridad pública, objetivo fundamental de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[316].

(4) Ausencia de regulación de límites de acceso a las autoridades. Según concluye el TJUE la Directiva 2006/24 no establece reglas claras y precisas que regulen el alcance de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta[317].

De lo anterior, la Gran Sala de TJUE declara que la Directiva 2006/24 cuyo objeto era permitir la conservación de los datos procedentes de la prestación de los servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones a fin de que las autoridades pudieran acceder a los mismos para prevenir delitos y luchar contra la delincuencia, es inválida puesto que su objetivo principal no es proporcional con la injerencia que constituye en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión. Ahora bien, en el año 2009 el derecho a la protección de datos de carácter personal adquiere una nueva regulación debido a la entrada en vigor del Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo

[316] Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland,* §§ 58 y 59.

[317] Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland,* §§ 60, 61, 62 y 65.

de la Comunidad Europea (2007/ C 306/01) (en adelante Tratado de Lisboa), donde se regula el derecho a la protección de datos de carácter personal de manera independiente y autónoma en el artículo 16.1 (antiguo artículo 286 TCE) del Tratado de Funcionamiento de la Unión Europea (TFUE), aun así quedaba todavía mucho por hacer a efectos de garantizar la libre circulación de los datos y, entre otros, el amparar las técnicas propias del *big data* sanitario desde una perspectiva jurídica, como más adelante se expondrá en el ámbito sanitario.

A pesar de lo anterior, se puede apreciar una mayor flexibilidad interpretativa por parte de los tribunales adaptada al contexto social que iba surgiendo a causa de las TIC, ya que por medio de la aplicación de lo establecido en el apartado primero del artículo 6 del citado Tratado de Lisboa, la Carta de Derechos fundamentales de la Unión Europea de 7 de diciembre de 2000 adquiere el mismo valor jurídico que los Tratados, lo que permitió que el TJUE otorgara en sus sentencias una interpretación del artículo 8 de la CDFUE más actualizada y adaptada al nuevo contexto social de las TIC y del IoT, puesto que tal y como se puede apreciar en la CDFUE, el citado derecho es regulado en precepto distinto y de manera independiente al derecho a la vida privada y familiar regulado tanto en el artículo 7 de la CDFUE, como en el artículo 8 del CEDH de 4 noviembre 1950. Si bien es cierto que el TJUE en reiteradas sentencias establece que la protección de los datos de carácter personal del art. 8 de la Carta, tiene una importancia especial para el derecho al respeto de la vida privada del art. 7 de la Carta, así lo señala en la ya citada sentencia *Digital Rights Ireland,* donde el TJUE concluye que:

"[…] la normativa de la Unión de que se trate debe establecer reglas claras y precisas que regulan el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respectos de tales"[318].

[318] Sentencia del Tribunal de Justicia (Gran Sala) de 8 de abril de 2014, *Digital Rights Ireland* §§ 54. Véanse igualmente, en relación con el artículo 8 del CEDH, las sentencias TEDH, Liberty y otros c. Reino Unido de 1 de julio de 2008, nº58243/00, §§ 62 y 63; Rotaru c. Rumanía, antes citada, §§ 57 a 59 y S y Marper c. Reino Unido, antes citada §§ 99).

Finalmente, debido a que las TIC, el IoT y, en los últimos años las herramientas *big data* y a la IA, han generado un cambio revolucionario en la sociedad del Siglo XXI, siendo uno de los ámbitos más afectados el de los datos personales, que por su carácter propiamente personal e íntimo merecen de una protección jurídica especial y, a efectos de equilibrar la libre circulación de datos personales y la protección de los mismos, el 25 de mayo de 2016 entró en vigor el 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 (Reglamento general de protección de datos) – en lo sucesivo, RGPD – a los efectos de dar respuesta a los nuevos retos y problemas jurídicos planteados en relación a la protección de los datos personales, a su tratamiento y a la libre circulación de estos, a causa de la evolución tecnológica y a la globalización, puesto que una de las relevantes consecuencias de las TIC y el IoT es la de generar grandes volúmenes de datos personales a gran escala y velocidad procedentes del intercambio de datos entre las instituciones públicas y privadas internas de los Estados miembros, así como del intercambio de datos entre los propios Estados miembros, incidiendo con mayor facilidad en la privacidad de los ciudadanos.

Por ende, el RGPD por el que se deroga la Directiva 95/46/CE resulta de aplicación a todos los Estados miembros de la Unión Europea desde el día 25 de mayo de 2018, debido a la necesidad de actualizar el marco jurídico europeo en el ámbito de protección de datos, ya que la Directiva 95/46 – normativa de aplicada durante más de dos décadas en el marco jurídico comunitario - había quedado obsoleta a causa del veloz cambio tecnológico procedente de las TIC, el IoT y, más recientemente la Inteligencia Artificial. Así pues, el RGPD es el resultado de una serie de disposiciones, algunas de ellas redactadas de manera novedosa e innovadora, otras adaptando lo establecido por la jurisprudencia del TJUE y, otras previamente reguladas en la normativa jurídica anterior, que por su relevancia han sido de nuevo tenidas en cuenta, reiterándose en el nuevo RGPD lo ya regulado en la normativa derogada, esto es, en la citada Directiva 95/46.

Así pues, no cabe duda de que, uno de los rasgos más relevantes, novedosos e innovadores del RGPD es la puerta que le abre al *big data* sanitario, permitiendo – como se verá más adelante – el tratamiento de los datos de salud sin necesidad del consentimiento del paciente en aquellos casos que sea para fines de interés general, medicina predictiva y salud pública, entre otros. La anterior situación viene a suponer un gran paso en el ordenamiento jurídico comunitario, así como en el propio ordenamiento jurídico de los estados miembros de la Unión Europea, pues como se verá, el legislador consciente de la importancia y del valor de los datos[319] y, en concreto, del valor de los datos de salud, permite desde una perspectiva jurídica su utilización, acceso y cesión de los mismos por parte de aquellos facultativos sanitarios, investigadores y científicos que necesiten de su conocimiento e información para seguir avanzando en la esfera sanitaria y, hacía una medicina predictiva, la prevención de enfermedades, una asistencia personalizada, ayuda en la toma de decisiones y tratamientos más eficaces y eficientes, siendo estos fines, entre otros, de interés común para toda la humanidad.

3.2. Contexto español

En el contexto jurídico nacional se ha de destacar que, previamente a que se dictase la citada STC 254/1993 se procedió por parte del legislador español al desarrollo legislativo del artículo 18.4 de la CE por medio de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante LORTAD) entrando en vigor el 31 de enero de 1993. La promulgación de la citada ley era sumamente necesaria en el contexto social y jurídico del momento, debido a que España constaba ratificado el "Acuerdo de Schengen"[320] donde se

[319] Considerando 2 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europeo, señala que: "Las cadenas de valor de datos se basan en diferentes actividades relativas a los datos: creación y recopilación de datos; agregación y organización de datos; tratamiento de datos; análisis, comercialización y distribución de datos; utilización y reutilización de datos. El funcionamiento eficaz y eficiente del tratamiento de datos es un componente fundamental en toda la cadena de valor de datos. No obstante, el funcionamiento eficaz y eficiente del tratamiento de datos y el desarrollo de la economía de los datos en la Unión se ven dificultados, en particular, por dos tipos de obstáculos a la movilidad de los datos y al mercado interior: los requisitos de localización de datos establecidos por las autoridades de los Estados miembros y las prácticas de dependencia de un solo proveedor en el sector privado".

[320] El *Acuerdo de Schengen*, actualmente ratificado por los países europeos Alemania, Australia, Bélgica, Dinamarca, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Islandia, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, República Checa, República Eslovaca, Suecia y Suiza, "es un acuerdo por el que varios países de Europa suprimieron los

comprometía a intercambiar información personal de sus ciudadanos con la policía de otros países, así como el hecho de que toda norma redactada por el legislador europeo en relación a la materia de protección de datos personales iba a formar parte automáticamente del ordenamiento jurídico interno, fueron estos motivos determinantes para que España aprobara citada ley a efectos de "quedar excluido de este espacio uniforme"[321].

A grandes rasgos, una de las aportaciones de la LORTAD al ordenamiento jurídico español fue la regulación de los principios de pertenencia, exactitud, actualización, racionalidad y congruencia de los datos, el principio del consentimiento del interesado para el tratamiento automatizado de los datos, así como del derecho de información, derecho de acceso y del derecho de rectificación y cancelación. En suma, principios y derechos que asentaron las bases jurídicas de las normativas posteriores sobre protección de datos de carácter personal[322].

---

controles en las fronteras interiores (entre esos países) y trasladaron esos controles a las fronteras exteriores (con terceros países). El acuerdo, firmado en la ciudad luxemburguesa de Schengen en 1985 y en vigor desde 1995, establece un espacio común – denominado espacio Schengen – que comprende una gran parte del continente europeo. Los países participantes aplican normas comunes para controlar las fronteras exteriores y también en materia de visados y de cooperación entre los servicios policiales y judiciales en el ámbito penal". Disponible en: http://www.interior.gob.es/web/servicios-al-ciudadano/extranjeria/acuerdo-de-schengen

[321] GONZÁLEZ MURUA, "Comentario a la S.T.C. 254/1993, de 20 de julio…", *op. cit.,* p. 229.

[322] GUICHOT REINA, *Datos personales y Administración Pública*…, *op. cit.*, pp. 65-66, señala en relación con la LORTAD que: "Establecía como finalidad perseguida con la regulación el «hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medio informáticos». Distinguía la intimidad, cuyo ámbito coincide con el protegido por los tres primeros párrafos del artículo 18 CE, y la privacidad, que tiene como ámbito más amplio. Mientras que la primera vendría a referirse a la esfera en que se desarrollan las facetas más singularmente reservadas a la vida de la persona – el domicilio, las comunicaciones – la privacidad cubriría todas aquellas facetas que, interrelacionadas gracias a las posibilidades informáticas, permiten obtener un perfil de la persona en cuestión, que después puede ser utilizado para diversos fines, limitando sus posibilidades de desenvolvimiento social. Ahora bien, la propia Exposición de Motivos cifraba el objto de la Ley en la delimitación de «una nueva frontera de la intimidad y del honor, una frontera que, sustituyendio los límites antes definidos por el tiempo y el espacio, los proteja frente a la utilización mecanizada, ordenada y discriminada de los datos a ellos referentes», y en «una adecuada configuración de la nueva garantía de la intimidad y del honor», así como en «hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos». Es decir, presentaba a la vez su objeto como la protección de la intimidad ante nuevos desafíos y como la garantía de un derecho disinto, el derecho a la privacidad". Asimismo, el art. 1 de la LORTAD señala como objeto "limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos", siendo de aplicación a tenor del art. 2 "a los datos de carácter personal que figuren en ficheros automatizados de los sectores publico y privado y a toda modalidad de su posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado".

Nuevamente, el Tribunal Constitucional tras la entrada en vigor de la citada ley, en la sentencia 94/1998, de 4 de mayo[323], asienta doctrina jurisprudencial al establecer que el derecho de protección de datos:

"[…] no sólo entraña un especifico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la L.O.R.T.A.D.-, 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 discriminatorios" (FJ 6 STS 94/1998, de 4 de mayo).

Subsiguientemente, la Ley Orgánica 5/1992 fue derogada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (en lo sucesivo LOPD), a efectos de seguir las directrices europeas establecidas en la Directiva 95/46/CE, siendo así adaptado nuestro ordenamiento jurídico a la normativa europea. Esta ley orgánica ha sido el segundo escalón de la evolución de la regulación del derecho fundamental de protección de datos en España, siendo a su vez complementada por innumerable jurisprudencia dictada por el Tribunal Constitucional y por los órganos de la jurisdicción contencioso-administrativa.

Sin embargo, debe apreciarse que en ese momento el derecho de protección de datos se encontraba estrechamente vinculado con el derecho a la intimidad, no es hasta que se dictan las SSTC 290 y 292/2000 de 30 de noviembre donde el Tribunal constitucional le reconoce el carácter de derecho autónomo e independiente[324].

[323]STC 94/1998, de 4 de mayo.

[324] En palabras de GUICHOT REINA, *Datos personales y Administración Pública*…, *op. cit.*, p. 143, afirma que: "Expuesto así, de forma sistemática, el estado de la cuestión ha de reconocerse, en primer lugar, que las SSTC 290 y 292/2000 suponen un evidente esfuerzo dogmático del TC por trazar los perfiles constitucionales del derecho a la protección de datos. Para ello, el TC ha hecho referencia a una notable multiplicidad de nociones jurídicas predicables de un derecho fundamental: «objetivo» (garantizar la vida privada personal y familiar); «función» (otorgar al titular del derecho un poder de control sobre los datos personales, y no sólo la posibilidad de evitar injerencias de terceros); «objeto» (cualquier dato personal, y no solo los «íntimos»); «contenido» (todas las facultades que permiten el control sobre los datos, y no sólo el derecho a exigir una abstención de un tercero), «límites» (los mismos que el derecho a la intimidad). Algunas de ellas resultan un tanto indefinidas y reiterativas, y no responden a todos los casos a categorías suficientemente decantadas en la doctrina constitucional (en especial, la «función» y el

Por un lado, la STC 290/2000 resuelve sobre el recurso de inconstitucionalidad contra los arts. 24, 31, 39, art. 40.1 y 2 y Disposición final tercera de la LORTAD promovido por el Consejo Ejecutivo de la Generalidad de Cataluña, aunque finalmente la impugnación quedó centrada en el art. 40.1 y 2 de la LORTAD, puesto que los demás preceptos de la LORTAD habían sido derogados por la LOPD, careciendo de sentido que el TC se pronunciase al respecto, según la doctrina constitucional citada en la propia sentencia. Por otro lado, la STC 292/2000 se pronuncia sobre el recurso inconstitucional contra los arts. 21.1 y 24.1 y 2 de la LOPD, promovido por el Defensor del Pueblo.

En concreto, sin entrar a profundizar en un análisis exhaustivo de ambas sentencias, resulta de interés destacar que la STC 290/2000, de 30 de noviembre de 2000, se manifiesta sobre dos extremos jurídicos sumamente relevantes: en primer lugar, tal y como se ha puesto de manifiesto anteriormente, sobre la impetración del derecho de protección de datos como un derecho fundamental autónomo e independiente frente a la "libertad informática"[325]. En segundo lugar, debido a la función de gran responsabilidad que tiene la Agencia de Protección de Datos, esto es, la de "velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación"[326], el TC se centra en concretar sus características principales como organización o elemento institucional del régimen de protección de datos de carácter personal, cuya función principal es la de control y atención de reclamaciones de los afectados, estableciendo el TC en la citada sentencia que:

"[…] la atribución de tales funciones y potestades a la Agencia de Protección de Datos para asegurar, mediante su ejercicio, que serán respetados tanto los límites al uso de la informática como la salvaguardia del derecho fundamental a la protección de datos

---

«objetivo» del derecho; o la noción de «objetivo», que está, o debiera estar, directamente imbricada con la de «objeto»)".

[325]Al respecto, el TC en el FJ7 de la STC 290/2000 señala que: "En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes".

[326]De conformidad con lo establecido en el art. 36 a) de la LORTAD.

personales en relación con todos los ficheros, ya sea de titularidad pública o privada" (FJ 9).

En síntesis, en relación con la STC 292/2000, de 30 de noviembre de 2000, resulta de interés tener en consideración que fue la sentencia pionera en justificar la autonomía e independencia del derecho de protección de datos desde un contenido propiamente jurídico partiendo de los principios y derechos regulados en la LOPD y de un análisis del art. 18.4 de la CE. En suma, se ha de destacar las siguientes aportaciones jurídicas:

(1) El TC en la citada sentencia amplía el objeto del derecho de protección de datos, abarcando tanto los datos íntimos de la persona como cualquier dato que empleado por terceros pueda afectar a los derechos – indistintamente de que sean fundamentales o no - de su titular, debido a que el objeto fundamental no es propiamente la intimidad individual, sino los datos de carácter personal, esto es, aquellos datos que identifiquen o faciliten la identificación de su titular.

(2) De igual modo, como novedad, el TC establece los poderes de disposición y de control por parte del titular de los datos personales, esto es, la capacidad que le otorga el derecho de protección de datos al titular de los mismos de poder decidir qué datos proporcionar a un tercero – indistintamente de que sea una organismo público o privado o un particular – así como el poder de decisión de qué datos puede el tercero recabar, para qué y quién los posee, teniendo la facultad en todo caso de oponerse a la misma[327].

[327] SUERO SALAMANCA, J.A., "Comentarios a la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre", 2001, p. 4. Documento disponible en: http://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf (última consulta 22/08/18) afirma que: "[…] podemos concretar jurídicamente, los poderes de disposición y control de los datos personales que constituyen el contenido del derecho fundamental a la protección de datos, de la siguiente manera: facultad de consentir la recogida de los datos; facultad de consentir la obtención y acceso a los datos personales; la facultad de consentir sobre su posterior almacenamiento y tratamiento y; la facultad de consentir el uso de los datos personales, o usos posibles, por un tercero, se la Administración Pública o un particular".

(3) Por otro lado, el TC restringe la posibilidad de cesión de datos (art. 11 y art. 21 LOPD) entre las Administraciones Públicas con las mismas competencias o de similares materias, o al tratamiento posterior con fines históricos, estadísticos o científicos. Para el resto de los casos, salvo que una norma con rango de Ley, para que se puedan ceder datos entre las Administraciones Públicas, será obligatoria la autorización y consentimiento de los titulares de los datos del fichero.

(4) En relación con el derecho de información al ciudadano (art. 2 y art. 5.1 LOPD) el TC señala que únicamente las Administraciones Públicas podrán infringirlo cuando la información afecte a la Defensa Nacional, a la seguridad pública, o la persecución de una infracción penal.

(5) Por último, el TC estima como excepciones lícitas por parte de la Administraciones Públicas, frente al ejercicio de los derechos de acceso, rectificación y cancelación por los ciudadanos las de los ficheros de las Fuerzas y Cuerpos de Seguridad y los ficheros de la Hacienda Pública (art. 23 LOPD).

En definitiva, la STC 292/2002 establece que el derecho de protección de datos es un derecho fundamental autónomo que controla todo tipo de información que permita identificar a una persona indistintamente de que la misma sea o no estrictamente íntima. Por ende, como derecho autónomo otorga una serie de facultades al titular de los datos personales sobre el poder de control y disposición de los mismos, tales como decidir acerca de los datos concretos que consiente proporcionar al responsable del fichero, bien sea Administración Pública, bien sea un tercero, conocer acerca de la identidad del responsable del fichero y del tercero al que se le cedan sus datos, así como de la finalidad de uso de los datos personales, encontrándose legitimado el titular de los datos para oponerse al uso de sus datos en caso de disconformidad. El objetivo fundamental de la LOPD recientemente derogada fue el de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas en el tratamiento de sus datos personales, a los efectos de amparar el derecho fundamental al honor, la intimidad personal y familiar y garantizar el pleno ejercicio de sus derechos personales en caso de alteración, pérdida, tratamiento o acceso no consentido de sus datos personales registrados en soporte informático o manual.

Por ende, la LOPD establecía una serie de obligaciones para los responsables de los ficheros de datos de carácter personal, tanto de entidades públicas como privadas, obligaciones que han de estudiarse de manera conjunta con las obligaciones reguladas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, donde se establece la obligación de todas las organizaciones de implantar medidas destinadas a garantizar la protección de los datos de carácter personal. En concreto, se ha de destacar las siguientes obligaciones que la LOPD regulaba:

En primer lugar, de conformidad con lo establecido en el artículo 4 de la LOPD con relación a la calidad de los datos, exigía que los datos de carácter personal a fin de que pudieran ser recogidos para su tratamiento debían ser adecuados, pertinentes y no excesivos con la finalidad determinada, explícita y legítima para la que se haya obtenido, de tal modo que, los datos personales no podían ser usados para otras finalidades incompatibles con la finalidad principal. Igualmente, los datos personales recabados debían ser datos exactos y actualizados a efectos de responder con la veracidad a la situación actual de titular de estos y, siendo igualmente cancelados en caso de dejar de ser necesarios o pertinentes. Por otro lado, el artículo 10 de la LOPD regulaba la obligación de secreto profesional y el deber de guardar los datos por parte tanto del responsable del fichero como aquellos que intervengan en el tratamiento de los datos personales, obligaciones que debían cumplir incluso una vez hubiera finalizado la relación con el titular del fichero.

Asimismo, sobre la información en la recogida de datos, el artículo 5 de la LOPD establecía que el titular de los datos debía ser informado de "modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de los datos y de los destinatarios de la información; del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante." Por ende, lo anterior debía aparecer de manera expresa

y claramente legible cuando se utilizasen cuestionarios u otros impresos para la recogida de los datos personales.

En relación con el consentimiento del afectado, se ha de destacar que el artículo 6 de la LOPD establecía que para el tratamiento de los datos de carácter personal era necesario el consentimiento inequívoco del afectado, excepto en aquellos casos regulados por la Ley. Así pues, no era necesario el consentimiento del titular en caso de que los datos de carácter personal fueran recogidos para el ejercicio de las funciones propias de las Administraciones Públicas, así como en caso de que fueran necesarios para un contrato o, en caso de figurar en cuentas accesibles al público.

De igual modo, ante datos especialmente vulnerables como lo son los datos sobre la ideología, afiliación sindical, religión o creencias, origen racial, salud o vida sexual de un apersona, era necesario como norma general el consentimiento expreso y por escrito del afectado para su recogida, tratamiento y cesión. A modo de excepción, la LOPD en su artículo 7 establecía que los citados datos personales que son especialmente vulnerables por la información sumamente privada e íntima que facilitan sobre una persona, podían tratarse cuando resultara "necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitario o tratamiento médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario o equivalente, sujeto al secreto profesional".

Sobre los datos relativos a la salud, el artículo 8 de la LOPD dejaba abierta la posibilidad de que la legislación estatal o autonomía sobre sanidad regulara de manera específica la cesión y tratamiento de los datos sanitarios de las personas que acudan o hayan sido tratadas por las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes, sin perjuicio del contenido del artículo 11 de la LOPD. Así pues, el artículo 11 de la LOPD acerca de la comunicación o cesión de datos en primer lugar, establecía una obligación general donde era necesario el consentimiento del interesado, así como que la finalidad del cedente estuviera directamente relacionada con el cesionario para que los datos personales del interesado pudieran ser comunicados o cedidos.

En segundo lugar, el citado precepto legal señalaba a modo de excepción los casos en los que no era necesario el cumplimiento de la anterior obligación, esto es cuando nos encontremos ante: (1) una cesión autorizada por la Ley; (2) datos recabados de fuentes con acceso público; (3) cuando fuera necesario el tratamiento con ficheros de terceros para el desarrollo de una relación jurídica previamente aceptada de manera legítima y libre, siempre y cuando sea limitada la finalidad que justifique la comunicación, en caso contrario nos encontraríamos ante una comunicación ilegítima; (4) cuando el cesionario sea el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales de Cuentas – o instituciones autonómicas con funciones análogas a estos – en el ejercicio de sus funciones; (5) cesión entre Administraciones Públicas cuyo objeto sea con fines históricos, estadísticos o científicos y; (6) datos sanitarios, en caso de situación de urgencia donde es necesario acceder a un fichero o realizar estudios epidemiológicos en los términos legales.

Por otra parte, la LOPD establecía en el artículo 12 que el tratamiento por cuenta de terceros debía estar regulado en un contrato donde constase por escrito – u otra forma que acredite su contenido y celebración – que el encargado del tratamiento únicamente iba a tratar los datos según las instrucciones que recibiera del responsable del tratamiento, así como que los datos no serían usados para otro fin distinto al estipulado en el contrato, ni tampoco los comunicación a otras personas ni siquiera para su conservación[328].

Asimismo, el encargado del tratamiento, tras cumplimiento de la prestación contractual, debía proceder a la destrucción de los datos personales (así como de otros soportes o documentos donde consten datos personales objeto del tratamiento) o a su devolución al responsable del fichero. Si por cualquier motivo, el encargado del tratamiento destinase "los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente", de conformidad a lo establecido en el apartado cuarto del artículo 12 de la LOPD. Igualmente, los ficheros de titularidad pública debían ser inscritos en el Registro

[328] En el contrato de tratamiento de datos personales por cuenta a terceros también deben constar recogidas las medidas de seguridad establecidas en el RD 1720/2007, de obligada implantación por parte del Encargado del Tratamiento.

General de la Agencia Española de Protección de Datos (RGPD), con previa publicación en el Boletín Oficial de una Disposición General con la declaración de los ficheros[329].

En relación con la tutela del derecho de los afectados de acceso, rectificación y cancelación, debía constar perfectamente establecido el procedimiento interno apropiado[330]. Otras de las obligaciones que se ha de destacar es la referente a la implantación del documento de seguridad – art. 9 LOPD y Título VIII, capítulo II, del RD 1720/2007 – donde debía constar incluida la normativa de seguridad de índole técnica y organizativa necesaria a fin de garantizar la seguridad de los datos objeto de tratamiento[331].

Por último, resulta relevante la obligación en relación con el sometimiento cada dos años[332] a una auditoría interna o externa a efectos de verificar el cumplimiento de las medidas de seguridad aplicables a ficheros y tratamiento automatizados por parte de los sistemas de información e instalaciones de tratamiento y almacenamiento de datos[333].

En base a las anteriores obligaciones, la LOPD establecía una serie de sanciones a los responsables de los ficheros de datos de carácter personal, que en función de la infracción cometida se clasificaron en leves, graves y muy graves. Igualmente, la LOPD regulaba una serie de sanciones cuya cuantía era graduada según fuera la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas y a cualquier otra circunstancia que resulte relevante para determinar el grado de incumplimiento legal y de culpabilidad presentes en los hechos sancionados. En caso de que la infracción

[329] Véanse al respecto los artículos 20, 25 y 26 de la LOPD, y Título V del R.D. 1720/2007.

[330] Arts. 15 a 17 de la LOPD, y Título III del R.D. 1720/2007.

[331] El documento de seguridad es de obligado cumplimiento para todo el personal con acceso a los datos automatizados de carácter personal y al sistema de información.

[332] La obligación de someterse a una auditoria es para aquellos ficheros que tienen registrados datos de carácter personal a partir del nivel medio que serán detallados en el siguiente epígrafe del presente trabajo.

[333] Arts. 96 y 110 del R.D. 1720/2007.

hubiera sido cometida por una entidad privada, la cuantía por una sanción leve era de una multa que oscilaba entre los 601 € a 60.101 €; por una sanción grave la multa era de 60.101 € a 300.506 € y, por una sanción muy grave de 300.506 € a 601.012 €. En caso de que el responsable del tratamiento de los ficheros fuere una Administración Pública, la sanción correspondiente era la propuesta de iniciación de actuación disciplinaria por parte del Director de la Agencia Española de Protección de Datos. En todo caso, ante una utilización o cesión ilícita de datos que vulnerase los derechos fundamentales del afectado o de terceros, el Director de la AEPD podía requerir el cese de su utilización o cesión ilícita a los responsables de los ficheros, indistintamente que fueran públicos o privados, si los mismos no obedecían al requerimiento, se procedería a la inmovilización de los ficheros por medio de resolución motivada.

De manera paralela a la publicación de la LOPD y del R.D. 1720/2007 se han dictado diversos Reales Decretos que desarrollan la LOPD, así como varias instrucciones publicadas en el Boletín Oficial del Estado por la Agencia Española de Protección de Datos, entre las que se ha destacar: el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, el Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio, la STC ya citada de 30 de noviembre de 2000, la Instrucción 1/1995, de 1 de marzo de la AEPD, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito; la Instrucción 2/1995, de 4 mayo, de la AEPD, sobre medidas que granizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal; la Instrucción 1/1996, de 1 de marzo de la AEPD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios y, la Instrucción 1/1998, del 19 de enero, de la AEPD relativa al ejercicio de los derechos de acceso, rectificación y cancelación.

Finalmente, la LOPD fue derogada por la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), teniendo como objeto, por un lado, adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de

27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones y, por otro lado, proteger el derecho fundamental de las personas físicas a la protección de datos personales y garantizar los derechos digitales de la ciudadanía, todo ello de conformidad con el artículo 18.4 de la Constitución Española. En definitiva, como se ha podido apreciar en el anterior contexto, tanto la jurisprudencia como la doctrina concluyen que el derecho de protección de datos no tiene como único objetivo salvaguardar el derecho a la intimidad, sino la identidad del hombre y su propia libertad[334], por lo que exige que el derecho de protección de datos se regularice como un derecho autónomo y particular del ordenamiento jurídico.

II. LA ADAPTACIÓN DE LA VIGENTE NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES AL ESCENARIO DIGITAL

Llegados a este punto y, tras el estudio exhaustivo del elenco de normas jurídicas comunitarias y estatales dictadas sobre la materia de protección de datos durante las últimas décadas a consecuencia del cambio tecnológico, pues como se ha podido apreciar en el epígrafe anterior, el avance tecnológico de las últimas décadas ha generado de manera inevitable un avance en el ordenamiento jurídico europeo y nacional, motivo por el que surge la necesidad de promulgar un nueva normativa de protección de datos a fin de garantizar un tratamiento lícito de los mismos, así como la libre circulación de los datos personales debido a las múltiples fuentes tecnológicas dispersas generadoras de grandes volúmenes de datos masivos.

Por ello, fue promulgado el Reglamento General de Protección de Datos Personales, en adelante RGPD[335], pues la normativa anterior era estrictamente

[334] LUCAS MURILLO DE LA CUEVA, *El derecho a la autodeterminación*…, *op. cit.*, p. 113; LÓPEZ GARRIDO, D. y MARTÍN PALLÍN, J. A., "La informática: un riesgo incontrolado", *Revista Vasca de Administración Pública,* núm. 20, 1988, p. 202.

[335]Sobre el Reglamento General de Protección de Datos en LÓPEZ CALVO, J. (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* Wolters Kluwer, Madrid, 2018; PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad,* Reus, Madrid, 2016; DELGADO CARRAVILLA, E. y PUYOL MONTERO, J., *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea,* Tirant lo Blanch, Valencia, 2018; PUYOL MONTERO, J., *Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018; AA.VV., *Guía rápida. Protección de datos. Aplicación del RGPD*, Francis Lefebvre, Madrid, 2018; RALLO LOMBARTE, A., "Hacia un sistema europeo de protección de datos: las claves de la reforma", *RDP*, Núm. 85, 2012, pp. 15-56*;* RALLO LOMBARTE, A. y

procedimental, burocrática y de "puro cumplimiento normativo"[336], en cierto modo limitadora desde el punto de vista del acceso y tratamiento de los datos personales, al otorgar de manera exclusiva y excluyente prioridad al consentimiento del titular de los mismos sin dejar lugar a la posibilidad de acceso por causas de interés general y de salud pública[337].

Finalmente, en los últimos años hemos sido testigos de la promulgación de la normativa vigente comunitaria y estatal sobre el derecho de protección de datos, lo que ha significado un cambio legislativo relevante dimanante de conceptos abiertos, principios nuevos y medidas de seguridad que permiten una eficaz adaptación a la evolución tecnológica, entre otras muchas novedades como a continuación se destacarán[338].

GARCÍA MAHAMUT, R. (Coords.), *Hacia un derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015; y TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de protección de datos personales", *REDE*, núm. 43, 2012, pp. 25-184.

[336] Por ejemplo, así lo describe LÓPEZ ALONSO, F.J., "¿Cómo abordar un análisis de riesgos en un tratamiento de datos de carácter personal sujeto al Reglamento General de Protección de Datos?", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, p. 711, donde aclara que: "Hasta ahora estábamos acostumbrados a aplicar una Ley y una normativa de desarrollo muy paternalista que nos marcaba en todo momento todas y cada una de las cosas que deberíamos hacer de forma exhaustiva, descuidando en muchas ocasiones el fondo de la norma, "la protección". Me refiero a ese cumplimiento que consistía en inscribir un fichero ante la Agencia Española de Protección de Datos (AEPD), crear un documento de seguridad, realizar las pertinentes auditorias, etc. Salvo aquellos clientes verdaderamente concienciados en protección de datos, los menos, desgraciadamente, bastaba con elaborar los documentos descritos y con suerte a los dos años, si el tratamiento así lo exigía, salían de la estantería en la que habían sido almacenados para hacer frente a la siguiente auditoría obligatoria, en resumen, puro cumplimiento normativo, sin más. Y de repente se tambalea todo y nace una norma, el RGPD, que supone un cambio de paradigma en materia de protección de datos".

[337] La normativa de protección de datos personales anterior al RGDFUE también incluía el consentimiento como supuesto de legitimación del tratamiento, añadiendo que debía haberse dado "de forma inequívoca" –art. 7.a) Directiva 95/46/CE-, es decir, que debía ser un "consentimiento inequívoco del afectado" –art. 6.1 LOPD-. La Directiva 95/46/CE señalaba que el consentimiento del interesado era "toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan" –art. 2.h)-, una definición que reproducía la LOPD con el añadido de "inequívoco" –art. 3.h)-. A esto hay que añadir la necesidad de un "consentimiento explícito" para las categorías especiales de tratamientos –art. 8.2.a) Directiva 95/46/CE-, que había sido transpuesto en nuestro país como consentimiento expreso –o expreso y escrito- para el tratamiento de los datos especialmente protegidos –art. 7.2 y 3 LOPD-, entre los que se incluían los datos relativos a la salud.

[338] LÓPEZ CALVO, J., "Reglamento Europeo de Protección de Datos: ejes relevantes" en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, pp. 609-678.

El nuevo modelo de protección de datos surge, por un lado, como respuesta a problemas tradicionales, tales como homogenizar la normativa jurídica de protección de datos en todos los Estados Miembros de la Unión Europea, armonizar el tratamiento de datos transfronterizo dentro de la Unión Europea o, como ha sido el gran desafío el tratamiento de los datos personales con terceros países y; por otro lado, surge como necesidad de dar respuesta a retos presentados por las nuevas tecnologías[339], tales como la tecnología *big data,* a efectos de hacer compatible esta tecnología que sustrae información y conocimiento de gran valor para la humanidad (sobre todo en el sector sanitario) a través del procesamiento de grandes bases de datos, de diversas fuentes y a gran velocidad con principios fundamentales de la protección de datos, tales como, el principio de transparencia, principio de minimización de los datos o el principio de limitación de los fines del tratamiento, sin desaprovechar a su vez los beneficios y oportunidades que aportan las tecnologías sobre todo en el ámbito sanitario y de la investigación biomédica y farmacéutica[340].

Por ello, en cierta medida, la vigente normativa europea y española de protección de datos resulta en cierto grado innovadora pues deja atrás una regulación de estricto cumplimiento administrativo y burocrático sobre la protección de los datos personales y el tratamiento adecuado de los mismos, dando paso a conceptos abiertos, principios flexibles, así como a la posibilidad de ponderar derechos fundamentales de interés público[341] con el derecho de protección de datos, donde el consentimiento del

[339] PÉREZ GÓMEZ, "Especialidades en el…", *op. cit.*, p. 874, señala que: "Las nuevas tecnologías tienen un general protagonismo en todo lo referente a la protección de datos personales, más aún en el sector sanitario donde la utilización masiva de historias clínicas y recetas electrónicas, así como el enorme potencial que la aplicación del *big data*, puede suponer para los avances en investigación y planificación del sistema nacional de salud, entre otros muchos ámbitos".

[340] CERVERA NAVAS, L., "El nuevo modelo europeo de protección de datos de carácter personal", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019 pp. 73-74.

[341] En ese sentido 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", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada,* núm. 49, Julio-Diciembre 2018, pp. 188-189, señala que: "La Unión Europea ha aprobado el 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 -Reglamento General de Protección de Datos Personales, en adelante RGPD, una norma que afecta intensamente al ámbito de la salud. La investigación sanitaria, la salud pública y la asistencia sanitaria requieren la realización de tratamientos de datos personales para garantizar derechos fundamentales como el derecho a la vida y a la protección a la salud –arts. 15 y 43 CE-, ejercer la libertad de creación científica y técnica –art. 20.1.b) CE y la libertad de empresa –art. 38 CE- y alcanzar intereses públicos y privados, lo que puede entrar en conflicto con el

titular de los datos[342] en algunos casos, como se verá, quedará en un segundo plano dejando de ser la base reguladora de obligatorio cumplimiento para un tratamiento lícito de los datos personales, sobre todo de los datos relativos a la salud, pues no cabe duda que la normativa vigente de protección de datos afecta poderosamente al ámbito de la sanidad, extremo que sin duda resulta relevante en la temática del presente trabajo y que más adelante se analizará en profundidad.

Además de proteger el tratamiento de los datos personales de las personas físicas[343], el RGPD tiene como objeto[344] garantizar la libre circulación de datos y a su vez, regular restricciones y prohibiciones para el caso de un uso injustificado de los datos personales, permitiéndose en consecuencia una cierta tolerancia en lo que respecta a la libre circulación de los datos de salud (en el campo de la investigación biomédica, farmacéutica y en la asistencia sanitaria) a fin de garantizar un equilibro de intereses y facilitar a las autoridades de control y a los tribunales la posibilidad de ponderar derechos fundamentales de interés general con el derecho de protección de datos frente a las denuncias que pudieran formular los titulares de los datos personales[345].

---

derecho fundamental a la protección de datos personales –art. 18.4 CE-. Por ese motivo, la legislación y la práctica sanitaria se fue adecuando progresivamente, al principio con el escepticismo de sus profesionales, primero a la LORTAD –aunque en menor medida-, y, posteriormente, de manera ya clara y decidida, a la LOPD2. La aprobación del RGPD pone una nueva tarea por delante, adaptarse ahora a esta norma de derecho derivado institucional de la Unión Europea que es obligatoria en todos sus elementos y directamente aplicable".

[342] Acerca del titular de los datos se ha de ampliar tanto a los familiares cuando nos encontremos ante los datos personales de personas fallecidas y, padres o tutores cuando nos encontremos ante menores de edad.

[343] Son datos personales los que aportan información acerca de una persona física identificable, es decir, que pueda ser identificada a través de un nombre, un número de identificación, datos de localización, un identificador en línea o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Consecuentemente, únicamente datos personales referentes a personas físicas, por tanto, los datos en relación personalidades jurídicas – ya sean públicas o privadas - quedarán propiamente excluidos de protección jurídica del RGPD, de conformidad con el artículo 4 RGPD y art. 6 LOPDGDD.

[344] Arts. 1.1 y 2.1 RGPD.

[345] TRONCOSO REIGADA, "Investigación, salud pública y asistencia sanitaria…", *op. cit.,* p. 196. De igual modo, DÍAZ GARCÍA, E., "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación", *DS Derecho y Salud,* Vol. 28, Extraordinario XXVII Congreso 2018, p. 234, señala que: "El RGPD viene a adaptar la normativa existente a la realidad actual presidida por la innovación, la especialización y la diferenciación, que supone la constante puesta en circulación de nuevos productos, servicios y sistemas basados en el tratamiento de datos de carácter personal. Dichos datos se encuentran expuestos a una serie de riesgos cuya materialización supone consecuencias negativas, tanto para las organizaciones (sanciones, crisis reputacionales etc..), como para los afectados, encontrándose el sector sanitario sometido a riegos de ciberataques por encontrarse altamente expuesto dada la sensibilidad y el valor de los datos manejados. Por otro lado, la confianza que suscita la relación médico paciente puede hacerse extensiva a la garantía de protección y seguridad de datos de salud, al mismo nivel que la confidencialidad o el secreto médico, de ahí la pertinencia de esta regulación".

El ámbito sanitario, no cabe duda de que es uno de los sectores más afectados por el RGPD planteando a su vez algunas particularidades debido a que nos encontramos ante datos especialmente sensibles y por consiguiente, merecedores de protección y, a su vez datos que suponen una gran fuente de información y conocimiento para salvar la vida del propio titular en caso de asistencia sanitaria, como para situaciones de interés general como resulta la asistencia sanitaria, la investigación biomédica y farmacéutica. En este sentido, otras de las novedades a destacar del Reglamento dentro del ámbito sanitario, es la regulación dada a los derechos del titular de los datos de salud, donde el legislador europeo amparándose en el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, les otorga a los datos relativos a la salud una regulación específica en el RGPD[346], que en el presente capitulo se analizará.

De igual modo, cabe tener en consideración que en el contexto nacional, la LOPDGDD nace como norma necesaria a efectos de adaptar el ordenamiento español al RGPD con el objeto de garantizar una regulación jurídica comunitaria uniforme[347] y transparente del derecho fundamental a la protección de datos[348] en una sociedad globalizada y de rápida evolución tecnológica donde los datos personales son cada vez

[346] El considerando 10 RGPD recuerda que: "el presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos persones ("datos sensibles"). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito". De igual modo, en el considerando 53 permite que los Estados miembros mantengan o introduzcan "otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de estos datos".

[347] En consecuencia, la LOPDGDD se promulga igualmente a efectos de dar cumplimiento al principio de seguridad jurídica del Derecho de la Unión Europea, debido a que el mismo obliga, entre otros, a que "la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España)" como es indicado por el legislador español en el apartado III del preámbulo de la citada ley.

[348] Art. 2.1 LOPDGDD "Ámbito de aplicación", destacándose dos salvedades en relación con la normativa derogada y con el RGPD: sobre la primera, se ha de hacer mención a que el ámbito de aplicación es más claro y conciso, pues la anterior LOPD se limitaba a establecer en el art. 2.1 que era "de aplicación a los datos de carácter personal registrados en soporte físico que lo haga susceptibles de tratamiento"; sobre la segunda, se ha de poner de manifiesto que la LOPDGDD a diferencia del RGPD no sólo regula el derecho de protección de datos personales, sino que también regula la garantía de los derechos digitales, mención que hay que hacer constar aunque no sea objeto de estudio del presente trabajo.

más el recurso fundamental de la sociedad de la información, así como para garantizar los derechos digitales de la ciudadanía[349].

En concreto, en lo referente al tratamiento de los datos relativos a la salud, el legislador español en la LOPDGDD ha considerado que el RGPD regula esta materia de manera completa, lo que generó que en ninguna de las fases de su aprobación previas a su publicación se plantease cuestión alguna referente a los datos salud a excepción de la problemática sobre su utilización en el sector de la investigación[350]. Por ello, la LOPDGDD tiene como objeto fomentar la investigación científica y, en particular, la investigación biomédica y farmacéutica[351], pues resulta indudable que la tecnología supone una evolución para la investigación científico - sanitaria, sobre todo la aportación de las herramientas *big data* en la investigación retrospectiva y prospectiva con los datos de salud y la recientemente denominada "medicina de las 5 P"[352]: personalizada, predictiva, preventiva, participativa y poblacional[353]. Finalmente, la LOPDGDD regula en una única disposición adicional, la decimoséptima, el tratamiento

[349] De conformidad a lo establecido en el apartado segundo del Preámbulo de la LOPDGDD y en su artículo 1, donde establece que: "La presente ley orgánica tiene por objeto: a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el 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, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución".

[350] FUENTES ESCOBAR, A., "Algunas cuestiones relevantes en el tratamiento de la LOPDGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, p. 163, afirma que: "De forma meramente enunciativa, las principales referencias a esta materia en el Proyecto serían las que hacen referencia al tratamiento de categorías especiales de datos como elemento a tener en consideración a la hora de llevar a cabo el análisis de riesgos (artículo 28.2 c) del Proyecto) o la exigencia de que los centros sanitario legalmente obligados a la llevanza de historias clínicas designen un delegado de protección de datos (artículo 34.1 l) del Texto). En relación con este último precepto es preciso poner de manifiesto que el texto final de la Ley ha incorporado una regla sumamente relevante en el ejercicio privado de la profesión médica, al excluir de esta obligación a "los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de sus pacientes, ejerzan su actividad a título individual".

[351] Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 69.

[352] Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 44; MARTÍNEZ MARTÍNEZ, R y ÁLVAREZ RIGAUDIAS, C., "El uso de datos con fines de investigación biomédica (Arts. 9 y 89 RGPD. Art. 9, Disposición adicional decimoséptima, Disposición final novena y Disposición transitoria sexta LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, p. 280, donde señalan que: "la quinta P, de poblacional, es creación del Dr. Julio Mayol".

[353] MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación…", *op. cit.*, pp. 279-280.

de datos de salud, incorporando especialmente en el apartado 2 una regulación específica para el tratamiento de datos relativos a la salud en el ámbito de la investigación biomédica y farmacéutica[354].

No obstante, la LOPDGDD en el apartado III del Preámbulo señala que el hecho de que los datos personales sean actualmente un recurso fundamental de la sociedad de la información a causa de la rápida evolución tecnológica y la globalización tiene una vertiente positiva y a su vez riesgos[355]:

"[…] el carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso".

Si bien es cierto que el acceso a la información por parte de un mayor número de actores supone un riesgo debido al difícil control del destino y uso, sin embargo, particularmente en el caso de los datos sanitarios nos encontramos ante un riesgo que hemos de asumir cuando la finalidad es para un bien común e interés general, puesto que el hecho de poner barreras de acceso a aquellos agentes que necesitan conocer de la información y conocimiento que se sustraiga tras un análisis *big data*, sería a su vez limitar la medicina personalizada, predictiva, preventiva y participativa y, en

[354]En este sentido, el legislador español tiene en consideración especialmente el considerando 33, en conexión con el 53 que permite el otorgamiento de consentimiento más amplios en supuestos en los que no sea posible la plena determinación de la finalidad del tratamiento a fin de "lograr el beneficio de las personas físicas y la sociedad en su conjunto" FUENTES ESCOBAR, "Algunas cuestiones relevantes…", *op. cit.,* p. 165.

[355] En el apartado IV del Preámbulo de la LOPDGDD, el legislador español reconoce que debido a que los riesgos y oportunidades que nos ofrece el mundo de las redes constan identificados en la actualidad "corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital". De igual modo, el legislador español en el citado apartado reconoce la necesidad de una reforma de la Constitución Española en la que la *era digital* sea incluida y donde se eleve a rango constitución "una nueva generación de derechos digitales", mientras tanto y, a la espera de la llegada de la citada reforma, el legislador aborda el sistema de garantía de los derechos digitales a través de la LOPDGDD poniendo en relación el artículo 18 de la Constitución Española con la reciente jurisprudencia ordinaria, constitucional y europea pronunciada al respecto.

consecuencia, a la evolución de la sanidad y de la investigación biomédica y farmacéutica[356].

Por último y, no menos importante, se ha de tener en consideración que la entrada en vigor de la LOPDGDD ha generado de manera directa dos modificaciones esenciales en la normativa sanitaria: en primer lugar, la modificación de la Ley 14/1986, de 25 de abril, General de Sanidad, donde se añade un nuevo Capítulo II al Título VI en relación con el tratamiento de datos de la investigación biomédica[357] y, en segundo lugar, se modifica el aparto 3 del artículo 16 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 y documentación clínica[358].

---

[356] Al respecto, FUENTES ESCOBAR, "Algunas cuestiones relevantes en el tratamiento…", *op. cit.,* p. 164, aclara que: "Así, ya en enero de 2018 la Federación de Asociaciones Científico Médicas Españolas (FACME) hizo público un comunicado en que se ponía de manifiesto que el Proyecto debía garantizar la licitud del uso secundario de los datos médicos con fines de investigación, como elemento fundamental para la adecuada garantía del avance de la investigación científica, que lógicamente debía considerarse de interés público. En este sentido se planteaba el problema de que la exigencia de un consentimiento específico para cada una de las finalidades del tratamiento de los datos de salud podía obstaculizar el desarrollo científico, al restringir el uso de los datos a la concreta investigación en que se hubieran obtenido, vedando la posible reutilización posterior de los datos para investigaciones no previstas en el momento en que el interesado prestó su consentimiento". Asimismo, añade que: "Todo ello conducía a la conclusión de que los requisitos de especificidad y carácter inequívoco para la prestación del consentimiento no deben ser interpretados en el ámbito de la investigación científica de un modo restrictivo, limitado a una concreta investigación de la que se facilite toda la información disponible, sino que cabe considerar que concurren en los supuestos en los que el consentimiento se presta en relación con un determinado campo de investigación, pudiendo extenderse en el futuro ese consentimiento, sin que ello lo vicio 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 investigación no prevista" – FUENTES ESCOBAR, "Algunas cuestiones relevantes en el tratamiento…", *op. cit.,* p. 165.

[357] Artículo 105 bis: El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

[358] Artículo 16: "[…] 3. 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 clínicos asistenciales, 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.

Sin embargo, a pesar de la voluntad de legislador tanto europeo como español de adaptar la normativa jurídica sobre protección de datos personales a la nueva era digital y tecnológica, no se encuentran todos los aspectos matemáticamente predefinidos, por lo que se estima necesario una norma sectorial específica de protección de datos personales relativos a la salud y de proyectos de investigación biomédica, farmacéutica y de asistencia sanitaria que apliquen herramientas *big data*, a efectos de garantizar una seguridad al titular de los datos y regular medidas adecuadas que se adapten al nuevo contexto tecnológico y sanitario, extremo que será analizado en detalle más adelante.

Por ello, llegados a este punto de la investigación, a partir de ahora y a lo largo de los capítulos cuatro y cinco se va a tratar de desarrollar uno de los objetivos principales de la tesis, esto es, fundamentar desde una perspectiva jurídica a través de un examen exhaustivo de la normativa vigente sobre protección de datos personales (tanto europea como nacional) la defensa de la necesidad de una norma específica de protección de datos personales relativos a la salud y de proyectos de investigación que apliquen herramientas *big data*, pues no cabe duda que la investigación en la mayoría de los casos tiene como finalidad la de proteger y mejorar la vida tanto a nivel particular como a nivel colectivo, aunque se ha distinguir igualmente entre "el interés público de la investigación y el interés privado de entidades privadas y, en ocasiones, de los propios investigadores"[359], como más adelante se expondrá.

Por consiguiente, una vez que se ha analizado en los capítulos anteriores, por un lado, el contexto del *big data* en general, así como de manera específica el *big data* sanitario y; en segundo lugar, una vez estudiada en profundidad desde una perspectiva

---

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".

[359] TRONCOSO REIGADA, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de…", *op. cit.*, p. 195, afirma que: "La investigación está destinada también a proteger la vida, que no sólo es un bien individual sino también un bien colectivo, sin perjuicio de que haya que distinguir entre el interés público de la investigación y el interés privado de entidades privadas y, en ocasiones, de los propios investigadores"; MARTÍN MORENO, J.M., "Epidemiología y respeto a la confidencialidad sobre los datos personales: a propósito de una propuesta de Directiva europea", *Gaceta Sanitaria*, Vol. 8, núm. 45, 1994, p. 320, señala que: "el reconocimiento del papel de la investigación y el derecho a que no haya más obstáculos que los que razonablemente imponen los principios éticos exigibles y el trabajo bien hecho".

jurídica, la evolución normativa del derecho de protección de datos personales desde sus inicios con la interpretación dada por el Tribunal Constitucional del artículo 18.4 de la Carta Magna hasta nuestros días, en los siguientes epígrafes del trabajo se estudiará la regulación especial dada al tratamiento de los datos de salud en la normativa de protección de datos vigentes, a efectos de que se aprecie la influencia y relevancia que tienen los datos sanitarios tanto para la salud pública como para la evolución del conocimiento y de la humanidad en su conjunto, lo que sin duda resulta de gran interés general para toda la sociedad, pues la salud – y con ello la vida – son derechos fundamentales que atañen a cada individuo de la población.

No obstante, a pesar de que el legislador europeo ha sido en todo momento consciente de lo anterior, motivo principal del nacimiento del RGPD[360], de manera sorpresiva, cuando en su día se analizó y estudió con detenimiento el RGDP para el desarrollo de este trabajo, la sensación resultó un tanto agridulce: pues, por un lado, satisfacción al apreciarse que el mundo jurídico y, sobre todo, que el legislador de la Unión Europea había sido por fin consciente de manera fehaciente de la importancia que tenía no limitar el acceso a los datos sanitarios cuando se trataba, entre otras, por razones de salud pública, investigación y medicina preventiva, otorgándole preferencia en determinados casos al interés general frente al particular del paciente en la ponderación de los derechos a la salud pública con el derecho a la intimidad, especialmente, al derecho a la protección de datos sanitarios del titular de los mismos; sin embargo, por otro lado, cierta decepción al detectarse tanto en la normativa europea (y posteriormente en la española) algunas carencias y limitaciones jurídicas – sanitarias relevantes en relación a la protección de datos relativos a la salud, siendo el resultado, de ambas normas, tanto la europea como la española, insuficiente, pues a pesar del intento de incluir la protección y el tratamiento de los datos de salud dentro del mismo marco jurídico general del derecho de protección de datos personales, el resultado más

[360] Al respecto hemos de traer a colación de lo visto anteriormente en el presente trabajo, que uno de los objetivos fundamentales del RGPD que el de legalizar la libre circulación de los datos salvaguardando a su vez el derecho de protección de datos de los titulares, otorgándole así una regulación específica al tratamiento de los datos sanitarios, debido principalmente a la información y conocimiento de valor que aportan en el ámbito de la salud pública y de la investigación biomédica, destacando el campo de la epidemiologia y clínica. Pues bien, lo cierto es que esa información y conocimiento en la mayoría de las situaciones se consigue a través de la aplicación de tecnologías de *big data*, de ahí la importancia de que los datos puedan circular de manera libre, siempre y cuando sean aplicadas las medidas y garantías idóneas que eviten riesgos innecesarios y posibles vulneraciones al derecho de protección de datos y consigo, al derecho de intimidad de los pacientes.

que resolutivo a efectos prácticos para los profesionales de la sanidad y de otros sectores, ha resultado caótico y en cierto grado, confuso, no sólo para ellos sino también para el resto de la población.

En particular, como prueba de lo anterior, tenemos los múltiples informes emitidos por la AEPD, por el Grupo de Trabajo del art. 39, así como de la propia Sociedad Española de Salud Pública y Administración Sanitaria, destacándose el informe bajo la rúbrica *Protección de Datos Personales y Secreto Profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD* de noviembre de 2017, todo ellos citados y analizados a lo largo del presente trabajo. Por ello, tras la publicación de ambas normas de protección de datos, se aprecia que continúa siendo necesaria una ley sectorial sobre el tratamiento y la protección de datos de salud en lo que respecta a la sanidad pública, investigación biomédica y con ello, a la aplicación de las técnicas de *big data*, como herramientas más eficaces y eficientes para sustraer información y conocimiento de los datos sanitarios.

Bien, cabe destacar que anteriormente a la redacción y promulgación del RGPD, en concreto, a principios de la década del 2000, ya subyace en el sector profesional de la salud y por parte de la doctrina del derecho sanitario, la defensa de la tesis de la insuficiencia de las leyes vigentes en el momento a efectos de garantizar una respuesta jurídica a los posibles problemas planteados en ese contexto y que pudieran plantearse a futuro a causa fundamentalmente de la implantación de las TIC[361] sobre el tratamiento de los datos relativos a la salud, siendo así prevenido por los grandes juristas la aprobación de una norma específica:

"[…] Álvarez -Cienfuegos Suárez[362], comentando este artículo en el año 2001, afirmó que la referencia genérica a la legislación sanitaria autonómica o estatal que realiza, constituía una clara insuficiencia de la Ley para contemplar las complejas

[361] En especial la implantación de la firma electrónica.

[362] ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M., "La aplicación de la firma electrónica y la protección de datos de la salud", *Actualidad Informática Aranzadi,* núm. 39, 2001, p.3.

garantías exigidas por el tratamiento de los datos relativos a la salud, por lo que aconsejó la aprobación de una norma específica"[363].

De igual modo, tras la entrada en vigor del RGPD y, previo a la promulgación de la LOPDGDD, varias fueron las instituciones que se pronunciaron sobre la necesidad de una ley específica de protección de datos de salud:

De un lado, en noviembre de 2017, la Sociedad Española de Salud Pública y Administración Sanitaria (SEPAS) publicó un informe sobre *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD,* donde parte de la "necesidad de disponer de una ley específica sobre protección de datos personales relativos a la salud, ley que por ende se enmarcaría en la normativa del sector sanitario, y sustituiría la disposiciones contenidas sobre la materia"[364].

De otro lado, la Sociedad Española de Epidemiología (SEE), el 17 de enero de 2018, en su declaración sobre la tramitación parlamentaria del proyecto de Ley orgánica de Protección de Datos "se concretan los motivos de su preocupación en la necesidad de una legislación específica de protección de datos de saludo, entendiendo que la misma no puede estar contenida en una ley de carácter sectorial"[365].

Por último, la Agencia de Protección de Datos a efectos de dar respuesta al asunto sobre la necesidad de una ley sectorial de protección de datos de salud, publicó el *Informe 073667/2018* donde afirma que el RGPD no supone una alteración a la normativa vigente española sobre el tratamiento de datos en el marco de la investigación biomédica, permitiendo así el RGPD una interpretación abierta y flexible sobre el consentimiento del paciente regulado en la Ley 14/2007, de 3 de julio, de Investigación

[363] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 5. Disponible en: https://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd/

[364] DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…", *op. cit.,* p. 232.

[365] DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…", *op. cit.,* p. 232.

Biomédica (LIB)[366]. Sin embargo, como bien apunta DÍAZ GARCÍA "el problema del informe es que únicamente hace referencia a la regulación de la LIB, y a la excepción contenida en el art. 58.2 de dicha norma" dejando de lado otras ramas de investigación y, en consecuencia, las normas que la regulan la investigación[367]. De igual modo, MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS señalan que:

"Sin embargo, los expertos en reiteradas ocasiones ponen de manifiesto las trabas que la normativa y su interpretación por el regulador planteaba a la investigación. Y durante la tramitación del proyecto del proyecto de la LOPDGDD se manifestó preocupación ante la inicial propuesta del proyecto de ley de una dilación de dos años respecto del tratamiento de datos de salud, siendo esta una materia que el Reglamento permite a los Estados Miembros regular localmente. El informe que emitió la autoridad de control española antes de la entrada en vigor del Reglamento no fue suficiente para que el sector de la investigación pública y privada pudiera abordar sus proyectos teniendo claro en qué medida el Reglamento les afectaba teniendo en cuenta las leyes

[366] En este sentido, MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación biomédica*…", op. cit.*, pp. 280-281, aclaran que: "Las enmiendas planteadas durante la tramitación parlamentaria trataron de (i) ofrecer seguridad jurídica respecto de ensayos clínicos en curso con la entrada en vigor del Reglamento, (ii) clarificar cómo aplicar los artículos 9.2.i) y j) del Reglamento, tanto respecto de la remisión a la ley local como a las salvaguardas del art. 89 del Reglamento, (iii) poner en valor la compatibilidad *ex lege* del art. 5.1.b) del Reglamento en esta materia, (iv) abordar el consentimiento amplio, (v) hacer uso de la habilitación a los Estados miembros de limitar ciertos derechos en la medida prevista en el art. 89.2 del Reglamento como habían hecho otros Estados miembros como Alemania y Austria y (vi) modificar trabas incompatibles con una investigación moderna en las normas locales que rigen la historia clínica. El texto que finalmente se ha aprobado ha incorporado algunas de esas enmiendas, pero también ha modificado otras de tal forma que han perdido su sentido original. Por ello, el art. 9 y la DA 17ª requieren ahora una labor de interpretación teleológica importante para no menoscabar las finalidades previstas en el Reglamento y en los propios expositivos de la LOPDGDD, esto es, facilitar la investigación científica con las debidas salvaguardas".

[367] En concreto, afirma DÍAZ GARCÍA que: "El problema del informe es que únicamente hace referencia a la regulación de la LIB, y a la excepción contenida en el artículo 58.2 de dicha norma, que permite bajo ciertas condiciones, entre otras, la necesaria aprobación por un Comité de Investigación, la utilización de muestras biológicas con fines de investigación biomédica para finalidades distintas de aquellas para las que fueron recogidas, sin el consentimiento del paciente. Sin embargo, no hace referencia alguna al resto de la investigación, ni concreta en qué medida y bajo qué condiciones, el RGPD ampara tratamientos de datos que se reclaman desde el punto de vista de los investigadores. Esta visión considera investigación clínica todo aquello que se realiza en seres humanos, sea del tipo que sea, incluyendo, por tanto, la investigación observacional y la experimental, y sometiéndolas todas a los mismos requisitos. Pero lo cierto es que junto a la LIB, debemos tener en cuenta otra serie de normas que regulan cada tipo de investigación, y a las que el informe no hace referencia alguna, como son la Ley 33/2011, de 4 de octubre, General de Salud Pública, que regula de manera específica la investigación en salud pública; el ya mencionado Real Decreto 1090/2015, en relación con los ensayos clínicos con medicamentos; la Orden SAS/3470/2009, de 16 de diciembre, por la que se publican las directrices sobre estudios posautorización de tipo observacional para medicamentos de uso humano; así como las Leyes 14/1986, de 25 de abril, General de Sanidad y la Ley 16/2003 de Cohesión y Calidad del Sistema Nacional de Salud" DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…", *op. cit.,* pp. 232-233).

locales, sin perjuicio de que confirmó que las causas de legitimación de los datos de salud no se limitaban al consentimiento en materia de investigación científica (interpretado de forma amplia), mencionando expresamente el art. 9.2.j) del Reglamento"[368].

No obstante, lo cierto es que habiendo transcurrido veinte años y, tras la promulgación de una multiplicidad de leyes[369] donde se han de incluir tanto leyes sanitarias como la normativa específica de protección de datos[370], actualmente y tras la publicación del RGPD y la LOPDGG, continúa subyaciendo en la actualidad la necesidad de una ley sectorial que regule de manera específica la protección y el tratamiento de los datos de salud que complemente de manera independiente las bases jurídicas asentadas por el RGPD, pues "esta afirmación hoy sigue siendo válida pues tales determinaciones legales son insuficientes para presuponer que disponemos de un régimen normativo básico bastante y actualizado de protección de datos de salud"[371]. Asimismo, de la necesidad de una ley sectorial nos advierte SERRANO PÉREZ en su intervención en el VI Congreso Internacional de Bioderecho celebrado en la Universidad de Murcia en abril de 2018 en relación con la confidencialidad y los nuevos usos de los datos en salud bajo la rúbrica "La necesidad de una ley de protección de datos en salud"[372], al afirmar que:

---

[368]MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación biomédica*...", op. cit.*, p. 280. Igualmente, se cita MARTÍNEZ MARTÍNEZ. R., "Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos", *Dilemata,* núm. 24, 2017, pp. 151-164. *Vid.* MARTÍNEZ MARTÍNEZ, "Big Data, investigación en salud y protección de datos personales: ¿Un falso debate?...", *op. cit.,* pp. 235-280.

[369]Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica -LBAP-; Ley 16/2002, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud -LCCSNS-; Ley 14/2007, de 3 de julio, de Investigación biomédica -LIB-; Ley 33/2011, de 4 de octubre, General de Salud Pública -LGCP-, Real Decreto 1090/2015, de 4 de diciembre, que aprueba el reglamento de ensayos clínicos con medicamentos, así como diversas leyes autonómicas, encontrándose actualmente vigentes: la Ley 14/1986, de 25 de abril, General de Sanidad, en lo no derogado por la LGCP; Ley 41/2002, de 13 de noviembre, Básica de Autonomía del Paciente; Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud y el Real Decreto 1020/2006, de 15 de septiembre; la Ley 33/2011, de 4 de octubre, General de Salud Pública y la Ley 14/2007, de 3 de julio, de Investigación Biomédica, destacándose sobre todo la vigente normativa de protección de datos: RGPD y LOPDGG.

[370] DE MIGUEL SÁNCHEZ, N., "Datos de carácter personal relativos a la salud: una obligada remisión a la normativa del sector sanitario", en AA.VV., *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, (Dir. A. Troncoso Reigada), Civitas, Madrid, 2010, p. 716.

[371] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p.5.

[372] SERRANO PÉREZ, M.ª M., "La necesidad de una ley de protección de datos en salud", *Bioderecho.Es,* núm. 8, 2018, p. 10.

"[…] quiero volver a incidir en la necesidad de contar con una norma sobre protección de datos en el ámbito de la salud que compendie, armonice y aclare las reglas y principios a aplicar endicho contexto, en la investigación epidemiológica y la investigación científica. Una regulación sectorial y que perpetuara la situación de remisiones con la que contamos en la actualidad sería una involución, teniendo en cuenta que estamos ante un momento propio para invertir dicho escenario".

En concreto, sobre esta cuestión SERRANO PÉREZ señala que "nos encontramos ante un momento legislativo en el que la elaboración de una ley orgánica de protección de datos es una tarea pendiente (tras la aprobación del REPD 2016/679)"[373], advirtiendo igualmente que la actual normativa vigente incrementa la disparidad actual existente en el tratamiento de los datos de salud en vez de enmendarla[374]. Al respecto, VALERO TORRIJOS y CERDÁ MESEGUER, afirman que:

"En definitiva, a pesar de los avances legislativos desde el año 2007, todavía persisten importantes insuficiencias y dificultades normativas que hacen cada vez más urgente una apuesta legislativa decidida para hacerles frente. En concreto, más allá del ámbito específico de la salud pública, la exigencia de que las entidades públicas difundan los datos utilizando formatos reutilizables es una premisa para integrar otro tipo de datos que, sin estar referidos específicamente al ámbito de la salud pública, podrían ofrecer un indiscutible valor a la hora de adoptar decisiones de políticas públicas que faciliten el impulso del control social, de la actividad económica así como, en definitiva, el desarrollo de modelos de negocio por parte del sector privado a partir de la integración del mayor número posible de catálogos de datos provenientes del múltiples fuentes de información"[375].

Lo cierto es que, reafirmando el criterio de los autores SERRANO PÉREZ, MARTÍNEZ MARTÍNEZ, VALERO TORRIJOS y CERDÁ MESEGUER tanto el RGPD como la LOPDGGD resultan normas insuficientes, caóticas e imprecisas debido al intento de

[373] SERRANO PÉREZ, "La necesidad…", *op. cit*., p.2.

[374] SERRANO PÉREZ, "La necesidad…", *op. cit*., p.2.

[375] VALERO TORRIJOS, J. y CERDÁ MESEGUER, J.I., "Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos de COVID-19", *Eunomía. Revista en Cultura de la Legalidad,* núm. 19, octubre 2020 – marzo 2021, p. 115.

regular conjuntamente y de manera entremezclada el articulado sobre materia tan compleja y extensa como lo es la del tratamiento de los datos sanitarios, con la normativa general de protección de datos personales. En especial, esta falta de precisión que se observa en la normativa estatal dimana principalmente por las siguientes causas: por un lado, la normativa estatal vigente de protección de datos remite de manera constante y continua a lo largo de su articulado a lo establecido en el RGPD, generando en la mayoría de las situaciones confusión al ciudadano por falta de claridad y precisión; por otro lado, delega gran parte de las cuestiones relevantes a los criterios de las autoridades de control[376] y de los Tribunales[377], cuestiones que, sin duda, de conformidad con el principio de seguridad jurídica deben ser aclaradas desde un primer momento por el propio legislador – europeo y/o español[378] – a los efectos de proporcionar un marco legislativo claro y preciso[379] tanto a los profesionales de la sanidad como a los profesionales del sector protección de datos y, sobre todo, a los

[376] ÁLVAREZ RIGAUDAS señala que "a pesar del proclamado objetivo de armonización del Reglamento, este deja margen de regulación a los Estados miembros de manera que existe un serio riesgo de no sólo no corregir sino de agravar la fragmentación existente en los Estados miembros. Los considerandos del Reglamento parecen asimismo querer proteger la investigación científica; sin embargo, esta intención no se compadece con el articulado. Para ello, se requerirá de las autoridades de control (individualmente o a través del mecanismo de consistencia) y de la Comisión que realicen interpretaciones con sentido común y coherencia con ese objetivo fundamental, para no restringir innecesariamente la investigación en el ámbito de la salud. El Reglamento incita a los Estados miembros a revisar las normas nacionales que regulan la investigación científica y otros intereses públicos relacionados con la salud, donde el sector público y privado están llamados a colaborar". Esta autora señala que "el desarrollo real de la investigación científica en España y en la Unión requerirá una interpretación conjunta coherente de la deficiente codificación al respecto por las autoridades de control y la Comisión, así como un uso responsable e inteligente por los Estados miembros de su capacidad de legislar al respecto", ÁLVAREZ RIGAUDAS, "Tratamiento de datos de salud…", *op. cit.,* p. 172.

[377] TRONCOSO REIGADA, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión…", *op. cit.*, pp. 197-198, afirma que: "Finalmente le corresponderá a los Tribunales conocer y resolver las eventuales controversias por la interpretación que del RGPD hagan las autoridades de control. El ordenamiento jurídico europeo, como no podía ser de otra manera, respeta la autonomía institucional de los Estados miembros en lo relativo a la aplicación judicial del RGPD y la independencia de los Tribunales. Por ello, éste no establece mecanismos de coordinación entre jueces. Los jueces de los Estados miembros son jueces naturales de la Unión Europea pero aplicarán el RGPD desde la perspectiva de su derecho interno. No obstante, existen distintos instrumentos que no nos corresponde analizar ahora para conseguir la convergencia dentro del Derecho de la Unión Europea en este ámbito. Así, la Comisión Europea tiene la facultad de plantear un recurso ante el TJUE si un Estado excede de sus competencias. Finalmente, el TJUE, a través de su jurisprudencia, servirá para asegurar una interpretación coherente del RGPD".

[378] En aplicación al principio de licitud y lealtad el RGPD concede flexibilidad a los Estados miembros para abordar esta materia por medio de ley específica, de conformidad en el art. 6.2 RGDP, donde establece que "Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo X".

[379] SERRANO PÉREZ, "La necesidad…", *op. cit*., p.2.

ciudadanos en calidad de titulares de los datos y, por consiguiente, del derecho del protección de datos.

En última instancia, la LOPDGG bajo el intento de evitar cometer el error del RGPD de entremezclar a lo largo de su articulado la regulación de la protección de datos personales con la regulación del tratamiento de los datos de salud, reduce la regulación de los datos de salud y de la investigación en una Disposición final decimoséptima y una Disposición final novena, que modifica la Ley 41/2002 sobre el acceso a la historia clínica con fines no asistencias, siendo estas insuficientes y poco aclaratorias, además de resultar en cierto modo llamativo el lugar que le otorga el legislador en la ley – disposiciones finales – a materias de gran relevancia como lo es lo de los datos de salud y el de la investigación, lo que denota un cierto desinterés legislativo, dando a entender una intención clara de salirse por la tangente a efectos de dar cumplimiento como fuere a lo establecido por el legislador europeo, sin finalmente aclarar nada al respecto acerca del tratamiento de los datos de salud, más bien, todo lo contrario.

En definitiva, el actual marco legislativo incentiva la incertidumbre jurídica generando así inseguridad jurídica, no únicamente a los ciudadanos, sino también, a los responsables del tratamiento, a los profesionales del sector de la sanidad, investigadores y, a los profesionales de protección de datos de la AEPD e incluso a los propios juristas incluyéndose a los Juzgadores cuya labor interpretativa será cada vez más relevante, pues, como se ha señalado, diversas son las cuestiones de notoria relevancia que la normativa vigente de protección de datos le delega tanto a ellos como a las autoridades de control, lo que generará que ante la duda y las diversas interpretaciones posibles muchos de los casos terminen siendo litigados en los tribunales, lo que también afecta, sin duda, al principio de economía procesal.

Así pues, nos encontramos ante deficiencias que incrementan la imposibilidad de aplicación lícita de tecnologías de *big data*, puesto que la normativa vigente de protección de datos se basa fundamentalmente en un modelo proactivo, dejando cierta flexibilidad al responsable del tratamiento sobre el tratamiento de los datos personales, incluyéndose los datos de salud, sin entrar a legislar sobre cuestiones de gran relevancia, lo que conlleva ante la incertidumbre a una interpretación restrictiva y limitativa por

parte del propio responsable del fichero – pues debe actuar con absoluta diligencia y precaución – como por la autoridad de control, así como de los propios tribunales. Así pues, la consecuencia de lo anterior es, nuevamente un marco legislativo que pone límites al tratamiento de los datos de salud, cuando en un principio el objetivo de ambas normas – la comunitaria y la estatal – es la legalización de la libre circulación de los datos para fines de salud pública e investigación biomédica, a efectos de que los terceros especialistas en análisis de *big data*, puedan acceder a los datos de salud y sustraer la información y conocimiento que resultarán de interés general, pues ampliará en ambos sentidos, el de la salud pública a través de la medicina predictiva facilitando una asistencia sanitaria más precisa y completa tanto al paciente como a la sociedad en su conjunto y, el de la investigación científica.

No cabe duda, como se ha podido apreciar en este trabajo que las tecnologías resultan hoy día fundamentales para el desarrollo humano, teniéndose especialmente en consideración la contribución y retos que presenta su integración en los sistemas de salud[380], donde la calidad y la viabilidad económica de una asistencia sanitaria depende fundamentalmente de una efectiva y eficiente incorporación de las nuevas tecnologías, lo que conllevará a una mejora de la calidad de vida de la sociedad, así como favorecer el desarrollo de herramientas como las del *big data* en el campo de la investigación, gestión, planificación, información, prevención, promoción en el diagnóstico o en el tratamiento.

Por ende, la implantación de estas tecnológicas es de gran utilidad a los efectos de dar soluciones prácticas reales de los pacientes en particular y, demandados por la sociedad en su conjunto, suponiendo en todo caso una mejora perceptible en la calidad y acceso a los servicios de salud del futuro[381]. De igual modo, la posibilidad de ampliar el conocimiento y la información por medio de tecnológicas de *big data* en el ámbito de

[380] A tales efectos *Vid.* la *Guía de la Cooperación Española para la incorporación de las TIC en las intervenciones de Salud en la Cooperación para el Desarrollo,* AECID y Ministerio de asuntos exteriores y de cooperación, enero, 2012.

[381] Al respecto, consúltese BARRERA, L., GONZÁLEZ F., VALENZUELA, J. y CEDEÑO, M.: *Impacto de las TICS en la Salud* [Documento sin paginación]. Disponible en: http://www.neopuertomontt.com/InformaticaMedica/lasticsenelsectorsalud.pdf (última consulta 10/01/20) e informe del MINISTERIO DE SANIDAD Y POLÍTICA SOCIAL, "Las TIC en el Sistema Nacional de Salud. El programa Sanidad en línea. actualización de datos enero 2010". Disponible en: https://www.mscbs.gob.es/profesionales/hcdsns/TICS/TICS_SNS_ACTUALIZACION_ES_2010.pdf (Última consulta 10/01/20).

salud pública y de la investigación biomédica debe ser objetivo fundamental de toda sociedad, como nos advierte BERNARDO VALDIVIESO – Director del área de planificación del Hospital *La Fe* de Valencia – al señalar que:

"[…] si queremos hacer sostenible el sistema estamos abogados a la medicina de la precisión […] El sector sanitario necesita nuevas herramientas que son las del *big data* o de inteligencia de negocio y necesita nuevas capacidades funcionales. Tenemos buenos médicos y buenos"[382].

Igualmente sobre esta cuestión SAÉZ AYERRA – Presidente de la Sociedad Española de Informática de la Salud - considera que "hay que hacer cambios tecnológicos para abordar proyectos *big data*[383]", como indica CARLOS MOCHO, - Director europeo de hmR – "la aportación de la información y del *big data* al sector salud y sanitario puede ser inmensa, no solo para la industria farmacéutica y desde la perspectiva de mercado farmacéutico, sino desde todos los puntos de vista y para todos los agentes"[384], por otro lado FEDERICO PLAZA – Director de *Government Affairs en Roche Pharmaceuticals* – afirma que "el *big data* es una fuente brutal desde el punto de vista epidemiológico. Cuando se desarrolla una nueva indicación los datos epidemiológicos son realmente útiles, sobre todo, cuando se avanza en necesidades que no están cubiertas todavía o enfermedades que aún no tienen tratamiento"[385] entre muchos otros a destacar.

[382] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, pp. 8 y 12. Documento disponible en: https://es.slideshare.net/AndresMacario2015/informe-big-data-y-salud?from_action=save (último acceso 22/01/20).

[383] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, p.40.

[384] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, p.66.

[385] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, p.57.

III. EL TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD, DATOS GENÉTICOS Y DATOS BIOMÉTRICOS EN LA NORMATIVA VIGENTE DE PROTECCIÓN DE DATOS PERSONALES

Al hilo de lo anterior, a lo largo del presente apartado, así como en el capítulo siguiente se estudiará con detenimiento el contenido de la normativa vigente de protección de datos centrándonos únicamente en lo referente a los datos relativos a la salud, destacándose a su vez aquellas limitaciones de la normativa y las cuestiones que se estima que deben ser reguladas por la ley especial de protección de datos de salud y de aplicación de herramientas *big data,* teniéndose en consideración los criterios asentados por la propia Sociedad Española de Salud Pública y Administración Sanitaria[386], y por algunos autores que como SERRANO PÉREZ, MARTÍNEZ MARTÍNEZ, DÍAZ GARCÍA, VALERO TORRIJOS, CERDÁ MESEGUER han destacado, a buen criterio, aquellas cuestiones de gran relevancia jurídica que se han de regular de manera específica y concreta por una ley sectorial de protección de datos de salud a fin de "que compendie y armonice la materia, ofreciendo una regulación conjunta y clarificadora"[387].

Así pues, escenarios estos que serán desarrollados a continuación – ampliándose otros que se estiman convenientes a nuestro criterio – de manera entremezclada con el contenido vigente de la normativa de protección de datos personales, a los efectos de facilitar a través de este trabajo desde la práctica jurídica la labor al legislador español cuando llegado su día – que sin duda llegará – se vea en la dicotomía de regular de manera independiente la protección de los datos de salud y las técnicas de *big data sanitario* por medio de una ley sectorial a los efectos de dar una respuesta a las exigencias respecto al tratamiento de datos de salud, así como de permitir desde un punto de vista legal la aplicación de tecnologías de *big data*, que cada vez más se encuentran más latentes en el contexto social, especialmente, en el ámbito sanitario.

---

[386] *Vid.* Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 11 y ss.

[387] SERRANO PÉREZ, "La necesidad…", *op. cit*., p. 5.

1. MEDIDA GENERAL SOBRE EL TRATAMIENTO DE LOS DATOS DE SALUD: LA PRIMACÍA DE CONSENTIMIENTO DEL PACIENTE

Como punto de partida, se ha de tener en consideración que de manera general la normativa vigente de protección de datos continúa otorgándole una gran relevancia jurídica al consentimiento del paciente[388], a pesar de que con la vigente normativa de protección de datos en algunos supuestos se permite un tratamiento flexible de los datos relativos a la salud sin necesidad de mediar consentimiento del paciente[389], como más adelante se detallará.

En concreto, de conformidad con el artículo 9 del RGPD, no se pueden tratar los datos personales relativos a la salud, los genéticos y biomédicos, salvo que medie el consentimiento explícito del titular para uno o varios fines específicos[390]. Así pues, en relación con el consentimiento informado, como novedad a destacar del nuevo RGPD es la voluntad "inequívoca" del consentimiento informado, donde a tenor del artículo 4.11 del RGPD se define 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 informativa, el tratamiento de datos personales que le conciernen"[391].

---

[388] ANDREU MARTÍNEZ, M.ª B. y PLANA ARNALDOS, M.ª C., "El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica",* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 144-145.

[389] En este sentido, recordemos que en la normativa jurídica anterior el consentimiento era elemento fundamental del contenido del derecho de protección de datos y, en consecuencia, el derecho del titular de los datos a ser informado fue considerado en su día por el TC en la STC 292/2000 (f.j. 13º) como parte que forma parte del derecho de protección de datos, como nos advierte FERNÁNDEZ SALMERÓN, *La protección de los datos personale*s…, *op. cit.*, p. 93, al afirmar que "Evidentemente, si el consentimiento sobre todos esos extremos es elemento nuclear del contenido del derecho de protección de datos, resulta obvio que el mismo ha de ser un consentimiento «informado». De otro modo, para que el consentimiento sea libre y consciente y abarque todas las operaciones a que hemos aludido, requiere una información previa. Pues bien, el derecho a ser informado ha sido considerado también por el TC como parte integrante del derecho a la protección de datos".

[390] De igual modo, el Considerando 32 del RGPD destaca que: "El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

[391] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 891, señala que: "Debe prestarse 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 (como por ejemplo marcando una casilla en un sitio web), una declaración verbal o escrita o cualquier conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales".

Por consiguiente, la voluntad inequívoca[392] del consentimiento informado por parte del interesado conlleva que el mismo sea posible de demostrar por parte del responsable del tratamiento, lo que exige que sea expreso y recogido por escrito. Además, otra cuestión relevante a tener en consideración es que, en caso de desequilibrio entre el titular de los datos personales y el responsable del tratamiento, el consentimiento dado de manera libre no conlleva que sea un fundamento jurídico válido para el tratamiento de los datos, puesto que es fundamental que los datos se adecuen a la finalidad para los que son solicitados, en caso contrario, su tratamiento será ilícito[393].

De manera particular, sobre el consentimiento informado en caso de menores de edad, debido a que estos pueden tener igualmente que los adultos acceso a las nuevas tecnologías e Internet, el legislador europeo estima apropiado regular tal extremo de manera detallada en el RGPD, siendo en todo caso respetada la autonomía y libertad del menor a pesar de encontrarnos ante afectados que exigen una mayor protección. Así pues, dentro del nuevo RGPD se establecen medidas y reglas específicas recogidas en el artículo 8 del RGPD, donde se establecen varias exigencias que se deben cumplir cuando nos encontremos ante el consentimiento otorgado por un menor, en concreto: (1) es lícito el consentimiento otorgado por una persona menor de edad, siempre y cuando tenga un mínimo de 16 años[394]; (2) la información sobre el tratamiento de los datos y sobre el consentimiento debe ser transmitida de manera clara e inteligible, por lo que se entiende que debe ser adaptada a la comprensión media exigible a una persona de 16 años; (3) exclusivamente el tratamiento de los datos personales del menor podrán serán utilizados para la finalidad por lo que fue otorgado[395]. El legislador europeo establece igualmente una aclaración en relación de que las disposiciones generales de Derecho

[392] ANDREU MARTÍNEZ y PLANA ARNALDOS, "El poder de disposición del titular como facultad principal del…", *op. cit.*, pp. 133-134, aclaran que: "El consentimiento es una declaración de voluntad procedente del sujeto titula de los datos personales por la que éste acepta que los mismos se sometan a tratamiento […] Por otra parte, la declaración de voluntad del interesado sólo puede considerarse correcta cuando se forma de manera consciente, racional y libre. En consecuencia, sólo será válida y producirá plenos efectos, la voluntad consciente y libremente declarada. En caso contrario, habrá que considerar viciado el consentimiento".

[393] *Vid.* al respecto el artículo 7 y, considerandos 42 y 43 del RGPD.

[394] En el caso de que el menor de edad tenga menos 16 años, el consentimiento sobre el tratamiento de sus datos personales será lícito cuando sea otorgado o autorizado por quien ejerza la patria potestad o tutela sobre el menor.

[395]El RGPD establece una margen de flexibilidad para los legisladores de los Estados miembro, permitiendo que se pueda fijar una edad inferior a los 16 años para otorgar el consentimiento, siempre y cuando no sea inferior a los 13 años.

contractual de los Estados miembros sobre las normas de validez, formación o efectos de los contrarios con menores de edad no quedan afectadas por lo estatuido por el RGPD, en concreto, en los artículos 8, 6.1. f), 12.1, 40.2 g) y 57.1.b), que son los que hacen referencia al tratamiento especial de datos sobre menores, entre otras, a la licitud del tratamiento, la obligación de transmitir la información relativa al tratamiento de forma clara, concisa, transparente e inteligible a través de leguaje claro y sencillo.

En el marco normativo europeo, el RGPD aporta una definición detallada del "consentimiento del interesado", en concreto en el art. 4.11 del mismo establece que:

"[…] el consentimiento del interesado es 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".

Por ende, en virtud de la definición apartada por el Reglamento, cabe destacar que, a efectos de que se considera que existe consentimiento por parte del interesado, es necesario que se den los siguientes requisitos: (1) aceptación por parte del interesado del tratamiento de datos personales que le conciernen; (2) a través de una manifestación de voluntad libre, específica, informada e inequívoca y; (3) sujeta en un acto declarativo o en una acción afirmativa clara.

De lo anterior, se desprende que, son requisitos fundamentales para la eficacia y validez del acto declarativo o la acción afirmativa en la que se sustente la aceptación del interesado del tratamiento de sus datos personales, los detallados a continuación:

1º.- Información detallada: previamente a la aceptación el interesado, es necesario e imprescindible que el interesado sea informado de manera específica acerca de la finalidad y destino del tratamiento de sus datos personales.

2º.- Acto voluntario y libre: el acto declarativo o la acción afirmativa clara ha de ser otorgada de manera voluntaria y libre por parte del interesado, sin estar sometido a ningún tipo de indicio que pueda derivar a error o vicio en el consentimiento, de tal modo, que el interesado de manera voluntaria y libre sin estar sometido a ningún tipo de

presión consienta que sus datos personales puedan ser tratados por terceros, ya sea una entidad pública o privada.

3º.- Manifestación inequívoca: la manifestación ha de ser clara, concisa e inequívoca, es decir, que no invoque a duda o equivocación alguna.

El acto afirmativo puede ser emitido por escrito – incluyendo medios electrónicos – o de forma verbal. Dicho acto afirmativo abarca distintas modalidades de emisión y otorgamiento: 1.- Marcar una casilla de un sitio web en internet; 2.- Escoger parámetros técnicos para la utilización de servicios de la sociedad de la información; 3.- En caso de solicitud por medios electrónicos, la misma ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que es prestado; 4.- Cualquier otra declaración o conducta que de manera explícita y clara indique la aceptación por parte del interesado del tratamiento de sus datos. De tal modo que, no constituyen consentimiento ni las casillas ya marcadas, ni el silencio o la inacción.

Asimismo, para cada una de las actividades del tratamiento será necesaria la emisión del consentimiento. La definición otorgada por el Reglamento acerca del "consentimiento del interesado", engloba dos conceptos sumamente relevantes, por un lado, el de "datos personales", y por otro lado la noción de "tratamiento", siendo definidos ambos igualmente por el legislador en el citado artículo 4 del Reglamento y que han sido analizados anteriormente en el presente trabajo.

De igual forma, el art. 6 de la LOPDGDD reproduce la definición de consentimiento de la afectado como consta recogido en el 4.11 del RGPD, añadiendo en su apartado segundo que ante la situación en la que nos encontremos ante una pluralidad de finalidades el titular debe consentir de manera específica e inequívoca cada una de ellas. Igualmente, el citado precepto en materia contractual señala que no podrá ejecutarse un contrato en aquellas finalidades en el que el afectado haya consentimiento el tratamiento y "no guarden relación con el mantenimiento, desarrollo o control de la relación contractual"[396].

[396] Igualmente, *Vid.* el art. 16.3 de la Ley 41/2002 referida a los usos de la historia clínica distintos de las finalidades asistenciales, siempre que no exista anonimización de los datos.

En caso de incumplimiento del tratamiento de los datos de las categorías del art. 9 del RGPD sin el consentimiento del interesado, nos encontraríamos ante una infracción muy grave de conformidad con el RGPD y la LOPDGDD[397].

Por ende, en lo que respecta al tratamiento de datos de salud, como se ha puesto de manifiesto, la regla general que establece la normativa vigente es la necesidad del consentimiento del paciente, no en vano, como se verá a continuación, la normativa establece algunas excepciones a la regla general en la que se permite el tratamiento de los datos relativos a la salud sin el consentimiento del paciente para otros fines distintos al asistencial y sin vinculación alguna al fin inicial.

2. EXCEPCIONES AL RÉGIMEN GENERAL DEL CONSENTIMIENTO: TRATAMIENTO LÍCITO DE LOS DATOS DE SALUD SIN EL CONSENTIMIENTO DEL PACIENTE DESTINADO A OTROS FINES DISTINTOS AL ASISTENCIAL

De manera general, tal y como ha sido analizado en el apartado anterior el RGPD y la LOPDGDD determinan que los datos genéticos, los datos biométricos dirigidos a identificar de manera unívoca a una persona y los datos relativos a la salud, entre otros, son datos de categoría especial debido a que contienen información vulnerable por pertenecer a la espera privada, personal e íntima de una persona, por lo que como norma general queda prohibido su tratamiento sin el consentimiento del interesado de conformidad con el apartado primero del artículo 9 del RGPD[398] y en el artículo 6 de la LOPDGDD[399]. Sin embargo, como se estudiará más adelante, la vigente

[397] *Vid.* Art. 72.1.e) LOPDGDD.

[398] El artículo 9 del RGPD regula las categorías especiales de datos ya existentes (origen étnico o racial, opiniones políticas o, la afiliación sindical, datos relativos a la salud, la vida sexual y sobre la orientación sexual), los datos de carácter genéticos y los biométricos, quedando prohibido de manera general su tratamiento salvo las excepciones que serán analizadas en el presente apartado.

[399] Como señala la Exposición de Motivos de la LOPDGDD, "también en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes" –Apartado V-. Así pues, La Exposición de Motivos de la LOPDGDD lleva a cabo "una interpretación extensiva" de las habilitaciones normativas, "como sucede, en particular, en cuanto al alcance del consentimiento del afectado" –Apartado V-.

normativa de protección de datos permite de manera flexible un tratamiento lícito de los datos de salud sin necesidad del consentimiento del paciente para otras finalidades distintas de la asistencial, como puede ser de interés público, salud pública o investigación biomédica y farmacéutica [400], así consta recogido en el apartado segundo del artículo 9 del RGPD, remitiéndose a tales excepciones que afectan en particular a los datos de salud o los genéticos y biomédicos el artículo 9 de la LOPDGDD[401].

[400] TRONCOSO REIGADA, "Investigación, salud pública y asistencia sanitaria…", *op. cit.,* p. 242 señala que: "El RGPD considera legítimos los tratamientos de categorías especiales de datos personales por razones de interés público en el ámbito de la salud pública. Así, si la previsión contenida en el art. 9.2.h) está destinada a garantizar la asistencia sanitaria como bien individual, la previsión del art. 9.2.i) está destinada a garantizar la salud pública como bien colectivo. El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado en el ámbito de la salud pública se hace, como señala el art. 9.2.i) del RGPD, por "razones de interés público". Por ello, como señala el Considerando 54 del RGPD, "este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines", es decir, no puede servir como una habilitación para entidades privadas. Así, a diferencia de las previsiones contenidas en el art. 9.2.h) y 9.2.j) del RGPD, que habilitan el tratamiento de categorías especiales de datos personales sin consentimiento del interesado en la asistencia sanitaria privada y en la investigación biomédica privada, y a diferencia de la previsión contenida en el art. 9.2.g) del RGPD, que permite los tratamientos de categorías especiales de datos personales por razones de interés público esencial que llevan a cabo entidades privadas, como las compañías aseguradoras, la previsión del art. 9.2.i) del RGPD va destinada a autoridades públicas o entidades privadas que cumplen competencias administrativas en el ámbito de la salud pública". Añadiendo el autor TRONCOSO REIGADA, "Investigación, salud pública y asistencia sanitaria…", *op. cit.,* p. 244, que: "Esto significa, llevando a cabo una interpretación sistemática, que el RGPD, por una parte, ha separado el tratamientos de categorías especiales de datos para la finalidad de investigación sanitaria de otros tratamientos para otras finalidades sanitarias como la prevención, la asistencia sanitaria y la gestión de servicios sanitarios –que se encuentran recogidas en el art. 9.2.h)– y la actividad de salud pública –que se encuentra prevista en el art. 9.2.i)-, y, por otra parte, que el RGPD ha regulado la legitimación del tratamiento de categorías especiales de datos personales para la investigación sanitaria con otros tratamientos para finalidades no sanitarias como el archivo en interés público, la investigación científica o histórica o la actividad estadística, lo que supone una cierta equiparación". Asimismo, MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación biomédica*…", op. cit.*, pp. 281-282; CRISTEA UIVARU, L., *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud,* Bosch Editor, Barcelona, 2018, pp. 101-102.

[401] En este sentido, PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 892, aclara que: "Así, con ocasión de la ejecución de un contrato en el que titular del dato es parte (por ejemplo, contratos de seguro, o la relación contractual entre el paciente y el profesional sanitario o entidad en la que este presta servicios); cuando sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; que el tratamiento se requiera para proteger intereses vitales del interesado o de otra persona física, caso habitual en la asistencia sanitaria; que se precise para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, lo cual puede suceder, por ejemplo, en los caos de externalización de determinados servicios públicos relacionados con la salud. Es legítimo el tratamiento sin necesidad de consentimiento, también cuando sea necesario para el cumplimiento de obligaciones de carácter laboral establecidas legalmente, o para finalidades de medicina preventiva o laboral, evaluación de su capacidad laboral diagnóstico médico, prestación de asistencia o tratamiento o la gestión de los sistemas y servicios e asistencia sanitaria o social…".

En consecuencia, se estima pertinente analizar a continuación de manera previa desde un punto de vista jurídico las expresiones "interés público", "salud pública" e "investigación científica" a fin de alcanzar una mayor comprensión e interpretación eficiente de la normativa vigente.

2.1. Aspectos conceptuales

A) Sobre la expresión "interés público" en la esfera sanitaria

Debido a la importancia que la normativa vigente de protección de datos le otorga al interés público cabe cuestionarnos por el significado de la citada expresión, en concreto, cabe destacar desde un principio lo establecido por el RGPD en su considerando 54 acerca del interés público y la salud pública donde señala que "ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas" haciendo a su vez referencia a la salud publica en los términos del Reglamento CE n.º 1338/2008:

"[…] el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria y las causas de mortalidad".

Sin embargo, lo cierto es que, el RGPD no concreta una definición acerca del interés público delegando su interpretación a las autoridades de control y los tribunales de los Estados miembros, limitándose a citar como único ejemplo de interés público el de "la protección frente a amenazas transfronterizas graves para la salud" en el art. 9.2. i) RGPD. De igual modo, por su parte, la AEPD ha añadido otros ejemplos de interés público junto con la citada protección de amenazas transfronterizas graves para la salud, entre los que se encuentran garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios o la inspección de

reclamaciones de los ciudadanos.[402] Por otro lado, el *Informe Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD suscrito por la Sociedad Española de Salud Pública y Administración Sanitaria en 2017* (en adelante, *Informe SESPAS*), añade como ejemplo de interés público: las enfermedades transmisibles; control de epidemias y de su propagación; amenazas transfronterizas graves; situaciones de urgencia humanitaria por catástrofes naturales o de origen humano[403].

En definitiva, se ha de entender que existe interés público en la esfera de salud pública en aquellas actuaciones y estudios epidemiológicos y de salud pública cuya finalidad directa sea prevenir de un riesgo grave para la salud de la población. En consecuencia, a efectos de ser detectado con prontitud el citado riesgo grave, así como a fin de efectuar una evaluación del peligro, se debe exigir y facilitar un acceso multidisciplinar a la información sanitaria, pues la información que proporciona la salud pública resulta esencial para la rápida detección del peligro, debiéndose acceder a la misma, en todo caso, aplicándose criterios de estricta necesidad, idoneidad y proporcionalidad de conformidad con lo establecido en los arts. 7 y 6 de la LAB [404].

Por último, la normativa otorga cierta prioridad a la investigación epidemiológica[405] ante el consentimiento del paciente siendo de interés público al constar acreditado que a través de los estudios epidemiológicos se prevén riesgos para la salud, por lo que resulta fundamental que los investigadores puedan acceder con

[402] Agencia Española de Protección de Datos, *Guía para pacientes y usuarios de la Sanidad*, 2019, p.6

[403] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 9.

[404] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, pp. 9-10 y p.12.

[405] A grandes rasgos, los autores Bermejo Fraile[405] y García García, entre otros, distinguen entre dos tipos de epidemiologia: por un lado, la epidemiologia de salud pública que es la que se dedica al estudio de la frecuencia y distribución de la enfermedad, sus causas y factores de riesgos y, por otro lado, la epidemiologia clínica que es la que se investiga por medio de personas con una enfermedad concreta o condición clínica particular por medio de la aplicación de principios y métodos epidemiológicos a los problemas encontrados en la medicina. *Vid.* BERMEJO FRIALE, B., *Epidemiología clínica aplicada a la toma de decisiones en medicina,* Gobierno de Navarra, 2001; GARCÍA GARCÍA, J. J., "Epidemiología clínica. Qué y para qué", *Revista Mexicana de Pediatría,* vol. 66, núm. 4, 1999, pp. 169-173, citado igualmente en Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 14.

facilidad y sin limitaciones a los informes y datos de salud que "resulten imprescindibles para la toma de decisiones en salud pública" de conformidad con lo establecido en el artículo 41.3 de la LGCP[406].

No en vano, en el caso de la epidemiología social los investigadores necesitan disponer de los datos sanitarios de los pacientes, así como el acceso a la historia clínica sin que previamente exista un riesgo o peligro para la salud pública, por lo que en principio este supuesto de hecho no entraría dentro de los casos de tratamiento lícito sin consentimiento del paciente, puesto que como se ha puesto de manifiesto anteriormente, la expresión "interés público" conlleva implícita la exigencia de riesgo para la salud pública. Por lo que el acceso a la historia clínica del paciente de manera directa y sin aplicación previa de técnica de anonimización resulta de vital importancia debido al hecho de que los científicos epidemiológicos ante estudios de epidemiologia social van a necesitar conocer y disponer de la identificación del paciente para una eficiente investigación a lo que respecta a determinados estudios epistemológicos, como: "a) vigilancia de las enfermedades de declaración obligatoria, b) vigilancia de enfermedades a través de sistemas de información microbiológica; c) estudio y control de brotes; d) investigación de reacciones adversas a la vacunación y mejora del

[406] Asimismo, como indica MARTÍNEZ MARTÍNEZ, R., "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley,* núm. 38, Sección Ciberderecho, marzo 2020, [Documento sin paginación]. Documento disponible en: https://diariolaley.laleynext.es/dll/2020/03/27/los-tratamientos-de-datos-personales-en-la-crisis-del-covid-19-un-enfoque-desde-la-salud-publica (último acceso 22/05/20), que: "desde el punto de vista de la legislación nacional el fundamento para el tratamiento de datos personales sin consentimiento podría derivar de lo dispuesto en: El artículo 26 de la Ley 14/1986, de 25 de abril, General de Sanidad, por el que se atribuye competencias a los servicios sanitarios ante la existencia de un riesgo inminente y extraordinario para la salud, en los siguientes términos; La Ley Orgánica 3/1986, de 14 de abril de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) que habilita para el control de los enfermos; La Ley 33/2011, de 4 de octubre, General de Salud Pública, amén de garantizar el derecho fundamental a la protección de datos en su artículo 9, establece el deber de todas las personas de comunicar datos o circunstancias que pudieran constituir un riesgo o peligro grave para la salud. La colaboración con los servicios competentes resulta esencial para el logro de los objetivos que del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica. Por otra parte, si COVID 19 es una variante de SARS (en español: Síndrome Respiratorio Agudo Grave), figura entre las enfermedades de declaración obligatoria del anexo I del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica; El párrafo segundo apartado c) de la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales habilita al uso de datos con fines de investigación en salud pública sin consentimiento en circunstancias como una epidemia".

programa de vacunaciones; e) mejora de programas de cribado poblacional; e) registro de tumores; f) mejora de registro de mortalidad[407].

Al respecto y, a los efectos de proporcionar mayor flexibilidad a los responsables y encargados del tratamiento de los datos de salud cuando no obre previo consentimiento del paciente ante las anteriores causas de investigación epistemológica social en los que no existe riesgo para la salud pública, en interpretación del art. 9.2 RGPD, la normativa jurídica configura dos posibilidades por las que se puede aludir que se permite realizar una investigación epistemológica sin previo consentimiento del paciente ante fines de medicina preventiva (art. 9.2.h) RGPD)[408] y fines de investigación científica (art. 9.2.j) RGPD)[409].

Dado que el RGPD no establece una definición de "interés público", desde un principio resulta de notoria importancia que la ley de protección de datos de salud fije el alcance de la expresión de interés público en el ámbito de la salud a efectos de excepcionar el consentimiento del interesado, teniendo en consideración dos puntos principales:

Por un lado, la definición dada por el Reglamento (CE) n.º 1338/2008 del Parlamento y del Consejo en el art. 3 letra c), sobre la expresión "salud pública", al entender por la misma "todos los elementos relacionados con la salud, a saber, el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos

[407] Orden de 26 de octubre de 2011, de Galicia, que específica los criterios técnicos y/o científicos para el acceso a la historia clínica a efectos epidemiológicos y de salud pública (DOG de 16- 11-2011). Igualmente se cita en Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 15.

[408] Opina DE MIGUEL SÁNCHEZ, N., "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *Revista Española de Protección de Datos,* núm. 3, 2006, p. 190, que los fines de prevención médica incluyen los estudios epidemiológicos. Y, en efecto, la prevención médica exige disponer de estudios epidemiológicos en los que apoyar los programas preventivos. El artículo 19.1 de la LGCP establece la prevención tiene por objeto reducir la incidencia y la prevalencia de ciertas enfermedades, lesiones y discapacidades en la población y atenuar o eliminar en la medida de lo posible sus consecuencias negativas mediante políticas acordes con los objetivos de esa ley. Igualmente, citado por Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 15.

[409] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 15.

asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad"[410].

Por otro lado, la finalidad de prevenir un riesgo grave para la salud como criterio limitador del interés público, donde entrarían exclusivamente aquellas situaciones de actuación y estudios epidemiológicos y de salud pública que supongan una amenaza sanitaria para la salud de la población, entre los que destacar, las enfermedades transmisibles; control de epidemias y de su propagación; amenazas transfronterizas graves; situaciones de urgencia humanitaria por catástrofes naturales o de origen humano; para garantizar elevador niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios o la inspección de reclamaciones de ciudadanos[411], quedando al margen la epidemiologia social cuya finalidad es la de mejorar la salud de la población sin existir previamente un riesgo o peligro grave para la salud de la población, característica esta que hace que sea incluida en la investigación científica y, no en la salud pública.

Por último, para los supuestos de estudios de epidemiologia donde se manejen datos masivos y datos identificados, es aconsejable que la ley sectorial regule la obligación del responsable del tratamiento de solicitar autorización previa a la autoridad de control y de los Comités de Ética de la Investigación, a los efectos de poder tratar los mismos, excepto en los casos que sean necesarios los datos para prevenir un riesgo o peligro grave para la salud de la población.

B) Sobre la percepción de la expresión "investigación científica"

Del análisis anterior acerca de la expresión "interés público" en el ámbito sanitario, ello nos permite distinguirlo con la expresión "investigación científica", puesto que se podría afirmar de manera general que el interés público también engloba aquellas investigaciones que tengan como finalidad mejorar la salud y la calidad de vida

[410]El RGPD en el considerando 54 también hace referencia a la citada definición de salud pública del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo.

[411] Véanse ejemplos citados en el cuarto capítulo del presente trabajo.

de la población, como puede ser, por ejemplo, investigar las causas de una enfermedad determinada o, la relación entre un contexto socioeconómico y una enfermedad, entre otros[412].

La diferencia principal entre "interés público" e "investigación científica" establecida por el RGPD subyace en que para el primero se requiere como finalidad evitar, reducir o prevenir un peligro grave y amenazante para la salud pública y; para el caso de la investigación científica, sin embargo, a pesar de ser una actividad de interés general no se requiere esa connotación de riesgo grave e inminente para la salud de la ciudadanía.

Sin embargo, entendemos que a efectos de eximir de responsabilidad, disciplinaria o civil, al responsable y encargado del tratamiento de los datos sanitarios a efectos de poder excepcionar la solicitud del consentimiento del paciente, deberá de acreditar de manera fehaciente y expresa el interés público del proyecto institucional, que en ningún caso podrá ser a nivel personal[413], de investigación concreta por el que se solicitaa el tratamiento de los datos de salud del paciente[414], asimismo debiendo ser los mismos adecuados, pertinentes y limitados de conformidad con el principio de minimización[415].

---

[412] ÁLVAREZ RIGAUDAS, por una parte, ha defendido una interpretación "amplia" de la finalidad específica, esto es, que la investigación científica se trate "como un fin preciso en sí misma y no necesariamente limitada a una enfermedad, terapia o medicamento determinados". Por otra parte, ha abogado también por un "consentimiento amplio": "si la causa de legitimación del tratamiento de datos de salud para la investigación científica se basara en el consentimiento del/de la paciente, es esencial que para que la investigación científica pueda llevarse a cabo, el consentimiento pueda cubrir no sólo el objeto del ensayo clínico o estudio primigenio sino fines de investigación más amplios ya que la ciencia avanza con descubrimientos basados en líneas de investigación que no necesariamente se pueden anticipar". ÁLVAREZ RIGAUDIAS, C., "Tratamiento de datos de salud", en AA.VV., en *Reglamento General de Protección de Datos. Hacía un nuevo modelo europeo de privacidad* (Dir. J. L. Piñar Mañas), Editorial Reus, Madrid, 2016, pp. 180 y 183.

[413]El Informe 0073/2010 de la AEPD exige esta premisa cuando afirma que "se desconoce si el investigador va a desarrollar el estudio a título personal o, si por el contrario, se trata de un proyecto institucional a realizar en el marco de algún programa de investigación concreto incluido en el Plan Nacional de Investigación Científica, Desarrollo e Innovación. Lo anterior es importante, a efectos de valorar si nos encontramos en presencia de un auténtico estudio científico y en consecuencia amparado por el supuesto de cesión contemplado en el artículo 11. 2 e) y 21. 1 de la Ley 15/1999, cuando aluden al fin científico del tratamiento de los datos personales como supuesto que excluye el consentimiento previo a la cesión de los mismos, si el cedente y cesionario son administraciones públicas".

[414] *Vid.* al respecto el considerando 159 del RGPD.

[415] Art. 89.1 RGPD y art. 5.1. c) RGPD.

En concreto, el Considerando 159 del RGPD aclara que "el tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública", además, de manera específica el RGPD respalda la investigación que utilice información procedente de registros de población.

La previsión del art. 9.2.j) del RGPD habilita los tratamientos de categorías especiales de datos personales sin consentimiento realizados por Administraciones Públicas y por entidades privadas y, por consiguiente, cubre tanto la investigación pública como la investigación privada, pues como hemos señalado precedentemente, la investigación biomédica y la asistencia sanitaria son actividades que, a diferencia de la actividad de salud pública, desarrollan tanto entidades públicas como privadas. No obstante, no resulta suficiente con afirmar que se lleva a cabo una investigación privada para reputar como legítimos estos tratamientos. Como señala el Considerando 159 del RGPD "para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas"[416].

[416] En relación con la investigación científica, GIL GONZÁLEZ, E., "Directrices del Grupo de Trabajo del Artículo 29 sobre el consentimiento en el Reglamento General de Protección de datos", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva LO3/2018 y Reglamento (UE). Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, p. 709, aclara que: "Este término no se encuentra definido en el RGPD, a salvo de la referencia del Considerando 159 de que debe interpretarse en sentido amplio. En atención a ello, el GT29 establece que puede tratarse de cualquier proyecto de investigación implementado de acuerdo con estándares metodológicos y éticos relevantes en un sector de actividad concreto. El GT29 interpreta el Considerando 33 en el sentido de que, en principio, el consentimiento podrá legitimar el tratamiento de datos personales con fines de investigación científica cuando esta finalidad esté concretada. Sin embargo, debido a la dificultad de concertar estos fines desde el inicio se podrá permitir que la información sobre la finalidad tuviese un carácter genérico, aunque, en caso de que se traten categorías especiales de datos, esta valoración deberá ser más estricta. En los casos en los que la finalidad de la investigación científica no pueda ser determinada, es posible utilizar otros mecanismos para garantizar la validez del consentimiento, tales como solicitar dicho consentimiento para las diferentes fases de investigación según vaya avanzado esta. Además, deberán aplicarse garantías necesarias, de acuerdo con el art. 89, como la minimización de

Si bien es cierto, la LOPDGGD en su Exposición de Motivos aborda el uso de los datos sin consentimiento en el ámbito de la investigación biomédica, estableciendo que "a tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos"[417].

Por último, como requisito indispensable de la investigación científica con utilización de historias clínicas, el responsable o encargado del tratamiento de los datos de salud debe ceder los datos de salud anonimizados o seudonimizados, lo que conlleva que disponga de un sistema de disociación automática, en caso de no disponer de la misma, cabe la posibilidad de poder ceder los datos de salud a una persona – física o jurídica, privada o pública – especializada en disociación de datos siempre y cuando esta sea distinta y separada del equipo de investigación. En concreto, en el ámbito de la salud, cuando se hace referencia a la investigación científica, nos estamos refiriendo bien, de manera general, a la investigación biomédica o, bien de manera particular, a la investigación clínica, así como a la investigación farmacéutica.

Por ello, en este sentido, en la ley sectorial específica de protección de datos de salud y *big data* sanitario, se estima conveniente que en la propia ley se establezca una definición de investigación biomédica como finalidad del tratamiento de los datos de salud sin necesidad del consentimiento del paciente[418], tiendo en consideración dos aspectos relevantes: en primer lugar, que debe ser una investigación institucional y, por consiguiente, no a nivel personal y; en segundo lugar, a modo de acotación, se han de citar como mínimo los ejemplos de fines de investigación científica que señala el considerando 159 del RGPD "el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado […] Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública"

---

datos, la seguridad, la transparencia o la anonimización. Al igual que en el resto de los casos, debe existir la posibilidad de retirar el consentimiento, a pesar de que ello pudiera perjudicar la investigación".

[417] Apartado V Exposición de Motivos de la LOPDGDD.

[418] Art. 9.2.j) RGPD.

2.2. El tratamiento lícito de datos sanitarios para fines de salud pública e investigación biomédica de interés público

Por lo que se refiere al ámbito de la esfera sanitaria, a pesar de que en la normativa vigente de protección de datos queda prohibido con carácter general el tratamiento de datos personales genéticos, datos biométricos dirigidos a identificar de manera univoca a una persona física y, los datos relativos a la salud, sin embargo, no será necesario el consentimiento explícito del paciente para fines de investigación científica o fines estadísticos, cuando el tratamiento es necesario para fines de medicina preventiva o, cuando el tratamiento es necesario por razones de interés público en el ámbito de la salud pública[419].

Igualmente, cabe tener en consideración que tanto el médico como el centro sanitario, público o privado, están obligados a facilitar la siguiente información al paciente para el tratamiento de datos de salud, así como en aquellas situaciones en los que los datos se obtienen de un tercero, se ha de informar al titular de los datos a la mayor brevedad posible de su origen y de lo detallado a continuación[420]:

En primer lugar, la identidad y los datos de contacto del responsable y, en su caso, de su representante, que puede ser médico privado, profesional sanitario de la compañía de seguro médico suscrito, hospital público o privado, o Servicio de Salud de la Comunidad Autónoma.

En segundo lugar, los datos del delegado de protección de datos, en el caso de que sea obligatorio tener delegado.

---

[419] En relación con la salud pública, PARIENTE DE PRADA, I., "Los datos de Salud en el Nuevo Reglamento Europeo de Protección de Datos", *I + S: Revista de la Sociedad Española de Informática y Salud,* ejemplar 122, 2017, p. 14 opina que: "En el caso de la salud pública, habrá que tener en cuenta la definición de salud pública que se establece en el Reglamento (CE) 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

[420] Agencia Española de Protección de Datos, *Guía para pacientes y usuarios de la Sanidad*, 2019. Disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

En tercer lugar, los fines del tratamiento a que se destinan los datos personales - entre otros, prestar asistencia sanitaria, investigación y docencia - así como la base jurídica, esto es, consentimiento, contrato, ejercicio de una potestad pública y proteger intereses vitales de una persona.

En cuarto lugar, se ha de informar al paciente de los destinatarios y las categorías de destinatarios de los datos personales, así, por ejemplo, ante una consulta de un médico que actúe por medio de una aseguradora privada debe facilitar los datos de salud del paciente a esta a efectos de que abone la indemnización por daños y perjuicios correspondiente.

En quinto lugar, el responsable debe informar al titular de los datos su intención de transferir datos personales a un tercer país u organización internacional.

De igual modo, el responsable tiene el deber de informar que los datos de la historia clínica serán conservados el periodo de tiempo necesario a efectos de garantizar una adecuada asistencia sanitaria de los pacientes y, como mínimo, cinco años[421].

Por otro lado, el responsable informará al paciente de su derecho a solicitar el acceso a los datos personales, así como su derecho de rectificar, suprimir y limitar su tratamiento, oponerse al mismo y el derecho a la portabilidad de los datos, no obstante, en caso de que los datos sean de interés público relacionado con la salud o por el cumplimento de obligaciones legales, el responsable puede limitar legalmente esos derechos al titular. Igualmente, el paciente debe ser informado del derecho a presentar una reclamación por un tratamiento ilícito de sus datos ante la AEPD o, las autoridades de protección de datos catalana, vasca o andaluza. Asimismo, el responsable del tratamiento informará al titular de los datos si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar los mismos.

[421] Se ha de tener en consideración que alguna ley autonomía ha ampliado el plazo mínimo de 5 años.

Así pues, el paciente será informado de la existencia de decisiones automatizadas, esto es, aquellas decisiones tomadas mediante procesos informáticos sin intervención humana, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o le afecten significativamente de modo similar, en este caso, el paciente afectado tendrá derecho a obtener información relevante sobre la lógica aplicada, así como la intervención humana, a expresar su punto de vista y a impugnar las decisiones.

Finalmente, en aquellas situaciones en las que el responsable del tratamiento realice un tratamiento ulterior de datos personales para una finalidad distinta a la inicial, debe facilitar al interesado, previamente al tratamiento ulterior, información sobre ese otro fin y cualquier información aclaratoria al respecto.

La anterior información, de conformidad con el principio de información y del principio de transparencia, debe ser facilitada de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Por consiguiente y, en consecuencia, la LOPDGDD siguiendo las pautas marcadas por el RGPD, permite el tratamiento de datos en la investigación en salud bajo los siguientes criterios:

De un lado, las personas con catorce años cumplidos deben prestar consentimiento para procederse al tratamiento de sus datos de salud. Para el caso de menores de trece años, se permite el tratamiento de los datos de salud siempre y cuando sus padres o tutores presten su consentimiento para su uso con fines de investigación y, en particular, la biomédica, abarcándose áreas generales vinculadas a una especialidad médica o investigadora. Por otra parte, y para los supuestos de menores de edad entre catorce y dieciocho años, los padres o tutores que ostenten la patria potestad o tutela del menor, podrán acceder a la historia clínica de sus hijos, puesto que el Código Civil establece que la patria potestad se ejerce en beneficio de los hijos menores de edad, así como velar por ellos, alimentarlos y educarlos, además, se ha de tener en consideración que el acceso a la información sanitaria por parte de los padres o tutores es fundamental para velar por los menores. Sin embargo, este derecho de acceso a la historia clínica del hijo/tutelado menor es únicamente para las personas que ostentan la patria potestad o la tutela, no para otros familiares.

Asimismo, el legislador español considera lícita y compatible la reutilización de datos personales con fines de investigación biomédica, en aquellas situaciones en las que se ha obtenido previamente el consentimiento del paciente para una finalidad concreta, siempre y cuando sean utilizados para finalidades o áreas de investigación relacionadas con el estudio inicial. En consecuencia, se interpreta que no es necesario que el paciente nuevamente preste su consentimiento a efectos de que sus datos puedan ser utilizados para finalidades o investigaciones análogas o relacionadas con la finalidad o proyecto inicial por el que previamente prestó su consentimiento, por consiguiente, entendiéndose lícita y compatible la reutilización de los mismos.

La LOPDGDD establece – de conformidad con el art. 13 del RGPD – dos *requisitos extras* a fin de garantizar un tratamiento leal y trasparente en la reutilización de los datos personales:

En primer lugar, que los responsables faciliten por medio de publicación en la página web corporativa del centro donde se realice la investigación o estudio clínico y, en su caso, en la del promotor, notificando por medio electrónicos u otro formato al afectado la información detallada en un lenguaje claro y transparente[422].

[422] En concreto, el responsable o encargado del tratamiento debe facilitar la siguiente información: : (1) identidad y datos de contacto del responsable y, en su caso, de su representante; (2) datos de contacto del delegado de datos, en su caso; (3) fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; (4) intereses legítimos del responsable o de un tercero cuando el tratamiento se base para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño (lo anterior no es de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones);(5) en su caso, de la identificación de los destinatarios o las categorías de destinatarios de los datos personales; en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, la referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho del que se hayan prestado en caso de transferencias (arts. 46, 47 y 49.1. 2.º del RGPD); (6) el periodo de tiempo por el que se van a conservar sus datos o, los criterios utilizados a efectos de concretar un plazo; (7) el derecho que ostenta de poder solicitar al responsable del tratamiento: el acceso a sus datos personales; su rectificación o supresión; (8) limitación de su tratamiento; oposición al tratamiento y; (9) el derecho a la portabilidad de los datos; (10) derecho a retirar el consentimiento en cualquier momento cuando prestó el mismo para el tratamiento de sus datos personales para uno o varios fines específicos incluyéndose el consentimiento dado explícitamente para el tratamiento de categorías especiales de datos personales; (11) derecho a presentar una reclamación ante una autoridad de control; (12) si está obligado a facilitar los datos personales y, de las consecuencias en caso de negación, en caso de la comunicación de datos personales sea un requisito legal o contractual o, necesario para suscribir un contrato; (13) de las decisiones automatizadas incluyéndose la elaboración de perfiles, así como la información relevante sobre la lógica aplicada, la importancia y las consecuencias previstas del tratamiento para el interesado; (14) información sobre el fin concreto – y otra información adicional - al que se van a destinar los datos personales en caso de que los datos sean utilizados para una finalidad

En segundo lugar, se requerirá a efectos de una reutilización de los datos personales leal y compatible informe previo favorable del Comité de Ética de la Investigación concreta en la que se van a utilizar los mismos.

De igual modo, se considera lícito el uso de los datos personales seudonimizados siempre y cuando se cumpla con los requisitos legales para el uso de datos personales seudonimizados con fines de investigación biomédica y asistencia sanitaria analizados anteriormente en el presente trabajo. En este supuesto se ha de destacar que el legislador nuevamente requiere a la entidad responsable de la investigación informe previo del Comité de Ética de la Investigación previsto en la normativa sectorial y, en su defecto, informe previo del delegado de protección de datos y, en defecto de este, informe previo de un experto con los conocimientos previos especializados del Derecho.

En el caso de los datos personales con fines de investigación biomédica, se podrá denegar al interesado el derecho de acceso a sus datos personales (art. 15 RGPD), el derecho de rectificación de los datos (art. 16 RGPD), el derecho a la limitación del tratamiento (art. 18 RGPD) y el derecho de oposición (art. 21 RGPD), siempre y cuando se establezcan las medidas adecuadas a efectos de garantizar los derechos y las libertades del interesado (entre las que se incluyen la técnica de la seudonimización cuando sea posible) y, siempre que se aprecie probabilidad de que el ejercicio de los citados derechos puedan imposibilitar u obstaculizar de manera grave la consecución de los fines científicos o sea necesaria su denegación a efectos de alcanzar esos fines[423].

En concreto, el legislador español establece que se podrá excepcionar los citados derechos en las siguientes situaciones: cuando el interesado deba ejercer los mismos de manera directa ante los investigadores o centros de investigación biomédica que utilicen datos anonimizados o seudonimizados; cuando el ejercicio de esos derechos afecte a los resultados de la investigación y; cuando "la investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad

---

distinta a la inicial, la citada información deberá ser proporcionada con anterioridad al tratamiento ulterior de los datos personales.

[423] MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación biomédica*…", op. cit.*, p. 285.

pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de ley"[424].

Por su parte, la LOPDGDD regula las siguientes pautas a seguir para el tratamiento lícito con fines de investigación biomédica y asistencia sanitaria: (1) realización de una evaluación de impacto a efectos de determinar los riesgos derivados del tratamiento, incluyéndose los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos; (2) sometimiento de la investigación científica a las normas de calidad, así como a las directrices internacionales sobre buena práctica clínica, en su caso; (3) adopción de medidas dirigidas a fin de garantizar que los investigadores no acceden a datos de identificación de los interesado, en su caso; (4) para el caso de que el promotor de un ensayo clínico no se encuentre establecido en la Unión Europea, se designará un representante legal establecido en la Unión Europea que puede coincidir con representante legal designado para aquellas actividades de tratamiento relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión o, con el control de su comportamiento, en la medida que tenga lugar en la Unión cuando el interesado resida en la UE pero sin embargo el responsable o encargado no se encuentra establecido en la Unión.

En suma, según interpretación extensiva por parte de la AEPD del art. 6 del RGPD sobre el tratamiento lícito de los datos, cabe tener en consideración que no es obligatorio que el médico[425] o el centro sanitario – público o privado – solicite el consentimiento al paciente a efectos de recoger y utilizar sus datos personales y de salud siempre y cuando vayan a ser utilizados para los siguientes fines:

(1) Para medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestación de los sistemas y servicios de asistencia sanitaria[426];

[424] *Vid.* apartado 2.e) de la disposición adicional decimoséptima de la LOPDGDD.

[425] En todo caso, debe ser un profesional sujeto a la obligación de secreto profesional, o que estén bajo se responsabilidad.

[426] La AEPD señala como base de legitimación para este tratamiento de datos el art. 6.1. b) del RGPD para las entidades aseguradoras de salud privadas, y el art. 6.1. c) del citado Reglamento para la sanidad pública.

(2) Por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios o la inspección de reclamaciones de los ciudadanos[427]y;

(3) Cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento, o cuando lo solicite un órgano judicial[428].

En suma, como se puede apreciar las anteriores razones tienen en común el interés público y la investigación científica como fundamentos principales que justifican el tratamiento lícito de los datos de salud[429].

Así pues, se puede deducir que, en la mayoría de los casos ni el médico ni el centro sanitario, público o privado, han de solicitar previamente el consentimiento del paciente, siempre y cuando se vayan a utilizar sus datos para prestar al mismo una asistencia sanitaria o, para las causas anteriormente citadas. Por ende, de conformidad con los artículos 9.2 y 89 RGPD, se exime de responsabilidad – patrimonial o civil - imputable al responsable o encargo del tratamiento por posible vulneración de derechos fundamentales del titular de los datos, esto es, al profesional y centros sanitarios, público o privado al establecer que no es obligatorio por parte de los mismos solicitar el consentimiento del paciente en aquellos casos en los que los datos de salud se destinen

[427] A tales efectos, la AEPD establece como base de legitimación el art. 6.1.e) del RGPD.

[428] En relación con este punto, la base de legitimación, según la AEPD se encuentra en el art. 6.1.d) del RGPD.

[429] En este sentido, el considerando 54 RGPD establece que: "El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

para fines de medicina preventiva, por razones de interés público en el ámbito de la salud pública y, cuando el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica, histórica o fines estadísticos.

En relación con el tratamiento de los datos de salud la AEPD confirma que la historia clínica informatizada es una herramienta positivamente valorada por los usuarios de la sanidad, siendo igualmente considerada por los profesionales sanitarios la fuente fundamental a efectos de identificar tratamientos y patología del paciente, así "para la medicina preventiva; para desarrollar líneas epidemiológicas; para generar estadísticas de riesgos de amplios sectores poblacionales; para prever incidencias futuras en la salud de la población; y para planificar sistemas de atención primaria a corto, medio y largo plazo"[430]. En consecuencia, resulta razonable y lógico desde una perspectiva jurídica y social el hecho de considerar lícito el tratamiento de los datos de salud del paciente sin su consentimiento por razones de interés público e investigación científica.

Si bien, a modo excepcional se permite el tratamiento de los datos relativos a la salud, genéticos y biomédicos sin el consentimiento del paciente en aquellos supuestos además que en los que sea necesario para la protección de intereses vitales del interesado o de una tercera persona física, se requieran los datos para el cumplimiento de una misión de interés público, para el cumplimiento de obligaciones de carácter laboral, para finalidades de medicina preventiva o laboral, así como por razones de interés público en el ámbito de la salud pública[431], para la prevención de epidemias[432] o

[430] Agencia Española de Protección de Datos, *Guía para pacientes y usuarios de la Sanidad*, 2019, p.4.

[431] Al respecto, hemos de traer a colación el Considerando 54 RGPD donde establece que: "El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo (1), es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

[432] Así, el Considerando 46 RGPD señala que: "El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente. deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base

investigación científica[433], histórica o fines estadísticos. De manera general, el RGPD prevé en el artículo 9.4 que los Estados miembros puedan "mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud". Así también lo establece el segundo párrafo del artículo 9.2 de la LOPDGG al señalar que "la ley podrá amparar el tratamiento de datos en el ámbito de la salud cuando asó lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte". Igualmente, la Disposición Adicional 17ª. 2 c) señala que "las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública".

No cabe duda que las anteriores excepciones del tratamiento de los datos de salud sin la necesidad del consentimiento del paciente guardan una estrecha vinculación con la aplicación de herramientas *big data* en el ámbito del sector sanitario, pues como se verá más adelante, la información y el conocimiento que se desprende del análisis de los datos relativos a la salud pueden ser empleados en los sistemas nacionales de salud en la esfera de la medicina preventiva, de la medicina poblacional en el sentido de hacer más complementaria la medicina personaliza a través de las muestras sobre las que se pueden extraer conclusiones, así como para mejorar el funcionamiento interno del sistema nacional de salud de cada país, localizando con más inmediatez las necesidades reales del mismo y significando una mejor gestión de los recursos y de las inversiones[434].

En definitiva, como se ha podido observar a pesar de que de manera general la normativa vigente de protección de datos continúa otorgándole un gran valor judicial al consentimiento informado del paciente como base jurídica que legitima el tratamiento

---

jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano".

[433] En este sentido, el Considerando 59 RGPD considera que entre los fines de investigación científica "también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública".

[434] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 893.

de los datos personales, sin embargo, la normativa vigente de protección de datos regula algunos supuestos que permiten un tratamiento lícito de los datos de salud sin necesidad de consentimiento del titular. Todo ello, con la finalidad de prevenir el problema que podría darse de la exigencia de un consentimiento específico para cada una de las finalidades del tratamiento de los datos de salud, ya que podría suponer obstaculizar el desarrollo científico y a su vez desproteger la garantía del avance de la investigación científica, que resulta igualmente de interés público "al restringir el uso de los datos a la concreta investigación en que se hubieran obtenido, vedando la posible reutilización posterior de los datos para investigaciones no previstas en el momento en que el interesado prestó su consentimiento"[435].

Sin embargo, como ha sido analizado en los anteriores supuestos excepcionales, la garantía no es tanto en cuanto que el paciente es quien autoriza el tratamiento de sus datos de salud, sino que más bien el paciente no tiene derecho para decidir e impedir que no se usen sus datos al existir un interés general y de salud pública. En cualquier caso, el paciente tiene derecho a que se le garantice su derecho a la intimidad, pero la protección de datos no es una capacidad de decisión al titular de estos para impedir su tratamiento, siempre y cuando exista un interés público. En este sentido, cabría afirmar que en el nuevo marco jurídico de protección de datos el consentimiento del paciente se encuentra superado, sobre todo en el ámbito sanitario y de la investigación biomédica, aunque en cualquier caso el paciente tiene derecho a que los datos se traten conforme a la base jurídica adecuada con las garantías adecuadas, por lo que podría en consecuencia negarse a que se usen sus datos si no se cumplen con las garantías y medidas, tal y como se configuran en el artículo 89 del propio Reglamento[436].

Así pues, debido a la flexibilidad del RGPD y la LOPDGDD, nos encontramos ante un enfoque proactivo[437] sobre el cumplimiento de la normativa vigente de

[435] FUENTES ESCOBAR, "Algunas cuestiones relevantes...", *op. cit.*, p.164.

[436] GARCÍA-RIPOLL MONTIJANO, M., "El consentimiento al tratamiento de datos personales", en AA.VV., *Protección de datos personales,* (Coord. I. González Pacanowska), Asociación de profesores de Derecho Civil, Tirant lo Blanch, Valencia, 2020, p.28.

[437] Así pues, LÓPEZ RUIZ, C.G., "La figura del delegado de protección de datos (DPO)", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva LO3/2018 y Reglamento (UE). Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018,

protección de datos por parte del responsable del tratamiento, encontrándose obligado en todo caso a actuar con diligencia, analizando cada situación y decidiendo sobre las medidas a aplicar en cada caso concreto, siendo responsable a su vez de su actualización y, bajo la carga de deber probar sus actuaciones diligentes ante el titular de los datos personales, la AEPD y los tribunales, en su caso, lo que conlleva implícito el deber de implantar los medios adecuados a efectos de dar cumplimiento a sus obligaciones. Debido a la importancia que tiene lo anterior en la protección de los datos relativos a la salud, a fin de que exista una concordancia y armonía entre la normativa vigente de protección de datos con la ley sectorial de protección de datos de salud, resulta de gran interés que norma específica en relación con el consentimiento del interesado en los casos de salud pública, contemple al menos cuatro escenarios diferentes: por un lado, el tratamiento lícito de los datos sin necesidad del consentimiento de paciente; por otro lado, el consentimiento del interesado para la investigación con muestras biológicas (debido a su importancia será tratado en epígrafe aparte); en tercer lugar, el consentimiento para tratamiento de datos de salud de personas fallecidas y; por último el consentimiento para el tratamiento de datos de salud de menores de edad.

A lo que respecta sobre el consentimiento el tratamiento lícito de los datos sin necesidad del consentimiento de paciente, es relevante que la ley sectorial tenga en consideración la cuestión de que el responsable del tratamiento, bien sea un centro sanitario público o privado, bien sea un profesional sanitario, sea conocedor de manera clara y concisa de los casos en los que no está obligado a solicitar el consentimiento a los pacientes para la recogida y utilización de los datos personales y de salud, lo que conlleva la exigencia legal de que la ley sectorial perfile en la medida de lo posible las situaciones de tratamiento lícito de los datos sin necesidad del consentimiento del paciente.

A continuación, tomando como referencia los criterios asentados por la propia normativa de protección de datos, así como por la AEPD, se facilita un listado

---

p.701, opina que: "El nuevo reglamento europeo supone un cambio de modelo, ya que se exige una proactividad por parte de todos nosotros. Todas las empresas, sean del tamaño que sean, deberán conocer bien sus políticas de protección de datos, diseñar unas medidas de imagen y semejanza de su negocio, vamos cada vez más a una especialización, un corte hecho a medida, ya no valen las plantillas rehechas. Hay que hacer un estudio más personalizado, conociendo el flujo de los datos desde que "entran" hasta que "salen" de la organización".

orientativo de algunos de los supuestos sin perjuicio de que llegado su momento sean ampliados en la ley sectorial:

(1)Fines de medicina preventiva o laboral; (2) Evaluación de la capacidad laboral del trabajador; (3) Diagnóstico médico al paciente; (4) Prestación de asistencia al paciente; (5) Tratamiento de tipo sanitario o social; (6) Gestión de los sistemas y servicios de asistencia sanitaria y social; (7) Por razones de interés público en el ámbito de la salud pública a efectos de prevenir riesgos o peligros graves para la salud de la población se podrán ceder datos identificativos de paciente sin su consentimiento; (8) Para la realización de estudios epidemiológicos a efectos de prevenir eficazmente la prevención de los riesgos para la salud pública; (9) Para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que interesado se encuentre incapacitado, física o jurídicamente a los efectos de dar su consentimiento o, en caso de que lo solicite un órgano judicial[438]. No en vano, la doctrina de manera unánime mantiene que cuando el Juzgador de oficio requiere la entrega de la historia clínica, bien en proceso penal, civil o contencioso-administrativo[439], el centro sanitario (público o privado) o el facultativo médico privado, están obligados a su entrega, de conformidad con el art. 16.3 LBAP[440], así como del artículo 118 CE que señala la obligada colaboración de las Administraciones sanitarias con la administración de justicia durante el proceso judicial y; (10) Fines de investigación científica donde se incluye la investigación básica o preclínica[441], la investigación clínica[442] y la investigación epistemológica social[443].

---

[438] A tales efectos, cabe destacar que, en el Decálogo de la Historia Clínica aprobado en marzo de 2017 por la Organización Médica Colegial, se establece que: "7. La historia clínica como medio de prueba. El uso judicial de la historia clínica en el ámbito civil requiere la previa autorización del paciente. En el ámbito penal, cuando la historia se convierte en elemento de prueba de un posible delito, se debe entregar; por parte del médico o del centro, la precaución deontológica estará en informar al juez de la existencia en la misma de datos sensibles que si son irrelevantes para la causa investigada, se podrían segregar del total del documento, manteniéndose protegidos. Una vez que la historia se halla en posesión del Juez, será éste el garante de su custodia y preservación de la confidencialidad de los datos contenidos en la misma".

[439] En estos términos, GUTIÉRREZ BARRENENGOA, A., "La historia clínica como prueba en el Proceso Judicial por responsabilidad médica", en AA.VV., *Responsabilidad médica civil y penal por presunta mala práctica profesional,* (Coord. O. Monje Balmaseda), Ed. Dykinson, Madrid, 2012, pp. 323-334, afirma que la historia clínica es un elemento esencial para dilucidar la existencia o no de responsabilidad en los procesos judiciales por responsabilidad médica, tanto contencioso-administrativo, civiles o penales.

[440] Sobre este asunto *Vid.* LARIOS RISCO, D., *Guía Práctica de Derechos de los Pacientes y de los Profesionales sanitario,* Thomson-Reuters Aranzadi, Cizur-Navarra, 2016, pp.165-195.

[441] La finalidad principal de la investigación básica o preclínica es la de conseguir un mejor conocimiento de los mecanismos moleculares, bioquímicos y celulares implicados en la etiopatogenia de las enfermedades, a la vez que determinar la importación de los aspectos epigenéticos en su génisis. En el

Asimismo, resulta fundamental que la ley sectorial delimite el consentimiento para el tratamiento de datos de salud de personas fallecidas ajustándose a lo establecido en la normativa vigente de protección de datos[444] en el caso del tratamiento de datos de salud de personas fallecidas deberá establecer que las personas vinculadas al fallecido – familiares, de hecho, herederos o aquellas designadas por el fallecido – pueden solicitar el acceso a los mismos, así como su rectificación o supresión, siempre y cuando no exista prohibición expresa del fallecido. De igual modo, se ha de hacer constar en la ley sectorial la prohibición al responsable del tratamiento de facilitar información que afecte a la intimidad del fallecido ni sobre las anotaciones subjetivas de los profesionales que consten en la historia clínica del mismo, ni que afecte a terceros.

Por último, la ley sectorial debería contemplar en el caso del consentimiento para el tratamiento de datos de salud de menores de edad los supuestos regulados por la actual normativa, tales como que: el menor con catorce años cumplidos podrá otorgar el consentimiento y tendrá acceso a sus datos de salud; igualmente, si nos encontramos ante un menor de trece años, se permite el tratamiento de los datos de salud siempre y cuando sus padres o tutores presten su consentimiento para su uso con fines de investigación biomédica, abarcándose áreas generales vinculadas a una especialidad médica o investigadora; por último para los supuestos de menores de edad entre catorce

---

caso de que sean precisos los vínculos de los resultados de la investigación con la evolución clínica del paciente se utilizan datos seudonimizados, en caso contrario, se suelen emplear muestras anónimas o anonimizadas.

[442] La investigación clínica es la referente a los ensayos clínicos con medicamentos, ensayos clínicos con prótesis, técnicas quirúrgicas…, estudios retrospectivos, tesis, proyectos fin de grados… a efectos de estudiar la prevención, diagnósticos y tratamiento de las enfermedades de los pacientes y el conocimiento de su historia natural.

[443] Es la investigación que tiene como objetivo mejorar la salud de la población sin que exista un riesgo o peligro grave. En la investigación epidemiológica social tiene una gran importancia trabajar con datos identificados o, en todo caso, seudonimizados para que la investigación sea de calidad y poder acceder con facilidad la identidad, por lo que la historia clínica electrónica es una de las fuentes principales.

[444] Sobre los datos de personas fallecidas, el art. 3 de la LOPDGDD establece que podrán acceder a los datos registrados en el fichero las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos y las personas o instituciones designadas expresamente por el fallecido, así como solicitar su rectificación o supresión siempre y cuando no exista prohibición expresa por escrito por parte de la persona fallecida o prohibición legal, en todo caso, los herederos podrán acceder a los datos de carácter patrimonial del causante. En caso de fallecimiento de menores y personas con discapacidad, también podrán acceder a sus datos personales y, en su caso, su rectificación o supresión, sus representantes legales y por el Ministerio Fiscal (que puede actuar de oficio o a instancia de persona física o jurídica interesada). Asimismo, en el caso de fallecimiento de personas con discapacidad, también podrán acceder a sus datos las personas designadas para el ejercicio de funciones de apoyo, si entre sus medidas de apoyo se encuentra la de acceso a sus datos personales y, en su caso, su rectificación o supresión.

y dieciocho años, los padres o tutores que ostenten la patria potestad o tutela del menor podrán acceder a la historia clínica de sus hijos.

2.3. El tratamiento ulterior de los datos personales para fines compatibles con el fin principal

A continuación, se observará otra medida novedosa del Reglamento que radica en la regulación del tratamiento ulterior de los datos personales. De manera general el RGPD indica que el tratamiento de aquellos datos personales con fines diferentes al fin inicial únicamente se puede permitir cuando sea compatible con los fines de recogida inicial, donde no se requiere una base jurídica distinta a la que permitió la obtención de los datos personales[445]. A pesar de ello, la nueva norma jurídica establece de manera específica un régimen para aquellas situaciones en las que nos encontramos ante operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos[446] al considerarse operaciones de tratamiento lícitas compatibles, pudiéndose determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros[447].

Lo anterior se debe a que el legislador europeo es consciente de la tensión entre el ordenamiento jurídico y los imparables avances tecnológicos, así como que en la actualidad los datos de salud no son utilizados únicamente para fines asistenciales sanitarios propios de las relaciones médico – paciente, sino que también los datos

[445] Considerando 50 RGPD.

[446] El Considerando 162 RGPD señala que: "Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas". Asimismo, el Considerado 162 establece que: "El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros".

[447] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 895, señala que: "Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior".

relativos a la salud pueden ser explotados para otros fines, tales como de investigación biomédica, de salud pública, desarrollo de tratamientos, mejora de la gestión sanitaria, entre otros.

En el marco jurídico español, el tratamiento ulterior de los datos personales se prevé genéricamente en la vigente LOPDGDD[448] y, de manera específica en el sector sanitario en la Ley 41/2002[449] en lo que se refiere a información sanitaria, según el *Informe 471* e *Informe 617/2008* de la AEPD es de aplicación el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

En consecuencia, en el caso de la aplicación de herramientas *big data* en el ámbito sanitario las opciones para que el tratamiento ulterior sea considerado lícito se amplían, puesto que estamos ante datos que engloban todas las opciones posibles de licitud que otorga el Reglamento, es decir, los mismos pueden ser usados para fines de interés público, investigación científica y estadística, pudiéndose dar varias operaciones de tratamiento lícitas compatibles a la vez en la mayoría de las situaciones, puesto que, por un lado entre los fines de investigación científica también se incluyen "los estudios realizados en interés público en el ámbito de la salud pública"[450](investigación biomédica); por otro lado, el tratamiento con fines estadísticos abarca igualmente, "recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos" que pueden ser utilizados, entre otros, para fines de investigación científica[451].

[448] Especialmente, el art. 25 LOPDGDD en materia de investigación estadística.

[449] Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

[450] Considerando 159 RGPD.

[451] Considerando 162 RGPD.

2.4. La anonimización y seudonimización: medidas adecuadas que garantizan datos abiertos y reutilizables

De igual modo, se ha de destacar que la finalidad para lo que se tratan los datos de salud puede ser incompatible con el derecho de protección de datos dando lugar a problemas sobre consentimiento del paciente, salvo que se adopten las medidas adecuadas para que los datos de salud dejen de ser datos personales de las personas físicas identificadas e identificables[452] y se conviertan en datos públicos y abiertos.

Así pues, resulta pertinente diferenciar cuando una persona es identificable a efectos de determinar la aplicación o no de la normativa de protección de datos personales, sobre todo en el sector sanitario y de la investigación es relevante diferenciar cuando nos encontramos ante un caso donde una persona física pueda resultar potencialmente identificable. Al respecto, el RGPD señala en el art. 4.1. que "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". Además, el Considerando 26 del RGPD establece que "para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos".

Por ende, la medida que regula el RGPD a efectos de proteger los datos personales es la "seudonimización"[453] y, que en el artículo 4.5 del RGPD se define

[452] El Considerando 26 del RGPD establece que "los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable".

[453] MIRALLES LÓPEZ, R., "Desvinculación datos personales: seudonimización, desidentificación y anonimización", *I + S: Revista de la Sociedad Española de Informática y Salud,* ejemplar 122, 2017, p. 8.

como "el tratamiento de datos personales de manera tal que ya no pueden atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".

Al respecto, en el considerando 28 del RGPD, el legislador europeo destaca que con la aplicación de la técnica de seudonimización, por un lado, los riesgos para los afectos pueden ser reducidos y, por otro lado, coopera con los encargados y responsables del tratamiento a fin de que cumplan sus obligaciones de protección de los datos, aclarando a su vez, que en ningún caso con la aplicación de la citada técnica se "pretende excluir ninguna otra medida relativa a la protección de los datos".

Así pues, con la técnica de la seudonimización los analistas de datos separan los datos identificativos del paciente de los datos de salud, aunque pueden volver a asociarse si es necesario mediante técnicas de ingeniera inversa[454]. Sin embargo, el mecanismo que garantiza, aunque no de un modo seguro como se apreciará más adelante[455], que los datos personales se conviertan en datos abiertos y públicos es la anonimización de los mismos, debido a que la seudonimización viene a implicar la aplicación de la normativa vigente de protección de datos[456], en el sentido, de que como

---

[454] Al respecto, entre otros, MOGOLLÓN GONZÁLEZ, S., "¿Existe de verdad la anonimización? El grupo del artículo 29 de Protección de Datos no lo pone fácil", *Noticias Jurídicas,* Conocimiento, Artículos doctrinales, Julio 2014, [Documento sin paginación]. Documento disponible en: https://www.audea.com/existe-de-verdad-la-anonimizacion-el-grupo-del-articulo-29-de-proteccion-de-datos-no-lo-pone-facil/ (último acceso 20/12/18); *Informe del experto núm. 12 Acceso a la historia clínica con fines de investigación. Estado de la cuestión y controversias*, Fundación Salud 2000, Julio 2015, p. 12; GÓMEZ PIQUERAS, C., "Disociación/anonimización de los datos de salud", *Revista Derecho y Salud,* vol. 18. núm. 1, 2009, p. 56.

[455] *Vid.* la publicación de la AEPD sobre *Orientaciones y garantías en los procedimientos de anonimización de datos personales* en el año 2016 donde se advierte de los riesgos de re-identificación y se aconseja que las medidas de evaluación de impacto se lleven a cabo de manera periódica, pues con la utilización de las tecnologías *Big Data* en las que no se empleen tiempo o coste desproporcionado se asume el riesgo de que una información supuestamente disociada, vinculada a otros datos personales pueda convertirse en un dato de una persona identificable, siendo posible la re-identificación https://www.agpd.es/portalwebAGPD/canal documentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf-. Asimismo, el Dictamen 5/2014 del Grupo de Trabajo del Artículo 29 sobre técnicas de anonimización.

[456] TRONCOSO REIGADA, "Investigación, salud pública y asistencia sanitaria…", *op. cit.,* p. 210, afirma que: "Hay que diferenciar la disociación o anonimización, que es definitiva y que impide la identificación de las personas afectadas, de manera que el tratamiento no entra dentro del ámbito de aplicación del RGPD –al no existir un tratamiento de datos personales-, de la disociación reversible, que aparecía ya en la Ley de Investigación Biomédica, a la que el RGPD denomina "seudonimización", que no es un proceso

se ha analizado anteriormente, tanto el RGPD como la LOPDGDD permiten acudir a conceptos abiertos como interés público, investigación científica y salud pública a fin de que puedan ser tratados de manera lícita los datos de salud de los pacientes sin necesidad de que sean anonimizados[457]. Por ello, se ha de garantizar por un lado que, la anonimización sea efectiva y, por otro lado, que las garantías técnicas se adapten al contexto actual, lo que conlleva a una dinámica dando lugar a un contexto tecnológico donde la normativa jurídica y las garantías actuales tensionan de manera constante con la tecnología[458].

En suma, nos encontraríamos ante una disociación reversible[459] cuando sea empleada una técnica que permita una operación inversa a través de un simple código.

---

concluido, no impide la identificación de las personas afectadas y es, por tanto, un tratamiento de datos personales".

[457] A pesar de ello, el RGPD señala que siempre que los fines de investigación científica o histórica, los fines estadísticos o los fines de archivo en interés público "puedan alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzará de ese modo" –art. 89.1, *in fine* RGPD- Así, el RGPD señala que "no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación". –Considerando 26 *in fine*-.

[458] El Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de dato personales del artículo 29, creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, en su Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril de 2014, establece que: "La anonimización es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación. La seudonimización consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo. La seudonimización no es un método de anonimización; simplemente, reduce la vinculabilidad de un conjunto de datos con la identidad original del interesado y es, en consecuencia, una medida de seguridad útil" […] los datos cifrados son un ejemplo clásico de «seudonimización. La información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir para establecer la correspondencia entre el código y los identificadores habituales de la persona (nombre, fecha de nacimiento, dirección, etc.) se guardan por separado" [..] los datos seudonimizados no constituyen información anonimizada, ya que permiten singularizar a los interesados y vincularlos entre conjuntos de datos diferentes. La probabilidad de que el seudoanonimato admita la identificabilidad es muy alta; por ello, entra dentro del ámbito de aplicación del régimen jurídico de la protección de datos. Esto reviste una especial relevancia en el contexto de las investigaciones científicas, estadísticas e históricas".

[459]El informe jurídico 0283/2008 de la AEPD interpreta que: "[…] En consecuencia, para entender que se ha efectuado correctamente la disociación, es necesario que se permita por ningún medio identificar al paciente. Del tenor de la consulta se desprende que cada centro médico va a otorgar un número de historia clínica a los datos de sus pacientes, quiere decir que en cada centro médico el número de historia será suficiente que existe la mera posibilidad, incluso remota, de que, mediante la utilización, con carácter previo, coetáneo o posterior de cualquier medio (proceso informático, programa, herramienta del sistema, etcétera), la información concerniente a los pacientes, que obre en poder del consultante, pueda revelar la identidad de los afectados, para que quede plenamente sometida a la Ley Organiza. En consecuencia, para que un procedimiento de disociación pueda ser considerado suficiente a los efectos de la Ley Orgánica 15/1999, será necesario que de la aplicación de dicho procedimiento resulte imposible asociar un determinado dato con un sujeto determinado. En este sentido, las disposiciones internacionales reguladoras de la protección de datos de carácter personal vienen a considerar que el afectado no será

Sin embargo, cuando sea necesario un esfuerzo mayor, esto es, invertir una cantidad de tiempo, gastos y trabajo desproporcionados, para recuperar la asociación, nos encontraríamos ante un dato irreversiblemente disociado[460].

Es fundamental que se tenga en consideración que en relación con el deber de confidencialidad se establece como obligación general en el artículo 5.1.f) del RGPD, así como en el artículo 5 de la LOPDGDD que los responsables y encargados del tratamiento de datos estarán sujetos al deber de confidencialidad, siendo esta obligación complementaria con los deberes de secreto profesional según normativa específica al respecto. Por consiguiente, esta obligación viene a repercutir de manera directa a los facultativos sanitarios al tratarse de profesiones sujetas al secreto profesional y confidencialidad de los datos, puesto que nos encontramos ante una obligación propia de toda profesión vinculada a la sanidad y de interés público, al ser la esfera de la salud uno de los puntos vitales más personales e íntimos de una persona. Así pues, en lo referente a los datos que aporten una información relativa a una persona física identificada o identificable deben ser protegidos mediante la aplicación de los principios de protección de datos. Sin embargo, la normativa vigente en el ámbito europeo y en el ordenamiento jurídico español autoriza el acceso a los datos de salud por parte de terceros a través de la técnica de la seudonimización con la finalidad de que a través de la aplicación de la citada técnica no se incumpla el secreto profesional ni el deber de confidencialidad por parte de los profesionales sanitarios, así como evitar posibles vulneraciones del derecho a la intimidad del paciente[461].

---

determinable cuando su identificación exija un esfuerzo desproporcionado que sea suficiente para disuadir a quien accede al dato de la identificación de la persona a la que el mismo se refiere".

[460] Art. 3.i) y 3.k) de la Ley 14/2007, de 3 de julio, de Investigación biomédica, en relación con el art. 5.1. e) del Reglamento de desarrollo de la LOPD.

[461] Como señala PÉREZ GÓMEZ, la seudonimización surge ante "la dificultad objetiva de emplear procesos de anonimización –entendidos inicialmente como procedimientos de disociación absoluta-, como una alternativa útil y práctica a la – en otro caso preceptiva- obtención de consentimiento del titular del dato, cuando se pretendan llevar a cabo finalidades de tratamiento en materia de investigación científica y biomédica en principio legítimas". Este autor pone el ejemplo de los biobancos donde "el material que se almacena se puede conservar con una finalidad genérica de investigación biomédica, pero no queda tan clara la específica finalidad que bajo dicho título pueda amparar el desarrollo de la ciencia y de los métodos de investigación en evolución constante: y esto implica que lo que un día fue almacenado con una finalidad, puede llegar a ser utilizado para otra radicalmente distinta sin que en principio exceda o escape del título de investigación biomédica, utilizado cuando fue incorporado al biobanco. En estos casos, la disociación absoluta pudiera dificultar la mejor explotación de la muestra, mientras que la aceptación de su tratamiento bajo estos nuevos parámetros aceptando la seudonimización como un medio aceptable de preservar la seguridad de los datos por los arts. 32.1.a) y 89.1 del Reglamento, se considera que puede resultar beneficioso para el desarrollo de estas investigaciones", PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 203.

En concreto, el artículo 25 RGPD, regula una "protección de datos desde el diseño y por defecto", a efectos de que las normas reguladas en el Reglamento sean eficaces y resistentes al paso de tiempo y al cambio tecnológicos e integren las garantías necesarias en el tratamiento, son introducidos principios de protección de datos "desde el diseño y por defecto" a modo de medidas técnicas y organizativas, como la seudonimización, de tal modo que el "responsable del tratamiento cumpla los requisitos del Reglamento y se protejan realmente los derechos de los interesados desde la planificación de los proyectos («desde el diseño») y en todo caso («por defecto»)"[462].

Con carácter previo al análisis de la citada técnica, procede tener presente que los datos personales seudonimizados que aporten información adicional, deben corresponder a una persona física identificable. De otra parte, a la hora de determinar si una persona física es o no identificable, debe tenerse en cuenta aquellos medios que pueden ser utilizados directa o indirectamente bien por responsable del tratamiento o cualquier otra persona a efectos de identificar a la misma, en concreto, siendo uno de los medios más destacados el de la singularización.

Igualmente, a fin de determinar la existencia de una probabilidad razonable de que puedan ser utilizados medios con el objetivo de identificar a una persona física, hemos de tener en cuenta todos aquellos factores objetivos, incluyendo desde la tecnología de la que disponemos en el momento del tratamiento, así como posibles avances tecnológicos, hasta los costes y el tiempo necesarios para la identificación. Por tanto, cuando nos encontremos, bien ante una información anónima, es decir información que no sea relativa a una persona física identificada o identificable, bien, ante aquellos datos que hayan sido convertidos en anónimos dejando de ser identificable el interesado, no serán de aplicación los principios de protección de datos.

El art. 89.1 RGPD establece que el tratamiento con fines de investigación científica exige, entre las garantías adecuadas para los derechos y las libertades de los interesados, la utilización de las técnicas de anonimización y seudonimización, extremo

[462] DÍAZ DÍAZ, E., "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*", Revista Aranzadi Doctrinal*, agosto 2016, núm. 6/2016 parte Estudio, p. 12.

que también regula en la Ley 14/2007, de 3 de julio, de Investigación biomédica (en adelante, LIB), donde hace referencia a los procedimientos de disociación o de anonimización el artículo 47 bajo la rúbrica "Información previa a la realización de análisis genéticos con fines de investigación en el ámbito sanitario", art. 50 sobre "el acceso a los datos genéticos por personal sanitario", en el art. 52 acerca de la "conservación de los datos" y sobre todo, en el Capítulo III sobre la "Utilización de muestras biológicas humanas con fines de investigación biomédica"[463], así como en la Disposición transitoria segunda sobre las muestras almacenadas con anterioridad a la entrada en vigor de la LIB.

En los términos aquí planteados, es particularmente de interés el significado que la LIB establece en relación con el concepto de anonimización, dato anonimizado o irreversiblemente disociado y, muestra biológica anonimizada o irreversiblemente disociada. Así pues, se entiende por anonimización "el proceso por el que deja de ser posible establecer por medios razonables el nexo entre un dato y el sujeto al que se refiere. Es aplicable también a la muestra biológica"[464]. Por otro lado, dato anonimizado o irreversiblemente disociado, es el "dato que no puede 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"[465].

De igual modo, muestra biológica anonimizada o irreversiblemente disociada, es una "muestra que no puede 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"[466]. Por último, una muestra biológica no identificable o anónima, es una "muestra recogida sin un nexo con una persona identificada o identificable de la que, consiguientemente, no se conoce la procedencia y es imposible trazar el origen"[467].

[463] Arts. 58 y concordantes de la LIB.

[464] Artículo 3 letra c) LIB).

[465] Art. 3 letra i) LIB).

[466] Art. 3 letra p) LIB).

[467] Art. 3 letra q) LIB).

La diferencia entre datos anónimos y datos seudonimizados viene regulada en el art. 26 del RGPD, donde se señala que: "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos"[468].

Por último, el art. 28 RGPD justifica la seudonimización como técnica que sustituye el consentimiento del afectado, estableciendo al respecto que "la aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos".

En suma, 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".

[468] En este sentido, MÉNDEZ GARCÍA, M.; 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", *Revista de Derecho y Genoma Humano,* Núm. Extraordinario, 2019, p. 221, aclaran que: "Así mismo, los datos seudonimizados únicamente serán accesibles al equipo de investigación si: - Existe un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación. - Se adoptan medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. - El Comité de Ética emite el correspondiente dictamen favorable cuando se utilicen datos seudonimizados para investigación".

Una vez examinado el elenco legal de la anonimización y de la seudonimización, cabe tener presente que a pesar de que la seudonimización resulta ser en principio una medida útil de seguridad, sin embargo, permite un fácil acceso a la identidad del titular de los datos, por ello, el legislador europeo en el RGPD establece que los datos seudonimizados deben estar protegidos por los principios y reglas estatuidos en el mismo. Igualmente sucede con la anonimización – como se ha comentado a lo largo del presente trabajo – los expertos afirman de manera retunda que no se puede garantizar que la anonimización sea irreversible.

Por ello el legislador europeo a los efectos de estimar si la anonimización es irreversible o no, emplea el criterio del esfuerzo exigido, de tal modo que si el esfuerzo exigido para la asociación de los datos personales y de salud no es razonable, los datos serán considerados anónimos, ya que supondrá invertir una cantidad de tiempo, gastos y trabajos desproporcionados para su reversibilidad[469]. No en vano, lo cierto es que el criterio establecido por el legislador europeo – y también regulado en la LIB – es indeterminado, puesto que cabe la posibilidad – y cada vez más – de que aparezcan nuevas técnicas de asociación cuyos resultados de identificar al titular de los datos puedan ser compensados económicamente de manera posterior.

Debido a lo anterior, resultan sumamente interesantes las aclaraciones que realiza el "Comité Europeo de Protección de Datos" en las Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, adoptadas el 21 de abril de 2020[470], en concreto:

"15. Por anonimización se entiende el uso de un conjunto de técnicas destinadas a suprimir la capacidad de asociar los datos a una persona física identificada o identificable mediante un esfuerzo «razonable». Esta «prueba de razonabilidad» debe tener en cuenta tanto los aspectos objetivos (tiempo, medios técnicos) como los elementos contextuales, que pueden variar de un caso a otro (carácter excepcional de un

[469] Al respecto, cabe recordar que el Grupo de Trabajo del Artículo 29 resolvió sobre estas cuestiones en su Dictamen 04/2007 sobre el concepto de datos personales (WP 136) y en su Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril de 2014, previamente analizados y citados en el presente trabajo.

[470] Documento disponible en: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_es (Último acceso 16/02/21).

fenómeno teniendo en cuenta, por ejemplo, la densidad de la población y la naturaleza y volumen de los datos). Si los datos no superan esta prueba, no se han anonimizado y, por tanto, se mantienen dentro del ámbito de aplicación del RGPD.

16. La evaluación de la consistencia de la anonimización depende de tres criterios: i) singularización (identificación de una persona dentro de un grupo mayor sobre la base de los datos); ii) vinculación (vinculación de dos registros de datos sobre la misma persona); y iii) inferencia (deducción, con una probabilidad significativa, de información desconocida sobre una persona).

17. El concepto de anonimización tiende a ser malinterpretado y suele confundirse con la seudonimización. La anonimización permite utilizar los datos sin ninguna restricción, mientras que los datos seudonimizados siguen entrando en el ámbito de aplicación del RGPD.

[…]19. Los procesos de anonimización y los ataques de reidentificación son ámbitos de investigación dinámicos. Es crucial que todo responsable del tratamiento que aplique soluciones de anonimización se mantenga al corriente de las últimas novedades".

En consecuencia, resulta de interés que las organizaciones (públicas o privadas) que realicen procesos de anonimización empleando tecnologías de *big data*, tengan el deber de realizar una política de anonimización, un protocolo de actuación y llevar a cabo medidas tecnológicas adoptadas al mismo[471], todo ello reforzado con garantías

[471] Como sugerencia a tener en consideración se cita la propuesta de MIRALLES LÓPEZ que denomina como: "el «ciclo de la desvinculación de datos personales» implicará disponer de las tecnologías, las personas y los procesos adecuados que permitan reducir al máximo el riesgo de re-identificación. Ese ciclo estaría dividido en una serie de fases que pueden describirse brevemente de la siguiente manera: 1. Debe iniciarse con el diseño del método de desvinculación, es decir, cómo tenemos previsto transformar los datos personales para protegerlos, obviamente incluyendo aquí potenciales evaluaciones de impacto, análisis de riesgos, etc. 2. La segunda fase del ciclo será la aplicación del método diseñado. 3. La tercera fase será verificar, antes de liberar la información, que efectivamente el riesgo de re-identificación está dentro de los márgenes aceptables y que la información resultante es de utilidad. Así en función del método de transformación, a efectos de re-identificación habrá que verificar si: • ¿Se puede singularizar a una persona concreta? • ¿Se pueden vincular registros relativos a una persona? • ¿Se puede inferir información relativa a una persona? 4. Y la última fase del ciclo será revisar periódicamente el proceso de desvinculación, a fin de valorar si el diseño inicial sigue siendo válido, y en caso de no serlo deberá procederse a su rediseño, iniciándose de nuevo el ciclo. De este modo, aplicando un proceso sistemático, estaremos dando respuesta a la protección de los datos personales, especialmente en escenarios de tratamiento de datos a gran escala que requieren de garantías adicionales, como sería el caso de la

jurídicas necesarias a fin de proteger los derechos de los titulares de los datos, tales como: "acuerdos de confidencialidad y cláusulas contractuales que garanticen la privacidad de la información incluso en caso de reidentificación; compromisos de mantenimiento de la anonimización de la información suscritos con los posibles destinatarios de la misma, así como de no realizar ninguna acción para la reidentificación; o auditorías de uso de la información anonimizada"[472].

Se desprende que, el RGPD no afectará a la referida información anónima, incluso si la misma es destinada con fines estadísticos o de investigación, siendo esto una gran ventaja y garantía para el *big data* y, en concreto, para el *big data* en el sector sanitario destinado a fines de investigación y estadísticos con el objeto de recopilar información y conocimiento a efectos de hacer efectiva una medicina predictiva. De igual modo, la LOPDGDD, establece una cierta seguridad a la seudonimización con fines de investigación en salud pública y biomédica, siempre que "exista una separación técnica y funcional ante el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la identificación" y que los datos seudonimizados sean accesibles al equipo de investigación cuando exista un compromiso expreso de confidencialidad y se adopten medidas de seguridad para evitar la reidentificación y el acceso a terceros no autorizados[473].

Otra de las garantías a destacar de la técnica de seudonimización es, la eficaz reducción de aquellos riesgos a los que los interesados afectados puedan verse sometidos, así como la íntegra seguridad del interesado del cumplimiento estricto por parte de los responsables y los encargos del tratamiento de sus obligaciones de protección de los datos, de ahí que, la introducción de la técnica de "seudonimización" en el RGPD, en ningún caso excluye medida alguna relativa a la protección de los datos[474]. A su vez, otra de las ventajas a destacar de la seudonimización en el sector sanitario es la que señala, DE MONTALVO JÄÄSKELAÄINEN:

---

reutilización de datos de salud y datos genéticos". (MIRALLES LÓPEZ, "Desvinculación datos personales: seudonimización, desidentificación y…", *op. cit.*, p. 9)

[472] *Vid.* al respecto Agencia Española de Protección de Datos. *Código de buenas prácticas en protección de datos para proyectos Big Data,* p. 26.

[473] A tenor de lo establecido en la D.A. 17ª. 2.d. de la LOPDGDD.

[474] Así pues, ÁLVAREZ RIGAUDAS ha defendido que: "[…] tratar de aplicar las técnicas de anonimización más apropiadas para mantener el valor científico del dato (lo que excluye en muchos casos la completa e

"Ciertamente, el interés general no permite el sacrificio del derecho individual, en este caso, el derecho a la intimidad y a la protección de datos del sujeto cuyos datos pretenden ser usados en beneficio de la salud de terceros. Sin embargo, sí cabe una decisión ponderada en la que la limitación a tal derecho sea capaz de superar el test de proporcionalidad. Y en relación con dicho test, el subprincipio de proporcionalidad en sentido estricto puede quedar salvaguardado, una vez acreditada que la medida es idónea y necesaria, lo que no debe ofrecer mayores dificultades, a través de una medida que permita salvaguardar el núcleo esencial del derecho. Así, la nueva figura de la seudonimización creemos que es la fórmula que permite superar en el conflicto concreto la proporcionalidad" [475].

Así pues, a efectos ejecutar la técnica de la seudonimización en el tratamiento de datos personales, es necesario poder regular una serie de medidas en relación a la misma, de tal modo, que permita a su vez que el responsable del tratamiento pueda realizar un análisis general, a la hora de adoptar aquellas medidas técnicas y organizativas necesarias a fin de garantizar la aplicación del RGPD al tratamiento correspondiente, manteniendo de manera independiente aquella información adicional en relación a los datos personales de una persona física concreta, indicando en todo momento el responsable del tratamiento de datos personales las personas autorizadas[476].

---

irreversible anonimización) y la protección de la confidencialidad del paciente". Así, "la seudoanonimización es precisamente un estándar obligatorio en los ensayos clínicos en la Unión Europea (y en muchas otras regiones del globo), precisamente para evitar o hacer más difícil la completa identificación del paciente, que suele ser irrelevante para la investigación científica (no así para la prestación sanitaria o para preservar la seguridad de medicamentos o dispositivos sanitarios). Es más, en un ensayo clínico, el/la investigador/a principal es quien está obligado/a a realizar la codificación y a conservar la tabla de conversión confidencial, sin que el/la promotor/a del ensayo pueda acceder a la tabla de conversión y, por ello, a los datos personales de origen (salvo en casos excepcionales)"; ÁLVAREZ RIGAUDAS, "Tratamiento de datos de salud…", *op. cit.,* pp. 180-181. Sin embargo, ÁLVAREZ RIGAUDAS, por una parte, critica que se establezca que "los datos seudonimizados siguen siendo datos personales, sin matizar la situación respecto de quien tiene acceso a los datos sin la capacidad legal o real de acceder a la tabla de conversión"; y, por otra parte, aludiendo que la seudonimización es una medida de seguridad considera que el RGPD acaba con la "estéril discusión mantenida por algunas autoridades de control bajo la Directiva 95/46/CE de la necesidad de contar con una causa de legitimación propia para llevar a cabo el tratamiento consistente en la seudoanonimización o anonimización (quedando claro que ya no es necesario)", ÁLVAREZ RIGAUDAS, "Tratamiento de datos de salud…", *op. cit.,* p. 184.

[475] DE MONTALVO JÄÄSKELAÄINEN, F., "Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del *Big Data"*, *Revista de Derecho Político,* núm. 106, septiembre-diciembre, 2019, p. 54.

[476] En este sentido el informe *Datos abiertos y sanidad: contexto tecnológico, actores implicados y marco jurídico*, Iniciativa Aporta impulsada por el Ministerio de Economía y Empresa, a través de la Entidad Pública Empresarial Red.es, y en colaboración con el Ministerio de Política Territorial y Función Pública,

La citada técnica de seudonimización de datos se encuentra estrechamente vinculada con el principio de minimización da datos como garantía que asegura la aplicación de medidas técnicas y organizativas del tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a efectos de que el responsable pueda asegurar un tratamiento que no permita identificar a los interesados, o que ya no lo permita.

A modo de excepción, el artículo 11 del Reglamento establece que el responsable del tratamiento no está obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir con lo regulado en el RGPD cuando se trate de datos anónimos, esto es, de datos personales tratados que no le permiten al responsable identificar a una persona física. En este sentido, la LOPDGDD en la disposición adicional decimoséptima en su apartado 2.b) autoriza a las autoridades sanitarias e instituciones públicas con competencias de salud pública a llevar estudios sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública. A pesar de que la finalidad se encuentra más que justificada desde un punto de vista jurídico y social – que es lo que en el presente trabajo se defiende - no podemos obviar que tales acciones conllevarían de manera inevitable e implícita una vulneración involuntaria del deber de secreto profesional por parte de los profesionales sanitarios. Por ello, a efectos de evitar la vulneración a la obligación de secreto profesional por parte de los profesionales sanitarios, así como el derecho a la intimidad del paciente – como se expondrá más adelante - tanto el legislador europeo como el legislador español, a modo de previsión, regulan la técnica de la seudonimización como técnica lícita del uso de los datos con fines de investigación en salud y, en particular, biomédica y farmacéutica.

En concreto, en el aspecto de confidencialidad, asunto que nos atañe, en la LOPDGDD se requiere a efectos de licitud, lo siguiente: por un lado, "una separación técnica y funcional entre el equipo de investigación y quienes realicen la

p. 28, señala que: "La exigencia de anonimización debería proyectarse especialmente sobre aquellos supuestos en que los datos de las personas usuarias de los servicios se pongan a disposición de una tercera parte ajena a la relación asistencial con el prestador principal del servicio sanitario que pretende reutilizar los datos para otra finalidad. En definitiva, teniendo en cuenta la singularidad del elemento tecnológico, el efectivo respeto de las normas de seguridad y de anonimización de los datos constituye una premisa ética y jurídica indiscutible sin cuyo estricto cumplimiento no debería admitirse la reutilización de los datos sanitarios, pues de lo contrario existiría un riesgo inadmisible para los derechos fundamentales y las libertades públicas".

seudonimización y conserven la información que posibilite la reidentificación." y, por otro lado, "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"[477].

Por consiguiente, de este modo los profesionales sanitarios y, en consecuencia la Administración Pública sanitaria y otros organismos privados que faciliten el acceso a los datos a quienes realicen la seudonimización y conserven la información de los pacientes, no incurrirán en el incumplimiento de la obligación del secreto profesional y confidencialidad de los datos, puesto que serán conocedores con certeza y seguridad que por exigencias legales quienes accedan a los datos de los pacientes para efectuar la seudonimización estarán separados tanto técnicamente como funcionalmente del equipo de investigación que posteriormente los trate y, de la existencia de contrato de confidencialidad y de no realizar actividad de reidentificación celebrado entre el equipo de investigación y la entidad (pública o privada) encargada de seudonimizar los datos personales, así como que se adoptaran medidas de seguridad específicas a efectos de evitar reidentificación alguna de los pacientes y el acceso de terceros no autorizados.

En consecuencia, se estaría respetando el derecho de la intimidad del paciente a pesar de que inevitablemente se continúa asumiendo un riesgo, puesto que la técnica de seudonimización no asegura una anonimización absoluta de los datos sanitarios, ya que es posible recuperar la identificación o la reidentificación del titular de los mismos, tal y como los especialistas en análisis de *big data* nos vienen confirmando. Extremo este que no tiene que ser valorado únicamente de manera negativa, puesto que, si bien es cierto que la recuperación de la identidad del paciente puede suponer una vulneración de su derecho a la intimidad, a su vez, es apreciado plausiblemente por la LOPDGDD, que en caso de que posteriormente se aprecie en la investigación que se desarrolle una existencia de peligro real y concreto para la seguridad o salud del titular o, suponga una amenaza grave para sus derechos, se permite que se proceda a la reidentificación de los datos en su origen a efectos de garantizar al mismo una adecuada asistencia sanitaria[478].

[477] Disposición Adicional decimoséptima de la LOPDGDD.

[478] Último párrafo del apartado 2.d) de la Disposición adicional decimoséptima de la LOPDGDD se establece que: "Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de

Por lo que es fundamental delimitar y definir la particularidad otorgada por el RGPD a las técnicas de anonimización y seudonimización como garantías para los derechos y libertades de los interesados, destacándose la exigencia legal de utilizar las citadas técnicas en el tratamiento de los datos sanitarios con fines de investigación[479].

No hemos de olvidar que el grupo de trabajo del artículo 29 en su Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril de 2014, concluye que las técnicas de anonimización pueden aportar garantías de privacidad y usarse para generar procesos de anonimización eficientes, pero solo si su aplicación se diseña adecuadamente, lo que significa que han de definirse con claridad los requisitos previos (el contexto) y los objetivos del proceso para obtener la anonimización deseada al mismo tiempo que se generan datos útiles. Igualmente, considera que los responsables del tratamiento deben ser conscientes de que un conjunto de datos anonimizados pueden entrañar todavía riesgos residuales para los interesados, pues: por una parte, la anonimización y la reidentificación son campos de investigación activos en los que se publican con regularidad nuevos descubrimientos y, por otra, incluso los datos anonimizados, como las estadísticas, pueden usarse para enriquecer los perfiles existentes de personas, con la consiguiente creación de nuevos problemas de protección de datos. Así pues, la anonimización no debe contemplarse como un procedimiento esporádico, teniendo el deber los responsables del tratamiento de datos de evaluar regularmente los riesgos existentes. En este sentido, MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, afirman que:

"Si se mantiene la idea de que la anonimización debe ser absoluta, será imposible alcanzarla en este ámbito porque una anonimización absoluta destruye el valor científico de los datos. Sin una aproximación contextual del riesgo razonable de reidentificación, difícilmente podremos crear grandes *data lakes* con la protección que merecen los pacientes y la seguridad jurídica requerida para la inversión en investigación"[480].

---

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".

[479] Al respecto art. 4 y art. 89.1, así como Considerandos 26 y 28 del RGPD.

[480] MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación biomédica*...", op. cit.*, pp. 283-284.

No obstante, ante el hipotético caso en el que se pudiera dar una reversión no autorizada de la seudonimización, el responsable del tratamiento debe obligatoriamente comunicar esa brecha de seguridad a la autoridad de control, de conformidad con lo establecido en el Considerando 75 del RGPD e igualmente, en el sector sanitario y de la investigación científica el responsable debe adoptar las medidas de seguridad y tratar los datos atendiendo a los principios de proporcionalidad y necesidad, sin perjuicio de que deba respetar otras normas específicas como en el caso de los ensayos clínicos, según establece el Considerando 156 del RGPD.

En suma, cabría afirmar que tanto la seudonimización, la desidentificación y la anonimización son una serie de medidas cuya finalidad es la de transformar los datos personales en otros datos cuyos titulares de los mismos no pueden ser identificados de manera directa, así pues, según sea el riego de re-identificación se aplicaran un nivel de protección u otro. En concreto: (1) en el caso de la seudonimización, que implicaría desvincular a la persona titular de los datos personales de los datos guardándose por separado toda la información con la posibilidad de que en un futuro se pueda volver a vincular (re-identificar) el riesgo dependerá de aquellos datos que puedan ser re-identificados y del uso de otras fuentes de información que permiten la re-identificación; (2) en el supuesto de la desidentificación, que supondría la desvinculación de la identificación de persona de los datos y a su vez la posterior destrucción de los datos que permitan una directa re-identificación, el riesgo es que cuando se usen otras fuentes de información no se puedan reidentificar a personas y; (3) la anonimización que implica que una vez que sea efectiva la desidentificación se aplican operaciones (funciones criptográficas, perturbación de datos, reducción de datos, etc.) a fin de impedir la re-identificación por medio de otras fuentes de información[481].

Por último, a modo de curiosidad, cabe destacar que la seudonimización y anonimización de los datos resultan sumamente relevantes en la esfera de investigación epidemiológica, la investigación que se dedica al estudio de enfermedades y todo tipo de casos relacionados con la salud. No obstante, se ha de tener en consideración que la investigación epidemiológica no siempre resulta eficaz la anonimización o la

[481] *Vid.* Web Future of Privacy Forum: https://fpf.org

seudonimización para realizarla con éxito, ya que en el caso de la epidemiología social – aquella que se realiza a efectos de mejorar la salud de la población – sin que previamente exista un riesgos o peligro grave de la salud pública - los investigadores necesitan conocer la identificación de los pacientes titulares de los datos sanitarios, acceso que debe ser permitido aún sin su consentimiento si se desea seguir avanzando en la medicina predictiva sin necesidad de que exista previamente un factor mayor como el riesgo para que se permita el acceso a los datos de salud, debido principalmente a dos motivos citados en el *Informe SESPAS*: por un lado, en la práctica no se obtiene más de un 45% o 50% de consentimientos, siendo cifras insuficientes para las investigaciones y, por otro lado, la anonimización no es solución eficiente y eficaz debido a que impide investigaciones de calidad puesto que la probabilidad de error con datos anónimos es bastante alta[482]. Igualmente, la técnica de la seudonimización puede ser beneficiosa para la investigación en los biobancos[483], como una medida aceptable que garantiza la seguridad de los datos por los arts. 32.1.a) y 89.1 del RGPD[484].

En la nueva era digital y tecnológica nos encontramos en una continua tensión entre la tecnología y las garantías jurídicas, puesto que desde un punto de vista jurídico y administrativo de gestión de los datos de salud si no podemos realizar análisis avanzado de información porque no disponemos de datos anonimizados, esto es, sino disponemos de mecanismos de anonimización para poder realizar análisis avanzados basándonos en técnicas y herramientas *big data*, tenemos un gran problema, como por ejemplo el generado en la pandemia mundial de la COVID-19 al no disponer la Administración Pública de un sistema estructurado de datos fiables y actualizados adaptado a las innovaciones tecnológicas, lo que ha generado graves deficiencias en el acceso y disposición de los datos de salud. En este sentido, VALERO TORRIJOS y CERDÁ MESEGUER, afirman que:

---

[482] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, pp. 14-15. Al respecto SERRANO PÉREZ, Mª M., SÁNCHEZ NAVARRO, C. y ZURRIAGA LLORENS, C., "A modo de reflexión y crítica en torno a la propuesta de reglamento europeo de protección de datos y algunas de las enmiendas presentadas en relación con la epidemiología y la salud", *Derecho y Salud,* vol. 23, núm. extraordinario, 2013, pp. 292-293.

[483] De conformidad con el art. 4.3. d) de la Ley 14/2007, de 3 de julio, de investigación biomédica, un Biobanco es: "aquel establecimiento público o privado, sin ánimo de lucro, que acoge una colección de muestras biológicas concebida con fines diagnósticos o de investigación biomédica y organizada como una unidad técnica con criterios de calidad, orden y destino".

[484] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 882.

"Esta dimensión se ha puesto de manifiesto de manera especialmente cruda durante la crisis generada por la pandemia de la COVID-19, donde la falta de transparencia, la no disponibilidad de datos fiables y actualizados, así como la incapacidad de la Administración Pública de afrontar los desafíos plantados sin la colaboración del sector privado nos obligan a replantear el modelo de gestión. A este respecto resulta imprescindible tener en cuenta las exigencias y posibilidades no sólo de la tecnológica sino, en particular, del Gobierno Abierto como plasmación actual del Estado democrático occidental según las exigencias actuales en el comienzo de la tercera década del siglo XXI"[485].

En definitiva, en cierto modo la normativa jurídica debe permitir una cierta interoperatividad[486] y libre circulación de los mismos, pues si limitamos la "disponibilidad de datos en formatos abiertos y reutilizables"[487] resulta imposible aplicar herramientas *big data* y, en consecuencia, estaríamos privando a los profesionales del sector de la sanidad e investigadores el acceso al conocimiento e información de inestimable valor para el sector de la medicina, de la investigación y de interés general que pueden solventar problemas dimanantes como los provocados durante la crisis ocasionada por la pandemia de la COVID-19, soluciones y respuestas

[485] VALERO TORRIJOS y CERDÁ MESEGUER, "Transparencia, acceso y reutilización de la información ante la transformación digital del sector público…", *op. cit.,* p. 105.

[486] DEL RÍO SOLÁ, M.L y y VAQUERO PUERTA C., "El impacto de la transformación digital en el sector sanitario", *Revista Española de Investigaciones Quirúrgicas*, REIQ 2019, Vol. XXII, núm. 3, p. 106, aclaran que: "Estamos avanzando hacia modelos de atención integral en la provisión de los cuidados de atención sanitaria y sociosanitaria de una forma coordinada y centrado en la persona. Para ello, se dispone hoy de nuevas herramientas que facilitan esta atención integral a las personas, como son las soluciones tecnológicas de movilidad y de sensores conectados que permiten abordar soluciones que pueden transformar la atención sanitaria".

[487] VALERO TORRIJOS, y CERDÁ MESEGUER, "Transparencia, acceso…", *op.cit*., p. 113, señalan que: "En definitiva, la necesidad de integrar sistemas de información pertenecientes a diferentes entidades sin una previa tarea de diseño y configuración más allá de las urgencias de la situación generada por la pandemia ha evidenciado la limitación del alcance del modelo puesto en marcha por lo que se refiere a las posibilidades y exigencias de la transparencia, en particular por lo que se refiere a la limitada disponibilidad de datos en formatos abiertos y reutilizables6. Se trata de un problema de singular relevancia, ya que el valor añadido se genera, sobre todo, obteniendo datos proporcionados por diversas fuentes que, como sucede con las Administraciones sanitarias, deberían establecer mecanismos de coordinación en la gestión de la información que permitan dan respuestas adecuadas ante situaciones ordinarias y, asimismo, de singular gravedad como la que se ha vivido durante los últimos meses. Así pues, la urgencia y gravedad de la crisis ocasionada por el COVID-19 ha obligado a poner en marcha un modelo de gestión que no ha sido capaz de aprovechar, al menos en su diseño inicial, el potencial de la innovación tecnológica, lo que se ha terminado proyectando en las deficiencias de la puesta a disposición de los datos…".

de gran interés para la sociedad en su conjunto, tanto para las generaciones del presente como del futuro[488].

Por ello, se estima conveniente que la ley sectorial recopile de manera taxativa los ámbitos donde es necesaria la identificación de la persona titular de los datos de salud recogidos en la historia clínica con fines de investigación epistemológica social debido a la alta probabilidad de error con datos anónimos que impiden investigaciones de calidad. En este sentido se plantea que se tenga en consideración la Orden de 26 de octubre de 2011, de Galicia, específica los criterios técnicos y/o científicos para el acceso a la historia clínica a efectos epidemiológicos y de salud pública, criterios que deben ser regulados o reiterados en la ley sectorial. En concreto, son: a) vigilancia de las enfermedades de declaración obligatoria, b) vigilancia de enfermedades a través de sistemas de información microbiológica; c) estudio y control de brotes; d) investigación de reacciones adversas a la vacunación y mejora del programa de vacunaciones; e) mejora de programas de cribado poblacional; e) registro de tumores; f) mejora de registro de mortalidad.

Igualmente, la ley deberá establecer que fuera de los citados ámbitos en los que debido a criterios técnicos o científicos epidemiológicos se requiere la identificación de la persona titular de las historias clínicas a tratar, los datos deben estar anonimizados o seudonimizados según sea el caso y la finalidad de los estudios epidemiológicos o con fines de salud pública[489].

Otros de los extremos que sería de interés que la ley de protección de datos de salud regulase como supuesto de garantía en la reidentificación, es el de la posibilidad

[488] Al respecto VALERO TORRIJOS y CERDÁ MESEGUER, "Transparencia, acceso…", *op.cit*., p. 108 afirman que: "En última instancia, se trata de superar tales limitaciones desde el potencial de la tecnología para articular soluciones que faciliten la innovación administrativa (Martín, 2018, p. 200); lo que requiere alumbrar un modelo basado en la gestión de la información a partir de su recogida masiva, así como su gestión inteligente y colaborativa (Cotino Hueso, 2017b, p. 398)".

[489]Al respecto, se ha de tener en consideración que los estudios epidemiológicos dependiendo de su temporalidad son clasificados en: retrospectivos (estudio longitudinal en el tiempo que se analiza en el presente, pero con datos del pasado, en los que generalmente se trabajó con datos anonimizados) y, prospectivos (estudio longitudinal en el tiempo que se comienza en el presente, pero los datos se analizan trascurrido un cierto tiempo, en el futuro, principalmente se trabaja con datos personalizados. Según el resultado obtenido, pueden ser, bien descriptivos, bien analíticos y esto últimos en observacionales (de prevalencia) o ensayos clínicos (de intervención). *Vid.* GÓMEZ PIQUERAS, "Disociación/anonimización de los datos de salud", *op. cit.,* p.53.

de prohibir la aplicación de procesos de reidentificación de las personas a través de asociación de datos personales a datos de salud ante casos de datos anonimizados.

Por último, se propone que a los efectos de garantizar la irreversibilidad de los procesos de anonimización de los datos personales utilizados en los proyectos de *big data*, es necesario que la ley sectorial regule el deber de las organizaciones (públicas o privadas) de valorar los riesgos de reidentificación posterior por medio de un proceso de evaluación de riesgos y aplicar la metodología de la Evaluación de Impacto de Protección de Datos (EIPD), así como gestionar los riesgos resultantes con medidas técnicas u organizativas a fin de garantizar los derechos de las personas en caso de reidentificación, tanto para el proceso de anonimización como durante todo el ciclo de vida de dichas iniciativas.

Igualmente, la ley sectorial debe contemplar el deber de las organizaciones de llevar a cabo una política de anonimización documentada y actualizada accesible al personal implicado en el tratamiento de datos anonimizados, así como el deber de implantar un protocolo de actuación del proceso de anonimización y el deber de adoptar medidas tecnológicas en el proceso de anonimización.

3. EL TRATAMIENTO DE DATOS PROCEDENTES DE MUESTRAS BIOLÓGICAS Y DE DATOS GENÉTICOS

3.1. Aspectos conceptuales

Desde la Ley Orgánica 15/1999 – derogada por la LO 3/2018 – en su artículo 7, ya constaban regulados los datos genéticos, datos biométricos y datos relativos a la salud como categorías especiales de datos personales necesitados de una protección más cualificada por ser particularmente sensibles debido a los relevantes riesgos que conlleva su tratamiento[490], por ello, el legislador europeo en el artículo 4 del RGPD establece unas definiciones genéricas sobre estos los mismos a fin de delimitar las diversas interpretaciones jurídicas que pudieran surtir en relación a su tratamiento y al

[490] Considerando 51 del RGPD.

derecho de protección de datos del titular de los mismos, definiciones que son igualmente compartidas por la LOPGDGG y, que a continuación se analizan.

A) Datos de Salud

De conformidad con el art. 4.15 del RGPD, son datos relativos a la salud, los "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud". Así pues, si desglosamos esta concepción amplia teniendo en considracion el Considerado 35 del RGPD, se podría afirmar que se incluyen[491] los siguientes datos: (1) Datos que dan información sobre el estado de salud física o mental pasado, presente o futuro; (2) Información sobre la persona física recogida en la inscripción a efectos de asistencia sanitaria, o en la prestación de esta[492]; (3) Números, símbolos o datos asignados a una persona física que la identifique de manera unívoca a efectos sanitarios; (4) Información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas y; (5) Cualquier otra información, precedente de enfermedades, discapacidades, así como el riesgo de padecerlas, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, procedente de cualquier médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Asimismo, el concepto de dato de salud también se amplía a aquellos datos que cumplan con algunos de las siguientes particularidades[493]: a) datos inherente o claramente de naturaleza medica; b) datos en bruto de los sensores, que se pueden usar por si mismos o combinándolos con otros datos para llegar a una conclusión respecto

[491] Considerando 35 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 datos personales y a la libre circulación de estos datos.

[492] Conforme establece la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88, p. 45).

[493]Grupo de Trabajo Artículo 29, *Annex: Health data in apps and devices,* 5 de febrero de 2015. Disponible en: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (última consulta 05/12/20), DE MIGUEL BERIAIN, I. y DE LORENZO Y APARICIO, R., *Claves prácticas sanitarias. Datos genéticos y relativos a la salud,* Francis Lefebvre, Madrid, 2020, p. 30.

del estado de salud o el riesgo de la salud de una persona; c) conclusiones inferidas sobre el estado o el riesgo de salud de una persona, con independencia de que estas conclusiones sean legítimas, adecuadas u oportunas[494]. De igual modo, el TEDH en la sentencia de 25 de enero de 1997 señala que:

"[…] el respeto al carácter confidencial de las informaciones sobre la salud, constituye un principio esencial del sistema jurídico de todas las Partes contratantes del Convenio. Es importante no solo para proteger la vida privada de los enfermos sino igualmente para preservar la confianza en los profesionales de la medicina y de los servicios de salud en general" donde una divulgación no consentida, puede conllevar "consecuencias desastrosas sobre la vida privada y familiar de la persona concernida y sobre su situación profesional, exponiéndola a su desaprobación y a un riesgo de exclusión".

En definitiva, de acuerdo con el criterio reiterado del Grupo de Trabajo del Artículo 29, el concepto de dato relativo a la salud es un concepto amplio que incluye múltiples fuentes y diferentes tipos de formas[495], no solo los pertenecientes a la esfera de la asistencia sanitaria a través de las historias clínicas, sino también al ámbito laboral, asegurador, deportivo, entre otros, lo que en consecuencia que se apliquen igualmente en estos ámbitos las medidas para su tratamiento que se aplican al ámbito estrictamente sanitario.

---

[494] Por ejemplo, el TJUE en la sentencia de fecha 6 de noviembre de 2003, asunto Lindqvist, consideró que es un dato de carácter personal relativo a la salud la referencia sobre una persona que se encuentra de baja laboral porque se ha lesionado un pie.

[495] Al respecto, DE MIGUEL BERIAIN y DE LORENZO Y APARICIO, *Claves prácticas sanitarias. Datos genéticos y…, op. cit.,* p. 30, aclaran que: "Estas precisiones no son suficientes para determinar la amplitud del concepto. De hecho, durante mucho tiempo han persistido (y probablemente aún persistan) dudas razonables sobre si un tipo de dato en concreto debería considerarse o no como dato relativo a la salud. Esto se debe, entre otras cosas, a que la propia definición de salud es compleja y/o a que son muchas las formas de caracterizarla, algunas de ellas tan amplias como la que nos proporciona el marco jurídico de la OMS, que considera que debe igualarse la salud a un estado de bienestar general". Asimismo, PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 875 citando a PÉREZ GÓMEZ, J. M., "El concepto de dato de salud y otras categorías afines de datos en el proyecto de Reglamento Europeo de Protección de Datos", *Actualidad de Derecho sanitario,* núm. 225, 2015, señala que. "el concepto de dato de salud se aplica a los datos personales cuando tienen una relación clara y estrecha con la descripción del estado de salud de una persona: los datos sobre el consumo de medicamentos, alcohol o drogas, así como los datos genéticos, son sin duda datos personales sobre la salud, especialmente si están incluidos en un expediente médico, en incluso, todo dato incluyendo alguno de carácter administrativo que se encuentren en los historiales clínicos".

En este sentido, debido a la relevancia jurídica de delimitar el concepto de datos de salud, se propone que, como punto de partida, la ley de protección de los datos de salud ofrezca una definición concisa sobre los datos relativos a la salud[496], a los efectos de proporcionar una normativa transparente, concisa y clara en lo que a su contenido respecta.

Como se ha podido apreciar, los datos de salud son datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios sanitaria, que revelen información sobre su estado de salud. No obstante, en la propuesta de ley específica de protección de datos cabría diferenciar entre los términos "datos médicos", "datos sanitarios" y "datos relativos a la salud o de salud" a efectos de delimitar el contenido de cada uno de ellos digno de ser regulado por la ley sectorial de protección de datos de salud. Por ende, podría afirmarse que el dato médico es aquella información generada por un facultativo sanitario[497], por otro lado, el dato sanitario es aquella información que se genera ante organismos sanitarios públicos o privados, incluyéndose al personal administrativo y al personal de investigación[498] y, por último, el dato de salud o dato relativo a la salud, como se ha visto anteriormente, es un concepto más amplio que engloba todas las informaciones que se generan el sector sanitario[499].

---

[496] JOVE VILLARES, D., "Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización"*, Revista Derecho y Salud*, núm. 1, 2017, p. 58, afirma que: "la concreción jurídica de la categoría dato de salud es uno de los desafíos que el legislador debe afrontar. Para ello, deberá procurar no caer en reduccionismos que puedan excluir determinadas informaciones que merecerían protección y, al mismo tiempo, ha de evitar incurrir en generalidades que acaben desnaturalizado la categoría datos especiales".

[497] Recomendación núm. R (97) 5 del Consejo de Europa sobre la protección de datos médicos de 13 de febrero de 1997 en el apéndice 1, define los datos médicos como "todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tenga una clara y estrecha relación con la salud y los datos genéticos".

[498] AA.VV., *La Ética y el Derecho ante la biomedicina del futuro,* Universidad de Deusto, Bilbao, 2006, p. 141.

[499] Al respecto, MIRALLES LÓPEZ, "Desvinculación datos personales: seudonimización, desidentificación y…", *op. cit.*, p.7 señala que: "Con el RGPD el legislador Europeo ha redefinido los datos relativos a la salud, obviamente manteniendo su esencia, en cuanto a que se refieren a la salud física y mental de una persona, pero pasando también a ser considerados como tales las informaciones derivadas de la prestación de los servicios de atención sanitaria, en tanto puedan revelar el estado de salud de las personas. Por tanto incluye información sobre la persona, recogida con ocasión de su inscripción en registros a efectos de asistencia sanitaria o con ocasión de la propia prestación de la asistencia; también cualquier número, código, símbolo o dato «asignado a una persona física que la identifique de manera unívoca a efectos sanitarios»; y continúa describiendo el considerando 35 del RGPD «la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una

En este sentido, debido a que los tres conceptos son empleados indistintamente tanto en el ámbito sanitario como en el jurídico, cabría exigir a la nueva ley sectorial acotar una definición precisa de los mismos al representar cada uno de ellos situaciones diferentes, a fin de "distinguir a determinadas categorías e informaciones como merecedoras de una protección reforzada. Qué tipologías de datos deben ser la incluidas y cuáles las descartadas es la decisión verdaderamente delicada y crucial que el legislador debe afrontar"[500], tomándose como criterio "el nivel de riesgo que el tratamiento de esos datos pueda suponer para otros derechos fundamentales[501].

B) Datos genéticos

El artículo 4.13 del RGPD, define los datos genéticos como datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona. Por consiguiente, los datos genéticos son aquellos datos personales que guardan relación con ciertas características genéticas, heredadas o adquiridas, de una persona física, provenientes de análisis de una muestra biológica de la persona física en cuestión, en concreto mediante un análisis cromosómico, un análisis de ácido desoxirribonucleico (ADN) y, un análisis de ácido ribonucleico (ARN) o, un análisis de cualquier otro elemento que permita obtener información equivalente[502].

De los anterior, según DE MIGUEL BERIAIN y DE LORENZO Y APARICI se pueden sustraer tres características fundamentales de los datos genéticos: (1) Proporcionan información sobre una persona física; (2) Proporcionan información sobre la salud y la

---

discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro»".

[500] JOVE VILLARES, "Datos relativos a la salud…", *op. cit.,* p. 60.

[501] JOVE VILLARES, "Datos relativos a la salud…", *op. cit.,* p. 64.

[502] Considerando 34 del RGPD.

fisiología del interesado; (3) Proceden del análisis de una muestra biológica de la persona en cuestión[503].

Por otro lado, el art. 3 j) de la Ley 14/2007, define el dato genético de carácter personal, como la información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros científicos. De igual modo, la Declaración Internacional sobre datos genéticos humanos de 16 de octubre de 2003 acordada en el seno de la UNESCO, en el artículo 4, señala que:

"[…] los datos genéticos humanos son singulares por su condición de datos sensibles, toda vez que pueden indicar predisposiciones genéticas de los individuos y que esa capacidad predictiva puede ser mayor de lo que se supone en el momento de obtenerlos; pueden tener para la familia, comprendida la descendencia, y a veces para todo el grupo, consecuencias importantes que persistan durante generaciones; pueden contener información cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas; y pueden ser importantes desde el punto de vista cultural para personas o grupos".

Al respecto, el Grupo de Trabajo del art. 29, en su documento de trabajo sobre datos genéticos, de 17 de marzo de 2004, señala que una correcta protección de los datos genéticos es condición previa a efectos de garantizar el respeto del principio de igualdad y salvaguardar el derecho a la salud[504].

Por último y, no menos importante, una vez analizados ambos conceptos, dato de salud y dato genético, se ha de destacar que lo que diferencia a ambos es que, el dato genético se encuentra más vinculado al ámbito de la investigación científica, civil o criminal, y en la esfera de la asistencia sanitaria al diagnóstico. Por consiguiente, nos

[503] DE MIGUEL BERIAIN y DE LORENZO Y APARICIO, *Claves prácticas sanitarias. Datos genéticos y…, op. cit.,* p. 31, señalan diversos problemas prácticos de estas características, en concreto: "- En realidad, los datos genéticos no solo afectan a la persona de la que se extrae la muestra, sino que proporcionan información sobre otras muchas relacionadas biológicamente con él o ella; - Hay que tener prsente que estos datos no solo proporcionan datos sobre la salud o fisiología de las personas, sino también sobre sus vínculos familiares y su origen étnico, lo que puede tener importantes consecuencias (TEDH 4-12-08, S. y Marper C. Reino Unido, 30562/04 y 30566/04); - Cabe recordar que el análisis del material genético propio no es la única fuente de datos genéticos del interesado".

[504] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 877.

encontramos ante categorías diferentes de datos, aunque el RGPD le aplica de manera general la misma normativa[505], motivo por el que en el presente trabajo se trata de manera general los datos relativos a la salud, además de por evidentes motivos puramente pragmáticos.

C) Datos biométricos

Los datos biométricos, de conformidad con el artículo 4.14 del RGPD, consisten en "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Asimismo, en el *Informe Jurídico 0342/2009* emitido por la AEPD los datos biométricos son definidos como "aquellos aspectos físicos que, mediante un análisis técnico, permiten distinguir las singularidades que concurren respecto e dichos aspectos y que, resultando que es imposible la coincidencia de tales aspectos en dos individuos, una vez procesados, permiten servir para identificar al individuo en cuestión (tales como huellas digitales, el iris del ojo, la voz, etc.)". Posteriormente, la AEPD en el *Informe 36/2020 sobre los procesos de reconocimiento facial empleados para la realización de evaluaciones*, ha aclarado que únicamente se ha de reconocer los datos biométricos como categoría especial de datos cuando el tratamiento técnico específico permita identificar de manera univoca a una persona física.

De igual modo, el TJUE considera los datos biométricos procedentes de las impresiones dactilares, datos de carácter personal debido a que contienen información única por la que podemos identificar de manera precisa y concreta a una persona[506].

[505] No en vano, se ha de hacer constar tal y como aclaran DE MIGUEL BERIAIN y DE LORENZO Y APARICIO, *Claves prácticas sanitarias. Datos genéticos y…, op. cit.,* p. 31, que: "[…] puede no ser así. Por ejemplo, los datos genéticos recabados para establecer la filiación de un individuo, o los que se emplean para investigaciones criminales difícilmente podrán considerarse como datos de salud. Del mismo modo, es obvio que muchos datos de salud no tendrán en ningún caso la consideración de datos genéticos".

[506] STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz), apartado 27: "Las impresiones dactilares están comprendidas en este concepto por contener objetivamente información única sobre personas físicas y permitir su identificación precisa (*Vid.*, en este sentido, en particular, TEDH, sentencia S. y Marper c. Reino Unido, de 4 de diciembre de 2008, Recueil des arrêts et décisions 2008-V, p. 213, § 68 y 84)".

Finalmente, el Grupo de Trabajo del art. 29, en el Dictamen 3/2012, sobre la evolución de las tecnologías biométricas, de 27 de abril de 2012, afirma que los datos biométricos pueden contribuir a aumentar el nivel de seguridad y a facilitar, acelerar y simplificar los procedimientos de identificación y autentificación.

3.2. El tratamiento de datos personales procedentes de muestras biológicas

A efectos de analizar el consentimiento para el tratamiento de datos personales procedentes de muestras biológicas obtenidas con fines de investigación biomédica hemos de partir de la Ley 14/2007, de 3 de julio, de Investigación biomédica, pues a pesar de que cabría interpretar que el consentimiento para su tratamiento va implícito en el consentimiento informado para su obtención[507], el artículo 58 del citado texto legal establece que "el consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización", añadiendo el artículo 60 Ley 14/2007, que "el consentimiento sobre la utilización de la muestra biológica se otorgará, bien en el acto de obtención de la muestra, bien con posterioridad, de forma específica para una investigación concreta".

Por otro lado, el art. 58 Ley 14/2007 en relación con el artículo 23 del RGPD, establece un límite al consentimiento, señalando que "de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i) de esta Ley. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación correspondiente, el cual deberá tener en cuenta, como mínimo, los siguientes requisitos: a) Que se trate de una investigación de interés general; b) Que la investigación se lleve a cabo por la misma institución que solicitó el consentimiento para la obtención de las muestras; c) Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente; d) Que no conste una objeción expresa del mismo; e) Que se garantice la confidencialidad de los datos de carácter personal".

[507] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 900.

Por último, la AEPD en su *Informe 73677/2018*, afirma que el RGPD no supone alteración alguna al marco normativo actualmente vigente en España en relación con el tratamiento de datos en el marco de la investigación biomédica, en el sentido de que dichos datos podrán seguir siendo tratados en los términos establecidos en la Ley 14/2007. No en vano, el citado informe ha obtenido diversas críticas por parte de juristas y profesionales del ámbito sanitario al entenderse de que la AEPD únicamente hace mención a la investigación biomédica, dejando al margen otros ámbitos del sector sanitario donde son utilizados datos de salud, datos genéticos y datos biométricos, como pudiera resultar la investigación farmacéutica, como se verá más adelante.

Así pues, en relación con el consentimiento del interesado para la investigación con muestras biológicas, se estima pertinente que la ley de protección de datos de salud refleje que, en el caso de la investigación con muestras biológicas, de manera general es obligatorio el consentimiento del paciente, se apliquen o no técnicas de anonimización. De igual modo, la ley sectorial ha de tener en consideración los siguientes extremos[508]:

De un lado, la posibilidad de que el consentimiento prestado por el sujeto fuente puede cubrir – siempre y cuando se haya informado al mismo previamente a la prestación del consentimiento – investigaciones que se realicen posteriormente relacionadas con la inicial, incluidas las realizadas por terceros y las cesiones de datos o muestras identificados o identificables, pero en ningún caso, podrán ser utilizados para estudios de investigación biomédica si el consentimiento fue prestado exclusivamente para fines diagnósticos y terapéuticos. De contrario, en caso de falta de información previa complementaria y cuando el consentimiento por el sujeto fuente haya sido prestado exclusivamente para la utilización de una investigación determinada, será necesario en todo caso solicitar un nuevo consentimiento informado al sujeto fuente; de otro lado, el derecho de restricción del sujeto fuente sobre el uso de las muestras; y en tercer lugar, las excepciones donde no es necesario el consentimiento del sujeto fuente para el tratamiento muestras codificadas o identificadas con fines de investigación, esto es: a) cuando no sea posible el consentimiento o; b) cuando suponga un esfuerzo razonable, lo que significa que suponga invertir una cantidad desproporcionada de

[508]De conformidad con el art. 58 de la Ley 14/2007, de 3 de julio, de Investigación biomédica.

tiempo, gastos y trabajo[509], siendo necesario en todo caso, el dictamen favorable del Comité de Ética de la Investigación.

3.3. El tratamiento de datos genéticos

Al igual que sucede con el tratamiento de datos personales procedentes de muestras biológicas, para el tratamiento de datos genéticos también nos tenemos que remitir al contenido de la Ley 14/2007[510], donde en relación con el consentimiento, el art. 48.1 exige que "el consentimiento expreso y específico por escrito para la realización de un análisis genético" añadiendo en el apartado tercero del citado precepto que "para acceder a un cribado genético será preciso el consentimiento explícito y por escrito del interesado. El Comité de Ética de la Investigación determinará los supuestos en los que el consentimiento podrá expresarse verbalmente. En todo caso, cuando el cribado incluya enfermedades no tratables o los beneficios sean escasos o inciertos, el consentimiento se obtendrá siempre por escrito".

Por otro lado, el art. 50 de la Ley 14/2007, en su apartado segundo y tercero señala que "los datos genéticos de carácter personal sólo podrán ser utilizados con fines epidemiológicos, de salud pública, de investigación o de docencia cuando el sujeto interesado haya prestado expresamente su consentimiento, o cuando dichos datos hayan sido previamente anonimizados. En casos excepcionales y de interés sanitario general, la autoridad competente, previo informe favorable de la autoridad en materia de protección de datos, podrá autorizar la utilización de datos genéticos codificados, siempre asegurando que no puedan relacionarse o asociarse con el sujeto fuente por parte de terceros".

Por último, el artículo 52 de la Ley 14/2007, establece un plazo general de conservación de los datos genéticos de cinco años desde la fecha de su obtención, no obstante, "los datos únicamente podrán conservarse, con fines de investigación, de

[509] De conformidad con lo establecido en el art. 24 del Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos.

[510] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 901.

forma anonimizada, sin que sea posible la identificación del sujeto fuente" (art. 52.3 Ley 14/2007).

4. LA UTILIZACIÓN DE LOS DATOS DE SALUD POR PARTE DE LA PROPIA ADMINISTRACIÓN PÚBLICA SANITARIA O A TRAVÉS DE UN TERCERO PARA OTROS FINES DISTINTOS AL ASISTENCIAL

Por último, a modo de clausura del presente epígrafe sobre el principio de finalidad y del tratamiento ulterior de los datos de salud, se estima conveniente tener presente desde un punto de vista jurídico la distinción entre la utilización de los datos sanitarios por parte de la propia administración sanitaria en calidad de responsable del tratamiento y, por otro lado, la utilización de los datos a través de un tercero (persona física o jurídica) que accede a los ficheros y/o registros de la administración sanitaria para un tratamiento ulterior de los mismos, bien con fines distintos al asistencial de interés para la propia administración sanitaria y los pacientes, bien para fines externos de interés general como podrían ser proyectos de investigación científica de desarrollo de un fármaco o tratamiento como el de la vacuna para la COVID-19, incluyéndose en este término además de otros centros sanitarios públicos o privados, las entidades mercantiles cuyo objeto de su actividad sea la analítica de datos a través de herramientas *big data* u otras tecnologías (*v.gr.* IA).

En este sentido, dependiendo de que los datos de salud sean utilizados de manera interna o externa para otros fines distintos al asistencial la base jurídica será diferente, en el sentido de que, si los datos son utilizados por la propia administración sanitaria a *nivel interno*, pero para otros fines distintos al asistencial resultará suficiente aplicar técnicas de seudonimización siguiendo las medidas y garantías estatuidas en el RGPD y en la LOPDGDD, pues no obviemos que se tratan de datos personales. Sin embargo, cuando los datos sean utilizados a nivel externo por un tercero (entidades u organismos privados) distintas a la propia administración sanitaria responsable del registro/fichero donde se encuentren registrados los datos de salud, deberá ser necesario aplicar técnicas de anonimización de los datos de salud a efectos de garantizar a su titular una mayor seguridad y protección de los mismos.

De igual modo, ante una utilización a nivel externo de los datos de salud por parte de un tercero cabe diferenciar nuevamente si ese tercero va a utilizar de manera exclusiva los datos de salud para una finalidad interna objeto de su actividad mercantil/profesional[511] o para cedérselos a otra entidad u organismo privado externo a fin de prestar un servicio o desarrollar un proyecto concreto de interés general o de salud pública[512], pues evidentemente según sea uno u otro el supuesto de hecho las garantías y medidas tecnológicas y jurídicas serán diferentes, siendo las del segundo caso más estrictas y limitadas. En todo caso, en ambas situaciones, el tercero que accede a los datos sanitarios de la Administración Pública no podrá explotar los mismos para otros fines distintos a la finalidad que de manera exclusiva y excluyente por la que se le haya permitido su utilización y tratamiento tras acreditar previamente el fin de interés general o de salud pública.

En consecuencia, debido a que lo anterior no consta regulado en su mayor parte en la normativa vigente de protección de datos ni comunitaria ni estatal, en el presente trabajo serán desarrolladas – como se apreciará más adelante – las garantías y medidas mínimas de protección de datos para proyectos de salud pública e investigación científica que apliquen herramientas *big data* como parte del contenido mínimo que debe regular la ley sectorial específica de protección de datos de salud, donde se tratará entre otros extremos, propuestas de técnicas de anonimización y seudonimización apropiadas, algunas cuestiones legales del tratamiento de *big data*, como el ámbito de aplicación material, las garantías sobre el consentimiento, el principio de transparencia, cuestiones legales acerca del responsable y el encargado del tratamiento, sobre la calidad y conservación de los datos de salud, derechos de los interesados, decisiones automatizadas y, otras garantías que se han de dar en los procedimientos del tratamiento de *big data* sanitario, así como medidas técnicas y de seguridad del tratamiento.

[511] Algunos ejemplos a citar serían el hospital que contrata una empresa de tecnología para desarrollar un programa para el hospital, la empresa farmacéutica que accede a los datos de salud de la administración sanitaria para desarrollar un fármaco (vacuna, medicamento…) de interés general, los pacientes derivados por el servicio público a los servicios concertados en ese caso el concertado no puede explotar los datos de salud para otros fines o, las empresas de análisis de datos contratadas directamente por la Administración Pública a fin de que accedan a los datos de salud para substraer de los mismos una determinada información y conocimiento, acceso que se podrá permitir siempre y cuando estos terceros cumplan con las medidas y garantías técnicas y legales.

[512] En este caso, un claro ejemplo sería el de la entidad privada que necesita utilizar los datos de salud de la Administración Pública sanitaria para un proyecto de investigación de interés general o salud pública que a su vez contrata a una empresa especializada en el análisis de datos por medio de aplicación de herramientas *big data*.

Así pues, se puede concluir que para el tratamiento de los datos personales y de salud en proyectos *big data* debe ser recabado el consentimiento del interesado/paciente de manera libre, explícita y por medio de solicitud escrita de forma inteligible, de fácil acceso y empleándose un lenguaje claro y sencillo, teniendo el derecho el interesado de retirar el mismo en cualquier momento[513].

No obstante, en caso de imposibilidad para recabar el consentimiento del interesado en las condiciones anteriormente señaladas, debido principalmente a situaciones de datos masivos de datos de salud procedentes de fuentes dispersas, de manera exclusiva, si nos encontramos ante proyectos de asistencia sanitaria de interés público e investigación biomédica donde conste acreditado el interés general, para el caso del consentimiento del interesado se propone que la ley sectorial específica de protección de datos sanitarios y aplicación de herramientas *big data* regule la posibilidad de poder sustituir el consentimiento por la autorización del Comité de Ética de la Investigación, quien deberá realizar una evaluación previa y de control al respecto, principalmente a fin de:

Por un lado, garantizar la inexistencia en el proyecto de fines incompatibles, dado que este extremo no siempre es posible conocerlo desde los inicios del proyecto donde se apliquen herramientas de *big data*, ya que es habitual los tratamientos posteriores con finalidades adicionales a la finalidad original, sobre todos si nos encontramos ante proyectos de salud pública o investigaciones científicas. A tales efectos, se recuerdan los criterios que establece el Grupo de Trabajo del Artículo 29 en su Dictamen sobre el principio de finalidad (WP 203), así como el art. 6.4 del RGPD, a fin de determinar si los usos posteriores de los datos personales son compatibles con la finalidad principal para la que fueron recabados, criterios orientativos a tener en consideración por parte del Comité de Ética de la Investigación, en concreto: (1) debe existir una relación entre la finalidad original y la finalidad o finalidades ulteriores; (2) el tratamiento ulterior debe encontrarse dentro de las expectativas razonables del interesado; (3) debe tenerse en cuenta la naturaleza de los datos objeto de tratamiento y la sensibilidad de los mismos; (4) debe considerarse el impacto que este tratamiento va

[513] Art. 7 RGPD.

a tener en los interesados y; (5) deben considerarse las medidas de protección que el responsable del tratamiento establece, en particular, las medidas técnicas y organizativas: encriptación, seudonimización, separación funcional, transparencia, oposición de al tratamiento, entre otras.

Por otro lado, garantizar que los datos recogidos para el tratamiento son adecuados, pertinentes y limitados en relación con los fines determinados, explícitos y legítimos de conformidad con el principio de minimización de datos, teniendo presente ante todo que los datos recabados necesarios y, por consiguiente, no son excesivos en relación con la finalidad principal del proyecto, así como que el tiempo de conservación no es desmesurado ni desproporcional.

Por último, a efectos de garantizar que el responsable y el encargado del tratamiento (en su caso), han adoptado las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, debiendo evaluar la Comisión de Ética de Investigación ante todo la existencia o no de riesgos asociados a destrucción, pérdida o alteración o, de acceso de terceros no autorizados. Así como garantizar, la existencia de límites del tratamiento de los datos por parte del responsable y el respeto de los derechos de acceso, rectificación, cancelación y oposición de los titulares de los datos de salud.

CAPÍTULO CUARTO

GARANTÍAS JURÍDICAS DEL DERECHO DE PROTECCIÓN DE LOS DATOS RELATIVOS A LA SALUD EN LA NORMATIVA VIGENTE

El presente capítulo guarda una estrecha vinculación con el anterior, no obstante, se ha decido desarrollar en capítulo aparte las garantías reguladas en la normativa vigente de protección de datos más influyentes en el sector sanitario a los efectos de salvaguardar el derecho de protección de datos de los pacientes o, de sus familiares para el caso de datos de personas fallecidas[514].

[514] TRONCOSO REIGADA, "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…", *op. cit.*, p. 196, afirma que: "[…] el RGPD, lejos de impedir las ventajas que el recurso a las nuevas tecnologías supone para la asistencia sanitaria, para la salud pública y para la investigación, lo que hace es poner el énfasis en fortalecer las garantías que conforman el derecho fundamental a la protección de los datos personales, atribuyendo a las personas –a los pacientes- un mayor control sobre sus datos personales sometidos a tratamiento". Igualmente, TRONCOSO REIGADA, A., "Autoridades de control independientes," en AA.VV., *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, p. 462.

De igual modo, se destacarán las limitaciones de la normativa vigente proponiéndose a su vez aquellas cuestiones específicas que deberían ser reguladas en una ley sectorial de protección de datos de salud y de aplicación de herramientas *big data* en proyectos de investigación de interés general y salud pública.

Asimismo, de manera paralela se hará continuo énfasis a la constante tensión[515] existente en la normativa de protección de datos generada por la creciente presión de la asistencia sanitaria, las propias demandas de los ciudadanos, el impacto de los nuevos tratamientos, los avances tecnológicos, en particular, de la aplicación de herramientas *big data* en el contexto del sector sanitario, por los sensores, la movilidad y por el gran volumen de información procedente de los datos masivos que se generan a gran velocidad en tiempo real.

I. PRINCIPIOS QUE GARANTIZAN UN TRATAMIENTO TRANSPARENTE, ADECUADO, PERTINENTE, LIMITADO Y PROACTIVO DE LOS DATOS RELATIVOS A LA SALUD

En el sector sanitario es de importancia proteger el derecho del paciente a ser informado de cuándo y cómo van a ser utilizados sus datos para otros fines distintos al asistencial, así como que tenga la posibilidad legal de comprobar la citada información directamente por sí mismo facilitándole el centro sanitario las vías y medios adecuados. Por ello, el RGPD regula los siguientes principios a efectos de garantizar un tratamiento transparente, adecuado, pertinente, limitado y proactivo de los datos.

1. PRINCIPIO DE LICITUD, LEALTAD Y DE TRANSPARENCIA

El RGPD establece como requisito necesario e imprescindible el de un tratamiento lícito de los datos, para ello, es necesario que los mismos sean tratados por medio de una de las siguientes vías:

[515] DEL RÍO SOLÁ y VAQUERO PUERTA, "El impacto de la transformación digital en el…", *op. cit.,* p. 106.

De un lado, por medio del consentimiento otorgado por el interesado que debe cumplir unos requisitos[516]: En primer lugar, es requisito fundamental que el consentimiento pueda ser acreditado por el responsable del tratamiento, por ello debe ser formulado mediante escrito en el que se muestre con claridad que el interesado es consciente de ello, así como que ha sido informado tanto de la identidad del responsable del tratamiento como de los fines de este. En concreto, el modelo de declaración de consentimiento facilitado por el responsable del tratamiento al interesado debe ser inteligible, de acceso fácil, redactado de manera clara y sencilla, sin ningún tipo de cláusula abusiva[517]. En segundo lugar, el consentimiento debe ser dado libremente, se entenderá que el consentimiento no ha sido prestado libremente cuando el interesado no posea una libre o verdadera capacidad de elección, o no pueda denegar o retirar su consentimiento sin que le suponga un perjuicio. Así pues, en caso de que exista desequilibrio evidente entre el interesado y el responsable del tratamiento, sin que sea posible que un único acto de otorgamiento del consentimiento sea válido para todas las circunstancias posibles de una situación concreta, es de obligado cumplimiento para el responsable del tratamiento – incluyendo las autoridades públicas – que para cada circunstancia concreta el interesado preste su consentimiento, o cuando el cumplimiento de un contrato dependa del consentimiento, aunque no sea necesario para el cumplimiento del mismo[518].

De otro lado, a través de una base legítima otorgada por una norma jurídica regulada dentro de la Unión Europea, ya sea Derecho emanado de la Unión o de los

---

[516] MARTOS DÍAZ, N., "Principios (Ars. 6-11 RGPD. Arts. 4-10 LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 333-337.

[517] Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p.29).

[518] DÍAZ GARCÍA, "La entrada en vigor del Reglamento…", *op. cit.,* p. 235. Asimismo, GONZÁLEZ GONZÁLEZ, P.A., "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata,* núm. 24, 2017, p. 119, aclara en relación con el principio de licitud que: "Existe otro supuesto que abre una puerta cuyos límites no está siempre claro si se deben traspasar, y este es el supuesto de la existencia de un "interés legítimo" perseguido por quien pretenda tratar datos personales o, incluso, de un tercero. Este supuesto del interés legítimo constituye un concepto jurídico indeterminado que, en cualquier caso, debe interpretarse siempre de forma restrictiva y nunca constituir una "habilitación genérica" para justificar cualquier tratamiento. De las diferentes casuísticas que pueden presentarse se ha ocupado el Grupo de Artículo 29 en su "Dictamen 6/20145, sobre el concepto de interés legítimo del responsable del tratamiento", cuya lectura complementaria puede resultar de sumo interés".

Estados miembros referenciados en el RGPD[519]. En este supuesto, nos encontramos ante una base jurídica o medida legislativa que sea clara y precisa para los destinatarios, no siendo necesario que se trate de un acto legislativo aprobado en un parlamento, sino que resultará suficiente que sea conforme a la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos, siempre y cuando el citado acto o medida sea de previsible aplicación para el interesado, no siendo necesario que cada tratamiento individual sea regulado por una norma específica. En concreto, la finalidad de la base jurídica es la de otorgar interés legítimo al responsable del tratamiento o, en caso de que el tratamiento sea necesario a efectos de cumplir con una situación de interés público o en el ejercicio de poderes públicos, debiendo ser en estos casos, el responsable del tratamiento una autoridad pública, bien sea persona física o jurídica de Derecho público, o de Derecho privado, como puede ser una asociación profesional con fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad.

Pues bien, en la esfera sanitaria, los citados principios en el tratamiento de datos serán tratados de manera lícita, leal y transparente en relación con el paciente. Igualmente, los datos deberán ser recogidos con fines determinados, explícitos y legítimos y, no serán utilizados con posterioridad para finalidades incompatibles con dichos fines, aunque pueden usarse para finalidades relacionadas estrechamente con la finalidad originaria para la que fueron solicitados, esto es, por ejemplo, si el paciente ha consentido en la utilización de sus datos para fines de una concreta investigación biomédica sobre cáncer de colon, se podrán utilizar sus datos de salud para otras investigaciones oncológicas, ya que esta segunda utilización se considera vinculada a la principal y, por consiguiente compatible con la misma.

En lo que respecta a la minimización de datos[520], únicamente se van a utilizar los datos adecuados, pertinentes y limitados a lo necesario en relación con los fines para los

[519] Independientemente de lo regulado en la base jurídica que otorgue legitimidad a un tercero para tratar determinados datos, el responsable debe cumplir las obligaciones que establece el RGPD o bien, establecer un contrato con el interesado donde se obligue a tomar medidas a favor del mismo, un contrato que respete los derechos del interesado y reconozca las obligaciones del responsable del tratamiento.

[520] Aclara DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…", *op. cit.,* p. 235 que: "[…] los datos han de ser adecuados, pertinentes y limitados a lo necesario en relación a los fines para los que son tratados. En este sentido, y en relación con los fines de investigación científica, el artículo 89 exige que el tratamiento se sujete a las garantías

que son tratos, así pues, a pesar de que esta información puede ser amplia en ocasiones dada la variedad de factores relacionados con la salud (deporte, comida, bebidas, enfermedades genéticas…), exclusivamente se van a recoger los datos mínimos necesarios para una adecuada asistencia sanitaria. En relación con el citado principio de minimización, el *Informe SESPAS 2017* establece una equiparación entre el mismo y el principio de proporcionalidad del Tribunal Constitucional, formado por tres caracteres esenciales: a) utilidad o adecuación; b) el de necesidad y; c) el de proporcionalidad strictu sensu o ponderación de los bienes en conflicto. Por ende, de conformidad con lo establecido en el apartado c) del artículo 5.1, acerca del principio de minimización, donde señala que los datos serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos)", lo que conlleva que únicamente podrán ser requeridos aquellos datos que se adecuen a la finalidad del tratamiento, debiendo ser excluidos o suprimidos aquellos otros datos personales que no se adapten a la finalidad y que resulten irrelevantes para el tratamiento.

Por otro lado, el principio de transparencia es uno de los principios fundamentales del derecho de protección de datos hasta el extremo de que el legislador europeo le otorga una gran potestad en el RGPD, convirtiéndose la transparencia en uno de los elementos básicos de la protección de datos, pues es condición esencial que la persona titular de los datos sea conocedora de primera mano del derecho a ser informado y el derecho a decidir sobre el tratamiento de sus datos personales por parte de un tercero[521].

---

adecuadas para los derechos y libertades de los sujetos, de acuerdo con el Reglamento, una de las cuales es la minimización de los datos, y que puede incluir la seudoanonimización siempre que de esa forma puedan alcanzarse sus fines. Aunque añade, que siempre que esos fines puedan alcanzarse mediante un tratamiento ulterior que no permita la identificación de los interesados, esos fines se alcanzarán de ese modo. Existe una preferencia por la anonimización, pero no resulta necesaria, como sí lo es en nuestra legislación actual. Los datos seudoanonimizados se definen en el considerando 26, como los que cabría atribuir a una persona física mediante la utilización de información adicional. Se trata del procedimiento que habitualmente se usa en investigación, con lo que la posibilidad de acogerse a las previsiones del reglamento en esta materia, supone un avance respecto de los condicionantes que existen en la actualidad. El considerando 156 también se refiere a este principio y a la seudoanonimización como garantía, remitiendo a los estados miembros el establecimiento de las garantías adecuadas para el tratamiento de datos personales con fines de investigación científica, no contemplando nada en este sentido el proyecto de LOPD".

[521] APARICIO SALOM, J., "Derechos del interesado (Arts. 12-19 RGPD. Arts. 11-16 LOPDGDD)", en AA. VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 345-346.

Por consiguiente, debido a que una de las características fundamentales del tratamiento de los datos es que ha de ser lícito y legal, resulta necesario para ello que la persona física titular de los datos sea consciente de manera clara de qué datos relativos a su persona están siendo recogidos, utilizados, consultados o tratados para otros fines distintos al asistencial. Dicha finalidad únicamente es posible a través del principio de transparencia, puesto que es el que va a exigir que toda información y comunicación facilitada a la persona física en relación con el tratamiento de sus datos personales sea de fácil acceso, inteligible y, anunciada mediante un lenguaje sencillo y claro. En concreto, el principio de transparencia hace hincapié en una información básica que ha de ser accesible y comunicada a los interesados, como la identidad del responsable del tratamiento, la finalidad de este y, otra información que ha de ser añadida a efectos de garantizar un tratamiento leal y transparente con y para las personas afectadas, no siendo así vulnerado de ningún modo su derecho a obtener información y comunicación del tratamiento de sus datos personales[522].

Así pues, en el ordenamiento jurídico se regula el principio de transparencia como uno de los principios más relevantes del tratamiento de los datos de acuerdo con el RGPD[523], donde se establece en el artículo 5.1. a) que "los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)". En efecto, con el principio de transparencia lo que se pretende es fortalecer un tratamiento lícito y leal de los datos, siendo sumamente importante que el ciudadano tenga la certeza y seguridad de que sus datos personales "se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados"[524]. Así pues, el principio de transparencia conlleva las siguientes exigencias legales:

---

[522] En este sentido, opina DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…", *op. cit.,* p. 235 que: "La licitud se basa en el apoyo en las bases jurídicas que luego trataremos específicamente, y en cuanto a la lealtad y transparencia no parece en principio que puedan obstaculizar la investigación en tanto que son principios también propios de dicha actividad".

[523] Al respecto aclara RODRÍGUEZ AYUSO, J.F., *Figuras y responsabilidades en el tratamiento de datos personales,* JB Bosch, Barcelona, 2019, p. 36 que: "La novedad que conlleva y supone el principio de transparencia no reside en obligar al responsable del tratamiento a proporcionar al interesado toda la información acerca de los tratamientos realizados sobre sus datos personales y la comunicación en torno a los derechos que este puede ejercitar al respecto, sino que el principio de transparencia hace referencia a la manera en que estas obligaciones tienen que ser cumplidas".

[524] Considerando 39 RGPD.

(1) Información y comunicación redactada con un lenguaje sencillo y claro a efectos de que sea de fácil comprensión para el titular de los datos personales.

(2) Garantizar un tratamiento leal y transparente a las personas afectadas de los datos personales facilitándoles información acerca del responsable del tratamiento y los fines del tratamiento (que en todo caso deben ser explícitos y legítimos y deben determinarse en el momento de su recogida), además de aquella información que pudiera resultar de interés[525], a efectos de obtener confirmación y comunicación de los datos personales por parte de sus titulares.

(3) Conocimiento fehaciente por parte de los afectados de los datos personales de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del procedimiento a seguir a fin de ejercer sus derechos en relación con el tratamiento.

(4) Necesidad de que los datos personales aportados sean adecuados, pertinentes y limitados a la finalidad del tratamiento (minimización de datos), por lo que se requiere un límite estricto del plazo de conservación. Para ello, el responsable del tratamiento debe establecer plazos para su supresión o revisión periódica.

(5) Garantía de rectificación o supresión de los datos personales inexactos.

(6) Seguridad y confidencialidad en el tratamiento de los datos personales, incluso a efectos de impedir el acceso o uso no autorizados tanto de los datos como del equipo utilizado en el tratamiento.

Del mismo modo, se ha de tener traer a colación, por un lado, el Considerando 39 del RGPD donde describe el principio de transparencia como el principio que garantiza al ciudadano el derecho a conocer con total claridad el hecho de que sus datos personales están siendo recogidos, utilizados, consultados o tratados, así como de la

[525] Al respecto, el artículo 12 del RGPD establece la obligación del responsable del tratamiento de implantar medidas necesarias a fin de facilitar al interesado toda la información acerca de sus datos, así como la información acerca de los derechos de acceso, rectificación y supresión, limitación del tratamiento, derecho a la portabilidad y derecho a la oposición, regulados de manera específica en los artículos 15 a 22 del RGPD.

forma y finalidad para la que sus datos están siendo tratados, describiendo a su vez el modo de cómo ha de realizarse la información a fin de cumplir con el principio de transparencia, debiendo ser conocedor el interesado de la identidad del responsable del tratamiento. Por otro lado, el Considerando 58, establece que la información debe ser concisa y, se ha de visualizar, haciendo especial mención a aquellas "situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea" por lo que resulta conveniente facilitar la información a través de un medio electrónico[526].

Por último, el Considerando 59 a fin de garantizar una efectividad del principio de transparencia establece que el responsable del tratamiento ha de facilitar al interesado los derechos de acceso, rectificación, supresión y oposición[527].

En el marco jurídico español, es el artículo 11.1 LOPDGDD el que bajo la rúbrica de "Transparencia e información al afectado" se limita a hacer mención del derecho de los interesados a ser informados sobre el tratamiento de sus datos personales.

Debido a lo anterior, resulta de interés que la ley sectorial sobre protección de datos de salud y *big data* sanitario en relación con el principio de transparencia, para el caso de los proyectos de investigación científica de interés general y de salud pública que apliquen herramientas *big data,* tenga en consideración que debido a que un mal uso o un uso indebido de las tecnológicas *big data*, puede desembocar en una falta de transparencia en la información facilitada al ciudadano titular de los datos personales y datos de salud, hasta el extremo que puedan darse situaciones en las que el afectado desconozca el trato real de sus datos una vez autorizado el acceso a los mismos. Por lo que es resulta de interés que la propia ley regule, ante todo, la obligación por parte del

[526] *V.gr.,* página *web*.

[527] APARICIO SALOM, "Derechos del interesado…", *op. cit.,* p. 347, aclara que: "En definitiva, la transparencia obliga a informar al interesado sobre el uso que un tercero realiza de los datos personales, pero también garantiza al interesado el derecho a tener la certeza de que conoce todos los detalles, circunstancias y condiciones que influyen en el tratamiento de los datos".

responsable y del encargado del tratamiento de facilitar información transparente sobre el tratamiento de los datos de salud al paciente incluyendo en la misma las diferentes consecuencias que pueda suponer para su privacidad.

Además, de manera paralela, regulando legalmente la citada obligación de información transparente sobre el tratamiento del *big data* se evitará que existan desequilibrios inesperados de información que puedan surgir posteriormente entre los afectados y los responsables del tratamiento (centros médicos públicos o privados o, profesionales sanitarios privados).

En los proyectos de salud pública e investigación biomédica en los que se apliquen técnicas de *big data*, el principio de transparencia es sumamente relevante puesto que es la fórmula que va a reforzar las garantías jurídicas de los tratamientos de datos de salud en los mismos, así como salvaguardar un tratamiento lícito de los mismos, puesto que una vez que el responsable del tratamiento o de fichero facilite al interesado de manera transparente información acerca del tratamiento, uso y destino que se va a aplicar a sus datos personales y datos de salud, estará legitimado para el tratamiento.

2. PRINCIPIO DE INFORMACIÓN

La normativa vigente de protección de datos exige que las personas físicas obtengan información acerca de los posibles riesgos, de las normas aplicables, así como de los derechos de los que son titulares y el modo de ejercer los mismos en caso de vulneración a consecuencia del tratamiento. Igualmente, el responsable del tratamiento de manera explícita y legitima debe detallar los fines específicos del tratamiento, así como determinar los mismos en el momento de su recogida. En concreto, el art. 12.2 del RGPD regula los requisitos básicos que debe contener la información a fin de garantizar el principio de transparencia y que, en todo caso, el responsable del tratamiento debe respetar, tanto en el momento del tratamiento de los datos, como en la tramitación y resultado del ejercicio y atención de los derechos que garantizan la protección de datos personales[528], así como de tomar las medidas necesarias para

[528] Considerando 59 del RGPD, establece que: "Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en

facilitar al interesado la información contenida en los arts. 13 y 14 RGPD, así como de las comunicaciones sobre el tratamiento (arts. 15 a 22 y art. 34 RGPD).

En el ámbito sanitario, el principio de información resulta sumamente relevante si tenemos en consideración de que el consentimiento de manera general debe ser informado, lo que conlleva una mayor exigencia al responsable del tratamiento del cumplimiento de las medidas necesarias y eficaces a fin de garantizar una información clara, concisa y detallada al paciente sobre el tratamiento de su datos de salud, pues como ha sido analizado, en la normativa vigente de protección de datos una información transparente es sumamente relevante a fin de garantizar el derecho de protección de datos personales a los interesados.

De igual modo, la ley de protección de datos da salud, debería incorporar en su contenido de manera específica el principio de información para el tratamiento de datos de salud del paciente, destacando entre otros, el derecho a ser informado de manera concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, entre otros, de los siguientes extremos: (a) de la identidad y los datos de contacto de responsable y, del representante si existiere; (b) de los datos de contacto del delegado de protección de datos, si fuera obligatoria su designación; (c) de los fines del tratamiento que se destinan los datos personales y la base jurídica del tratamiento; (d) de los destinatario o las categorías de destinatarios de los datos personales, en su caso; (e) de la intención del responsable de transferir datos personales a un tercer país u organización internacional; (f) del plazo de conservación de los datos de salud o los criterios fijados para determinar el mismo en caso de imposibilidad; (g) del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos; (h) el derecho a retirar el consentimiento en cualquier momento; (i) del derecho a presentar una reclamación ante una autoridad de control; (j) de las consecuencias posibles de no facilitar los datos si nos encontramos ante un supuesto de comunicación de datos personales por exigencias legales o contractuales; (k) de la existencia de decisiones

---

su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas".

automatizadas incluida la elaboración de perfiles; (i) de otras finalidades que sean distintas a la finalidad principal en caso de tratamiento ulterior de los datos personales; entre los más destacables.

3. PRINCIPIO DE FINALIDAD

De igual modo el principio de finalidad se regula como un requisito imprescindible y esencial el de especificar de manera clara y precisa la finalidad del tratamiento de los datos personales, puesto que los datos personales tratados deben ser pertinentes, limitados y adecuados en base a las finalidades detalladas por el responsable, donde juega un papel relevante el hecho de que sea garantizado al titular de los datos y demás interesados un plazo máximo de conservación, en caso contrario, nos encontraríamos ante una vulneración del derecho de protección de datos del interesado[529].

Igualmente, es necesario garantizar al interesado la posibilidad de rectificar o suprimir todos aquellos datos personales inexactos o que no se ajusten a la realidad. Así pues, el RGPD exige un tratamiento garantista de los datos personales, puesto que debe garantizar a sus titulares un tratamiento seguro y confidencial, incluyendo la posibilidad de impedir el acceso o uso no autorizados tanto de los datos tratados como del equipo utilizado[530].

En relación con el principio de finalidad, se estima apropiado que la ley sectorial de protección de datos de salud tenga en consideración responsable del tratamiento de los datos debe determinar de manera explícita la finalidad del tratamiento, así como la prohibición de utilizar los datos de salud para finalidades incompatibles con la finalidad

[529] Al respecto, señala DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…", *op. cit.,* p. 235, que: "Los datos habrán de ser 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. Una de las preocupaciones de los investigadores era precisamente conocer la licitud de la utilización de datos de una investigación determinada para otras ulteriores o sobrevenidas y diferentes a la inicial, sin necesidad de repetir todo el proceso".

[530] Considerando 39 RGPD.

principal para la que el paciente prestó su consentimiento, igualmente, estando permitido para finalidades análogas o conexas con la principal.

De igual modo, la ley sectorial debe tener presente que ante proyectos de salud pública e investigación biomédica de interés general, normalmente, los responsables y encargados del tratamiento de los datos de salud, van a ser centros sanitarios, públicos o privados, profesionales sanitarios, científicos e investigadores de organismos públicos o privados, así como centros de investigación públicos o privados, donde se incluye la industria farmacéutica, entre otras y, que en el contexto del *big data* los fines pueden variar con el fin principal por el que se recabaron los datos, pudiéndose perseguir fines diferentes al inicial e incluso que no consten especificados de antemano[531], pues como es sabido, a través del análisis de big data lo que se pretende, entre otros, es identificar nuevas tendencias y adelantarse a la enfermedad.

En este caso, resulta relevante que el responsable del tratamiento cumpla fundamentalmente con las siguientes obligaciones: (1) determinar la finalidad del proyecto para el que se van a tratar los datos de salud e informar de la posibilidad de que los fines posteriores pueden variar con principal; (2) identificar al tercero autorizado en caso de proceder a la delegación del tratamiento a una organización externa; (3) elección de un único encargado que trate los datos personales por cuenta del responsable del tratamiento y; (4) en caso de existencia de acuerdo de corresponsabilidad del tratamiento celebrado entre varios responsables, se deberá informar al interesado de los aspectos básicos del acuerdo.

En los proyectos de tratamiento de *big data* es sumamente relevante regular la figura del encargado, por lo que se debe delimitar de manera clara en la ley sectorial. Así pues, teniéndose en consideración definición dada por el RGPD[532], el encargado siempre actuará por cuenta del responsable desarrollando actividades, tales como la de suministrar los medios o la plataforma (cloud computing), instalar o mantener las herramientas informáticas de *big data*, realizar el análisis de *big data*, entre otras. De

[531] MANTERO, A., "Regulating big data. The guidelines of the council of europe in the context of the european data protection framework", *Computer Law & Security Review*, Vol. 33, Issue 5, October 2017, p. 25.
[532] El art. 28 RGPD define encargado como la persona física o jurídica, autoridad, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

contrario, el encargado será considerado responsable en aquellos supuestos en los que actúe por su cuenta o celebre un nuevo vinculo jurídico con los titulares de los datos de salud concretando a su vez una finalidad, por lo que se entenderá que nos encontramos ante un nuevo tratamiento. Igualmente, el encargado será considerado responsable en aquellos supuestos en los que el encargado destine los datos personales y de salud a otra finalidad distinta no recogida en el proyecto, los comunique a terceros no autorizados o permita su acceso a los mismos. En todos estos supuestos, el encargado (nuevo responsable) deberá informar al interesado sobre su identidad en calidad de nuevo responsable, de las categorías de los datos y de los destinatarios del tratamiento.

Por otro lado, particularmente, en los proyectos de *big data* es sumamente importante la relación contractual entre el responsable y el encargado del tratamiento, por lo que debe ser de obligatorio cumplimiento para ambas figuras la celebración de un contrato de arrendamiento de servicios donde consten por escrito, entre otras, las condiciones del objeto del contrato, la duración, naturaleza y finalidad del tratamiento, la tipología de los datos personales (de salud), categorías de interesados (pacientes) y, ante todo, los derechos y obligaciones de cada una de las partes (responsable y encargado).

Asimismo, llegado el plazo de vigencia del contrato sin procederse a su renovación o prorroga, el encargado deberá destruir o devolver al responsable del tratamiento los datos objeto del tratamiento, así como otros datos personales que se hayan generado a causa del contrato. Por último, otro de los puntos que la ley sectorial debe tener en consideración, es la obligación de comunicación e información del encargado al responsable en caso de que proceda a la subcontratación de servicios (a quien se le aplicará las mismas obligaciones que al encargado), debiendo informar el encargado al responsable principalmente del tipo de servicio subcontratado, así como de las garantías de cumplimiento de la normativa de protección de datos por parte de la persona física o jurídica (pública o privada) subcontratada.

4. EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA O PREVENTIVA

A continuación, se analizaran las garantías y mecanismos que el RGPD ofrece más influyentes en el sector sanitario que producen el cambio de un enfoque reactivo a otro proactivo en la gestión de los tratamiento de datos personales (espacialmente datos de salud) a fin de concienciar y modificar las actuaciones de los responsables sanitarios, pues como ser verá, el Reglamento se centra en la necesidad de una actitud proactiva de los responsables y encargados del tratamiento quienes están obligados a establecer políticas efectivas y medidas que aseguren un cumplimiento efecto de la normativa de protección de datos personales, medias y políticas que deberán acreditar *(accountability)* tanto de manera interna como externa[533].

En concreto, el artículo 5.2 del RGPD se regula el principio de responsabilidad proactiva o preventiva (*accountability*) por el que el responsable o encargado del tratamiento queda obligado de demostrar que cumple tanto con los principios dimanantes del tratamiento de datos como de la normativa jurídica al respecto. Por ende, se le exige al responsable o encargado una actitud proactiva en el sentido de que ha de demostrar de manera prolongada en el tiempo el cumplimiento de la normativa jurídica de protección de datos y de los principios fundamentales relativos al tratamiento de estos, siendo sumamente relevante que en todo momento sea protegida la confidencialidad de los datos personales a través de medidas que garanticen su protección y un menor riesgo en el tratamiento[534]. En este sentido, DÍAZ GARCÍA señala que:

"El reglamento supone un reforzamiento y ampliación de los derechos de los ciudadanos en relación con sus datos de salud, a los que considera como categoría

[533] SANTOS MORÓN, Mª J., "Tratamiento de datos, sujetos implicados, responsabilidad proactiva", en AA.VV., *Protección de datos personales,* (Coord. I. González Pacanowska), Asociación de profesores de Derecho Civil, Tirant lo blanch, Valencia, 2020, pp. 55-56.

[534] Al respecto, GARCÍA, R. (2017). El Reglamento General de Protección de Datos y su aplicación en el ámbito sanitario, *I+S Revista de la Sociedad Española de Informática y Salud,* Núm. 127, febrero, pp. 17-18, indica: "El catálogo de medidas de cumplimiento incluye: • Mantener un registro de actividades de tratamiento • Aplicar medidas de Protección de Datos desde el Diseño y de Protección de Datos por Defecto. • Aplicar medidas de seguridad adecuadas. • Llevar a cabo Evaluaciones de Impacto. • Consultar con las autoridades de protección de datos la puesta en marcha de determinados tratamientos. • Designar a un Delegado Protección de Datos (DPD). Notificación de Quiebras de Seguridad. • Posibilidad de adhesión a códigos de conducta y esquemas de certificación…".

especial de datos, dado que constituyen parte de la esfera más íntima de las personas. Y supone, también, un cambio fundamental para aquellos que tratan datos personales, al establecerse como principio regulador, el de responsabilidad activa, es decir, la necesidad de asumir la protección de datos desde un punto de vista preventivo para evitar que haya que actuar una vez que el daño se ha producido"[535].

De igual modo, sobre el principio de responsabilidad proactiva, SARRIÓN ESTEVE nos advierte que:

"Pues bien, consideramos de gran relevancia que el principio de *accountability* o de responsabilidad proactiva lleve a la implantación de protocolos de actuación en materia de protección de datos que sean muy garantistas cuando se trate de datos sensibles, y sobre todo cuando se trate de datos correspondientes a menores"[536].

Por último, LOMAS HERNÁNDEZ, sobre la responsabilidad proactiva en relación con el tratamiento masivo de datos, opina que:

"Estamos ante una obligación de gran importancia en el entorno sanitario por cuánto uno de los supuestos que mayores riesgos presenta para el tratamiento de la información, son todas aquellas situaciones de pérdida de confidencialidad de datos sujetos al secreto profesional, supuestos en los que se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad, y en particular de menores de edad y personas con discapacidad, y cuando se produzca una tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales. (art. 28.2 de la LOPDGDD)"[537].

---

[535] DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación*...", op. cit.,* p. 233.

[536] SARRIÓN ESTEVE, J., "Las novedades de la nueva normativa de protección de datos y su aplicación a los ensayos clínicos de menores", *DS: Derecho y Salud,* Vol. 27, 2017, p. 235. De igual modo, GONZÁLEZ GONZÁLEZ, "Responsabilidad proactiva en los tratamientos…", *op. cit.,* p. 120.

[537] LOMAS HERNÁNDEZ, V., "Principales Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales desde la Perspectiva Sanitaria", *I+S: Revista de la Sociedad Española de Informática y Salud,* núm. 134, 2019, p. 10.

En definitiva, nos encontramos ante una garantía jurídica sobre el tratamiento de los datos personales para el titular de los datos que se traduce en una obligación tanto para el responsable como para el encargado del tratamiento de los datos, debido a que deben adoptar medidas técnicas y organizativas apropiadas a efectos de garantizar y acreditar que el tratamiento de los datos personales cumple con lo establecido en la normativa vigente de protección de datos, tanto con el RGPD como en la LOPGDDG, medidas que deben ser respetadas especialmente en el ámbito sanitario[538].

Asimismo, en proyectos *big data* es sumamente necesario que los mismos se adapten y respeten el principio de responsabilidad por parte de los responsables y encargados del tratamiento (públicos o privados) de implar medidas de garantía y cumplimiento de la normativa de protección de datos, así como establecer mecanismos internos y externos que evalúen su fiabilidad y demuestren su efectividad en caso de que las autoridades de control lo requieran (principio de responsabilidad proactiva), de conformidad con lo establecido en el art. 24[539] y art. 5.2.[540] del RGPD. En consecuencia, es de interés que la ley sectorial haga referencia al citado principio de responsabilidad, estableciendo a su vez medidas comunes de responsabilidad, tomando como base las medidas asentadas por el Grupo de Trabajo del Artículo 29[541].

---

[538] LOMAS HERNÁNDEZ, "Principales Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales…", *op. cit.,* p. 10.

[539] Art. 24 RGPD establece que "1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. 2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. 3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

[540]Art. 5.2 RGPD señala que "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

[541]Sobre este punto, el GT29, señala las siguientes medidas comunes de responsabilidad: el establecimiento de procedimientos internos previos a la creación de nuevas operaciones de tratamiento de datos personales (revisión interna, evaluación, etc.); el establecimiento de políticas escritas y vinculantes de protección de datos que se tengan en cuenta y se valoren en nuevas operaciones de tratamiento de datos (p.ej., cumplimiento de los criterios de calidad de datos, notificación, principios de seguridad, acceso, etc.) que deben ponerse a disposición de las personas interesadas; la cartografía de procedimientos que garanticen la identificación correcta de todas las operaciones de tratamiento de datos y el mantenimiento de un inventario de las mismas; el nombramiento de un delegado de protección de datos; la oferta adecuada de formación en protección de datos a los miembros del personal; esto debe incluir a los responsables de los procesos de datos personales (como los directores de recursos humanos), pero también a los administradores de tecnologías de la información, desarrolladores en general, y

5. PRINCIPIO DE LA PRIVACIDAD DESDE EL DISEÑO (*PRIVACY BY DESIGN)* Y POR DEFECTO (*PRIVACY BY DEFAUL*)

El artículo 25 del RGPD regula el principio de privacidad desde el diseño exigiendo la obligación al responsable del tratamiento de integrar los principios de protección de datos en el diseño de cualquier sistema, aplicación o tecnología a través del cual se efectúe cualquier tratamiento de datos personales[542]. En consecuencia, el citado principio supone que el responsable del tratamiento desde el inicio del desarrollo tiene la obligación de verificar la adecuación del futuro proyecto a la normativa de protección de datos y elegir un diseño que combine la obtención de las funcionalidades que se pretenden en relación con la privacidad y el cumplimiento del RGPD. Igualmente, el citado principio supone que en caso de que el diseño del proyecto se encuentre bien planteado desde un punto de vista funcional, pero sin embargo no garantice la privacidad, el responsable deberá de volver a diseñar el mismo hasta que resulte eficiente en términos de privacidad, todo ello con la finalidad de compatibilizar desde el principio del proyecto la funcionalidad del mismo y la privacidad de los usuarios, a efectos de evitar posteriores sacrificios en cada uno de ellos o en ambos[543].

Por otro lado, la privacidad por defecto (art. 25 del RPGD) obliga a los responsables del tratamiento que apliquen las medidas técnicas y organizativas apropiadas a efectos de garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. En consecuencia, esta exigencia debe ser aplicada tanto a la cantidad de datos personales recogidos, como a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad, es decir, los responsables del tratamiento deben

directores de unidades comerciales. Deben asignarse recursos suficientes para la gestión de la privacidad, el establecimiento de procedimientos de gestión del acceso y de las demandas de corrección y eliminación de datos con transparencia para las personas interesadas; • El establecimiento de un mecanismo interno de resolución de quejas de los interesados. En este ámbito puede jugar un papel destacado el Delegado de Protección de Datos; El establecimiento de procedimientos internos de gestión y notificación eficaces de fallos de seguridad (violaciones de seguridad); La realización de evaluaciones de impacto sobre la privacidad en circunstancias específicas; La aplicación y supervisión de procedimientos de verificación que garanticen que las medidas no sean sólo nominales, sino que se apliquen y funcionen en la práctica (auditorías internas o externas).

[542] Comité Europeo de Protección de Datos, *Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto Versión 2.0***,** 20 de octubre de 2020. Disponible en: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_es

[543] GARCÍA MEXÍA, P., *Derechos y libertades, Internet y TICs*, Ed. Tirant lo Blanch, Valencia, 2014, p. 17.

autocontrolar su "voracidad" recopiladora de datos, limitándose a recoger y tratar aquellos que sean realmente necesarios para las finalidades del tratamiento. En consecuencia, el responsable del tratamiento deberá abstenerse en tratar los datos que excedan de este propósito, así como proceder a la eliminación automática de los datos personales que tenga registrados una vez que dejen de ser necesarios para los fines para los que fueron recopilados[544].

En consideración a lo anterior, se propone que la ley sectorial de protección de datos de salud y *big data* sanitario, regule también aquellos principios relativos a la protección de datos desde el diseño y por defecto, a fin de asegurar que el responsable del tratamiento desde la fase inicial del proyecto relacionado con *big data* sanitario tiene en cuenta la privacidad y el cumplimiento de la normativa vigente de protección de datos (comunitaria y estatal), la ley sectorial debe recoger los principios fundamentales de la protección de datos desde el diseño y por defecto de conformidad con lo establecido en el artículo 25 del RGPD[545].

Por ende, con el objetivo de que el proyecto sea diseñado integrando la privacidad desde un principio en las nuevas tecnologías y prácticas del mismo, incorporando desde las primeras fases del proyecto, las medidas técnicas y organizativas apropiadas a fin de cumplir con la normativa de protección de datos y proteja a su vez los derechos de los interesados, la ley sectorial debe recoger en un apartado los principios fundamentales relativos a la protección de datos desde el diseño y por defecto. En concreto[546]:

De un lado, el principio de proactividad, que exige que el responsable del tratamiento actúe previniendo la pérdida de la privacidad de la información anticipándose a ello. De otro lado, el principio de privacidad por defecto, a fin de

[544]GARCÍA MEXÍA, *Derecho y libertades…, op. cit.,* p. 64.

[545] RODRÍGUEZ AYUSO, *Figuras y responsabilidades…, op. cit.,* p. 125, señala que: "Si atendemos a la evolución experimentada a largo tiempo por el concepto de privacidad desde el diseño, observamos que, pese a que este principio puede ser de aplicación a cualquier modalidad de dato personal, su aplicación ha de tener un mayor rigor con determinados datos personales especialmente sensible, tales como aquellos de naturaleza médica o de carácter financiero."

[546]Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño*, Octubre 2019, pp. 7-11.

garantizar que los datos se encuentran protegidos de manera automática y por defecto en la totalidad del sistema informático y en las buenas prácticas que se lleven a cabo en el proyecto.

Otro de los principios a destacar es el principio de privacidad desde el diseño que alude a que la protección de la información se encuentre incluida en el propio diseño del proyecto y en los procesos propios de organismo público o entidad privada que lo ejecute.

De igual modo, el principio de funcionalidad completa, a efectos de garantizar la privacidad y la seguridad de manera conjunta desde todas las funcionalidades y necesidades de los implicados en el proyecto. En relación con el anterior se encuentra el principio de seguridad y protección completa de los datos, que asegura que los datos son protegidos de manera segura durante todo el ciclo de vida, esto es, desde su recolección, conservación hasta su destrucción.

Otro de los principios fundamentales es el principio de visibilidad y transparencia, exige al responsable del tratamiento que los componentes y operaciones permanezcan visibles y transparentes a los usuarios y proveedores a fin de garantizar a los interesados que los datos están siendo destinados a los objetivos y compromisos indicados. Por último, el principio de respeto a la privacidad de los usuarios, que obliga a los desarrolladores y operadores del proyecto a adoptar las medidas de privacidad idóneas a fin de respetar sobre todo y ante todo desde un principio la privacidad de los interesados.

6. PRINCIPIO DE EXACTITUD

De igual modo, de conformidad con el principio de exactitud, los datos consignados en las bases de datos y otras fuentes sanitarias deberán ser exactos y deberán estar lo más actualizados posible. Por ende, en el caso de las historias clínicas debe ser el profesional sanitario quien se encargue de determinar los datos que sean de suprimir, rectificar y actualizar.

Se ha de tener en consideración que los datos se deben conservar durante no más el tiempo del necesario para findes del tratamiento de los datos personales, aunque normativa vigente permite un mantenimiento durante periodos más largos para fines de archivo, en interés público, findes de investigación científica, histórica o fines estadísticos. En el caso de la historia clínica, se debe mantener vigente y actualizada durante el periodo de tiempo que se va a prestar asistencia sanitaria a efectos de facilitar la misma en cualquier procedimiento judicial, efectuar estudios epidemiológicos, docencia e investigación biomédica en general[547].

En este sentido, se considera necesario que ley específica de protección de datos de salud tenga en cuenta que en todo caso el responsable del tratamiento debe implar las medidas necesarias para que los datos sean lo más exactos y actualizados posibles, siendo sumamente necesario que la ley sectorial haga énfasis en el hecho de que el profesional sanitario es el único que tiene potestad de suprimir o rectificar los datos de salud reflejados en las historias clínicas.

7. PRINCIPIO DE CALIDAD

De manera general, el RGPD regula el principio de calidad donde se le exige al responsable del tratamiento que los datos personales sean tratados de manera lícita, leal y transparente, que sean datos pertinentes y adecuados a la finalidad que motiva la recogida, que se encuentren estrictamente limitados a los necesarios según la finalidad para la que son recopilados, la prohibición de la utilización de los datos para fines incompatibles con la finalidad originaria, así como que los datos sean exactos y estén actualizados.

En concreto, el principio de calidad de los datos debe ser especialmente respetado en los proyectos de *big data* donde existe un mayor riesgo en materia de privacidad al tratar con datos masivos de datos personales y de datos de salud procedentes de fuentes dispersas, lo que genera en consecuencia, mayores

[547] "Los datos habrán de ser exactos, y si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan" en DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación*... ", op. cit.,* p. 235.

probabilidades de realizar tratamientos con fines incompatibles a la finalidad originaria, gestionar datos desactualizados o erróneos dando lugar a resultados incorrectos o a la toma de decisiones que no se ajusten a la realidad, así como dificultar la gestión de los derechos del titular de los datos.

Debido a lo anterior, resulta relevante que la ley sectorial en esta parte específica regule las bases fundamentales para el cumplimiento del principio de calidad de los datos en los proyectos de investigación biomédica y de asistencia sanitaria de interés general que apliquen técnicas de *big data*, regulando a tales efectos deberes de obligado cumplimiento por parte del responsable del tratamiento o fichero, tales como: (1) deber de efectuar un análisis previo al proyecto donde conste delimitado, entre otros, la tipología de los datos necesarios, la finalidades iniciales y otras finalidades que se intuya que posteriormente puedan surgir relacionadas y compatibles con la inicial, así como el tiempo de duración de los datos; (2) deber de recabar los datos exclusivamente necesarios para los fines del tratamiento, gestionando así los datos, adecuados, pertinente y no excesivos; (3) deber de organizar la información y el conocimiento sustraído de los datos de manera lógica y ordenada a fin de evitar acumulación innecesaria de datos; (4) deber de implantar protocolos de verificación periódica y continua del tratamiento a efectos de comprobar su licitud adaptabilidad al proyecto; (5) deber de cumplir con el principio de minimización de datos y; (6) deber de efectuar revisiones periódicas automáticas y técnicas de revisión y actualización de información, entre otros que se pudieran destacar.

De manera similar sucede con la conservación de los datos de salud en los proyectos de *big data*, debido a los riesgos que se pueden dar en la forma en la que se realiza su almacenamiento, así como en el periodo durante el que se almacenen, es de suma importancia que la ley sectorial establezca medidas y criterios mínimos de seguridad a seguir por parte del responsable del tratamiento, tales como establecer protocolos de acceso concretos en función del tipo de usuarios, realizar el cifrado de la información y, si es posible, emplear técnicas de monitorización del sistema que sean objeto de auditorías periódicas, además de aquellas que el responsable estime oportunas tras los resultados del análisis de riesgos o evaluación de impacto.

Igualmente, puntualizar que la duración del almacenamiento de datos dependerá fundamentalmente del momento en el que se satisfaga la finalidad o finalidades del proyecto, aunque en el caso de las historias clínicas, como ya vimos anteriormente, se conservará durante el tiempo que dure la asistencia sanitaria al paciente, para facilitarla en vía judicial, para la realización de estudios epidemiológicos, docencia e investigación; o, en su defecto, durante el tiempo que establezca la normativa aplicable.

Por ende, en relación con el principio de limitación del plazo de conservación, se propone que la ley sectorial tenga en cuenta, por un lado, que los datos que permitan la identificación del paciente serán conservados no excediéndose del tiempo necesario para su tratamiento y, por otro lado, que se permitirá una conservación prolongada para los casos de fines de archivo de interés público, fines de investigación científica, histórica o estadísticos. Igualmente, haciéndose constar que, en todo caso, la historia clínica se conservará durante el tiempo que dure la asistencia sanitaria al paciente, para facilitarla en vía judicial, para la realización de estudios epidemiológicos, docencia e investigación.

8. PRINCIPIO DE INTEGRIDAD Y CONFIDENCIALIDAD

En última instancia, en relación con el principio de integridad y confidencialidad, se ha de hacer constar que los datos de salud deben ser tratados por el responsable del tratamiento aplicando medidas técnicas u organizativas apropiadas a los efectos de garantizar una seguridad adecuada de los mismos, incluyéndose una protección contra el tratamiento y acceso de terceros no autorizados o ilícito y contra su perdida, destrucción o daño accidental[548].

[548] DÍAZ GARCÍA, "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación…*", op. cit.,* p. 235, sobre el principio de integridad y confidencialidad la autora detalla que: "los datos han de ser tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Se trata de lo que en el apartado segundo del trabajo llamamos responsabilidad activa o preventiva, que implica que cada servicio de salud debe establecer su propio registro de actividades de tratamiento. Esto lleva consigo varias obligaciones como pueden ser realizar análisis de riesgos tanto para la seguridad de los datos, como para los derechos de los ciudadanos; implantar medidas de seguridad adecuadas; establecer procedimientos de notificación de brechas de seguridad, y llevar a cabo las denominadas evaluaciones de impacto, que pueden ser necesarias en determinados proyectos de investigación, y que formarán parte de los documentos necesarios para su aprobación".

Ahora bien, en el caso de datos sanitarios, el RGPD considera los mismos como datos de interés público, en consecuencia, otorga así interés legítimo al responsable del tratamiento, siempre y cuando la finalidad del tratamiento sea para el cumplimiento de una misión realizada en interés público o en intereses vitales del interesado, como, por ejemplo, en caso de epidemias y su propagación o en situaciones de emergencia humanitaria, cuestión esta que será trata más adelante en el presente trabajo.

En definitiva, de manera general, el RGPD señala que se puede constituir una base jurídica sostenible para el tratamiento mediante ese interés legítimo del que es galante el responsable del tratamiento a efectos de poder acceder a datos personales, o de un tercero, siempre y cuando no nos encontremos en situaciones donde a la hora de ponderar los intereses o los derechos y libertades del interesado con los intereses del responsable del tratamiento, no primen los primeros sobre los segundos. Sin embargo, a pesar de que exista ese interés legítimo y así sea reconocido, el RGPD exige de manera imperativa al responsable del tratamiento una "evaluación meticulosa", incluso en el caso de que el interesado pudiera prever razonablemente en el momento de la recogida de sus datos personales, que a los mismos puede tener acceso otro responsable del tratamiento con un interés legítimo, a mayor abundamiento, el RGPD, en caso de que no exista esa prevención razonable de un tratamiento ulterior de sus datos personales por parte del interesado, otorga prioridad a los intereses y los derechos fundamentales del mismo frente a los intereses del responsable del tratamiento.

En relación con lo anterior, cabe plantearse, por un lado, si prevalecen los intereses de los pacientes a los intereses de la sociedad en su conjunto, por otro lado, si un paciente puede negarse a dar su consentimiento para el tratamiento de sus datos siendo éstos esenciales y necesarios para un responsable del tratamiento cuya finalidad de la actividad para que requiera esos datos es un proyecto sanitario cuyo estudio va a beneficiar a la sociedad en su conjunto. Por último, si todos los pacientes se negasen a dar su consentimiento para el tratamiento de sus datos sanitarios ¿estaríamos ante una situación que afectaría al interés público? En cierto modo, como ha sido analizado anteriormente, el RGPD a efectos de evitar la mencionada consecuencia negativa, entre otras, otorga a los datos personales referentes a la salud una cierta autoridad como excepción a la prohibición de tratar categorías especiales, siempre y cuando sean de interés público, en concreto, cuando nos encontremos con fines de supervisión y alerta

sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud, siendo posible la citada excepciones en el campo de la salud "incluida la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos"[549].

Por tanto, el RGPD a pesar de que prohíbe el tratamiento de los datos que pertenecen a categorías especiales de datos personales, de manera excepcional permite y autoriza el tratamiento de estos cuando nos encontremos con fines relacionados con la salud, siempre que sea necesario para alcanzar fines que beneficien a las personas físicas y a la sociedad en general, cuyo objetivo sea el interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Asimismo, el RGPD establece que a pesar de que se permita el tratamiento de categorías especiales de datos personales sin el consentimiento del interesado por razones de interés público en el ámbito de la salud pública, el Derecho de la Unión Europea o de los Estados miembros debe regular medidas específicas y adecuadas que protejan los derechos fundamentales y los datos personales de las personas físicas. Por lo que respecta a la salud pública, el Reglamento (CE) n. º1338/2008 del Parlamento Europeo y de Consejo, regula como fines de interés público:

"[…] todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinados que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad"[550].

[549] Considerando (52) REPD.

[550] Reglamento (CE) N.º 133/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31,12,2008, p. 70).

Por consiguiente, cabe señalar que cuando nos encontremos ante terceros como empresarios, compañías de seguros o entidades bancarias traten los datos personales con otros fines que no sean los detallados anteriormente, no se les permitirá el tratamiento de datos relativos a la salud por razones de interés público.

Acerca de este principio, resultaría apropiado que la ley sectorial de protección de datos de salud destaque el deber del responsable del tratamiento de aplicar medidas técnicas y organizativas a efectos de garantizar una seguridad de los datos de salud en lo que a su tratamiento respecta.

Igualmente, en concreto, sobre la divulgación de las publicaciones científicas donde se han manejado datos de salud, resulta de interés que la ley sectorial establezca límites[551] a los efectos de garantizar la confidencialidad de la información clínica, tales como: prohibición de la difundir datos identificativos de los sujetos que han participado en la investigación y, la obligación de autorización expresa del sujeto para los casos en los que sea necesario su identificación y para los casos de publicación de imágenes médicas u otro soporte audiovisual que permita identificar a los participantes.

Por otro lado, en lo que respecta al acceso a la receta médica electrónica, la ley de protección de datos de salud debería regular aquellas situaciones en las que no es necesario el consentimiento del paciente para el tratamiento y cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, así como las medidas a implantar a efectos de garantizar la confidencialidad de la asistencia médica y farmacéutica, la intimidad personal y familiar de los ciudadanos y la protección de sus datos de carácter personal[552].

[551] De acuerdo con lo establecido en el considerando 159 RGPD, artículos 5.5 y 27.3 de la LIB.

[552] De conformidad con lo establecido en los artículos 11 y 19.2 del Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación hospitalaria.

II. MEDIDAS QUE GARANTIZAN UN ADECUADO TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD

1. MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO

En relación con las medidas de seguridad del tratamiento, el art. 32 RGPD introduce un análisis de riesgos a fin de que el responsable y encargado del tratamiento apliquen medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, en concreto señala que:

"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".

Por otro lado, para el caso en el que el tratamiento se vea afectado por una vulnerabilidad producida por un riesgo el segundo apartado del art. 32 del RGPD señala se han de haber previsto previamente los daños en caso de destrucción, pérdida o alternación de los datos indistintamente de su naturaleza[553] por lo que la adhesión a un código de conducta puede resultar de gran utilidad a fin de que el responsable o encargado del tratamiento puedan acreditar su cumplimiento de la obligación de garantizar un nivel de seguridad adecuado[554].

En concreto, el artículo 32 RGPD exige a los responsables y encargados del tratamiento una responsabilidad activa a fin de que estos se anticipen a los posibles riesgos que pudieran generar un perjuicio o daño en el derecho de protección de datos de los ciudadanos, todo ello a través de medidas de seguridad tales como: "a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la

[553] Art. 32.2 RGPD establece que: "Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

[554] Art. 32.3 RGPD señala que: "La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo".

confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento". Así pues, las citadas medidas tienen el objetivo de evaluar los riesgos y minimizar el posible impacto que pudiera darse en un futuro a causa de un riesgo concreto, pero que en ningún caso tienen la finalidad de "garantizar el riesgo cero, ya que no existe"[555], extremo relevante que se ha de tener en consideración.

De igual modo, la responsabilidad activa de los responsables y encargados de los tratamientos dimana de la obligación de analizar y evaluar los riesgos a través de un análisis de riesgos "con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos"[556], para lo que el Comité[557] ha de proporcionar directrices sobre una aplicación de medidas oportunas y, así a su vez el responsable y el encargado del tratamiento puedan acreditar el cumplimiento de su deber de realizar un análisis de riesgos con relación al tratamiento de datos[558]. En concreto, este análisis de riesgos consiste, por un lado, en un análisis de riesgos propiamente dicho (examen de los principales activos, posibles amenazas, coste de impacto y consecuencias para los afectados)[559] y, por otro lado, el tratamiento de riesgos (organización de los activos a efectos de minimizar un posible impacto a través de adopción de medidas que le permita al responsable continuar estando activo)[560].

---

[555] LÓPEZ ALONSO, "¿Cómo abordar un análisis de riesgos en un tratamiento de datos de carácter personal sujeto…", *op. cit.*, p. 713.

[556] Considerando n.º 76 RGPD.

[557] De conformidad con lo establecido en el Considerando n.º 139 del RGPD, el Comité de protección de datos es un organismo independiente de la Unión Europea con responsabilidad jurídica propia. Está compuesto por un presidente, los directores de las autoridades de control de los Estados miembros y el Supervisor europeo de protección de datos.

[558] Considerando n.º 77 RGPD.

[559] LÓPEZ ALONSO, "¿Cómo abordar un análisis de riesgos en un tratamiento de datos de carácter personal sujeto…", *op. cit.*, p. 715.

[560] LÓPEZ ALONSO, "¿Cómo abordar un análisis de riesgos en un tratamiento de datos de carácter personal sujeto…", *op. cit.*, p. 716, afirma que: "Para realizar un análisis de un tratamiento es recomendable hacer una tabla en la que se señalen los activos que se van a analizar; las amenazas a las que están sometidos los activos; el valor que tienen los activos en relación con los interesados y la propia organización; la valoración del daño en relación con la matriz compuesta por la confidencialidad, integridad y disponibilidad; la probabilidad de que la amenaza se materialice; el riesgo calculado a través de la aplicación de la fórmula que da como resultado el valor del activo multiplicado por el daño multiplicado

Por último, los responsables o encargados del tratamiento están obligados a "adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto"[561] todo ello a efectos de asegurar el cumplimiento de los principios, derechos y garantías regulados en el RGPD. En ese sentido, se estima pertinente que la ley sectorial regule de manera específica algunas medidas de seguridad, como por ejemplo las siguientes:

Por un lado, sobre las medidas de seguridad para la instalación de cámaras de videovigilancia, entre otras cuestiones, se estima conveniente que la ley sectorial regule las situaciones en las que se está permitido su uso en los centros sanitarios a los efectos de garantizar la seguridad de las personas y de las instalaciones (lugares de acceso, pasillos y corredores, no dentro de la consulta médica), así como las obligaciones del centro sanitario[562].

De igual forma, a criterio del legislador, cabe la posibilidad de que la ley sectorial incluya dentro de su regulación el régimen de un registro central[563] donde se almacenen y capturen los datos de salud de los pacientes a fin de garantizar una circulación libre y acceso directo a los mismos entre los profesionales sanitarios y los

---

por la probabilidad, y, por último, determinar si el riesgo es aceptable o no para la organización, determinando las acciones que se deberán tomar".

[561] De acuerdo a lo establecido en el Considerando n.º 78 RGPD.

[562] V. gr.: obligación de informar sobre su existencia a través de carteles informativos e informar al paciente, en caso de que lo solicite, sobre la finalidad de la instalación de las cámaras de videovigilancia, el tiempo de mantenimiento de las grabaciones, del responsable de la grabación y, la posibilidad de ejercer derechos.

[563] Actualmente en España se reconocen diversos registros de información sanitaria existentes en diferentes ámbitos profesionales y científicos, de conformidad con el artículo 58.5 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud. En concreto, se encuentran reconocidos los siguientes registros: 1) Registro de Recursos y Calidad asistencial en las Unidades Clínicas de Cardiología (Registro RECALCAR); 2) Base de Datos Conjunta de la Red Española de Registros de Cáncer (REDECAN), integrada por todos los registros poblacionales de cáncer en España, y el Registro Español de Tumores Infantiles (RETI-SEHOP); 3) Registro de la Infección Nosocomial en las Unidades de Cuidados Intensivos dependiente de la Sociedad Española de Medicina Intensiva, Crítica y Unidades Coronarias (SEMICYUC) de la Fundación Española del Enfermo Crítico; 4) Registro Base de Datos de la Red Española de Costes Hospitalarios dependiente dela Fundación Instituto MAR de Investigaciones Médicas (IMIM); 5) Registro de Análisis del Retraso en el Infarto Agudo de Miocardio (ARIAM) dependiente de la Sociedad Española de Medicina Intensiva, Crítica y Unidades Coronarias; 6) Registro de Variaciones de la práctica médica en el Sistema Nacional de Salud (Atlas VPM) dependiente del Instituto Aragonés de Ciencias de la Salud y; 7) Registro Español de Fertilidad dependiente de la Sociedad Española de Fertilidad. A tales efectos visítese la web del Ministerio de Sanidad donde se pueden localizar las resoluciones de reconocimiento de cada uno de los citados registros: https://www.mscbs.gob.es/estadEstudios/estadisticas/sisInfSanSNS/registros/registros.htm

distintos centros de salud públicos de todo el territorio español, así como de los registros de efectos adversos[564], estatuyendo las garantías necesarias a fin de proteger los datos de salud del afectado por el efecto adverso.

No parece que exista duda, tampoco, que la ley de protección de datos de salud incluya en su contenido la regulación del acceso y la protección de los datos contenidos en la carpeta personal de salud, como nuevo soporte informático donde el paciente tiene almacenados de manera personal la información de su salud. Así pues, se considera oportuno que, entre otros extremos, la ley regule el modo de acceso a la carpeta personal, las personas legitimadas para su acceso, la titularidad del fichero donde se almacenan los datos personales y de salud, así como los derechos de acceso, rectificación, cancelación y oposición del titular en relación con la misma.

2. MEDIDAS DE DEFENSA DEL TITULAR DEL DERECHO A LA INTIMIDAD PERSONAL

Con carácter general, las medidas de defensa del titular del derecho a la intimidad es el derecho de ejecutar una acción de reclamación de daños y perjuicios por medio de demanda judicial contra la persona (física o jurídica) que vulnere su derecho. Además, la ley legitima expresamente a otras a efectos de ejercitar el derecho debido al fallecimiento del titular, estando legitimados[565]: (1) en primer lugar la persona o personas a las que hubiera designado a tal efecto en su testamento; (2) en segundo lugar, en defecto de personas directamente expresamente designadas por el fallecido, estarán legitimados los parientes más próximos del fallecido como el cónyuge, ascendientes, descendientes y los hermanos de la persona afectada y; (3) en defecto de los anteriores, estará legitimado el Ministerio Fiscal, que puede actuar de oficio o a instancia de parte de una persona interesada. En consecuencia, las citadas personas legitimadas operaran en el supuesto de fallecimiento del titular del derecho a la intimidad, pudiendo ejercitar la acción en tres momentos diferentes: por un lado, cuando la intromisión se produce después del fallecimiento del titular, por otro lado, cuando la intromisión se produce en

[564] Arts. 59 y 60 de la Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

[565] Art. 4 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

vida del titular del derecho y posteriormente fallece sin ejercitar la acción y se demuestra que no ejercitó la acción en su día por imposibilidad y, por último, cuando la intromisión se ha producido en vida del titular, el mismo ejercitó la acción en su día y fallece durante el procedimiento sin que el Juzgador dictara sentencia, realmente, están legitimados para continuar con el procedimiento ya iniciado por el titular en vida.

Una vez iniciado el procedimiento, versará por parte del Juzgado en comprobar si el acto encaja en alguno de los supuestos de intromisión ilegítima del derecho a la intimidad y si en el caso en cuestión se han dado algunos de los límites generales recogidos en la ley.

Finalmente, si la sentencia es estimatoria, la misma debe de acordar: poner fin a la intromisión ilegítima, restablecer al perjudicado en el pleno disfrute de los derechos, es decir, protegerle y, prevenir o impedir intromisiones ulteriores [566]. A efectos de lograr las citadas finalidades, la sentencia debe establecer una serie de medidas, tales como medidas cautelares encaminadas al cese inmediato de la intromisión, ordenar en la propia sentencia la difusión de la misma para que sea conocido públicamente su contenido con el objetivo de establecer la protección e incluso la dignidad del titular y, condenar al demandado a la indemnización por daños y perjuicios al titular del derecho a la intimidad por el perjuicio presuntamente ocasionado y, que el titular del derecho no tiene que demostrar que ha sufrido. Por último, el Juzgador tendrá en cuenta a fin de valorar si se ha lesionado: por un lado, el derecho el daño material tanto el daño emergente como el lucro cesante, consistente en el menoscabo patrimonial del titular del derecho vulnerado, y por otro lado, el daño moral, que normalmente existe siempre ante una vulneración del derecho a la intimidad, para lo que se tendrá en cuenta: las circunstancias del caso; la lesión efectiva producida y; el beneficio obtenido por el causante de la lesión como consecuencia de la misma[567].

[566] Art. 9.2 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[567] Art. 9.3 de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

3. MEDIDAS Y GARANTÍAS DE DEFENSA DEL PACIENTE FRENTE A LA VULNERACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN EL RÉGIMEN ESPAÑOL

Como puede imaginarse, la vigente normativa de protección de datos personales regula diversos procedimientos en caso de posible vulneración de la normativa de protección de datos como medidas y garantías del paciente afectado en caso de tratamiento ilícito de sus datos de salud por parte del responsable o encargado del tratamiento. A este respeto, la LOPDGDD establece en su artículo 63 que el régimen aplicable será de los procedimientos tramitados por la Agencia Española de Protección de Datos (en adelante, AEPD) previamente regulados por parte del Gobierno a través de real decreto, encontrándose sometidos, en todo caso, a lo dispuesto en el RGPD, así como en la LOPDGDD y disposiciones reglamentarias que se dicten en su desarrollo y, de carácter subsidiario por las normas generales sobre los procedimientos administrativos, a los efectos de salvaguardar los derechos de defensa y audiencia de los interesados[568].

En concreto, la LOPODGG regula dos procedimientos fundamentales según asea el objeto de la reclamación, estableciendo para cada uno de ellos diferentes formas de iniciación y duración. Así pues, podemos diferenciar entre, por un lado, procedimiento por falta de atención de solicitud del afectado por ejercicio de sus derechos y, por otro lado, procedimiento a los efectos de concretar la existencia de infracción regulada en la normativa vigente de protección de datos personales.

3.1. Procedimiento por falta de atención de solicitud de ejercicio de sus derechos por parte del responsable o encargado del tratamiento

En aquellos casos en los que sea tramitada reclamación por parte del afectado alegando fundamentalmente que no ha sido atendida su solicitud por parte del responsable o encargado del tratamiento de ejercicio del derecho de acceso a los datos personales e información sobre el tratamiento, derecho de rectificación, derecho de

[568] BRITO IZQUIERDO, N., "Recursos, responsabilidad y sanciones (Arts. 77-84 RGPD. Arts. 63-78 LOPDGDD)" en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo),Wolters Kluwer, Madrid, 2019, pp. 670-677.

supresión («el derecho al olvido»), derecho a la limitación del tratamiento, incumplimiento de la obligación de notificación relativa a la rectificación o supresión de los datos personales o la limitación del tratamiento, derecho a la portabilidad de los datos, derecho de oposición y derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles que produzca efectos jurídicos al afectado o le afecte significativamente[569], el procedimiento será iniciado por medio de acuerdo de admisión a trámite adoptado por la AEPD[570], quien tendrá que notificar al afectado su decisión sobre su admisión o inadmisión en el plazo de tres meses[571].

Igualmente, previa resolución, la AEPD podrá remitir la reclamación al delegado de protección de datos designado por el responsable o encargado del tratamiento o al organismo de supervisión adherido. Subsidiariamente, en defecto de los anteriores, la AEPD podrá remitir la reclamación directamente al responsable o encargado del tratamiento a los efectos de que dar respuesta en el plazo de un mes[572]. Posteriormente, una vez notificado al reclamante el acuerdo de admisión a trámite en su caso, el procedimiento se ha de resolver en el plazo de seis meses, transcurrido este plazo el interesado podrá considerar estimada su admisión en caso de no recibir notificación al respecto[573]. Se ha de observar, además, que cabe la inadmisión a trámite de la reclamación formulada por parte del afectado previa evaluación por parte de la AEPD cuando la cuestión reclamada no sea sobre protección de datos personales, carezca de fundamentación, sea abusiva o no se aporte indicios racionales de la existencia de infracción alguna, así como cuando el responsable o encargado del tratamiento hubiera adoptado las medidas adecuadas a efectos de poner fin a la vulneración de la normativa de protección de datos, siendo necesario, o bien que no se haya generado perjuicio alguno al afectado a causa de infracciones consideradas leves, o bien que se garantice plenamente el derecho del afectado por medio de las medidas aplicadas[574].

[569] Derechos reconocidos en los artículos 15 a 22 del RGPD.

[570] Art. 64.1 LOPDGDD.

[571] Art. 65.5 LOPDGDD.

[572] Art. 65.4 LOPDGDD.

[573]Art. 64.1 LOPDGDD.

[574] Apartados 2 y 3 del art. 65 LOPDGDD.

3.2. Procedimientos de determinación de existencia de infracción legal

En los supuestos en los que nos encontramos ante una infracción de lo dispuesto en la normativa vigente de protección de datos, la ley diferencia diversos procedimientos a efectos de determinar la existencia o no infracción legal, en concreto: por un lado, el procedimiento a través de acuerdo de inicio tramitado por iniciativa propia de la AEPD. Por otro lado, el procedimiento tramitado directamente por el afectado ante la AEPD. En este caso, previamente la AEPD decidirá sobre la admisión a trámite de la reclamación sobre la posible infracción legal por parte del responsable o encargado del tratamiento, siguiendo lo establecido en el art. 65 de la LOPDGDD, analizado en el apartado a) sobre el procedimiento de admisión a trámite de la reclamación por falta de atención de solicitud de ejercicio de sus derechos por parte del responsable o encargado del tratamiento.

En tercer lugar, se encuentra el procedimiento iniciado por medio de adopción del proyecto de acuerdo de inicio de procedimiento sancionador. Para aquellos casos en los que se han de aplicar lo dispuesto en el artículo 60 RGPD sobre la «cooperación entre la autoridad de control principal y las demás autoridades de control interesadas», dándose traslado formal al interesado a los efectos de lo previsto en el art. 75 de la LOPDGDD[575]. Y en último lugar, como procedimiento de cierre se regula el procedimiento tramitado de una autoridad de control de otro Estado miembro de la UE de la reclamación formulada ante la misma a la AEPD, al considerarse que es la AEPD la que tiene la condición de autoridad de control principal para la tramitación de la reclamación. En este sentido, el párrafo quinto del apartado 2 del artículo 64 LOPDGDD se establece que los procedimientos tendrán una duración máxima de nueve meses a contar, bien desde la fecha del acuerdo de inicio, bien, en su caso desde la fecha del proyecto de acuerdo de inicio, produciéndose la caducidad una vez trascurrido el plazo de nueve meses y, por tanto, el archivo de las actuaciones.

[575] Artículo 75 LOPDGDD, establece que: "Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas".

Por último, debe destacarse como requisito indispensable que se dictará por parte de la Presidencia de la AEPD a efectos de ejercer la potestad sancionadora, acuerdo de inicio de procedimiento donde se concretarán los hechos, identidad de la persona o entidad que haya vulnerado la normativa de protección de datos, así como la infracción y sanción correspondiente a la misma[576].

A) Actuaciones previas de investigación

Por su parte, la LOPDGDD concreta una serie de actuaciones previas de investigación a la adopción del acuerdo de inicio de procedimiento y, tras la admisión a trámite de la reclamación, así como en supuestos en que la AEPD haya actuado por propia iniciativa, actividad de investigación que deberá ser efectuada por los propios funcionarios de la AEPD o por "por funcionarios ajenos a ella habilitados expresamente por su Presidencia"[577] con la finalidad de "logar una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento[578]". No obstante, cabe señalar que ante los casos en los que se manejen un tráfico masivo de datos personales, como puede ser ante análisis por medio de la técnica *big data*, la AEPD en todo caso, actuará en caso de ser necesaria una investigación del tratamiento.

En virtud de lo anterior, se ha tener en consideración que las actuaciones previas de investigación se han de efectuar en un plazo máximo de 12 meses[579] y, estarán sometidas a lo dispuesto en los artículos 51 a 54 LOPDGDD, sobre potestades de investigación y planes de auditoría preventiva.

[576] Al respecto, el párrafo segundo del art. 68 LOPDGDD añade que: "Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo".

[577] Art. 52.2 LOPDGDD.

[578] Art. 67 LOPDGDD

[579] "[…] a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la AEPD actúe por propia iniciativa o como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.3 de esta ley orgánica" (art. 67.2 LOPDGDD).

B) Medidas provisionales y de garantía de los derechos

Teniendo todo lo anterior presente, se relaciona a continuación una serie de medidas provisionales y de garantía de los derechos[580] que serán llevadas a cabo durante las actuaciones previas de investigación o una vez iniciado un procedimiento para el ejercicio de la potestad sancionadora, medidas que serán adoptadas por la AEPD a los efectos de salvaguardar el derecho fundamental de protección de datos, en especial los derechos y las libertades de los interesados.

Por ende, la LOPDGDD regula una medida con carácter más reactivo que preventivo, pero indudablemente efectiva, es la de ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplimiento de lo anterior, proceder a la inmovilización de los datos, ante tratamientos de datos personales (su comunicación o transferencia internacional) supongan un menoscabo grave del derecho de protección de datos. De igual modo, ante la iniciación de un procedimiento por falta de atención de solicitud de ejercicio de sus derechos por parte del responsable o encargado del tratamiento, la AEPD podrá por medio de resolución motivada – y previa audiencia al responsable del tratamiento – obligar al mismo a atender el derecho solicitado. La presente medida podrá ser adoptada por la AEPD en cualquier momento incluso previamente a la iniciación del procedimiento, debiéndose dar el trámite habitual al resto de cuestiones objeto de la reclamación.

En último lugar, el art. 66 LOPDGDD se refiere también a la determinación del alance territorial para aquellos casos en los que la AEPD considere que no tiene condición de autoridad de control principal a efectos de tramitar alguno de los procedimientos anteriormente indicados, debe en tal caso remitir sin más trámite la reclamación formulada a la autoridad de control principal que considere oportuna, lo que implicará el archivo provisional del procedimiento, sin perjuicio de que la AEPD dicte resolución adoptando la decisión de desestimación o rechazo de la reclamación por parte del autoridad de control principal finalmente competente, notificando la misma al reclamante e informando de ello al responsable del tratamiento.

[580] Art. 69 LOPDGDD.

Así pues, resulta de interés que la ley sectorial sobre el procedimiento de ejercicio de los derechos de protección de datos del paciente reincida en la obligación del responsable del tratamiento de responder por medio electrónico (salvo manifestación contraria del interesado) en el plazo de un mes (prorrogable dos meses por causas de extrema complejidad o volumen) la solicitud del interesado ejerciendo sus derechos, salvo imposibilidad de identificación del mismo por parte del responsable del tratamiento, para lo que podrá solicitar información adicional al solicitante.

De igual modo, ante supuestos en los que los derechos de los interesados supongan un obstáculo o imposibiliten gravemente las finalidades científicas en el ámbito de la investigación biomédica o por cumplimiento de obligaciones legales, sería conveniente que la ley de protección de datos de salud regulase los límites a los derechos a los interesados[581], tales como, el derecho de acceso a los datos y a obtener información, derecho de rectificación, derecho a la limitación del tratamiento, derecho de oposición y derecho al olvido, a los efectos de garantizar el alcance de los fines científicos.

Se ha de observar, además, que debido a que las funciones generales del Ministerio Fiscal en los procedimientos judiciales es la de promover la acción de la justicia en defensa de la legalidad, así como de los derechos de los ciudadanos y del interés público tutelado por la ley, de oficio o a petición de los interesados y velar por la independencia de los Tribunales y, ante todo defender el interés social[582], resulta de

[581] De conformidad con el art. 89.2, art. 17 RGPD, considerando 156, 69 y art. 32 LOPDGDD con relación al bloqueo de datos.

[582] Art. 1 del Estatuto Orgánico del Ministerio Fiscal, aprobado por la Ley 50/1981, de 30 de diciembre. Asimismo, el art. 3 señala las siguientes actuaciones del Ministerio Fiscal: "Para el cumplimiento de las misiones establecidas en el artículo 1, corresponde al Ministerio Fiscal: 1. Velar por que la función jurisdiccional se ejerza eficazmente conforme a las leyes y en los plazos y términos en ellas señalados, ejercitando, en su caso, las acciones, recursos y actuaciones pertinentes. 2. Ejercer cuantas funciones le atribuya la ley en defensa de la independencia de los jueces y tribunales. 3. Velar por el respeto de las instituciones constitucionales y de los derechos fundamentales y libertades públicas con cuantas actuaciones exija su defensa. 4. Ejercitar las acciones penales y civiles dimanantes de delitos y faltas u oponerse a las ejercitadas por otros, cuando proceda. 5. Intervenir en el proceso penal, instando de la autoridad judicial la adopción de las medidas cautelares que procedan y la práctica de las diligencias encaminadas al esclarecimiento de los hechos o instruyendo directamente el procedimiento en el ámbito de lo dispuesto en la Ley Orgánica reguladora de la Responsabilidad Penal de los Menores, pudiendo ordenar a la Policía Judicial aquellas diligencias que estime oportunas. 6. Tomar parte, en defensa de la legalidad y del interés público o social, en los procesos relativos al estado civil y en los demás que establezca la ley. 7. Intervenir en los procesos civiles que determine la ley cuando esté comprometido el interés social o cuando puedan afectar a personas menores, incapaces o desvalidas en tanto se provee de los mecanismos ordinarios de representación. 8. Mantener la integridad de la jurisdicción y competencia

interés que la Ley de protección de datos de salud haga especial mención a la necesidad de intervención del Ministerio Fiscal[583] como parte en los procedimientos judiciales iniciados de oficio o por interesado por causas de posible vulneración del derecho de protección de datos del paciente ante situaciones donde existan dudas jurídicas si consta justificada la finalidad de salud pública o investigación biomédica cuando sean tratados los datos de salud del paciente sin su consentimiento.

Por último, debido a que la normativa vigente de protección de datos (comunitaria y estatal), así como el Tribunal de Justicia de la Unión Europea[584], otorgan un papel sumamente relevante a las autoridades de control a efectos de garantizar una efectiva protección de las personas físicas con respecto al tratamiento de sus datos personales. Por ello, se propone que la ley sectorial regule acciones de obligado cumplimiento por parte del responsable y encargo del tratamiento ante las autoridades de control cuando realicen proyectos de *big data* sanitarios, tanto en el momento inicial del diseño del proyecto como durante la realización y desarrollo del mismo.

---

de los jueces y tribunales, promoviendo los conflictos de jurisdicción y, en su caso, las cuestiones de competencia que resulten procedentes, e intervenir en las promovidas por otros.9. Velar por el cumplimiento de las resoluciones judiciales que afecten al interés público y social. 10. Velar por la protección procesal de las víctimas y por la protección de testigos y peritos, promoviendo los mecanismos previstos para que reciban la ayuda y asistencia efectivas. 11. Intervenir en los procesos judiciales de amparo, así como en las cuestiones de inconstitucionalidad en los casos y forma previstos en la Ley Orgánica del Tribunal Constitucional. 12. Interponer el recurso de amparo constitucional, así como intervenir en los procesos de que conoce el Tribunal Constitucional en defensa de la legalidad, en la forma en que las leyes establezcan. 13. Ejercer en materia de responsabilidad penal de menores las funciones que le encomiende la legislación específica, debiendo orientar su actuación a la satisfacción del interés superior del menor. 14. Intervenir en los supuestos y en la forma prevista en las leyes en los procedimientos ante el Tribunal de Cuentas. Defender, igualmente, la legalidad en los procesos contencioso-administrativos y laborales que prevén su intervención. 15. Promover o, en su caso, prestar el auxilio judicial internacional previsto en las leyes, tratados y convenios internacionales. 16. Ejercer las demás funciones que el ordenamiento jurídico estatal le atribuya. Con carácter general, la intervención del fiscal en los procesos podrá producirse mediante escrito o comparecencia. También podrá producirse a través de medios tecnológicos, siempre que aseguren el adecuado ejercicio de sus funciones y ofrezcan las garantías precisas para la validez del acto de que se trate. La intervención del fiscal en los procesos no penales, salvo que la ley disponga otra cosa o actúe como demandante, se producirá en último lugar".

[583] No obstante, sin perjuicio de que en la ley procesal correspondiente mencione la intervención del Ministerio Fiscal ante procedimientos judiciales de materia de protección de datos de salud.

[584]A tales efectos, el TJUE en el comunicado de prensa n.º117/15, de 6 de octubre de 2015, sentencia en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner, señala expresamente que "aunque el Tribunal de Justicia tiene competencia exclusiva para declarar la invalidez de un acto de la Unión, las autoridades nacionales de control a las que se haya presentado una solicitud pueden, aun cuando una Decisión de la Comisión declare que un país tercero ofrecer un nivel de protección adecuado de los datos personales, examinar si la transferencia de los datos de una persona a ese país respeta las exigencias de la legislación de la Unión sobre la protección de esos datos así como acudir ante los tribunales nacionales, al igual que la persona interesada, con el fin de que éstos planteen una cuestión prejudicial sobre la validez de esa Decisión".

En consecuencia, se pueden dividir estas acciones a efectuar por parte del responsable de tratamiento en aquellas que debe realizar ante la autoridad de control en el momento del diseño y aquellas acciones que se deben realizar durante el desarrollo del proyecto *big data*. Así pues, en el momento del diseño, el responsable del tratamiento debe, por un lado, consultar previamente a la autoridad de control sobre los resultados de la EIPD efectuada, sobre todo comunicar la existencia de alto riesgo si lo hubiera a fin de que la autoridad de control le resuelva sobre la existencia o no de vulneración de la normativa de protección de datos y, asesorar por escrito al responsable mientras no dicte resolución definitiva sobre el alto riesgo cuestionado[585].

En cambio, el responsable del tratamiento en su consulta debe comunicar a la autoridad de control de las medidas técnicas y organizativas concretas convenientes implantar en el proyecto *big data* a efectos de cumplir con normativa de protección de datos, de dicha cuestión también deberá pronunciarse la autoridad de control en su resolución sobre la suficiencia de las medidas, en caso de no ser suficientes, asesorar sobre otras medidas pertinentes de implantación[586]. Por otro lado, el responsable del tratamiento en el momento del diseño debe adoptar e implantar las medidas técnicas y organizativas apropiadas en proyectos *big data* (tanto las propuestas por la organización como por la autoridad de control) a efectos de poder demostrar posteriormente a la autoridad de control que el tratamiento es conforme a la normativa vigente de protección de datos[587].

Posteriormente, en el momento del desarrollo del proyecto *big data* sanitario, el responsable del tratamiento debe obligatoriamente: (1) Disponer de un Registro de actividades de tratamiento asociadas al mismo debido a que nos encontramos ante proyectos de investigación biomédica o asistencia sanitaria de interés público donde se manejan datos incluidos en las categorías especiales de datos personales como son los de salud (art. 9.1 RGPD), registro que pondrá a disposición de la autoridad de control pertinente[588]; (2) Notificar a la autoridad de control de las posibles violaciones de

[585] Art. 35 RGPD.

[586] Art. 57.1 RGPD.

[587] Art. 24.1 RGPD.

[588] Art. 30 RGPD.

seguridad de los datos personales vinculados a un proyecto *big data*[589]; (3) Nombrar a un Delegado de Protección de Datos ante la realización del proyecto *big data*[590], a fin de que el mismo se coordine y coopere con la autoridad de control correspondiente[591] y; (4) Deber general de cooperar con la autoridad de control en el desempeño de sus funciones a fin de garantizar la protección de la privacidad de los interesados en el proyecto *big data* en el sector de la salud pública o de la investigación biomédica y farmacéutica.

Así es dable llegar a la conclusión, de que la ley sectorial en su parte especial regule los anteriores deberes y obligaciones del responsable del tratamiento ante la autoridad de control en proyectos de *big data* sanitario, al ser la misma una institución diseñada por el legislador europeo a efectos de garantizar el cumplimiento de la normativa de protección de datos en cada uno de los Estados miembros.

Asimismo, dada la experiencia de la pandemia provocada por el patógeno COVID-19, la ley sectorial debe prever las situaciones de urgencia sanitaria que supongan un alto riesgo para la salud pública a efectos de acelerar la colaboración público-privada en los procesos de investigación y de toma de decisiones, a efectos de permitir un tratamiento lícito por parte de los centros sanitarios y de investigación, así como así como otras entidades, públicas o privadas, que tengan como finalidad resolver y/o prevenir problemas dimanantes de la situación de urgencia sanitaria aplicando herramientas *big data* o IA, sin ser necesaria la autorización e informe favorable previo de la autoridad de control de protección de datos o/y del Comité de Ética de la Investigación.

[589] Art. 33 RGPD.

[590] La obligatoriedad de nombrar a un DPD dimana principalmente del riesgo de que los proyectos *Big Data* puedan ser calificados como tratamiento a gran escala por el gran volumen de datos a manejar.

[591] Art. 37 RGPD.

III. EL SECRETO PROFESIONAL Y EL DERECHO DE CONFIDENCIALIDAD DE LOS PACIENTES

1. MARCO JURÍDICO

El secreto profesional y el deber de confidencialidad de los datos sanitarios por parte de los profesionales de la sanidad, así como por aquellas personas que tienen acceso a los mismos, son deberes que dimanan directamente del derecho a la intimidad del paciente puesto que el citado derecho en el ejercicio de la medicina queda reflejado fundamentalmente en la relación de confianza entre los facultativos sanitarios y el paciente (en particular, en la relación médico – paciente) primordial para una asistencia sanitaria eficiente, así como el no consentimiento por parte del paciente a la privada, incluyendo el derecho a la intimidad corporal, en la prohibición de difusión de la información obtenida, así como en la protección de los datos personales, entre otros.

Debido a lo anterior – se anticipa – existe un amplio marco jurídico del secreto profesional y confidencialidad de los datos siendo este un deber – ético y jurídico - protegido desde la Declaración Universal de los Derechos Humanos hasta los Códigos Deontológicos. Así pues, desde el ámbito del Derecho internacional, se ha destacar el artículo 10.1 del Convenio del Consejo de Europa para la protección de los Derechos Humanos y la Dignidad del Ser Humano con respecto a las aplicaciones de la biología y la medicina, de 4 de abril de 1997, así como el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948. En el Derecho comunitario, resulta evidente hacer mención – aunque será esta cuestión por tratar en profundidad más adelante – al artículo 5.1.f) del Reglamento (UE) 2016/679, así como de las siguientes recomendaciones del Consejo de Europa: 1) Recomendación R (81) 1, de 23 de enero de 1981, del Comité de Ministros del Consejo de Europa a los Estados Miembros, relativa a la reglamentación aplicable a los bancos de datos médicos automatizados. 2) Recomendación R (83) 10, de 23 de septiembre de 1983, del Comité de Ministros del Consejo de Europa a los Estados Miembros, relativa a la protección de los datos de carácter personal utilizados con fines de investigación científica y de estadística. 3) Recomendación R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estado Miembros, sobre Protección de datos médicos.

Por otro lado, en el ordenamiento jurídico español, se ha de destacar las siguientes normas jurídicas:

En primer lugar, los artículos 18.1, 24 y 43 de la Constitución Española. De igual modo, el Código Penal (en adelante CP) en relación con el delito de descubrimiento de secretos ajenos, en su artículo 197 configura varias formas de comisión, tutelándose en cada una de ellas el derecho fundamental a la intimidad personal y familiar y a la propia imagen. Igualmente, el artículo 199.2 CP tipifica la conducta delictiva del delito de revelación de secretos por parte del profesional que en incumplimiento de su obligación de reserva divulgue los secretos de otra persona. Por último, los artículos 413 a 418 CP se regulan los delitos en relación con la "infidelidad en la custodia de documentos y de la violación de secretos", en concreto, el artículo 417 del CP castiga la conducta de revelación de secretos o información por parte de la autoridad o funcionario público de los que tenga conocimiento a razón de su cargo y no deba divulgarlos.

En materia de protección de datos personales, el artículo 5 del LOPDGPP, artículo que será estudiado detenidamente en los siguientes puntos del presente trabajo. Por otro lado, los artículos 2.1, 2.2, 7.3 y 7.4 de la Ley Orgánica 1/1982, de 5 de mayo de protección civil al honor, a la intimidad y a la propia imagen, en concreto su artículo 7.4 establece como intromisión ilegítima la revelación de datos personales de una persona o familia conocidos a través de la actividad profesional u oficial de quien lo revela, imponiendo la obligación de indemnizar el daño causado a causa de la intromisión. De manera específica, la Ley 14/1986 de 25 de abril, General de Sanidad, reconoce a los pacientes y usuarios de centros sanitarios públicos como privados (art. 10.15) el derecho a la intimidad y confidencialidad de la información relacionada con su caso (arts. 10.1 y 10.3), así como en el artículo 7 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 y documentación clínica. Igualmente, en la Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud el artículo 19 j) se protege la confidencialidad del paciente, así como en la Orden por la que se aprueba el Reglamento General para el Régimen, Gobierno y Servicio de las Instituciones Sanitarias de la Seguridad Social, de 19 de julio de 1972 en el art. 148.3 se regula el derecho de los enfermos asistidos a que se mantenga el secreto profesional

sobre la enfermedad del paciente de conformidad con lo establecido en las normas deontológicas.

De manera específica la Ley 30/1979, sobre extracción y trasplante de órganos, en su artículo 4.d) donde establece que se ha de garantizar el anonimato del receptor y, en el Real Decreto 1723/2012, de 28 de diciembre, por el que se regulan las actividades de obtención, utilización clínica y coordinación territorial de los órganos humanos destinados al trasplante y se establecen requisitos de calidad y seguridad en su artículo 5, ambas normas jurídicas regulan el secreto profesional en materia de extracción y trasplante de órganos. Igualmente, consta regulado el secreto profesional y el deber de confidencialidad en casos de interrupción voluntaria del embarazo, en el artículo 6 del Real Decreto 831/2010, de 25 de junio, de garantía de la calidad asistencial de la prestación a la interrupción voluntaria del embarazo, así como con las técnicas de reproducción asistida, de conformidad con el artículo 18. 2 y 3 de la Ley 14/2006, de 26 de mayo. De igual modo, cabe señalar que en el sector farmacéutico, a pesar de que no afecta directamente a los profesionales sanitarios, sí que es un sector estrechamente vinculado con la sanidad, por lo que igualmente en el Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios, en los artículos 16, 32, 59, 62, 97 y 106 se regula la confidencialidad como garantía de transparencia e idoneidad por parte del sector farmacéutico.

Desde la ética profesional variados son los códigos deontológicos que regulan la responsabilidad del deber de confidencialidad y la obligación de secreto profesional de los facultativos sanitarios como conductas propias de diligencia en cumplimiento de la *lex artis* de la profesión de la medicina. En concreto, se han de destacar los artículos 27 a 31, además de los artículos de otros capítulos 58.3, 62.2, 62.3, 62.7, 64.2 del Código de Deontología Médica. Guía de Ética Médica (Madrid, julio 2011), los artículos 29 a 42 del Código de Deontología y Normas de Ética Médica del Consejo General de Colegios de Médicos de Cataluña (Barcelona, 24-1-2005), los artículos 19 a 21.3 del Código Deontológico de la Profesión de Enfermería (Madrid, 14-7-1989, corregido y ratificado en resolución 2/1998), los artículos 23 a 29 del Código de Ética de Enfermería del Colegio Oficial de Ayudantes Técnicos *sanitario*s y Diplomados en

Enfermería de Barcelona de 1986, así como el artículo 11 del Código Deontológico de la profesión de Diplomado en Trabajo Social de 29 de mayo 1999.

2. DE LA INTIMIDAD A LA CONFIDENCIALIDAD Y EL SECRETO PROFESIONAL

Es un hecho notorio que todo dato, hecho o vivencia que forma parte de la esfera personal (o familiar) de una persona igualmente de manera implícita resulta confidencial se encuentra reservado frente a los demás, debido a que la confidencialidad tiene como finalidad proteger la información íntima que el titular del derecho a la intimidad decide no divulgar o dar a conocer a otros[592]. Por ende, todo dato que se considere confidencial pertenece de manera intrínseca al ámbito de la intimidad del paciente.

Por su parte, el secreto profesional en el sector sanitario aparece por vez primera en el Juramento Hipocrático de la Asociación Médica Mundial (AMM) en 1948 como un compromiso ético del profesional sanitario con el paciente, a través de la siguiente declaración:

"Todo lo que habré visto u oído durante la cura o fuera de ella en la vida común, lo callaré y lo conservaré siempre como secreto, si no me es permitido decirlo. Si mantengo perfecta e intacta fe en este juramento que me sea concedida una vida afortunada y la futura felicidad en el ejercicio del acto, de modo que mi fama sea alabada en todos los tiempos; pero si fallara el juramento hubiera jurado en falso, que ocurra lo contrario".

[592] *Vid.* SSTC 115/2000, de 5 de mayo; 83/2002, de 22 de abril, y 99/2002, de 6 de mayo. *Vid.* O'CALLAGHAN MUÑOZ, "Personalidad y derechos de la personalidad...", *op. cit.*, p. 1249; GARBERÍ LLOBREGAT, *Los procesos civiles de protección del honor...*, *op. cit.*, p. 140; ALBALADEJO, *Derecho Civil..., op. cit.*, pp. 463 y 464; LACRUZ BERDEJO et al., *Elementos de Derecho Civil..., op. cit.*, pp. 92 y 93; LASARTE, C., *Principios de Derecho Civil*, Tomo I, Parte General y Derecho de la Persona, Madrid, Marcial Pons.

Sin embargo, poco queda ya del secreto profesional de juramento hipocrático en el sentido de que entonces era consagrado más bien como un deber del buen profesional sanitario, sin tener en cuenta el derecho de confidencialidad del paciente[593]. En la actualidad a pesar de que el concepto de secreto profesional y el concepto de confidencialidad frecuentemente en la práctica se suelen confundir empleándose ambos de manera indistinta, lo cierto es que el secreto profesional es un deber ético – legal del profesional sanitario hacía el paciente y, la confidencialidad es un derecho del paciente en relación a sus datos personales que puede ejercer tanto directamente frente a los facultativos sanitarios, como frente a toda persona – física o jurídica – que tenga acceso a sus datos. En consecuencia, se puede afirmar que el deber de secreto médico dimana del derecho del paciente a la confidencialidad de sus datos personales.

En síntesis, el secreto profesional es un deber ético y legal que se le exige a los facultativos sanitarios – fundamentalmente a los profesionales de medicina y de la enfermería – a efectos de preservar la información sobre la salud y vida del paciente a la que hayan podido acceder y conocer de manera directa o indirecta en el ejercicio de su profesión, siempre y cuando no medie autorización expresa del paciente o no existan límites legales que permita su divulgación[594].

Al respecto el Tribunal Supremo en la Sentencia de fecha 4 de abril de 2001 manifiesta que:

"[…] nos encontramos ante una obligación impuesta por la Ley General de Sanidad 14/86, de 25 de abril, donde en el párrafo tercero de su artículo 10 establece el derecho a los ciudadanos "a la confidencialidad de toda la información relacionada con su proceso y con estancia en instituciones sanitarias", y concurrente en el historial clínico-sanitario, en el que según el artículo 6.1 del citado texto legal deben "quedar plenamente garantizado el derecho del enfermo a su intimidad personal y familiar y el

[593]TRONCOSO REIGADA, A., "La confidencialidad de la historia clínica", *Cuadernos de Derecho Público,* Núm. 27, 2006, pp. 45-147; TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio,* Tirant lo Blanch, Valencia, 2010, pp. 1099-1268; DE MIGUEL SÁNCHEZ, N., *Secreto médico, confidencialidad e información sanitaria,* Ed. Marcial Pons, Madrid, 2002, pp. 266-317; SUAREZ RUBIO, S. M.ª., *Constitución y privacidad sanitaria*, Tirant lo Blanch, Valencia, 2015, pp. 287-311.

[594]Fundación de Ciencias de la Salud, *Intimidad, confidencialidad y secreto. Guías de ética en la práctica médica*, 2015, p. 7 y ss. Documento disponible en: https://www.cgcom.es/sites/default/files/guia_confidencialidad.pdf (última consulta 23/11/19).

deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica".

Por ende, desde una perspectiva jurídica el secreto profesional es un deber legal de interés público que emana de la profesión de la medicina y de la enfermería encaminado a preservar la seguridad, intimidad y honor de los enfermos y sus familiares y, desde una perspectiva ética, el secreto profesional es un valor moral estrechamente unido a la dignidad, la intimidad del paciente y de la confidencialidad de sus datos[595].

[595] En este sentido, se ha destacar diversas recomendaciones para los profesionales sanitarios a efectos de preservar la intimidad y confidencialidad de los datos de carácter personal de los pacientes de la *Guía de intimidad, confidencialidad y protección de datos de carácter persona* de la Consejería de Sanidad Junta de Castilla y León:

(a) *"Respecto a la intimidad corporal*: 1) Tanto con un paciente vestido como desnudo debe respetarse su "espacio físico" y al entrar en la habitación o en la sala de consulta en que se encuentre el paciente se llamará previamente a la puerta. 2) Las puertas de las salas de consultas y habitaciones donde se realicen exploraciones deben permanecer cerradas durante las mismas, salvo situaciones excepcionales. Cuando la habitación es compartida, se deben utilizar las cortinas separadoras al explorar a cada paciente. 3) En las exploraciones, cuidados o actividades de higiene que lleven a cabo los profesionales deberá respetarse la intimidad del paciente, indicándole con anterioridad la intención de iniciar una exploración física y si para ello es preciso que se descubra una parte del cuerpo. 4) Debe respetarse el derecho a la intimidad de todas las personas y especialmente de las más vulnerables (ancianos, enfermos mentales, menores, etc.). 5) No se deben grabar ni difundir por cualquier medio, imágenes que permitan identificar a los pacientes sin su previa y expresa autorización.

(b) *Respecto a la información sobre la salud del paciente*: 1) No pueden revelarse datos de salud u otros datos personales del paciente sin su expreso consentimiento o sin que una norma lo establezca. 2) Respecto a los comentarios sobre la salud de los pacientes realizados en lugares públicos (pasillos, ascensores, cafeterías, etc.) hay que evitarlos, incluso aunque el interlocutor sea un profesional sanitario que participe en el proceso asistencial. 3) Si un trabajador del centro sanitario hace preguntas sobre un paciente en cuyo cuidado no está involucrado no se le debe dar información que no haya sido autorizada por el propio paciente. 4) La información asistencial sólo se facilitará al paciente o a aquellas personas vinculadas a él por razones familiares o de hecho que aquél permita de manera expresa o tácita. La ley prevé que se debe informar a personas distintas del paciente en los supuestos en que sea necesario completar o sustituir un déficit de capacidad. 5) El paciente puede prohibir que se dé información asistencial sobre su proceso a cualquier persona. Esta decisión debe ser plenamente respetada y constar por escrito. 6) Ante cualquier pregunta de personas ajenas al paciente, el profesional debe remitirle al paciente mismo, o a sus familiares, quienes considerarán si se les ha de informar o no. 7) La información ha de ofrecerse al paciente o a los familiares, en su caso, en lugares específicos y reservados, evitando en lo posible informar en los pasillos o en lugares de paso del público en general. 8) En el caso de solicitud de ambulancias, no debe constar el diagnóstico clínico del paciente. Pueden utilizarse descripciones funcionales como "incapacidad para deambular" o "disnea extrema". Si es preciso adjuntar información clínica para otro destinatario se enviará en sobre cerrado. 9) El personal que acceda a información que contenga datos de carácter personal, ya sea de ficheros automatizados o de otro tipo, no podrá realizar copias para uso privado o personal.

(c) *Respecto a la historia clínica*: 1) La historia se redactará y se elaborará de forma comprensible. 2) Las hojas de interconsultas, los resultados de pruebas diagnósticas y las historias clínicas, que pasan por muchas manos y no todas implicadas en el tratamiento, deben circular de modo que se preserve la confidencialidad de los datos. 3) Para las anotaciones subjetivas del profesional y datos de terceras personas se debe reservar un apartado específico y separado de los datos

clínicos del paciente y del resto de información, en la medida en que constituyen un límite en el acceso a la historia clínica. 4) Sólo debe entregarse la historia clínica al paciente o a sus representantes debidamente autorizados y acreditados. Los familiares tienen derecho a acceder a la información de pacientes fallecidos, salvo que aquél lo haya prohibido explícitamente. 5) Salvo situaciones excepcionales la información confidencial no debe darse por teléfono. 6) Tendrán acceso a la historia clínica de un paciente los profesionales que realicen su diagnóstico y tratamiento, como instrumento fundamental para su adecuada asistencia. El personal de gestión y administración tendrá limitado su acceso a los datos necesarios para el desempeño de sus funciones. 7) Todo el personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto. 8) Los profesionales sanitarios deben participar en los procesos de centralización de la historia clínica, formulando sugerencias sobre los niveles de acceso a la información que deben habilitarse y, en particular, sobre la conveniencia de mantener reservados determinados accesos. 9) Los profesionales deben conocer las medidas de seguridad aplicables para las funciones que desempeñan, así como notificar cualquier anomalía que detecten y pueda afectar a la seguridad de la información.

(d) *En el caso de ficheros automatizados*: 1) Para minimizar los riesgos de vulneración del derecho a la confidencialidad, cada profesional sanitario con actividad asistencial deberá tener una clave (incluidos los residentes y sustitutos) que no deberá ceder a nadie y de cuyo uso será el único responsable. 2) El personal administrativo debe acceder a aquella parte de la historia que deba conocer por el ejercicio de sus funciones y siempre accederá a través de clave intransferible. 3) Una vez finalizada la sesión de trabajo en el ordenador, debe cerrarse la ventana de consulta para impedir que cualquier persona ajena pueda utilizarla sin necesidad de usar la clave.

(e) *Respecto a la destrucción de documentos*: Los documentos que contengan datos de carácter personal y que ya no sean de utilidad, deberán destruirse por completo mediante métodos que aseguren su completa eliminación de forma que no sea posible extraer información ni identificar a la persona a la que se refieran". Consejería de Sanidad de la Junta de Castilla y León, *Guía de intimidad, confidencialidad y protección de datos de carácter personal*, pp. 27-29. Disponible en: http://www.enfermerialeon.com/docs/comision_deo/GuiaConfidencialidadDatosJCyL.pdf)

De igual modo, en junio de 2003, la Junta Directiva de la Sociedad Española de Sanidad Pública y Administración Sanitaria (SESPAS), publicó el *Manifiesto en defensa de la confidencialidad y el secreto médico, Gac Sanit,* Núm. 17, Vol. 4, pp. 337-339, donde establece las siguientes quince cuestiones fundamentales de protección de datos sanitarios: 1. La intimidad es un valor ético y jurídico amparado por la Constitución y por la legislación vigente en nuestro país, y como tal hay que demandarlo y protegerlo por profesionales y usuarios. 2. El valor supremo de la vida y la defensa de la salud son motivo de que en la intimidad de la consulta médica se revelen secretos que no se confían ni siquiera a los más allegados; por eso la confidencialidad y el secreto médico son imprescindibles en la relación médico-paciente. 3. Los datos médicos pertenecen a cada paciente, y éste tiene todos los derechos sobre los mismos. El profesional sanitario, a quien el paciente se los confía, actuará como depositario, ejerciendo esos derechos como agente y responsable ante el paciente. 4. Los datos médicos son tan relevantes que si falla la confidencialidad no sólo está en peligro la intimidad, sino el ejercicio de otros derechos fundamentales, como el derecho al trabajo, a la educación, o la defensa de la salud y de la vida. El derecho a la confidencialidad que tiene todo paciente es la única garantía para la defensa de su intimidad. 5. El paciente tiene el derecho a ser informado de un modo que pueda comprender: acerca del responsable, destino y uso de sus datos personales; a que se requiera su consentimiento previo para la recogida y utilización de los datos, y el derecho a acceder, rectificar y cancelar dichos datos; en definitiva, el paciente tiene autonomía y poder de disposición sobre sus datos personales. Como establece el Tribunal Constitucional, todo paciente tiene el derecho fundamental a la protección de sus datos de carácter personal, que persigue garantizar un poder de control sobre los datos, su uso y su destino. 6. El secreto es un deber del médico y un derecho del paciente. El secreto médico se ha de proteger en el tratamiento de los datos sanitarios, ya sea en medios manuales o informatizados, como se establece en la legislación vigente, exigiendo las medidas de seguridad apropiadas que garanticen la protección de los datos personales de los pacientes. Sin estas medidas de seguridad no se deberán tratar los datos de salud. 7. Sólo en contadas ocasiones y bajo el imperio de la Ley, el derecho a la confidencialidad puede subordinarse a otras consideraciones. El allanamiento de la intimidad, como el de la propia morada, sólo puede justificarse por derechos superiores de otros o el bien común, como en el caso de la salud pública, pero debe tenerse en cuenta que, a diferencia de la morada y otros bienes, la intimidad perdida no se puede restituir. 8. En casi todas las ocasiones, el anonimato estricto es idéntico al secreto y los datos anónimos pueden cumplir casi todas las tareas de administración. Sólo contadas informaciones clínicas

No es extraño, por tanto, que algunos de los deberes principales de los profesionales sanitarios respecto a la intimidad del paciente a destacar en la práctica de la medicina sean: (1) Preguntar al paciente, al inicio de la relación clínica, si quiere ser informado y a quien más quiere que se informe; (2) No informar (verbalmente ni por escrito) a nadie sin el consentimiento del paciente y a él según su deseo; (3) Acceder únicamente a los datos de la historia clínica necesarios para un fin legitimo; (4) Extremar el cuidado en la utilización de la HCI (no ceder claves, no dejar el programa abierto…); (5) Evitar los comentarios sobre pacientes en lugares inadecuados o con interlocutores no autorizados; (6) Tratar al paciente con consideración y respecto en cualquier situación; (7) Proteger su intimidad física; (8) Solicitar al paciente

---

personalizadas son relevantes para la gestión clínica y ninguna es relevante para la gestión de la información misma, por lo que ninguna de estas excusas puede utilizarse para justificar el almacenamiento masivo o centralizado de información sanitaria personalizada. 9. La informatización de las consultas y la historia electrónica de salud constituyen un factor de progreso; no obstante, en su utilización deben considerarse los peligros para la confidencialidad de los datos, por su almacenamiento fácil de ocultar, su infinita capacidad de copia y transferencia, indetectable y de ínfimo coste, y sus ilimitadas posibilidades de procesamiento y cruce. No puede garantizarse que la protección de los datos médicos centralizados sea infranqueable, teniendo en cuenta que el interés y el valor de tanta información son elevados: basta una única fuga, en un único punto para que los daños sean catastróficos e irreparables. El almacenamiento masivo centralizado de la información clínica es el que mayores riesgos supone para el secreto y la confidencialidad, comparando con las bases de datos distribuidas. Deben por tanto primarse soluciones tecnológicas pequeñas y repartidas, ya posibles, que eviten tan elevado riesgo. 10. La concentración de datos los hace codiciables, por lo que deben existir razones irrefutables para justificar el almacenamiento masivo o centralizado de información. La amenaza a la confidencialidad así creada, exige una total transparencia en este tipo de iniciativas, sancionadas por el consenso de grupos independientes (científicos, profesionales, judiciales, políticos, ciudadanos, económicos y comerciales) en cuanto a la pertinencia y relevancia de los datos precisos. 11. También debe determinarse –en la fase previa a toda implantación de almacenamientos masivos o centralizados– el tiempo de almacenamiento y las garantías y medios de destrucción irreversible de la información y todas sus copias, una vez cumplida su función. 12. Los sistemas pequeños y repartidos permiten proteger la confidencialidad, la intimidad de los pacientes y el secreto médico, como establece el Código de Deontología Médica; los sistemas de informatización médica tendrán implantadas las medidas de seguridad necesarias que eviten que otras personas accedan a los datos de los pacientes. Asimismo, todos los ficheros con historias clínicas y datos de salud estarán bajo la responsabilidad de un médico, y los ficheros con datos sanitarios no deberán conectarse a redes no médicas, como algunas redes institucionales. Esto, actualmente, no se respeta. 13. Es necesario establecer una legislación propia para proteger la intimidad de los pacientes, que nadie pueda ser discriminado por información relativa a la salud y la salvaguarda del secreto médico, en desarrollo específico de los artículos 14 y 18 de la Constitución. Es vital que la salud de una persona y los datos relativos a la misma nunca puedan ser usados en su contra o para su discriminación, sean o no sus depositarios «legítimos». 14. Es necesario que todos los ciudadanos defiendan y requieran el secreto médico a los profesionales sanitarios que les atienden. La legislación es importante, pero han de ser los propios pacientes los que exijan su derecho a estar informados sobre qué se hace con sus datos, a decidir quién los maneja y a defender el secreto médico. 15. El secreto es asimismo una prerrogativa del médico, manifestación de su derecho a la objeción de conciencia en las relaciones administrativas, profesionales o de cualquier otra. (VIGUERAS PAREDES, P., "Intimidad, confidencialidad y protección de la información sanitaria. Estudio práctico del acceso al aplicativo Selene por facultativos del Servicio Murciano de Salud", *Revista Bioderecho.es,* Núm. 6, 2017, pp. 9-11).

autorización explícita para todas aquellas actuaciones cuyo fin no sea procurarle asistencia (filmaciones, prácticas de estudiantes…)[596].

3. LIMITACIONES LEGALES DEL SECRETO PROFESIONAL

A pesar de que el facultativo sanitario tiene el deber principal de guardar secreto profesional, el artículo 30.1 del Código de Deontología Medica de 2011 regula algunos supuestos que permite al médico revelar el secreto profesional previo asesoramiento del Ilustre Colegio de Médicos al que pertenezca su colegiación. Estas causas justificadas son las siguientes:

"a. En las enfermedades de declaración obligatoria. b. En las certificaciones de nacimiento y defunción. c. Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas, o a un peligro colectivo. d. Cuando se vea injustamente perjudicado por mantener el secreto del paciente y éste permita tal situación. e. En caso de malos tratos, especialmente a niños, ancianos y discapacitados psíquicos o actos de agresión sexual. f. Cuando sea llamado por el Colegio a testificar en materia disciplinaria. g. Aunque el paciente lo autorice, el médico procurara siempre mantener el secreto por la importancia que tiene la confianza de la sociedad en la confidencialidad profesional. h. Por imperativo legal: 1. En el parte de lesiones, que todo médico viene obligado a enviar al juez cuando asiste a un lesionado. 2. Cuando actúe como perito, inspector, médico forense, juez instructor o similar. 3. Ante el requerimiento en un proceso judicial por presunto delito, que precise de la aportación del historial médico del paciente, el médico dará a conocer al juez que éticamente está obligado a guardar el secreto profesional y procurará aportar exclusivamente los datos necesarios y ajustados al caso concreto".

En consecuencia, ante las anteriores situaciones constará justificada la relevación del secreto profesional por parte del facultativo sanitario sobre todo a fin de salvaguardar otros derechos y evitar generar mayores daños y perjuicios a terceras personas a causa de la enfermedad de la que padece el paciente. Por ejemplo, ante la

[596] IRABURO, M., "Confidencialidad e intimidad*", An. Sist. Sanit. Navar.*, Vol. 29, Suplemento 3, 2006, p. 58.

situación en la en la que un paciente de 24 años diagnosticado de esquizofrenia paranoide y con alucinaciones auditivas le revela al su médico que va a matar a una persona identificándole a la misma e incluso, amenaza con quitarse la vida, ante el dilema de que, si protege a la persona que amenaza matar, puede incentivar a que el paciente se suicide y, si no protege a la persona que amenaza matar, puede poner en grave riesgo la vida de ésta ¿qué debe hacer el médico al respecto? Según la *Guía de ética en la práctica médica*[597] editada por la Fundación de Ciencias de la Salud, los valores implicados son: por un lado, la protección de la vida del propio paciente y de la otra persona que amenaza matar y, por otro lado, el derecho que el paciente tiene al respecto de su intimidad y confidencialidad de sus datos y, el deber correlativo del profesional a respetarlos, basado principalmente en la relación de confianza médico – paciente.

Por ello, debido a los valores implicados, las recomendaciones que la citada guía ofrece al médico son las siguientes: por un lado, dado que las declaraciones de los pacientes la mayoría de las ocasiones no son ciertas, la labor del médico es la de procurar corroborar los datos que el paciente aporta a través de entrevistas con los familiares, pedir colaboración a otros compañeros, a trabajadores sociales, a psicólogo o a psiquiatras. Por otro lado, en caso de psicopatología grave (alucinaciones y delirios) se ha de someter al paciente a una exploración psicopatológica a través de la intervención de un especialista en psiquiatría. Asimismo, se ha de tener en consideración que, ante situaciones agudas, en ocasiones se ha de ingresar temporalmente al paciente intentando pedirle permiso para su internamiento a efectos de que sea voluntario y de respetar todo lo posible su autonomía por muy mínima que sea ésta. Por último, se ha de poner en conocimiento de la autoridad judicial en un plazo máximo de 24 horas el ingreso psiquiátrico del paciente, pues todo ingreso psiquiátrico de persona incapaz requiere de autorización judicial.

Como se puede apreciar, en todas y cada una de las recomendaciones ha primado salvaguardar la salud del paciente sin necesidad de vulnerar su derecho a la intimidad y confidencialidad y, por consiguiente, sin incumplir el profesional sanitario

[597] Fundación de Ciencias de la Salud, *Intimidad, confidencialidad y secreto. Guías de ética en la práctica médica*, 2015, p. 7 y ss.

con su deber de secreto profesional. Con el anterior caso práctico, se observa que en la mayoría de las ocasiones la solución al problema de priorizar, o bien, el derecho a la intimidad y el derecho de confidencialidad del paciente, o bien, proteger la vida del paciente y de otras personas revelando el secreto profesional, resulta complicada debido a los valores en riesgo, así como a las diversas posibilidades de obrar por parte del facultativo sanitario.

Por último y, no menos importante, se ha de tener en consideración algunas limitaciones legales del secreto profesional. Así pues: en caso de que el paciente autorice al facultativo sanitario revelar datos de su salud a terceros (empresa en la que es trabajador, compañía de seguros…) no podrá sancionar posteriormente al profesional sanitario. De igual modo, en la situación en la que el facultativo sanitario revele datos del paciente por estado de necesidad a efectos de evitar un mal propio o ajeno estará exento de responsabilidad criminal siempre y cuando se den los requisitos legales (art. 20 CP), por ejemplo, el deber de denunciar un delito, debiendo presentar en su caso el parte de lesiones (259 y 262 LECr. y 408 CP); el deber de impedir un delito (450.1 CP); el deber de testificar como perito o testigo (410 CP); el deber de comunicar casos de enfermedades infectocontagiosas[598], entre otros.

En relación con la anterior, resulta conveniente que la ley sectorial en relación con el deber de secreto profesional de los responsables y encargados del tratamiento de datos de salud facilite una definición genérica del secreto profesional en el ámbito sanitario, así como del alcance del deber en consideración con doctrina jurisprudencial, haciendo especial mención al extremo de que en los casos de tratamiento y cesión de datos de salud anonimizados irreversibles no existirá vulneración alguna a dicho deber. Igualmente, es fundamental delimitar en la ley de protección de datos de salud los sujetos implicados en el deber de secreto profesional.

[598] *Vid.* Orden SSI/445/2015, de 9 de marzo, por la que se modifican los anexos I, II y III del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica, relativos a la lista de enfermedades de declaración obligatoria, modalidades de declaración y enfermedades endémicas de ámbito regional.

Además, es imprescindible que la ley sectorial regule de manera taxativa las excepciones fundamentales del deber de secreto profesional a los efectos de que los profesionales sanitarios sean conocedores de manera clara y concisa de su responsabilidad por causa de incumplimiento de la *lex artis*, haciendo referencia de manera detallada en concreto a las siguientes situaciones excepcionales: por un lado, sobre el secreto compartido, regulación de los casos de declaración de enfermedades transmisibles, vigilancia de salud pública, comunicación de datos de salud entre Administraciones sanitarias para el ejercicio de competencias iguales o sobre materias similares y fines de investigación biomédica; comunicaciones a registros nominales de efectos adversos de medicamentos; el secreto compartido en el ámbito asistencial y; registros de instrucciones previas. Por otro lado, en relación con el secreto divulgado, regulación de las situaciones excepcionales dimanantes de denuncias de delitos públicos, del deber del profesional sanitario de colaborar con la administración de justicia en calidad de perito o testigo; detección de enfermedades que impliquen un grave perjuicio para la salud de familiares biológicos; existencia de un riesgo grave para terceros; expedición de certificados de nacimiento y de fallecimiento; acceso a la historia clínica con fines judiciales y; vigilancia de la salud de los trabajadores, entre otros.

Por último, en lo que respecta al acceso a los datos de salud por parte de las autoridades de control, Ministerio Fiscal y de los defensores del pueblo, puesto que de acuerdo con la normativa vigente de protección de datos, así como a lo asentado por la diversa normativa sobre el deber de secreto profesional del médico y al derecho de confidencialidad del paciente, se deduce que el responsable y encargado del tratamiento de los datos de salud (profesionales sanitarios, centros de salud públicos o privados) y, aquellas personas que interfieran el tratamiento del paciente (profesionales sanitarios) están obligados al secreto profesional y al deber de custodia de los datos (personales y de salud) hasta incluso después de finalizar la relación con su titular. Sin embargo, las autoridades de control, el Ministerio Fiscal y los defensores del pueblo pueden acceder a los datos de salud para el ejercicio de sus funciones de investigación, surgiendo como efecto adverso, la obligación del responsable y del encargado del tratamiento de permitir su acceso. Como es sabido, en la esfera de los procedimientos judiciales, resulta de notoria importancia que tanto el personal de los órganos judiciales, como en aquellos litigios donde intervenga el Ministerios Fiscal y los defensores del pueblo

donde resulte necesario en aras del derecho a la tutela judicial efectiva, conocer de los datos de salud de una o varias de las partes implicadas o interesadas en el procedimiento, puedan acceder a los datos de salud, siempre y cuando sea en el ejercicio de sus funciones y queden obligados al deber de secreto profesional, extremos que deben ser tenidos en consideración por la ley de protección de datos de salud[599].

En consecuencia, debido a lo anterior, otros de los aspectos a tratar por parte de la ley sectorial es el de regular los criterios a seguir por parte de los responsables y encargados del tratamiento cuando se encuentren obligados de permitir su acceso a los datos a la autoridad de control, Ministerio Fiscal y defensor del pueblo, de acuerdo con el principio de confidencialidad y a efectos de no incumplir el deber de secreto. Asimismo, se estima pertinente que la ley sectorial regule también que, en todo caso, los citados criterios serán de igual cumplimiento por parte de las autoridades de control, Ministerio Fiscal y defensores del pueblo, quienes una vez accedan y conozcan los datos sanitarios asumirán de manera automática el deber de confidencialidad y de secreto profesional.

4. SOBRE EL SECRETO PROFESIONAL Y EL DERECHO DE CONFIDENCIALIDAD EN EL ACCESO A LA HISTORIA CLÍNICA

La historia clínica[600] es un instrumento que tiene como finalidad primordial la de facilitar la asistencia sanitaria y garantizar una asistencia adecuada al paciente[601], por

[599] Al respecto, advierte SERRATO MARTÍNEZ, L., "El régimen legal de acceso a la historia clínica y sus garantías", *Revista Jurídica de Castilla y León,* núm. 17, 2009, p. 200 que "la historia clínica ante los Tribunales tiene un extraordinario valor probatorio. Constituye uno de los mejores instrumentos de defensa en juicio del médico diligente, pero también sirve para proteger al enfermo cuando la asistencia prestada no ha sido correcta. Un procedimiento judicial puede tener por objeto averiguar si el personal sanitario, a consecuencia de su actuación profesional, ha incidido en responsabilidad contractual o extracontractual por el incumplimiento de la «lex artis ad hoc» (proceso civil), si dicho personal ha cometido un delito o falta (proceso penal) o si existe responsabilidad patrimonial de la Administración por el funcionamiento normal o anormal de los servicios sanitarios (proceso contencioso-administrativo). La historia clínica también puede ser requerida para su aportación en un proceso de naturaleza laboral o de Seguridad Social".

[600] GALÁN CORTÉS, J. C., "Relevancia jurídica de la historia clínica", *Salud Rural,* Vol. 14, núm. 7, 1997, pp. 83-89, señala que: "la historia clínica es el elemento esencial de acreditación por parte del médico de su conducta con el paciente en todo momento, al reflejar toda la información relacionada con la asistencia dispensada al propio paciente. La historia clínica, convertida en prueba material por orden del juez, es el testimonio más objetivo de la calidad o de la falta de calidad del trabajo médico. Además, también es fundamental a la hora de acreditar la existencia del preceptivo consentimiento informado previo a toda intervención y, de la información suministrada al paciente, debiendo quedar plenamente garantizados el

ello, es el conjunto de documentos sobre los procesos asistenciales a los que ha sido sometido el paciente, incorporando toda información trascedente a los efectos de facilitar un conocimiento veraz y actualizado sobre la salud del mismo. En consecuencia, todo acceso a efectos de garantizar una asistencia adecuada al paciente sería un acceso lícito, estando el facultativo sanitario autorizado para ello, de conformidad con el principio de vinculación asistencial regulado con el art. 16.1 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derecho y obligaciones en materia de información y documentación clínica. Así pues, autores como GÓMEZ PIQUERAS, que considera que la historia clínica es "el instrumento básico del buen ejercicio sanitario"[602]. En este sentido, el autor TRONCOSO REIGADA, defiende la estrecha vinculación de la historia clínica con el derecho constitucional a la vida (art. 15 CE) y con el derecho a la protección de la salud (art. 43 CE), considerando a su vez la historia clínica como un deber del profesional sanitario[603].

Por otro lado, la historia clínica resulta ser la fuente primara de información para otros fines legítimos y constitutivos del sistema sanitario a los que pueda resultar de gran utilidad, como: judiciales, epidemiológicos, de salud pública, de investigación o de docencia.

En relación con la historia clínica electrónica el *Informe SESPAS* señala que "es finalidad principal de la historia clínica electrónica facilitar la asistencia sanitaria, y como finalidad complementaria posibilitar la investigación científica"[604], considerando a su vez que es una herramienta esencial para todos los profesionales sanitarios, bien se dediquen a la asistencia sanitaria, bien a la investigación científica y epidemiológica[605].

---

derecho a la intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica".

[601] De conformidad con lo establecido en el artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derecho y obligaciones en materia de información y documentación clínica.

[602]GÓMEZ PIQUERAS, C., "La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", en AA.VV., *El derecho a la protección de datos en la historia clínica y la receta electrónica,* (Coord. Cáliz Cáliz et al.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, p. 134.

[603]TRONCOSO REIGADA, "La confidencialidad…", *op. cit.*, pp. 45-46, 70.

[604] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 50.

[605] Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 52.

Sin duda, tal y como subraya el autor PEREIRA ÁLVAREZ, la historia clínica electrónica ha traído un nuevo "escenario de integración y accesibilidad"[606].

Sin embargo, a pesar de lo anterior, la historia clínica supone la principal causa de vulneración del secreto profesional del médico y del derecho a la confidencialidad del paciente, debido a su fácil acceso y por la agilidad en la que la mayoría de las ocasiones los profesionales tratan la información de sus pacientes, poniéndose en la mayoría de las ocasiones en peligro, por un lado, la confidencialidad de los datos relativos a la salud de las personas, y de otro, la protección de la salud y la integridad física de una persona. Por ende, a pesar de las diversas ventajas que ha supuesto la implantación de la historia clínica en el sector sanitario mejorando la calidad de la asistencia sanitaria, también se dan ciertos riesgos sobre el acceso indebido a los datos e información sanitaria[607], siendo múltiples los problemas sobre la protección de datos y el acceso a la historia clínica que tienen que afrontar los profesionales sanitarios en el día a día de la profesión. Por ello, a continuación, se estudiarán varios supuestos prácticos a los efectos de apreciar de manera cercana y concisa los conflictos actuales y patentes en la práctica de la medicina sobre el secreto profesional y el derecho de confidencialidad en el acceso a la historia clínica, así como las diversas medidas o mecanismos de prevención llevados a cabo en la práctica con el objetivo de evitar accesos indebidos a la historia clínica por los profesionales sanitarios.

Particularmente, un conflicto que suele ser habitual es el dimanante entre accesibilidad y protección de la historia clínica en el que se encuentran implicados valores como el derecho a la información de los familiares del paciente, el derecho del paciente a la confidencialidad y el derecho del médico a la reserva de sus anotaciones subjetivas. Por ejemplo, un paciente que sufre una enfermedad grave sometido a tratamiento, donde el médico que le trata observa cierto interés de los familiares en la herencia del mismo y, por consiguiente, un desinterés en su recuperación, debido a que teme que en el domicilio podría ser desatendido por sus familiares escribe esta

[606] PEREIRA ÁLVAREZ, M., "El tratamiento de los datos en las HCE y las medidas de seguridad: una aproximación desde el punto de vista técnico. Especial referencia al nuevo Reglamento de desarrollo de la LOPD", en AA.VV., *El Derecho a la Protección de Datos en la Historia clínica y la Receta electrónica* (Coord. R. Cáliz Cáliz, et al.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, p. 309.

[607] VIGUERAS PAREDES, "Intimidad, confidencialidad y protección de la información sanitaria. Estudio práctico del acceso al…", *op. cit.,* p. 2.

suposición en la historia clínica a efectos de que el resto de los profesionales sanitarios tengan constancia de ello en caso de nuevo ingreso. Al cabo de unas semanas, el paciente fallece y, los familiares solicitan la historia clínica al centro sanitario alegando mala praxis del médico que trató a su pariente, tras apreciar el medico documentalista las anotaciones del clínico sobre el interés de los familiares en la herencia del enfermo ¿debe entregar el contenido completo de la historia clínica a los parientes o debe respetar la privacidad de las anotaciones subjetivas del médico optando por la confidencialidad de los datos y el secreto profesional? Según la *Guía de ética en la práctica médica*[608] la solución más optima por parte del médico documentalista es la de entregar una copia a los familiares de la historia clínica sin incluir los datos que haga referencia a las anotaciones subjetivas del clínico ni aquellos datos que puedan vulnerar la confidencialidad del paciente, dado que el acceso de los familiares a la historia clínica no es ni por interés terapéutico para el enfermo (ya fallecido) ni tampoco es un derecho de acceso por medio de representación acreditada de manera fehaciente.

Por tanto, ante supuestos semejantes, la Fundación de Ciencias de la Salud en la citada *Guía de ética en la práctica médica*, recomienda las siguiente medidas a los efectos de prevenir el acceso indebido a la historia clínica: (1)Documentar por escrito las medidas de control del uso de la historia desde su salida del fichero hasta su evolución, siendo responsabilidad de cada centro la elaboración de este documento y su difusión y conocimiento por todo el personal que pueda tener acceso (gestión y utilización) a las historias clínicas; (2) Obligatoriedad de que las hojas de interconsulta y las historias clínicas que circulan por diferentes sitios dentro de las instalaciones del centro sanitario, sin que todo el mundo tenga derecho acceso a su contenido, deben ir en sobre cerrado; (3) Evitar el uso de correo electrónico, fax u otro medio de comunicación telemático, ya que suponen un elevado riesgo para la confidencialidad al no tener seguridad de que el receptor es la persona indicada, salvo que el facultativo sanitario tenga un conocimiento de su correcto uso o pueda asegurar la debida recepción de la información de manera; (4) En todo caso, se ha de reservar una apartado específico en la historia clínica para las anotaciones subjetivas a los efectos de que puedan ser ocultadas/suprimidas las mismas a personas que no tenga derecho de acceso a las mismas. (5) realizar un archivo separado de la documentación clínica correspondiente a

[608] Fundación de Ciencias de la Salud, *Intimidad, confidencialidad y secreto. Guías de ética en la práctica médica*, 2015, p. 35-36.

la historia clínica, así como de la documentación administrativa que no forma parte de la misma; (6) Compartir la información de la historia clínica con las personas involucradas en el seguimiento del paciente (profesionales estrictamente implicados) a los efectos de no vulnerar el derecho fundamental a la garantía de una buena atención del paciente; (7) Los familiares tienen derecho de acceso a la información de los pacientes fallecidos, salvo que expresamente el fallecido lo haya prohibido o así lo establezca una ley[609].

Otro conflicto recurrente en la práctica de la medicina es el dimanante de la situación en la que el familiar del enfermo al que atiende por descuido de los facultativos sanitarios dejando la historia clínica en el mostrador del control de enfermería, accede a la historia clínica del otro enfermo de la cama contigua, teniendo acceso a información relevante tal como situación familiar (soltero, casado, si está solo o acompañado…), si es fumador y, a resultados de test médicos que determinan si es portador de un virus determinado - como el de VIH, por ejemplo – comentando posteriormente esa información a sus familiares y allegados.

Por consiguiente, ante la anterior situación y similares, la citada *Guía de ética en la práctica médica*, recuerda la importancia de una protección correcta de la historia clínica en los controles de enfermería a los efectos de evitar el acceso al contenido de la misma por personas no implicadas en la asistencia del paciente, a los efectos establece las siguientes medidas de prevención a los profesionales sanitarios: (1) Evitar descuidos y accesos indebidos por parte de terceros a las historias clínicas evitando prisas innecesarias cuando se están manejando las mismas; (2) Actuar siempre con sentido común en el momento de actuación con el paciente y su entorno a los efectos de prevenir riesgos e inseguridades; (3) No permitir el acceso a la historia clínica a cualquier facultativo sanitario si no es su paciente, a pesar de estar trabajando dentro del centro sanitario, ya que el acceso a la misma debe estar siempre justificado por un motivo asistencial, excepto en casos permitidos por ley; (4) Si no encontramos ante un paciente portador de un virus, se ha de educar sanitariamente de las medidas de prevención de contagio tanto a todos los profesionales sanitarios, como a los pacientes que se encuentren en riego. Al hilo de lo anterior, cabe traer a colación la sentencia del

[609] Art. 3 de la LOPDGDD.

Tribunal Supremo 532/2015, de 23 de septiembre, sobre la protección de la información contenida en la historia clínica, donde el su fundamento jurídico quinto establece que:

«[…] toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley, formando parte de su derecho a la intimidad (art. 7.1 Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica). La historia clínica definida en el art. 3 de esta ley como el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial, estaría comprendida en ese derecho a la intimidad y además forma parte de los datos sensibles, el núcleo duro de la privacidad, cuyo mero acceso, como hemos descrito, determina el perjuicio de tercero; el del titular de la historia, cuyos datos más íntimos, sobre los que el ordenamiento le otorga un mayor derecho a controlar y mantener reservados, se desvelan ante quien no tiene autorizado el acceso a los mismos»[610].

En lo que respecta a la jurisprudencia dictada acerca del acceso indebido por profesionales asistenciales, se han de destacar la Sentencia del Tribunal Supremo, Sala de lo Contencioso-Administrativo, de 20 de febrero 2012, la Sentencia núm. 532/2015 del Tribunal Supremo, Sala de lo Penal, Sección 1ª, de 23 de septiembre, las Sentencias de la Audiencia Provincial de Palma de Mallorca de 26 de enero y 16 de febrero de 2015, así como la Sentencia del Tribunal Supremo de 18 de octubre de 2012 que condena a una enfermera por entrar a la historia clínica de su ex cuñado en el proceso de divorcio de su hermana[611].

[610]Según señala VIGUERAS PAREDES, P., "La historia clínica: acceso, disponibilidad y seguridad", *Revista Bioderecho.es*, núm. 6, 2017, pp. 2- 3, la doctrina señala los siguientes caracteres a la historia clínica: "a) Única, con la máxima integración de la información del paciente, al menos por cada centro. b) Segura, pues debe contener todos los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos. c) Auténtica, pues debe garantizar su contenido y de los cambios operados en ella, así como la posibilidad de su reproducción futura. d) Confidencial, protegiendo la intimidad del paciente y el acceso indebido a su documentación clínica.5 e) Disponible, facilitando el derecho de acceso a las personas legitimadas. f) Legible y ordenada, para garantizar la asistencia sanitaria al paciente".

[611] GONZÁLEZ GARCÍA, "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos…", *op. cit.,* pp. 274-285.

De manera general, en la actualidad se ha tratado de solventar el problema tratado por medio la implantación de diversos mecanismos a fin de evitar un acceso indebido a la historia clínica por parte de los profesionales de salud, tales como: formación específica a los profesionales de la salud en materia de confidencialidad en relación con el derecho de protección de datos; implantar *software* que requieran protocolos de acceso a los datos más eficaces (*v.gr.,* mecanismo de tarjeta sanitaria con chip con certificado digital titularidad de cada facultativo sanitario instaurado por el sistema gallego IANUS[612]); módulos de acceso a la historia clínica según el tipo de datos (*v.gr.,* sistema de consignación de información en distintos módulos de especial custodia instaurado por el sistema gallego IANUS) y según sea la categoría profesional del sanitario que accede (procediéndose al bloqueo de determinados datos respecto al acceso de concretos perfiles profesionales); implantación de *software* que detecte accesos injustificados e indebidos (*v.gr.,* plataforma centralizada de *loGC* del *Ib-Salut* – Servicio de Salud de las Islas Baleares); registros de acceso[613]; auditorías efectuadas por la propia Administración Pública o por empresas externas[614] y; control por parte de los afectados[615].

Como se ha podido apreciar, la historia clínica es la fuente principal de los datos de salud al ser el soporte donde se encuentran los documentos relativos a los procesos asistenciales de cada paciente, incluyéndose la identificación de los profesionales sanitarios que han intervenido en los mismos, cuyo objeto principal es facilitar la asistencia sanitaria al paciente proporcionando a los profesionales de la salud datos veraces y actualizados del estado de salud del mismo. Por ello, en materia de protección de datos de salud resulta relevante que la ley sectorial regule, entre otros, aspectos relativos a su tratamiento tales como que: el responsable del tratamiento de los datos de la historia clínica es el profesional sanitario o el centro médico (público o privado), regulación de las obligaciones del responsable del tratamiento destacándose entre otros,

[612]Sistema instaurado por el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y el acceso de la historia clínica en Galicia.

[613] Art. 103 del Reglamento de desarrollo de la LOPD y, art. 23 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

[614] *Vid.* Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, p. 51 y *Documento WP131*, de 15 de febrero de 2007, del Grupo de Trabajo del Artículo 29, p. 21.

[615] Articulo 15 y 34 RGPD; art. 13 LOPDGDD.

la obligación de elaborar una historia clínica unificada, interoperable y que contenga módulos de especial custodia para los datos personales más sensibles, la obligación de custodiar la historia clínica y de implantar las medidas de seguridad necesarias a efectos de evitar extravíos o accesos ilegítimos de terceros, así como el derecho del paciente de solicitar una copia de la misma y el derecho de rectificación y supresión de algunos de los datos, rectificación que únicamente podrá ser realizada por el profesional sanitario competente.

Igualmente, especial mención debe efectuar la ley sectorial con relación a las personas legitimadas para acceder a la historia clínica del paciente desde los profesionales sanitarios a terceros autorizados, así como regular el acceso lícito a la historia clínica con fines de gestión, inspección, evaluación, acreditación y planificación de servicios sanitarios, regulando particularmente el derecho de acceso a la historia clínica por parte del interesado, el derecho de rectificación y el derecho de supresión de datos de la historia clínica. Por su parte, regular asimismo las situaciones de acceso y cesión de datos sanitarios entre las Administraciones Públicas y con entidades privadas.

IV. DE LA RESPONSABILIDAD DE LOS RESPONSABLES DEL TRATAMIENTO DE LOS DATOS DE SALUD EN EL SECTOR SANITARIO

De igual modo, queda destacar aquellos supuestos legales en los que los responsables del tratamiento de los datos de salud tanto en el sector sanitario público y privado son responsables, abarcándose por un lado, la responsabilidad patrimonial de la Administración pública sanitaria y la responsabilidad civil de los centros sanitarios privados, así como la responsabilidad civil de los responsables de tratamiento de datos de salud en el ámbito público – privado y, por último, se analizará la eximición de responsabilidad imputable al responsable y encargado del tratamiento de los datos de salud por motivos de interés público y fines científicos.

1. LA RESPONSABILIDAD PATRIMONIAL DE LA ADMINISTRACION SANITARIA

La responsabilidad patrimonial con la cual aludimos al deber que tiene un sujeto de reparar el daño patrimonial que le haya ocasionado a otro, corresponde estudiarla dentro del derecho civil, el cual diferencia entre la responsabilidad contractual y la responsabilidad extracontractual. Por derivación de los principios generales que se han fijado en el ámbito civil, la responsabilidad extracontractual, que es a la que nos vamos a referir en este apartado, se ha extendido a otros órdenes jurídicos, estando el régimen general civil regulado en el artículo 1902 y siguientes del Código Civil. No obstante, se ha de destacar que los inicios de la responsabilidad de la Administración Pública dimanan de la Ley de Expropiación forzosa de 1954[616], regulando en el Capítulo II bajo la rúbrica "De la indemnización por otros daños" la responsabilidad directa de la misma al establecer que "dará también lugar a indemnización con arreglo al mismo procedimiento toda lesión que los particulares sufran en los bienes y derechos a que esta Ley se refiere, siempre que aquélla sea consecuencia del funcionamiento anormal o anormal de los servicios públicos", en el artículo párrafo primero del artículo 121 del citado texto legal.

En concreto, se analizará la responsabilidad extracontractual propia y específica de los poderes públicos sanitarios que presenta una naturaleza estrictamente jurídico-administrativa, aunque en su fundamento último tome prestadas nociones básicas de la teoría general elaborada en el ámbito civil. La nota más importante que caracteriza a la responsabilidad extracontractual de los poderes públicos, también denominada responsabilidad patrimonial, es su carácter objetivo, o lo que es lo mismo, que se construye al margen y con independencia de que exista o no culpa en el sujeto que causa el daño. De manera general, el régimen jurídico que regula la responsabilidad patrimonial, así como el procedimiento para exigirla, se encuentra específica y exclusivamente regulado en el Derecho Administrativo. A nivel constitucional, el artículo 9.3 CE establece un principio general por el cual todos los poderes públicos son susceptibles de generar responsabilidad, sin perjuicio de que al aludir a cada concreto poder público otras normas, o incluso la propia Constitución, establezca preceptos

[616] RODRÍGUEZ LÓPEZ, P., *Responsabilidad patrimonial de la administración en materia sanitaria,* Ed. Atelier, Barcelona, 2007, pp. 22-25.

específicos que regulen la materia. Por otro lado, el artículo 106.2 CE establece que los particulares, en los términos establecidos por la ley, tendrán derecho a ser indemnizados por toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor y siempre que la lesión sea consecuencia del funcionamiento de los servicios públicos.

De igual modo, sobre la responsabilidad patrimonial de la administración sanitaria se ha de tener en consideración el artículo 43 CE donde en el párrafo primero reconoce el derecho a la protección de la Salud de lo que se interpreta una evidente universalidad de la asistencia sanitaria ocupando un lugar patrimonial.[617] Igualmente, en el párrafo segundo del citado precepto, señala que compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios, considerándose así pues la sanidad como Servicio Público.[618]

Como quiera el artículo 149 de la Constitución Española reserva al estado la competencia exclusiva para regular el régimen jurídico de la responsabilidad patrimonial en todas sus vertientes, y no solo a nivel a básico, es por lo que en los artículos 32 y siguientes de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP) incluye y regula el régimen jurídico de la responsabilidad patrimonial aplicable a todas las esferas administrativas. Así pues, textualmente el artículo 32 del citado texto legal establece que "los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes o derechos, salvo en caso de fuerza mayor, siempre que la lesión sea a consecuencia del funcionamiento normal o anormal de los servicios públicos".

No en vano, tal y como se ha señalado al principio, cabe afirmar que la responsabilidad patrimonial de la Administración Pública es objetiva y directa, en el sentido de que las Administraciones Públicas son responsables de las lesiones producidas en sus instalaciones durante el periodo de tiempo en el que el ciudadano es

[617] TORRES GARCÍA, T.F., "Responsabilidad patrimonial de la administración sanitaria", en AA.VV., *Lecciones de Derecho sanitario* (Coord. M. Juane Sánchez), Ed. Servizo de Publicacións, Cataluña, 1999, pp. 569-570.

[618] CUETO PÉREZ, M., *Responsabilidad de la Administracion en la Asistencia Sanitaria*, Ed. Tirant Monografías, Valencia, 1997.

garante de la seguridad en particular. En relación a la responsabilidad patrimonial de la Administración Pública sanitaria[619], de conformidad con el párrafo segundo del artículo 43 de la Constitución Española, así como con lo estatuido en la Ley 14/1986, de 25 de abril, General de Sanidad (en adelante LGC), los poderes públicos deben velar por la protección y tutela de la salud púbica, siendo competencia exclusiva del Estado la sanidad exterior, las relaciones y acuerdos sanitarios, la colaboración exterior (entre otros), competencia de las Comunidades Autónomas las asumidas en los propios Estatutos de cada Comunidad Autónoma y aquellas delegadas por el Estado y, por último, es competencia de las Corporaciones Locales las atribuidas en los Estatutos de Autonomía y la Ley de Bases del Régimen local.

En este sentido, cuando nos encontramos ante la situación de que la responsabilidad pueda ser exigida de manera simultánea e indistinta a varias Administraciones Públicas, estaríamos ante un caso típico de responsabilidad concurrente. El artículo 33 de la LRJAP regula un régimen específico de responsabilidad patrimonial en el caso de que sean varias las Administraciones Públicas las que provoquen una lesión a consecuencia de un trámite conjunto.

En consecuencia, cabría afirmar que la responsabilidad es solidaria entre las Administraciones Públicas, existiendo la posibilidad de que posteriormente se determine la Administración Pública responsable del daño causado. De igual forma, cuando nos encontramos ante la situación de que la responsabilidad de una lesión sea concretada en una única Administración Pública, se ha de señalar: en primer lugar, la competencia; en segundo lugar, el interés público tutelado y; en tercer lugar, la intensidad de la intervención.

El órgano jurisdiccional competente para conocer de las reclamaciones por responsabilidad patrimonial de las Administraciones Públicas es el orden contencioso –

[619] Según señala GUICHOT REINA, E., "La responsabilidad patrimonial de los poderes públicos", en AA.VV.., *Lecciones de Derecho Administrativo. Parte General, Volumen II,* (Coord. C. Barrero Rodríguez), Editorial Tecnos, Madrid, 2017, p. 228: "El caso de la sanidad pública, con creces el sector en el que se plantean mayores demandas de responsabilidad, es paradigmático. La jurisprudencia se ha visto forzada a decir alto y claro que no puede haber responsabilidad si el funcionamiento fue correcto conforme a lo que se deriva de los conocimientos médicos actuales y se siguieron los protocolos médicos para esa concreta actuación (lex artis ad hoc), pues de lo contrario el sistema de responsabilidad se convertiría en un seguro colectivo de saludo que no es ni está llamado a ser".

administrativo, de conformidad con lo establecido en el artículo 144 de la LRJAP, en concreto, en la esfera sanitaria, en principio será competente el Ministerio o la Consejería de Sanidad, o bien, el Consejo de Ministro o Consejo de Gobierno autonómico. Por consiguiente, a efectos de que una reclamación sea viable desde una perspectiva jurídica debe cumplir los siguientes requisitos: (1) la lesión debe ser efectiva; (2) además debe poder ser evaluada económicamente; (3) el lesionado debe poder ser individualizado de manera específica a fin de podérsele reconocer el derecho de indemnización; (4) debe darse un nexo causal entre la Administración Pública y la lesión generada y; (5) por último inexistencia de causas de exoneración (fuerza mayor o el deber de reclamante de suportar el daño). No obstante, se ha tener en consideración que tanto en los casos de funcionamiento normal como anormal del sistema sanitario público la Administración Pública será responsable del daño causado. Igualmente, cuando la responsabilidad sea imputada aun facultativo sanitario, la Administración después de resarcir los daños y perjuicios al paciente – reclamante, podrá ejercer acción de repetición contra el personal sanitario responsable.

Se ha de observar, además, que la diversidad de los servicios sanitarios pueden ser prestados, bien de manera directa por parte de la administración sanitaria, en cuyo caso la misma asumirá íntegramente la responsabilidad dimanante de un funcionamiento normal o anormal, bien a través de la creación de una entidad gestora de la Seguridad Social[620] con personalidad jurídica propia, en cuyo caso la responsabilidad será derivada a la misma, siéndole aplicado el régimen de responsabilidad establecido en la LRJAP en calidad de organismos autónomos o entidades públicas pertenecientes a la Administración institucional, independiente de que su intervención sea motivo de una acción de Derecho público o de Derecho privado, pues el art. 106.2 CE no efectúa exclusión alguna, siendo por consiguiente de aplicación a todas las Administraciones Públicas del Estado[621].

---

[620] A las Entidades gestoras y servicios comunes de la Seguridad Social les será de aplicación la LRJAP de conformidad con lo establecido en la Disposición adicional decimotercera del citado texto legal.

[621] En este sentido, la doctrina mayoritaria, citándose entre otros a, MERINO MOLINS, V., "La responsabilidad patrimonial de la Administracion en el ámbito de la sanidad", *Actualidad Administrativa,* núm. 6, 2003, p. 137, y a MIR PUIGPELAT, O., *La responsabilidad patrimonial de la Administracion sanitaria*, Civitas, Madrid, 1991, p.73, establecen que la responsabilidad de los organismos autónomos y las entidades públicas se ha de someter al Derecho Administrativo indistintamente de que los daños hayan sido ocasionados por organismos públicos como por Entidades gestoras públicas sujetas a derecho privado, siendo éste de aplicación subsidiaria a efectos de alcanzar una eficiencia mayor en la prestación de los servicios.

En último lugar, queda destacar que el procedimiento a seguir a efectos de exigir responsabilidad patrimonial a la administración sanitaria es por medio del procedimiento administrativo regulado en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. El citado procedimiento puede iniciarse de oficio o a instancia del interesado, en este último caso, la instancia debe constar de una individualización de la lesión en la persona lesionada, el nexo causal del daño con la Administración sanitaria, una evaluación económica de los daños e identificar el momento del daño, así como en caso de que fuera el particular quien inicie el procedimiento, debe aportar todo documento que sustente sus alegaciones manifestadas en la reclamación. Igualmente, se ha de hacer hincapié en una peculiaridad en relación con el plazo para interponer la reclamación en el sector sanitario, puesto que de manera general la reclamación de responsabilidad patrimonial de la Administración debe interponerse en el plazo de un año desde que se produce la lesión, sin embargo, en el ámbito sanitario, si la lesión es personal, el plazo comienza a computarse desde el momento en que el daño se manifieste o se determine el alcance de las secuelas, ante lesiones continuar el plazo comienza desde el momento en que la lesión deje de producirse y, ante daños permanentes, el plazo para reclamar comienza desde el momento en que se determine la permanencia de las secuelas.

El procedimiento de responsabilidad patrimonial sanitaria finaliza por terminación convencional o mediante propuesta de resolución motivada, también por resolución presunta o silencio administrativo, donde si transcurridos seis meses el procedimiento no ha sido resuelto, la reclamación se entiende desestimada. Ante una desestimación de la reclamación, el perjudicado puede interponer recurso potestativo de revisión en el plazo de un mes, siendo el mismo resuelto por el mismo órgano que dictó la resolución. Si finalmente, de nuevo es desestimada la reclamación, en el plazo de dos meses (a contar desde que finaliza el procedimiento) o seis meses (en caso de silencio administrativo) el perjudicado puede interponer demanda de reclamación de daños y perjuicios contra la Administración Pública sanitaria ante la jurisdicción contencioso-administrativa.

2. RESPONSABILIDAD DISCIPLINARIA DE LOS FACULTATIVOS SANITARIOS

La responsabilidad disciplinaria es que se le impone a un funcionario cuando incumple los deberes propios de su cargo, ya sea por abuso o extralimitación. En concreto, el régimen disciplinario del personal sanitario se regula en la Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud, regula el régimen disciplinario del personal sanitario. Se ha de observar, además, que en el citado texto legal se clasifican las faltas disciplinarias en muy graves[622], graves[623] y leves[624].

---

[622] Así pues, de conformidad con lo establecido en el apartado segundo del artículo 72 son faltas disciplinarias muy graves las detalladas a continuación: "a) El incumplimiento del deber de respeto a la Constitución o al respectivo Estatuto de Autonomía en el ejercicio de sus funciones; b) Toda actuación que suponga discriminación por razones ideológicas, morales, políticas, sindicales, de raza, lengua, género, religión o circunstancias económicas, personales o sociales, tanto del personal como de los usuarios, o por la condición en virtud de la cual éstos accedan a los servicios de las instituciones o centros sanitarios; c) El quebranto de la debida reserva respecto a datos relativos al centro o institución o a la intimidad personal de los usuarios y a la información relacionada con su proceso y estancia en las instituciones o centros sanitarios; d) El abandono del servicio; e) La falta de asistencia durante más de cinco días continuados o la acumulación de siete faltas en dos meses sin autorización ni causa justificada; f) El notorio incumplimiento de sus funciones o de las normas reguladoras del funcionamiento de los servicios; g) La desobediencia notoria y manifiesta a las órdenes o instrucciones de un superior directo, mediato o inmediato, emitidas por éste en el ejercicio de sus funciones, salvo que constituyan una infracción manifiesta y clara y terminante de un precepto de una ley o de otra disposición de carácter general; h) La notoria falta de rendimiento que comporte inhibición en el cumplimiento de sus funciones; i) La negativa a participar activamente en las medidas especiales adoptadas por las Administraciones públicas o servicios de salud cuando así lo exijan razones sanitarias de urgencia o necesidad; j) El incumplimiento de la obligación de atender los servicios esenciales establecidos en caso de huelga; k) La realización de actuaciones manifiestamente ilegales en el desempeño de sus funciones, cuando causen perjuicio grave a la Administración, a las instituciones y centros sanitarios o a los ciudadanos; l) El incumplimiento de las normas sobre incompatibilidades, cuando suponga el mantenimiento de una situación de incompatibilidad; m) La prevalencia de la condición de personal estatutario para obtener un beneficio indebido para sí o para terceros, y especialmente la exigencia o aceptación de compensación por quienes provean de servicios o materiales a los centros o instituciones; n) Los actos dirigidos a impedir o coartar el libre ejercicio de los derechos fundamentales, las libertades públicas y los derechos sindicales; ñ) La realización de actos encaminados a coartar el libre ejercicio del derecho de huelga o a impedir el adecuado funcionamiento de los servicios esenciales durante la misma; o) La grave agresión a cualquier persona con la que se relacionen en el ejercicio de sus funciones; p) El acoso sexual, cuando suponga agresión o chantaje; q) La exigencia de cualquier tipo de compensación por los servicios prestados a los usuarios de los servicios de salud; r) La utilización de los locales, instalaciones o equipamiento de las instituciones, centros o servicios de salud para la realización de actividades o funciones ajenas a dichos servicios; s) La inducción directa, a otro u otros, a la comisión de una falta muy grave, así como la cooperación con un acto sin el cual una falta muy grave no se habría cometido; t) El exceso arbitrario en el uso de autoridad que cause perjuicio grave al personal subordinado o al servicio; u) La negativa expresa a hacer uso de los medios de protección disponibles y seguir las recomendaciones establecidas para la prevención de riesgos laborales, así como la negligencia en el cumplimiento de las disposiciones sobre seguridad y salud en el trabajo por parte de quien tuviera la responsabilidad de hacerlas cumplir o de establecer los medios adecuados de protección".

[623] Asimismo, tienen consideración de faltas graves las siguientes actuaciones: "a) La falta de obediencia debida a los superiores. b) El abuso de autoridad en el ejercicio de sus funciones. c) El incumplimiento de sus funciones o de las normas reguladoras del funcionamiento de los servicios cuando no constituya falta muy grave. d) La grave desconsideración con los superiores, compañeros, subordinados o usuarios. e) El

Por otro lado, las sanciones que se pueden imponer de conformidad con lo establecido en el artículo 73 de la Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud, son, por un lado, la separación del servicio, por otro lado, traslado forzoso con cambio de localidad, en tercer lugar, suspensión de funciones, en cuarto lugar, traslado forzoso a otra institución o centro sin cambio de localidad y por último, apercibimiento, que será siempre por escrito y, sólo se impondrán por faltas leves. Asimismo, se ha de tener presente que las sanciones impuestas por faltas muy graves prescribirán a los cuatro años, las impuestas por faltas graves a los dos años y a los seis meses las que correspondan a faltas leves. El procedimiento sancionador se iniciará con la apertura del expediente disciplinario en cuestión a los efectos de sancionar al personal sanitario por comisión de alguna de las faltas anteriormente citadas.

En concreto, la formalización del expediente disciplinario personal sanitario se iniciará por el nombramiento de Instructor y Secretario por el órgano competente de la respectiva Comunidad Autónoma, dependiente de la Consejería de Sanidad correspondiente. Posteriormente, se procederá a la formulación del Pliego de Cargos y,

---

acoso sexual, cuando el sujeto activo del acoso cree con su conducta un entorno laboral intimidatorio, hostil o humillante para la persona que es objeto del mismo. f) Los daños o el deterioro en las instalaciones, equipamiento, instrumental o documentación, cuando se produzcan por negligencia inexcusable. g) La falta de rendimiento que afecte al normal funcionamiento de los servicios y no constituya falta muy grave. h) El incumplimiento de los plazos u otras disposiciones de procedimiento en materia de incompatibilidades, cuando no suponga el mantenimiento de una situación de incompatibilidad. i) El incumplimiento injustificado de la jornada de trabajo que, acumulado, suponga más de 20 horas al mes. j) Las acciones u omisiones dirigidas a evadir los sistemas de control de horarios o a impedir que sean detectados los incumplimientos injustificados de la jornada de trabajo. k) La falta injustificada de asistencia durante más de tres días continuados, o la acumulación de cinco faltas en dos meses, computados desde la primera falta, cuando no constituyan falta muy grave. l) La aceptación de cualquier tipo de contraprestación por los servicios prestados a los usuarios de los servicios de salud. m) La negligencia en la utilización de los medios disponibles y en el seguimiento de las normas para la prevención de riesgos laborales, cuando haya información y formación adecuadas y los medios técnicos indicados, así como el descuido en el cumplimiento de las disposiciones sobre seguridad y salud en el trabajo por parte de quien no tuviera la responsabilidad de hacerlas cumplir o de establecer los medios adecuados de protección. n) El encubrimiento, consentimiento o cooperación con cualquier acto a la comisión de faltas muy graves, así como la inducción directa, a otro u otros, a la comisión de una falta grave y la cooperación con un acto sin el cual una falta grave no se habría cometido.

[624] Igualmente, se consideran faltas leves: "a) El incumplimiento injustificado del horario o jornada de trabajo, cuando no constituya falta grave. b) La falta de asistencia injustificada cuando no constituya falta grave o muy grave. c) La incorrección con los superiores, compañeros, subordinados o usuarios. d) El descuido o negligencia en el cumplimiento de sus funciones cuando no afecte a los servicios de salud, Administración o usuarios. e) El descuido en el cumplimiento de las disposiciones expresas sobre seguridad y salud. f) El incumplimiento de sus deberes u obligaciones, cuando no constituya falta grave o muy grave. g) El encubrimiento, consentimiento o cooperación con cualquier acto a la comisión de faltas graves".

una vez concluido el trámite desde la puesta a disposición del expediente y admitida y practicada la prueba, se procederá por parte del instructor a la valoración de lo actuado y a la formulación de la propuesta de resolución donde será calificados jurídicamente los hechos. Por último, se ha de tener presente que durante la tramitación del expediente disciplinario se podrán imponer medidas provisionales al expedientado según se estime pertinente por parte del instructor.

3. LA RESPONSABILIDAD CIVIL DE LOS CENTROS SANITARIOS PRIVADOS

La responsabilidad civil en el ámbito sanitario es una responsabilidad civil extracontractual, de carácter subjetivo, donde rige la obligación de medios y la *lex artis ad hoc*. En primer lugar, nos encontramos ante una responsabilidad extracontractual debido principalmente al hecho de que en el ámbito de la sanidad pública no existe un contrato entre médico y paciente, por lo que en la mayoría de los casos se aplica el artículo 1.902 del Código Civil, donde se establece que: "el que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado." Por consiguiente, según interpretación del anterior precepto, a efectos de concretar la existencia de responsabilidad extracontractual debe darse una acción culposa o negligente; producirse un año; debe darse una relación o nexo causal entre la conducta culposa o negligente y el daño ocasionado al paciente[625].

En segundo lugar, la responsabilidad civil sanitaria es una responsabilidad subjetiva debido al hecho de que la responsabilidad extracontractual emana de la de la culpa de quien genera el daño, naciendo así la obligación del agente de reparar el mismo. Por el contrario, la responsabilidad objetiva es la responsabilidad que se deriva por el simple hecho de que exista un daño sin la exigencia del que el mismo sea generado con culpa, esto es, por el mero hecho de darse el daño se puede exigir responsabilidad objetiva al quien lo generó indistintamente de que haya actuado o no correctamente. Así pues, la jurisprudencia de manera acertada unánime ha limitado la reclamación de responsabilidad objetiva al entender que a un profesional sanitario únicamente se le podrá exigir responsabilidad subjetiva por una conducta dolosa o

[625] *Vid.* RODRÍGUEZ AYUSO, *Figuras y responsabilidades…, op. cit.,* pp. 80-82.

negligente, no pudiendo ser en ningún caso demandado por responsabilidad objetiva, responsabilidad que cabe exigir a los organismos sanitarios, ya sean públicos, como el Instituto Nacional de la Salud o, privados.

De igual modo, cabe tener presente que la doctrina jurisprudencial requiere la necesidad de que el paciente-reclamante pruebe el daño, así como la existencia de nexo causal entre la culpa o negligencia del profesional sanitario y el daño reclamado en el momento de exigir responsabilidad subjetiva al mismo, así pues, teniendo en todo caso el reclamante la obligación de probar los hechos que sustenta su reclamación. De contrario, el Tribunal Supremo[626] de acuerdo con la Teoría del riesgo[627] admite la técnica de la inversión de la carga de la prueba en los casos de resultado desproporcionado o existencia de obstrucción de pruebas, donde el facultativo médico deberá ser quien pruebe que actuó correctamente.

En tercer lugar, otras de las características de la responsabilidad civil es que rige la obligación de medios y no de resultados, es decir, según doctrina jurisprudencial del Tribunal Supremo el deber de correcta asistencia médica que nace del contrato de arrendamiento de servicios (y no de obra) entre el médico y el paciente es una obligación de medios y no de resultados como base de la prestación asistencial, es decir, el médico se obliga a suministrar al enfermo los cuidados que requiera según el estado de la ciencia, pero no a curarlo. En concreto, el Alto Tribunal en la sentencia de 25 de abril de 1994 señala los siguientes deberes imputables al médico:

"[…] (1) utilizar cuantos remedios conozca la ciencia médica y estén a disposición del médico en el lugar en que se produce el tratamiento de manera que la actuación del facultativo se rija por la denominada *lex artis ad hoc*; (2) informar al paciente, o en su caso, a los familiares del mismo, siempre que ello resulta posible, del diagnóstico de la enfermedad o lesión que padece, del pronóstico que de su tratamiento pueda normalmente esperarse, de los riesgos que del mismo puedan derivarse, especialmente si es quirúrgico, y si los medios disponibles fuesen insuficientes, debe hacerse constar tal circunstancia para permitir la opción del paciente por otro centro más

[626] Véanse STS 29-03-1988 y STS 04-02-02.

[627] La teoría del riesgo defiende la postura jurídica de que quien provoca un riesgo que le reporta un beneficio debe asumir la responsabilidad si causa un daño.

adecuado; (3) continuar el tratamiento del enfermo hasta el momento en que éste pueda ser dado de alta, advirtiendo al mismo de los riesgos que su abandono le pueden comportar, (4) en los supuestos de enfermedades o dolencias que puedan calificarse de recidivas, crónicas o evolutivas, informar al paciente de la necesidad de someterse a los análisis y cuidados preventivos que resulten necesarios para la prevención del agravamiento o repetición de la dolencia".

En lo que respecta a la responsabilidad civil del profesional sanitario rige la *lex artis ad hoc* esto es, el deber de cuidado o diligencia debida con la que debe actuar el facultativo sanitario en una situación concreta con el paciente de acuerdo con las reglas que rigen su profesión. No en vano lo anterior, en relación con el tratamiento de los datos de salud, se ha de tener en consideración que la AEPD no suele sancionar al profesional sanitario que accede de manera indebida e ilícita a la historia clínica de un paciente, sino que frecuentemente sanciona a los Servicios de Salud, públicos o privados, al considerar que ha sido el centro de salud como empleador del profesional sanitario el que ha incumplido con su deber de establecer las medidas de seguridad adecuadas a efectos de evitar un acceso indebido de la historia clínica, siendo por consiguiente el verdadero responsable el centro sanitario en calidad de empleador. Por último y, no menos importante, se ha de señalar que en vía judicial cabe la posibilidad de formular denuncia ante la jurisdicción penal[628] frente al profesional sanitario que accede ilícitamente a datos de salud por la comisión de un delito de descubrimiento y revelación de secretos, previsto y penado en el artículo 197 y concordantes del Código Penal[629].

---

[628] Así pues, sobre el deber de secreto de los médicos, el Alto Tribunal en su sentencia de fecha 4 de abril de 2001 señala que "nos encontramos ante una obligación impuesta por la Ley General de Sanidad 14/86, de 25 de abril, donde en el párrafo tercero de su artículo 10 establece el derecho a los ciudadanos "a la confidencialidad de toda la información relacionada con su proceso y con estancia en instituciones sanitarias", y concurrente en el historial clínico-sanitario, en el que según el artículo 6.1 del citado texto legal deben "quedar plenamente garantizado el derecho del enfermo a su intimidad personal y familiar y el deber de guardar el secreto por quien, en virtud de sus competencias, tenga acceso a la historia clínica".

[629] En relación con el delito de descubrimiento de secretos ajenos, el Código Penal en su artículo 197 configura varias formas de comisión, tutelándose en cada una de ellas el derecho fundamental a la intimidad personal y familiar y a la propia imagen. De igual modo, el artículo 199.2 tipifica la conducta delictiva del delito de revelación de secretos por parte del profesional que en incumplimiento de su obligación de reserva divulgue los secretos de otra persona. Por otro lado, los artículos 413 a 418 CP se regulan los delitos en relación con la "infidelidad en la custodia de documentos y de la violación de secretos", en concreto, el artículo 417 del CP castiga la conducta de revelación de secretos o información por parte de la autoridad o funcionario público de los que tenga conocimiento a razón de su cargo y no deba divulgarlos.

4. RÉGIMEN SANCIONADOR: LA RESPONSABILIDAD IMPUTABLE A LOS RESPONSABLES DE TRATAMIENTO DE DATOS DE SALUD[630]

De conformidad con lo establecido la nueva normativa de protección de datos – europea y española – el incumplimiento de lo estipulado tanto en el RGDP como en la LOPDGDD implica sanciones económicas para los sujetos responsables con multas administrativas de 10.000.000,00 euros como máximo o, tratándose de una empresa, el 2 % de la factura global anual, cuando sea una infracción cometida por el responsable y el encargado, por los organismos de certificación y autoridad de control por incumplimiento de sus obligaciones legales, en virtud de lo regulado en el art. 83.4 RGPD en relación con el art. 71 LOPDGDD[631].

Igualmente, se impondrá multas administrativas de 20.000.000,00 euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen del negocio total anual del ejercicio financiero anterior, de conformidad con los establecido en el art. 83.5 RGPD (art. 71 LOPDGDD) por: "(a) infracción de los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento; (b)infracción de los derechos de los interesados a tenor de los artículos 12 a 22 RGPD; (c) por las transferencias de datos personales a un destinatario de un tercer país o una organización internacional a tenor de los artículos 44 a 49; (d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX RGPD; (e) por el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control. Por consiguiente, según sea el precepto legal infringido puede dar lugar a la comisión de una infracción de carácter leve, grave o muy grave, así pues, como

---

[630] Especialmente para la elaboración de este apartado se ha tomado como base la *Guía para pacientes y usuarios de la Sanidad* emitida por la Agencia Española de Protección de Datos, 2019. Disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

[631] En este sentido, algunos autores señalan que: "la responsabilidad del responsable no deriva de una eventual falta de diligencia en la selección o supervisión del comportamiento del encargado (culpa in eligendo, culpa in vigilando), sino de una asunción primaria de todos los daños que puedan ocasionarse a raíz de un tratamiento de datos personales en el cual haya definido sus fines y medios", RUBÍ PUIG, A., "Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD", *Revista de Derecho Civil,* vol. V, núm. 4, octubre-diciembre 2018, p. 68. Por el contrario, hay otros autores que hacen referencia a que la responsabilidad es subjetiva, lo que incluye la culpa in vigilando, *v.gr.,* NIETO GARRIDO, E., "Derecho a indemnización y responsabilidad", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, p. 561.

infracción leve se destaca, por ejemplo: la no inscripción del fichero de datos personales en el Registro General de Protección de Datos, no proporcionar la información necesaria a los pacientes que solicitan sus datos de salud o la de incumplir el deber de secreto. Igualmente, entre las sanciones graves se encuentra el incumplimiento de la finalidad de los datos para los que se han recogido, proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas o, mantener los ficheros que contengan datos personales sin las debidas condiciones de seguridad[632].

En última instancia, como sanciones muy graves se tipifican, por ejemplo, las siguientes causas: no atender de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición; la comunicación o cesión de datos de carácter personal, más allá de los casos en que estén permitidas y, la omisión de forma sistemática del deber legal de notificación de la inclusión de datos persona en un fichero, entre otros[633].

La normativa vigente de protección de datos regula un régimen especial aplicable a los centros sanitarios públicos y a sus profesionales de la sanidad, al tratarse de categorías especiales de responsables o encargados de los tratamientos de datos personales por pertenecer, según sea el caso, bien a la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local, bien a los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, bien a autoridades administrativas independientes o, bien a corporaciones de Derecho público cuyas finalidades del tratamiento se relacionan con el ejercicio de potestades de Derecho público. Así pues, entre otras actuaciones, cabe destacar, según se prevé en el

[632] En opinión de ARIAS POU, M., "Definiciones a efectos del Reglamento General de Protección de datos", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, p.123: "La cuestión principal para el responsable hace responsable del fichero es decidir para que se van a utilizar los datos y qué medio se van a emplear en los tratamientos que se van a realizar". De igual modo, CORRAL SASTRE, A., "El régimen sancionador en materia de protección de datos en el Reglamento general de la Unión Europea", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, p. 573, señala que: "el régimen sancionador que establece la Ley orgánica de protección de datos actual queda postergado a la aplicación de aquellos supuestos que queden fuera del ámbito de aplicación material del reglamento".

[633] A los efectos, los arts. 72, 73 y 74 LOPDGDD.

artículo 77 LOPDGDD, que la resolución dictada por la AEPD sancionando a un centro sanitario público deberá ir acompañada con aparecimiento y, estableciendo las medidas necesarias a los efectos de cesar la conducta sancionada y evitar nuevas infracciones. Asimismo, la AEPD sin perjuicio de lo anterior, podrá iniciar expediente disciplinario contra el profesional sanitario por tratamiento ilícito de los datos de salud, si lo estima oportuno.

En colación con lo anterior, entre los casos reales más relevantes, destacar[634]: la sanción impuesta por la AEPD a un médico de Gijón por una multa de importe total de 60.101 euros por arrojar envases de biopsias con datos personales de los pacientes, siendo tipificada como infracción muy grave[635]. Por otro lado, la apertura de la AEPD procedimiento de declaración de infracciones de Administraciones Públicas al Hospital y Ayuntamiento de Inca por filtrar datos personales de los pacientes que fueron usados para visitas de cortesía de corte electoral[636].

Igualmente, la sanción de la AEPD con 6.000,00 euros a un Centro Médico de Cartagena (Murcia) por hacer uso de los datos personales de un cliente de la empresa con la cual se había fusionado[637]. Así como, el apercibimiento de la AEPD a un Hospital de Cuenca por ceder datos personales e historiales médicos de los pacientes a una clínica privada, sin cifrar la información, siendo igualmente sancionada la clínica privada por una multa de 40.001 euros por ceder datos sin proteger la identidad de los pacientes en una subcontratación de servicios[638].

---

634 *Vid.* ROYO V. y MÉLER, N., "Multas impuestas por la AEPD en aplicación del RGPD: motivos y cuantías", *Diario La Ley*, 5 de septiembre, 2019, pp. 1-4.

635 Noticia emitida por el periódico "EUROPAPRESS ASTURIAS" de fecha 28 de diciembre de 2009. Disponible en: https://www.europapress.es/asturias/noticia-agencia-proteccion-datos-sanciona-medico-gijon-tirar-envases-biopsias-datos-personales-20091228134816.html

636 Noticia emitida por el periódico "ULTIMA HORA" de fecha 13 de mayo de 2011. Disponible en: https://www.ultimahora.es/noticias/local/2011/05/13/40271/la-agencia-de-proteccion-de-datos-abre-un-expediente-al-hospital-de-inca.html

637 *Vid.* el siguiente enlace: https://www.adelopd.com/la-aepd-sanciona-con-6000e-a-un-centro-medico-de-cartagena/

638 Noticia emitida por el periódico "eldiario.es" de fecha 8 de febrero de 2016. Disponible en: https://www.eldiario.es/clm/Proteccion-Datos-consentimiento-pacientes-Cuenca_0_482252094.html

A pesar de lo anterior, se ha de hacer constar tal y como señala LÓPEZ ÁLVAREZ (2016) que "el nuevo Reglamento establece parámetro de cumplimiento que obliga a demostrar la existencia de diligencia debida por parte de los responsables y encargados, de forma que, si no existe, se estaría incumplimiento de facto el Reglamento"[639].

Al respecto, en vía judicial, se estima pertinente citar la Sentencia núm. 111/2012 de 8 febrero dictada por el Tribunal Superior de Justicia de Navarra, donde se condena a la Administración Pública por responsabilidad patrimonial debido al funcionamiento anormal del servicio público sanitario dimanante de los daños ocasionados al haberse tomado fotografías de los pacientes familiares de los demandantes sin su consentimiento y haberse producido acceso ilegítimos a su historia clínica informatizada. Así pues, el Tribunal Superior de Justicia de Navarra establece que:

"[…] existe un funcionamiento anormal del servicio público sanitario en este caso, porque no ha podido impedir el acceso casi indiscriminado de profesionales no implicados en el diagnóstico y tratamiento de la paciente al historial clínico informatizado de la misma, accesos que por ello se han considerado ilegítimos. […] en todo lo que exceda de acreditar que los accesos al historial clínico informatizado se hacen con las garantías y en los términos exigidos por las normas de aplicación de las que antes se ha hecho mención. Se ha evidenciado que las medidas de seguridad y protocolo de trabajo de la Administración sanitaria en orden a la garantía de la protección de datos y del acceso a los historiales clínicos informatizados no son suficientes porque no han garantizado esta confidencialidad del historial clínico informatizado de Amparo al permitir el acceso a personal y profesionales que no tenían que ver con su tratamiento".

Asimismo, sobre el mismo caso, la sentencia de primera instancia dictada por el Juzgado de lo Contencioso-Administrativo n.º 1 de Pamplona, núm. 196/2011, de 25 de

[639] LÓPEZ ÁLVAREZ, L.F., "La responsabilidad del responsable", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, p. 291. Igualmente, *Vid.* COSTA HERNANDIS, R., "Responsabilidad del responsable del tratamiento (Art. 24 RGPD. Art. 28 LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 409-419.

mayo, señala que: "el Servicio de Salud Navarro ha centrado su actividad en protección de los datos íntimos de los paciente en fomentar la concienciación de los profesionales sobre la confidencialidad o secreto de los datos relativos a la salud de los usuarios más que en poner "barreras" efectivas de accesibilidad de dichos datos, para evitar que el interés personal en unos casos, la curiosidad en otros o el chismorreo en otros más, se pongan por encima de la conciencia individual de los profesionales como, parece ser ha sucedido en el presente caso".

Así pues, la citada sentencia es un claro ejemplo de la relevancia jurídica que supone el de que la Administración sanitaria cumpla con la obligación de implantar medidas de seguridad y protocolo de trabajo – como el de la formación de los facultativos sanitarios en materia de confidencialidad y protección de datos como medida preventiva – a los efectos de evitar accesos indebidos a la historia clínica que generan graves daños y perjuicios a los pacientes titulares de los datos de salud, así como de garantizar la confidencialidad del historial clínico informatizado[640].

V. DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES RELATIVOS A LA SALUD

De igual modo otras de las garantías jurídicas a destacar reguladas en el RGPD son los derechos del titular de los datos personales. De manera general, el Reglamento establece que, ante una información errónea o incierta de los datos personales, o bien el titular de los datos, o bien su representante legal o representante acreditado[641], tienen derecho a acceder a la misma, rectificar, cancelar u oponerse mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero. No obstante, cuando el responsable de fichero estime y demuestre que la solicitud es manifiestamente infundada o excesiva, sobre todo por ser repetitiva, puede optar entre "cobrar un canon

[640] No en vano, ante la posibilidad de resarcir el daño *Vid.* RUBÍ PUIG, ,"Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD*…", op. cit.,* p. 65, señala que "la responsabilidad podrá beneficiar a los perjudicados para el resarcimiento de los daños causados, puesto que muchas funciones del tratamiento de datos son encargados a grandes empresas con menores riegos de insolvencia para resarcir el daño".

[641] Debido a que nos encontramos ante derechos personalísimos, el responsable del fichero puede denegar el derecho de acceso, rectificación, cancelación, oposición, limitación y portabilidad, a toda persona que no sea titular de los datos o no acredite de manera fehaciente la representación legal del titular.

razonable en concepto de costes administrativos afrontados o, negarse a actuar respecto a lo solicitado", según establece el párrafo quinto del artículo 12 del RGPD. De igual forma, en caso de que el reclamante considere que no han sido atendidos sus derechos en tiempo y forma legales por parte del responsable del fichero, tiene la opción de acudir a la Agencia Española de Protección de Datos a fin de que sus derechos sean satisfechos. En el ámbito sanitario, caben destacar los siguientes derechos regulados en el RGPD más influyentes:

- Derecho de acceso (artículo 15, Considerando 63 RGPD). Es el derecho del interesado de poder acceder a sus datos personales y poderlo ejercer a fin de conocer y verificar la licitud del tratamiento, incluyéndose en el sector sanitario "el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas", añadiendo el Considerado 63 una exigencia muy relevante a tener en cuenta en las historias clínicas electrónicas al señalar que "si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales".

  Igualmente, este derecho tiene dos límites, por un lado, se podrá ejercer siempre y cuando no afecte "negativamente a los derechos y libertades de terceros, incluidos el derecho a la propiedad intelectual", lo que protege en materia sanitaria el especial tratamiento de las anotaciones subjetivas que los profesionales realizan en las historias clínicas (art. 18.3 de la Ley 41/2002)[642] y, por otro lado, se podrá ejercer siempre y cuando no afecte al interés público (Considerando 73 RGPD)[643].

[642] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, pp. 896-897.

[643] APARICIO SALOM, "Derechos del interesado…", *op. cit.,* pp. 367-372; RODRÍGUEZ AYUSO, J.F., *Garantía administrativa de los derechos del interesado en materia de protección de datos personales,* JB Bosch, Barcelona, 2021, pp. 47-57.

- Derecho de supresión (artículo 17, Considerando 65 RGPD). Es el derecho del interesado a que tanto el responsable del tratamiento como otros responsables que estén tratando sus datos tomen medidas y supriman todo dato personal, réplica, copia o enlace a los mismos[644].

  Indistintamente, en el RGPD se establecen una serie de limitaciones[645] al derecho al olvido reconocido previamente en la STJUE de 13 de mayo, caso Google, donde se concluye que el interesado puede solicitar el bloqueo de sus datos personales en los resultados de búsquedas, los vínculos que conduzcan a informaciones que le conciernen y que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público[646].

- Derecho a la limitación del tratamiento (artículo 18, Considerando 67 RGPD). El interesado puede limitar el tratamiento de los datos (1) cuando sea impugnada la exactitud de los datos personales; (2) cuando el tratamiento sea ilícito y el interesado se oponga la supresión de los datos, el responsable no los necesite, pero el interesado los requiera para la formulación, ejercicio o defensa de reclamaciones o; (3) cuando el interesado haya ejercicio su derecho de oposición[647].

- Derecho a la portabilidad de datos (artículo 20 RGPD). El interesado tiene derecho a recibir sus datos personales y haya facilitado a un responsable de tratamiento a efectos de poderlos transmitir a otro responsable, por ende, el responsable anterior está obligado a facilitar los mismos al interesado en un formato estructurado, común uso y lectura mecanizada[648].

---

[644] APARICIO SALOM, "Derechos del interesado…", *op. cit.,* pp.374-377.

[645]Así pues, el derecho al olvido del interesado será limitado, por ejemplo, cuando nos encontremos ante el ejercicio del derecho a la libertad de expresión e información, para el cumplimiento de obligaciones legales o en el ejercicio de poderes públicos, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, investigación científica o histórica, fines estadísticos, o bien, formulación, ejercicio o defensa de reclamaciones.

[646] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 897.

[647] APARICIO SALOM, "Derechos del interesado…", *op. cit.,* pp.382-385; RODRÍGUEZ AYUSO, *Garantía administrativa…, op. cit.,* pp. 145-148.

[648] Al respecto nos advierte LOMAS HERNÁNDEZ, "Principales Novedades de la Ley Orgánica 3/2018…", *op. cit.*, p.10, que: "Téngase en cuenta que el tratamiento de datos sanitaros en el ámbito de la sanidad pública, no pivota sobre la base jurídica del consentimiento del interesado, sino que se apoyaría sobre el

No en vano lo anterior, el RGPD en el art. 89.2 diferencia la regulación de las excepciones a los derechos para los tratamientos con fines de investigación científica, histórica o con fines estadísticos, así como de las excepciones a los tratamientos con fines de archivo en interés público, estatuyendo en el art. 89.3 que "cuando se traten datos personales con fines de archivo en interés público, el Derecho de la Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15 –derecho de acceso-, 16 –derecho de rectificación-, 18 –derecho a la limitación del tratamiento-, 19 –obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento-, 20 –derecho a la portabilidad de los datos- y 21 –derecho de oposición-, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines". Asimismo, el Considerando 65 del RGPD señala que "los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido" […] Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos".

En materia de protección de datos, como es sabido, la historia clínica – en papel o electrónica – es la herramienta fundamental donde consta depositada – a puño y letra o digitalmente – toda la información personal y de salud de los pacientes, abarcando todos los documentos acerca de los procesos asistenciales de cada paciente, con la identificación de los médicos y demás profesionales sanitarios, a efectos de obtener la máxima integración posible de la documentación de cada paciente, al menos, en el ámbito de cada centro sanitario. Igualmente, se ha recordar que el objetivo fundamental de la historia clínica es el de facilitar una asistencia sanitaria a través de la incorporar en la misma información relevante para el conocimiento veraz y actualizado del estado de salud del paciente.

---

cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, bases jurídicas que como ya ha quedado expuesto, hunden sus raíces en la Ley". Asimismo, MIRALLES LÓPEZ, R., "Derecho de portabilidad (Art. 20 RGPD. Art. 17, 95 LOPDGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 387-395; y, RODRÍGUEZ AYUSO, *Garantía administrativa…, op. cit.,* p. 224.

Pues bien, debido a la multitud de profesionales sanitarios, así como de centros sanitarios pertenecientes a la Administración Pública sanitaria o centros sanitarios privados que pueden tener acceso de manera directa a la historia clínica de cada paciente, a pesar de que en la normativa vigente de protección de datos – tanto en el RGPD como en la LOPDGDD – nada se menciona acerca de quién le corresponde la propiedad de la historia clínica, sin embargo, sí que se consideran responsables del tratamiento de los datos depositados en la historia clínica al facultativo médico o el centro sanitario, público o privado. En concreto, el responsable del tratamiento de los datos de salud y, en su caso, de su representante, puede ser médico privado, profesional sanitario de la compañía de seguro médico suscrito, hospital público o privado, o Servicio de Salud de la Comunidad Autónoma.

Igualmente, el paciente puede dirigir sus reclamaciones sobre el tratamiento de sus datos y el ejercicio de sus derechos al delegado de protección de datos a efectos de que atienda las reclamaciones efectuadas contra el responsable. En concreto, tienen la obligación de tener delegado de protección de datos los hospitales (públicos y privados); centros de salud, centros de atención especializada, clínicas. Por el contrario, ni tiene la obligación de tener delegado de protección de datos las consultas privadas de un profesional sanitario.

En síntesis, de un lado, bien el médico o centro sanitario, público o privado, tiene la obligación principal de elaborar la historia clínica, custodiar la misma, establecer las medidas de seguridad – que deben ser evaluadas periódicamente – a efectos de evitar su pérdida y el acceso de terceros no autorizados, así como de garantizar un nivel de seguridad adecuado, teniendo en consideración el estado de la técnica, los coste de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como aquellos riesgos de probabilidad y gravedad variables para los derechos y libertades de los pacientes. Igualmente, las medidas de seguridad que se implementen, por un lado, en caso de incidente físico o técnico deben permitir la restauración de la disponibilidad y el acceso a los datos personales de forma inmediata y, por otro lado, deben garantizar en la confidencialidad, integridad y disponibilidad de los datos.

El paciente o titular de los datos de salud, tiene derecho a solicitar una copia de su historia clínica pudiendo perfectamente facilitar posteriormente la misma a otro centro sanitario o especialista, igualmente tiene derecho a revisar la historia clínica a los efectos de solicitar posteriormente rectificación o supresión de algunos de los datos, en su caso. Por consiguiente, el responsable del tratamiento tiene la obligación de atender los derechos legales al interesado, excepto en aquellas situaciones en las que sea imposible identificar al mismo, en el plazo de un mes prorrogable por dos meses si es un asunto complejo o existe un elevado número de solicitudes. En caso de que la solicitud no sea tramitada, el responsable tiene la obligación de informar al paciente afectado en el plazo de un mes los motivos por los que no se ha sido tramitada, así como la opción de acudir a la AEPD o a los órganos judiciales. No obstante, con relación a la historia clínica a efectos de salvaguardar la responsabilidad de los responsables del tratamiento[649], se han de tener presentes los siguiente extremos y particularidades establecidos para el derecho de acceso, derecho de rectificación y derecho de supresión de datos de la historia clínica por parte del paciente afectado:

En primer lugar, sobre el derecho de acceso a la historia clínica la LAP señala que el paciente podrá acceder a la documentación de la historia clínica siempre y cuando no perjudique el derecho de confidencialidad de los datos de terceras personas que consten recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de profesionales sanitarios quienes podrán oponerse al acceso de las anotaciones subjetivas que consten la historia clínica del paciente. En este sentido, cabe destacar que el derecho de acceso no incluye la identificación de los profesionales sanitarios que acceden a la historia clínica, salvo que una ley lo permita expresamente. Por otro parte y, para el supuesto de fallecimiento del paciente, los centros sanitarios – públicos o privados – así como los profesionales en ejercicio individual de la medicina únicamente permitirán el acceso a la historia clínica a las personas vinculadas al mismo, bien sea por razones familiares, o bien, por razones de hecho, salvo prohibición expresa previamente emitida por el paciente fallecido. En todo caso, en caso de existir riesgo para la salud de un tercero, se permitirá un acceso limitado a la historia clínica del falleció a los datos de salud necesarios. En ningún concepto, se permite el acceso a información que afecta a la

[649] LÓPEZ ÁLVAREZ, "La responsabilidad del responsable…", *op.cit.,* pp. 275-294.

intimidad del fallecido ni que perjudique a terceros o a las anotaciones subjetivas de los facultativos sanitarios.

Por consiguiente, ante situaciones de asistencia sanitaria habituales, exclusivamente podrán acceder a la historia clínica el responsable – médico o profesional sanitario, el centro o la administración sanitarios – y el encargado del tratamiento, que normalmente será los prestadores de servicios externos, como los que realizan análisis de sangre y otras pruebas contratadas con terceras entidades especializadas en las mismas. Por ende, los citados responsables y encargados del tratamiento, deberán tomar las medidas adecuadas que garanticen fundamentalmente que las personas que se encuentren bajo su autoridad e instrucciones accederán a los datos personales del paciente únicamente para realizar su trabajo y, en ningún concepto deberá acceder para facilitar información de un paciente a terceros no autorizados. En este sentido, se aprecia que el RGPD permite que los responsables del tratamiento de los datos puedan ceder los datos de salud a otras entidades diferentes que pertenezcan a la estructura interna del centro salud – privado o público – donde se han recogido y tratado, siempre y cuando exista legitimación para ello, por ejemplo, el médico privado o centro sanitario que facilita a la aseguradora con la que tiene concierto de seguros médicos celebrado la información mínima a efectos de que esta le abone la prestación sanitaria realizada.

De igual modo, para el supuesto de la revisión de prevención de riesgos laborales, en el caso que el empleador solicite datos sanitarios de sus empleados no podrá acceder a la misma, la información que se le facilite al mismo únicamente es la siguiente: si el trabajador es apto, si no lo es y, en caso de ser apto si necesita de alguna adaptación, pero en ningún concepto se le informará de los resultados de las pruebas médicas de sus trabajadores. No obstante, caso distinto es el de la información que se le facilita al empleador de los partes de baja de sus trabajadores, donde el facultativo que está tratando al trabajador incapacitado facilitará dos copias del parte, una para el trabajador y otra para la empresa donde trabaja. El parte de baja contienen los datos personales del trabajador, así como la fecha de la baja, la fecha del siguiente reconocimiento, la contingencia causante, el código de diagnóstico, el código nacional de ocupación del trabajador, la duración estimada del proceso y, en algunos casos, la

aclaración de que el proceso es recaída de uno anterior señalándose al respecto la fecha de la baja del proceso anterior.

En segundo lugar, en relación con el derecho de rectificación de la historia clínica, el responsable del tratamiento tiene la obligación de facilitar sin dilación indebida al interesado la rectificación de los datos personales inexactos y a que se completen los datos personales que se encuentren incompletos. Igualmente, el interesado deberá aportar al responsable del tratamiento documentación acreditativa del error a los efectos de subsanar el mismo, rectificación que en el caso de datos sanitarios corresponde exclusivamente al profesional sanitario, quien decidirá de si finalmente procede o no rectificación del dato.

En tercer lugar, acerca del derecho de supresión de datos de la historia clínica, se ha tener en consideración que en la esfera sanitaria es un derecho especialmente limitado debido a que no podrán suprimirse los datos de salud del paciente– salvo expresa autorización del profesional sanitario – en aquellos casos en los que estén siendo tratados para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social; tratamientos por razones de interés público en el ámbito de la salud pública, a efectos de garantizar una asistencia sanitaria segura y de calidad, así como de los medicamentos y productos sanitarios.

Por consiguiente, resulta excepcional la cancelación de los datos que forman parte de la historia clínica del paciente, a mayor abundamiento si tenemos en cuenta que nos encontramos ante un documento que no únicamente tiene como finalidad la de garantizar una asistencia adecuada al paciente, sino que también puede ser utilizado en cualquier momento a fin de garantizar el interés público o el cumplimiento de obligaciones legales, ya que la historia clínica puede ser utilizada también en procedimientos judiciales, epidemiológicos, de salud pública, de investigación o docencia. Finalmente, a efectos de evitar imputabilidad alguna al responsable y al encargo del tratamiento de los datos de salud, la AEPD recomienda no facilitar información telefónica a un paciente sobre su estado de salud o el resultado de las

pruebas realizadas, al considerar que puede existir riesgo de que sea un tercero no autorizado para acceder a la misma.

De igual modo, cabe la posibilidad de facilitar la información al paciente vía teléfono siempre y cuando exista un protocolo de identificación del solicitante de la información, mediante solicitud de nombre y apellidos, nombre de DNI, número de teléfono facilitado previamente por el paciente al facultativo sanitario, dirección de correo electrónico, número de tarjeta sanitaria, esto es, cualquier dato identificativo personal que conste en su historia clínica a efectos de que el profesional sanitario pueda proceder a su comprobación, a efectos asegurar que es el paciente el que solicita la información y no una tercera persona. Por otro lado, se ha de hacer constar que el centro hospitalario – público o privado – no puede informar a terceros del ingreso de un paciente ni de la ubicación, a no ser que conste previamente el consentimiento del paciente para facilitar esa información o, de sus familiares, en caso de incapacitación del paciente. Se ha de apreciar, que además de los responsables de los tratamientos y los encargados de los tratamientos, según se aprecia en el artículo 70 LOPDGDD, existen otros sujetos responsables sometidos al régimen sancionador del RGPD y de la citada ley orgánica, como: los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta[650].

Por último, en lo referente al derecho al olvido, el RGPD reconoce al interesado el derecho a que sus datos sean suprimidos y dejen de tratarse una vez que dejan de ser necesarios para los fines que fueron tratados. Sin embargo, en el caso de los datos sanitarios, se permite una retención ulterior por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica, histórica o con fines estadísticos.

[650] GIL GONZÁLEZ, "Directrices del Grupo de Trabajo del Artículo 29 sobre el consentimiento en el Reglamento General…", *op. cit.,* p. 702 resume que: "El GT29 recuerda que, cuando el tratamiento de datos se legitima en el consentimiento, los interesados tendrán derecho de portabilidad, supresión u olvido (en este último caso, cuando se haya retirado el consentimiento), así como los derechos de acceso, rectificación y limitación del tratamiento. Por su parte, el derecho de oposición no se puede aplicar cuando el tratamiento se basa en el consentimiento, aunque la retirada de este pudiera llevar al mismo resultado".

Es evidente que en los proyectos de salud pública e investigación biomédica de interés general donde se apliquen técnicas de *big data*, el responsable del tratamiento deba garantizar a los interesados los derechos que por defecto le son de aplicación a todo titular de los datos personales de conformidad con lo establecido en los artículos 15 y concordantes del RGPD, donde se regulan los derechos de acceso, rectificación y oposición, así como el de decisiones individuales automatizadas, derecho de limitación del tratamiento, o en derecho a la portabilidad de datos, extremo este que igualmente debe ser recogido en la parte específica de la ley de protección de datos de salud. No obstante, se ha de matizar que en los tratamientos de *big data* el problema a resolver dimana de aquellos usos y tratamientos futuros y no previstos en el momento en el que se recaban los datos de salud, además de la complejidad de mantener informado de los nuevos usos y finalidades al titular de los datos, lo que viene a dificultar a su vez la tarea de recabar de nuevo o ampliar el consentimiento del mismo, así como de informar de manera continuada a los afectados de cómo ejercitar sus derechos y, lo complejo que puede resultar para el responsable o encargado del tratamiento responder a las solicitudes de los interesados.

Por ello, a efectos de evitar los anteriores problemas, sería conveniente que la ley sectorial recogiera algunas medidas que el responsable del tratamiento debería implantar previamente al inicio del tratamiento de *big data*, tales como: (1) implantación de un sistema de fácil acceso y localización a la información donde se detalle de manera clara y transparente al interesado el modo y el procedimiento a seguir a los efectos de hacer valer sus derechos frente al responsable y al encargado del tratamiento; (2) facilitar información al interesado acerca del origen de los datos, de las comunicaciones de datos a terceros, así como de las transferencias internacionales efectuadas o pendientes de efectuar en un futuro cercano; (3) facilitar información al interesado sobre el proceso de anonimización y del riesgo residual de reidentificación, en su caso y; (4) adaptación y actualización de las herramientas tecnológicas.

Por último, a efectos de adaptar el art. 22 RGPD sobre las decisiones automatizadas a la ley sectorial, se debe tener en consideración el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluyéndose en este extremo la elaboración de perfiles donde se utilizan datos

personales para valuar determinados aspectos personales de una persona física, que produzca efectos jurídicos en él o le afecte significativamente de modo similar, pudiéndose oponer a dicho tratamiento. Así como que, por un lado, en todo caso se permite el tratamiento automatizado cuando la decisión sea necesaria para la celebración o ejecución de un contrato entre el interesado y el responsable del tratamiento o se base en el consentimiento explícito del interesado y, por otro lado, que en los proyectos de salud pública e investigación biomédica de interés general o en caso de que exista consentimiento explícito del interesado, no será de aplicación la prohibición general de adoptar decisiones individualizadas automatizadas basadas en datos personales sensibles, siempre y cuando el responsable y encargado del tratamiento tomen las medidas adecuadas para salvaguardar los derechos e intereses del interesado.

VI. LAS NOTIFICACIONES DE LA BRECHA DE SEGURIDAD Y LA EVALUACIÓN DE IMPACTO EN EL SECTOR SANITARIO

De manera general, además de las anteriores garantías, es imprescindible tener presente que el responsable del tratamiento de los datos de salud en caso de violación de la seguridad de estos debe notificar la misma a la autoridad de control competente a la mayor brevedad posible en el plazo de 72 de horas, salvo causa justificada de dilación. Igualmente, en caso de que la violación de la seguridad de produzca en el encargado del tratamiento, éste deberá notificar la misma al responsable. Todo ello a efectos de salvaguardar el derecho de protección de datos del interesado, pues la autoridad de control competente deberá comprobar la causa de la violación de la seguridad de los datos personales, su efecto, así como las medidas adoptadas por el responsable o, en su caso, el encargado del tratamiento[651].

Asimismo, ante una violación de la seguridad de los datos de salud que suponga un alto riesgo para el interesado afectando a sus derechos y libertades, el responsable del tratamiento debe comunicar dicha violación al mismo, excepto en aquellas situaciones que, bien se haya adoptado medidas de protección técnicas y organizativas apropiadas aplicadas en concreto a los datos personales en los que se haya violado la seguridad, bien se haya tomado medidas ulteriores a fin de garantizar la improbabilidad

[651] Art. 33 RGPD.

de que se dé un alto riesgo para los derechos y libertades o, bien que venga a significar un esfuerzo desproporcionado, el cumplimiento de las anteriores condiciones serán comprobadas previamente por la autoridad de control pertinente a efectos de garantizar la procedencia o no de la comunicación de la violación de la seguridad al interesado en caso de que exista alto riesgo para sus derechos y libertades[652].

Otra de las garantías especialmente relevante por su influencia en el *big data* es la evaluación de impacto relativa a la protección de datos[653], puesto que en el caso en el que sean utilizadas nuevas tecnológicas que supongan un alto riesgo para los derechos y libertades de los interesados, el responsable del tratamiento debe realizar previamente al tratamiento de los datos, una evaluación de impacto de las operaciones de tratamiento en la protección de los datos personales[654].

Por ende, como se ha podido apreciar el RGPD regula una serie de obligaciones del responsable del tratamiento de los datos personales y, en su caso, al encargado, entre las que se ha de destacar: (1) obligación de adoptar las medidas técnicas y organizativas con el fin de proteger los datos, como la aplicación de las políticas de protección de datos, la seudonimización y la minimización de datos, integración de garantías necesarias en el tratamiento, transparencia de las funciones y tratamiento de datos, entre

---

[652] Art. 34 RGPD.

[653] *Vid.* Art. 35 RGPD y las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 adoptadas el 4 de abril de 2017 por el Grupo de Protección de Datos del art. 29. Al respecto, señala RODRÍGUEZ AYUSO, *Figuras y responsabilidades…, op. cit.,* pp. 128-129, que: "A través de esta exigencia, se persigue optimizar el cumplimiento de la nueva normativa, toda vez que ha de constituir un instrumento eficaz para que el responsable del tratamiento sea capaza de implementar decisiones en lo que respecta a la aplicación de medidas específicas en función del riesgo que conlleva el tratamiento, dando satisfacción al principio de responsabilidad proactiva. Así, por medio de la imposición de este deber, se persigue simplificar los procedimientos de protección de datos para el responsable del tratamiento, garantizando a medio y largo plazo la satisfacción adecuada de dicha regulación. De igual modo, a través de la incorporación de esta novedad se busca, de un lado, reforzar la información de los interesados en torno a los riesgos que comporta el tratamiento de sus datos personales, y, de otro, incrementar la seguridad en el tratamiento de los mismos."

[654] En concreto, en el apartado 7 del art. 35 RGPD establece que: "La evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas".

otras; (2) obligación de informar a las autoridades de control, la violación de la seguridad de los datos personales en un plazo de 72 horas y comunicar al interesado, en un leguaje claro y sencillo de la citada violación y, en cooperación con la autoridad de control[655] y; (3) obligación de realizar una evaluación de impacto de las operaciones del tratamiento, que tiene como finalidad tanto asegurar la protección de los datos personales como de colaborar con el proceso de toma decisiones, en el caso de que el tratamiento de datos suponga un alto riesgo para los derechos y libertades de las personas físicas.

En suma, respecto al sector sanitario desde una perspectiva jurídica la nueva normativa de protección de datos se basa en un modelo de la responsabilidad proactiva de los responsables del tratamiento de los datos (art. 5.2 RGPD) a efectos de que por el propio diseño de los ficheros y por defecto[656] los mismos incorporen medidas organizativas y técnicas que aseguren y garanticen una protección de los datos personales objeto del tratamiento de conformidad con lo establecido en los artículos del RGPD relativos a la responsabilidad del responsable del tratamiento (art. 24) y a la protección de datos desde el diseño y por defecto (art. 25). Así pues, el RGPD y la LOPDGDD establecen los siguientes mecanismos con la finalidad de prevenir un acceso indebido de la historia clínica por parte de los facultativos sanitarios:

En primer lugar, la obligación de los responsables y encargados del tratamiento de determinar medidas técnicas y organizativas apropiadas a efectos de garantizar y acreditar que el tratamiento es conforme a la legalidad vigente (art. 28 RGPD), garantizando en todo caso un nivel de seguridad adecuado al riesgo del tratamiento concreto de los datos (art. 32 RGPD). En este sentido, la LOPDGDD, en la Disposición Adicional primera señala que "el Esquema Nacional de Seguridad incluirá las medidas

[655] La comunicación de la violación de la seguridad de los datos al interesado no será necesaria cuando el responsable del tratamiento haya adoptado las medidas de protección técnicas y organizativas y, cuando se hayan adoptado medidas que garanticen que no existe alto riesgo para los derechos y libertades del interesado, o bien cuando suponga un esfuerzo desproporcionado, por lo que se optará por una comunicación pública o similar.

[656] A efectos de asegurar que únicamente sean objeto de tratamiento los datos personales exclusivamente necesarios para el fin específico para el que fueron recabados.

que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado adaptado a lo establecido en el art. 32 del RGPD[657].

En segundo lugar, la evaluación de impacto de las operaciones del tratamiento[658], en aquellos casos que supongan un alto riesgo para los derechos y libertades de las personas físicas, los responsables del tratamiento tienen la obligación de proceder a la evaluación del impacto de las operaciones de tratamiento de los datos personales, siempre y cuando las operaciones concretas no hayan sido previamente revisadas por una autoridad de control o delegado de protección de datos sin que haya habido cambios desde la última actualización[659] (Considerando 83 y art. 25 RGPD). Igualmente, en este sentido, la LOPDGDD regula supuestos de mayores riesgos a efectos de que sean apreciados por los responsables y encargados, en concreto, en el caso de los datos sanitarios, un mayor riesgo sería el supuesto de la pérdida de confidencialidad de datos sujetos al secreto profesional 28.2 a) LOPDGDD y, el

[657] En caso de que no sean adoptadas las citadas medidas de seguridad por los responsables y encargados del tratamiento estarían incurriendo en una infracción grave de conformidad con lo establecido en el art. 73 RGPD.

[658] HERAS, R., "RGPD: Evaluación de impacto", *I+S Revista de la Sociedad Española de Informática y Salud,* núm. 127, Febrero 2017, pp. 24 – 25, señala que: La evaluación de impacto en términos de protección de datos personales (EIPD) es una herramienta que permite evaluar de forma anticipada cuáles son los riesgos a los que están expuestos los datos personales según los tratamientos que el responsable o encargado del tratamiento lleve a cabo con los mismos. Se podría afirmar que la evaluación de impacto es un análisis de riesgos para un determinado tratamiento que permite identificar los riesgos sobre los datos de los interesados y establecer una serie de medidas para reducirlos hasta conseguir un nivel de riesgos aceptable por el responsable o encargado. Por tanto, la EIPD se puede considerar como recurso de carácter preventivo que debe utilizar el responsable o encargado del tratamiento para poder identificar, evaluar y gestionar los riesgos a que están expuestas sus operaciones de tratamiento con el objetivo de garantizar los derechos y libertades de los interesados. Al tratarse de una herramienta de carácter preventivo, el responsable o encargado debe tenerla en consideración desde el inicio del tratamiento de datos personales, es decir en la fase de diseño de un producto, servicio o sistema de información debe desarrollar las acciones preventivas necesarias para poder identificar, evaluar y tratar los riesgos asociados al tratamiento de datos personales que va realizar con la puesta en funcionamiento de ese producto, servicio o sistema de información para así asegurar el cumplimiento de los principios de protección de datos recogidos en el Reglamento y garantizando los derechos y libertades de las personas afectadas por ese tratamiento". En el mismo sentido, GONZÁLEZ GONZÁLEZ, "Responsabilidad proactiva en los tratamientos…", *op. cit.,* p. 125, aclara que: "El RGPD establece la necesidad de efectuar una evaluación de impacto sobre la protección de datos con carácter previo al inicio del tratamiento cuando se traten datos personales utilizando nuevas tecnologías que, por su naturaleza, alcance, contexto o fines, entrañen un alto riesgo para los derechos y libertades de las personas, como ocurre cuando se efectúa una evaluación sistemática y exhaustiva de aspectos personales de personas físicas, en base a en un tratamiento automatizado, como ocurre con la elaboración de perfiles, con todas las consecuencias antes apuntadas. Lo mismo ocurre cuando se tratan a gran escala, categorías especiales de datos, como son los datos de salud, o se produce una observación sistemática a gran escala de una zona de acceso público. El término "gran escala" puede tener unos límites de aplicación quizás difusos para otros tratamientos, pero forma parte intrínseca de los tratamientos masivos que aquí estamos considerando".

[659] Grupo de Trabajo del artículo 29.

supuesto de que se produzca el tratamiento no meramente incidental o accesorio de las categorías especiales de datos – entre los que se incluyen, como se es conocido, los datos de salud – de los arts. 9 y 10 del RGPD, en consecuencia, como señala MARTÍN JIMÉNEZ:

"La meta que persigue la evaluación de impacto es determinar el grado de afección en los derechos de las personas físicas desde aproximaciones objetivas diferentes; en un caso desde la óptica de la protección de los datos personales, en otro desde la equiparación oportunidades entre géneros y en el tercero a través de la defensa de la salud pública"[660].

En tercer lugar, la creación de códigos de conducta o directrices de "buenas prácticas para mitigar el riesgo" a efectos de que los responsables y encargados del tratamiento pueden adherirse a los mismos (arts. 40 y 41 RGPD; art. 38 LOPDGDD).

Asimismo, establecer de sistemas de certificación que acrediten que los responsables y encargados del tratamiento cumplen con la normativa de protección de datos personales (art. 42 RGPD y art. 39 LOPDGDD).

De igual modo, a los efectos de proteger el sistema de seguridad del tratamiento de los datos personales, la normativa vigente regula como mecanismo el deber de comunicar la violación de la seguridad en el menor tiempo posible (Considerandos 85, 86 y 87 RGPD), tanto a la seguridad del control (art. 33 RGPD) como, en su caso, al propio interesado (art. 34 RGPD). Asimismo, se ha de tener en consideración que el incumplimiento de este deber supone una infracción – grave o leve – según sea el supuesto de hecho concreto (art. 73, letras q), r), s) y 74 ñ) RGPD).

Esta cuestión es abordada por parte del legislador en el ámbito sanitario como una de las novedades del RGPD, puesto que debido a la sensibilidad de los datos relativos a la salud, datos genéticos o datos biométricos, la normativa vigente de protección de datos desde la perspectiva de la privacidad por defecto exige una máxima protección desde el inicio del tratamiento automatizado de la información incorporada

[660] MARTÍN JIMÉNEZ, R., "Evaluación de impacto en la Protección de Datos: Paralelismos", *I+S: Revista de la Sociedad Española de Informática y Salud,* núm. 134, 2019, p. 24.

en los datos personales destinados a la asistencia sanitaria e investigación biomédica y farmacéutica. Así pues, el principio de responsabilidad proactiva[661] actúa como garantía exigiendo a las organizaciones público[662] y privadas pertenecientes al ámbito sanitario una acreditación fehaciente del cumplimiento de la normativa vigente de protección de datos, lo que supone en consecuencia como señala PÉREZ GÓMEZ "un mayor esfuerzo para documentar y conservar todos los aspectos del tratamiento de datos de carácter persona"[663].

La evaluación de impacto en el ámbito sanitario tiene una gran relevancia puesto debe realizarse una evaluación sistemática y exhaustiva ante casos en los que se traten los datos personales para adoptar decisiones relativas a personas físicas "basada en la elaboración de perfiles[664] de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos" de acuerdo con lo establecido en el art. 35 y Considerando 75 del RGPD. En otro de los supuestos en los que se ha de realizar una evaluación de impacto es ante situaciones en las que se efectúe el

[661] En este sentido nos aclara PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 884, que: "Esto se traduce en una exigencia de mayor proactividad por los responsables de los ficheros, algo que reviste particular importancia cuando tienen por objeto el tratamiento de datos sensibles como suele suceder en el sector sanitario y farmacéutico. Siempre que el responsable considera que el tratamiento de datos previsto pudiera entrañar riesgos para los titulares de los datos, deberá plantear una consulta prevista ante la autoridad de control correspondiente (art. 36 Reglamento)".

[662] En el ámbito del sector público en el sector sanitario o en la investigación clínica es destable el Considerando 78 del RGPD cuando específica que "los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos".

[663] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 884.

[664] El art. 4.4 del RGPD define la "elaboración de perfiles" como: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física". Al respecto, PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 886, aclara que: "En el ámbito sectorial que nos ocupa, la utilización de perfiles compilando datos personales en principio de carácter no relacionado con la salud pero que reflejen determinados hábitos o comportamientos de una persona física que, en virtud de una relación causa-efecto estimada estadísticamente pudieran tener un reflejo en la salud futura del individuo, pudiera dar lugar a consecuencias para el titular de los datos a la hora, por ejemplo, de contratar seguros, contratar créditos a largo plazo, iniciar una nueva relación laboral. Desde un punto de vista finalista, resulta evid3ente que esos datos compilados con esa finalidad de alcanzar conclusiones relacionadas con la salud presente o futura del sujeto van a tener que ser calificados como datos relacionados con la salud y por lo tanto solo podrían ser tratados en los términos previstos y con las limitaciones recogidas en el citado art. 22 Reglamento. Por ese motivo, el responsable del tratamiento debe utilizar procedimientos adecuados y aplicar medidas técnicas y organizativas apropiadas para garantizar que se reduzca al máximo el riesgo de error y que no existan inexactitudes, así como asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, a que den lugar a medidas que produzcan tal efecto".

tratamiento sistemáticamente a gran escala[665], como sucede de manera habitual en la asistencia sanitaria pública[666], aunque no resultará obligatoria en el supuesto en el que el tratamiento de datos personales lo realice un solo médico, otro profesional de la salud[667]. El contenido de la evaluación de impacto en el sector sanitario debe cumplir con el contenido mínimo del apartado siete del art. 35 del RGPD, analizado al inicio del presente epígrafe, debiendo igualmente de intervenir un delegado de protección[668] de datos externo o interno[669].

Por último, la normativa vigente de protección de datos española[670], en la Disposición adicional 17ª. 2.f) considera obligatoria la evaluación de impacto en la protección de datos y la consulta previa, en todos y cada uno de los supuestos de tratamiento con fines de investigación en salud pública y biomédica.

De igual modo, El RGPD tampoco establece obligación específica alguna para las entidades sanitarias a los efectos de proceder a la elaboración de una Evaluación de Impacto en la Protección de Datos. En un principio el RGPD estableció que la obligación por parte de las autoridades de control de publicar un listado recogiendo las distintas operaciones de tratamiento que requieran una Evaluación de Impacto sobre la protección de datos[671].

---

[665] El art. 35.3.1. b) RGPD sobre el tratamiento a gran escala de datos sensibles, señala que: "tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10", añadiendo el apartado 5 del citado precepto 35 de la RGPD que: "La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité".

[666] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, pp. 884-885.

[667] De acuerdo con lo establecido en el Considerando 19 del RGPD: "[…] el tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud".

[668]Art. 35.2 RGPD.

[669] Art. 37.6 RGPD.

[670] Así pues, como ha sido analizado anteriormente, el art. 28 de la LOPDGDD incluye como obligaciones generales del responsable y encargo del tratamiento la determinación de las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la regulación vigente.

[671] Art. 35 RGPD.

Por ende, en mayo de 2019 la AEPD procedió a la publicación de las *Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4)*[672] donde se aprecia que las entidades sanitarias cumplen varios de los criterios asentados por la AEPD, entre los que destacar los criterios 4, 5 y 6 en relación con el tratamiento de los datos de categorías especiales recogidas en el art. 9.1. RGPD, datos biométricos y datos genéticos, por lo que las entidades sanitarias, públicas o privadas, estarían obligadas a elaborar una EIPD, cuestión esta que posteriormente viene a corroborar la LOPDGDD en la Disposición adicional decimoséptima sobre el tratamiento de datos de salud, estableciendo en su apartado segundo letra f) la obligación de elaborar una EIPD donde se incluya el modo especifico de los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos cuando el tratamiento sea para fines de investigación biomédica y asistencia sanitaria de interés público.

[672]Agencia Española de Protección de Datos, *Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4),* 2019. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf, en el mismos la AEPD establece que "Debe entenderse como una lista no exhaustiva: 1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos. 2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato. 3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc. 4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos. 5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física. 6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin. 7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía *WP243 Directrices sobre los delegados de protección de datos (DPD)* del Grupo de Trabajo del Artículo 29. 8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos. 9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de catorce años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia. 10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas. 11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD".

Por consiguiente, debido a la importancia de la elaboración del EIPD en el sector sanitario, convendría que la ley sectorial recogiera en su articulado un apartado donde perfile aquellas situaciones en las que el responsable del tratamiento de datos de salud está obligado a realizar una EIPD con carácter previo a proceder a poner en funcionamiento los tratamientos en el caso de existir probabilidad de alto riesgo para los derechos y libertades de las personas físicas debido a la naturaleza, alcance, contexto o fines de los datos de salud, así como las directrices[673] a seguir en la misma a los efectos de determinar la existencia o no de alto riesgo en el tratamiento de los datos de salud, riesgo que será incrementado cuando se utilicen nuevas tecnologías para el tratamiento según el RGPD.

Por último, teniéndose en consideración los altos riesgos para la privacidad implícitos en la utilización de las tecnologías de *big data* por el hecho de manejar fuentes dispares de datos, la ley sectorial debe incorporar entre su articulado el deber de las organizaciones (públicas o privadas) de incluir en los proyectos *big data* una EIPD[674] que demuestre el tratamiento logra un objetivo específico y legítimo, así como que se han adoptado las medidas de seguridad necesarias.

VII. GARANTÍAS INSTITUCIONALES DE PROTECCIÓN DE DATOS EN EL ÁMBITO SANITARIO

1. GARANTÍA GENERAL: EL DELEGADO DE PROTECCIÓN DE DATOS EN EL SECTOR SANITARIO

La figura del delegado de protección de datos (también, DPD)[675], regulada en el artículo 37 del RGPD, consiste en la persona – con conocimientos de Derecho y

[673] Grupo de Trabajo del Artículo 29 en la guía *WP248 Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD*.

[674] El contenido mínimo de la EIPD debe ser el establecido en el art. 35 RGPD.

[675] En este sentido, LÓPEZ RUÍZ, C.G., "La figura del delegado de protección de datos (DPO)", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, p. 695, aclara que: "El DPO cubre la necesidad de las empresas de contar con la ayuda de una persona con conocimientos especializados en la práctica de protección de datos personales, siendo la figura que rinde cuentas ante el cumplimiento de la normativa, convirtiéndose en una pieza clave de la

protección de datos, sin necesidad de que sea jurista – que se encarga principalmente de informar y asesorar al responsable o al encargado del tratamiento de los datos acerca de sus obligaciones legales, supervisar que cumple con la normativa de protección de datos personales y, cooperar y actuar como enlace con la autoridad de control, de conformidad con lo establecido en el artículo 39 del RGPD[676]. En consecuencia, el sector sanitario, especialmente en el ámbito de la asistencia sanitaria, es el que más se ha visto afectado por su implantación puesto es que es el sector donde el titular de los datos personales mantiene un contacto directo con el responsable del tratamiento, esto es, con la entidad pública o privada que realiza el tratamiento a causa de la asistencia sanitaria[677].

Igualmente, el delegado de protección de datos debe ser designado por el responsable y el encargado del tratamiento en los siguientes supuestos: (1) cuando nos encontremos ante un tratamiento llevado por una autoridad u organismos públicos (se incluyen los hospitales y centros sanitarios públicos, excepto los tribunales en ejercicio de su función judicial); (2) ante actividades principales que requieran de un control habitual y sistemática de interesados a gran escala y; (3) ante actividades principales del responsable o encargado que consistan en el tratamiento a gran escala de categorías especiales de datos personales (art. 9 RGPD) y condenas o infracciones penales (art. 10

---

organización. Aun siendo intermediario entre las partes, interesados o las autoridades supervisoras, los DPO no son personalmente responsables en caso de incumplimiento del RGPD. En este caso, continuará siendo el responsable de garantizar el cumplimiento de la normativa el responsable o el encargado de tratamiento de los datos de carácter personal, siendo los primeros que han de nombrar y dotar al DPO de todos los recursos necesarios de cara al efectivo desempeño de sus funciones"; RODRÍGUEZ AYUSO, *Figuras y responsabilidades…, op. cit.,* pp. 148-163.

676 VILLASECA, M., "El Delegado de Protección de Datos", *I+S Revista de la Sociedad Española de Informática y Salud,* núm. 127, Febrero 2017, p. 21, señala que: "El RGPD regula de forma detallada las circunstancias a tener en cuenta para la designación del Delegado de Protección de Datos, estableciendo una serie de supuestos de designación obligatoria por parte de los responsables y encargados cuando: • El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial. • Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o • Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10. Además, el RGPD abre la posibilidad de que los países de la Unión, a través de su normativa específica puedan establecer otros supuestos en que haya que nombrar a un DPD". Igualmente, SARRIÓN ESTEVE, "Las novedades de la nueva normativa de protección de datos y su aplicación a los ensayos clínicos de…", *op. cit.*, pp. 235-236; SÁNCHEZ ORS, C., "El Delegado de Protección de Datos (Arts. 37-39 RGPD. Arts. 34-37 LOPDGDD)", AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 494-496.

677 PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 887.

RGPD). En consecuencia, se podría afirmar que cuando se trata de datos de salud en todo caso es de obligado nombramiento del delegado de protección de datos según las directrices que ha publicado el Grupo de Trabajo 29 (GT29), así como la AEPD, debido a que los datos de salud se pueden ver afectados por cada uno de los supuestos anteriores, especialmente con el supuesto destinado a las actividades principales del responsable o el encargado del tratamiento consistan en operaciones de tratamiento que requieren una observación habitual y sistemática del interesado a gran escala, indistintamente que el responsable del tratamiento sea un organismos público o privado[678], sin embargo, según criterio de PÉREZ GÓMEZ, que se comparte en este trabajo:

"[…] desde un punto de vista práctico, no parece eficiente que todos y cada uno de los centros sanitarios – por ejemplo, en los centros de salud – deban disponer de un DPD, y en ese sentido, habrá que poner en relación este precepto con el actual art. 14.4 Ley 41/2002, al que se remite el propio precepto de LOPDGDD, donde se establece que serán las Comunidades Autónomas las que aprobarán las disposiciones necesarias para que los centros sanitarios adopten las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y así, interpretando sistemática unas normas con otras podemos alcanzar la conclusión de que, si organizativamente así parece razonable, puede ser designado uno o varios DPD por cada área de salud sin menoscabo de lo señalado por la LOPDGDD"[679].

De igual modo, cuando nos encontremos ante operaciones donde se apliquen herramientas de *big data* (en el sector sanitario) será obligatorio nombrar a un delegado de protección de datos en el tratamiento de gran escala de categorías especiales de datos (datos de salud), pues según el Considerando 91 del Reglamento, en el término "gran escala" se incluirán las operaciones "que persigan tratar una cantidad considerable de

[678] Al respecto, LÓPEZ RUIZ, "La figura del delegado de protección de datos…", *op. cit.*, p. 696, señala que: "Por actividades principales entendemos tanto las operaciones fundamentales o claves para llegar a los objetivos del responsable del tratamiento o el encargado del tratamiento, como aquellas operaciones intrínsecas que forman parte de estas operaciones – por ejemplo, el tratamiento de los datos de salud de un hospital".

[679] PÉREZ GÓMEZ, "Especialidades en el sector sanitario…", *op. cit.*, p. 888.

datos personales a nivel regional, nacional o supranacional y que podrán afectar a un gran número de interesados y entrañen probablemente un riesgo"[680].

Finalmente, se ha de tener en consideración que la figura del delegado de protección de datos en el sector salud, además de tener conocimiento sobre la normativa de protección de datos y la normativa sanitaria, "debe tener una cualificación profesional sobre el conocimiento de las organizaciones sanitarias y capacidad para mantener una relación fluida con ellas"[681].

Sin embargo, el RGPD no establece obligación específica alguna para las entidades sanitarias a los efectos de designar un DPD, por ello, resulta de gran interés que en la ley sectorial entre su articulado destine un apartado especial a esta materia a los efectos de aclarar aquellas situaciones en las que es obligatorio para los centros sanitarios, públicos y privados, proceder a designar DPD, al entender la AEPD que existen figuras sanitarias que no tienen la obligación de tener delegado de protección de datos, como la del profesional sanitario con consulta privada donde ejerza individualmente su actividad, indistintamente de que quede obligado al mantenimiento de las historias clínicas de los pacientes[682].

En concreto, con relación a la designación del DPG, si dado el caso, de manera general son todas las entidades sanitarias (públicas y privadas) las que tienen la citada obligación al encontrase obligadas legalmente al mantenimiento de las historias clínicas

---

[680] En este sentido LÓPEZ RUIZ, "La figura del delegado…", *op. cit.*, p. 697, aclara que: "Se desprende la imposibilidad de concretar una cifra exacta para determinar si es o no gran escala, y, por tanto, se deberán tener en cuenta los siguientes factores: - El número o proporción de los interesados involucrados. – El volumen de datos o abanico de diferentes conceptos de datos se procesan. – La duración o permanencia de la actividad del tratamiento de datos. – El alcance geográfico del tratamiento de los datos. Podrían considerarse incluidos en estos criterios y, por tanto, ser sujetos obligados a tener dentro de su organización un DPO, las entidades aseguradoras y reaseguradoras, entidades responsables de sistemas de información crediticia, colegios profesionales, centros sanitarios, entidades dedicadas al juego on-line, empresas que realicen un tratamiento de datos personales para publicidad basada en el comportamiento por parte de un motor de búsqueda o aquellas que realicen seguimiento de tarjetas de transporte público, entre otras. Por último, en caso de duda de si una organización tiene que contar o no con un DPO, se recomienda que los responsables y encargados del tratamiento documenten el análisis interno llevado a cabo para determinar si deben o no nombrar un DPO, teniendo en cuenta todos los factores determinantes".

[681] ESPAÑA, M., directora de la Agencia Española de Protección de Datos, entrevista en *I+S, Revista de la Sociedad española de informática y salud,* Impacto del Nuevo Reglamento de Protección de Datos en el ámbito sanitario, Núm. 127, febrero 2018, p. 11.

[682] Agencia Española de Protección de Datos, *Guía* para *pacientes y usuarios de la Sanidad*, 2019, p.7.

de los pacientes y, al tratarse de categorías especiales de datos personales[683], resulta de interés que conste así recogido en la ley sectorial junto con las excepciones legales, todo ello a los efectos de mayor claridad y transparencia para los profesionales del sector de la salud. No en vano, se ha de hacer constar que a pesar de que en la LOPDGDD se establece la obligación de las entidades sanitarias – públicas y privadas - de designar un DPD[684]. y, de igual modo, la AEPD así aclara[685], en particular, su actual directora, Mar España, indica que "cualquier centro hospitalario debe tener un registro de actividades de los tratamientos a los efectos de efectuar un análisis de riesgo y, en su caso, una evaluación de impacto, implantar medidas técnicas, organizativas y de seguridad y contar con un delegado de protección de datos […] su función principal es asesorar sobre el cumplimiento de la normativa y concienciar a los profesionales, para lo que debe tener conocimientos en derecho y práctica en protección de datos"[686]. Sin embargo, en la LOPDGDD no constan reguladas las situaciones excepcionales que podrían ser ampliadas a todos y cada uno de los sectores de la sanidad, que, aun estando obligadas legalmente al mantenimiento de las historias clínicas de los pacientes, se le exime de la obligación de la designación de un DPD.

2. GARANTÍA ESPECÍFICA EN EL ÁMBITO SANITARIO: EL COMITÉ DE ÉTICA DE LA INVESTIGACIÓN

Por último, queda destacar como garantía del tratamiento de los datos en el ámbito sanitario la figura del Comité de Ética de la Investigación regulada en la disposición adicional decimoséptima de la LOPDGDD, cuyas competencias principales se encuentra la de emitir informe previo a la reutilización de datos personales con fines de investigación en materia de salud, biomédica y farmacéutica cuando se utilicen los datos para otras finalidades o áreas de investigaciones relacionadas con la finalidad por la que el paciente prestó su consentimiento para la utilización de sus datos de salud, siendo requisito imprescindible que el informe emitido por el Comité de Ética de la

[683] Art. 37.1 RGPD.

[684] Art. 34.1. letra l) LOPDGDD.

[685] Agencia Española de Protección de Datos, *Guía* para *pacientes y usuarios de la Sanidad*, 2019, p.7

[686] Periódico Expansión, *Los retos de protección de datos en el sector sanitario: el DPO y la Evaluación de Impacto,* 22 de julio 2019 [en línea]. Documento disponible en: https://www.expansion.com/juridico/opinion/2019/07/22/5d358541468aebd9208b45fd.html

Investigación sea favorable a efectos de que la reutilización de los datos sea lícita y compatible.

Asimismo, se requiere informe previo del Comité de Ética de la Investigación para un uso lícito de los datos personales seudonimizados con fines de investigación en salud pública y en biomédica[687]. Actualmente, entre los miembros de los citados Comités de Ética en el ámbito de la salud, biomédico o del medicamento, que tenga entre sus actividades de investigación el tratamiento de datos de salud personales, seudonimizados o anonimizados, por obligación legal deben constar con un delegado de protección de datos o, en su defecto, con un experto con conocimientos suficientes del RGPD.

Por ende, los Comités de Ética guardan un papel relevante en el sector sanitario y en la investigación científica[688], por tanto, conviene que la ley de protección de datos de salud guarde un espacio en su articulado a la regulación de los mismos en lo que a su intervención y funciones en materia de protección y tratamiento de los datos de salud respecta, además si tenemos presente, como bien advierte la profesora SERRANO PÉREZ "que en el campo de la investigación científica carecen de una regulación general" [689]. Por ende, algunos de los extremos a destacar que deberían ser recogidos por la ley sectorial sobre los Comités de Ética en materia de protección de datos de salud, son: de un lado, para que una investigación tenga la consideración de científica (pública o privada) en el marco sanitario y legal, es requisito necesario la aprobación previa por parte del Comité de Ética de la Investigación correspondiente. De otro lado, en los casos de investigaciones clínicas hospitalarias, a fin de que los investigadores puedan acceder

[687] MARTIN URANGA, A., "El nuevo Reglamento Europeo de Protección de Datos: una oportunidad para avanzar en investigación biomédica con las garantías adecuadas para los pacientes", *I + S: Revista de la Sociedad Española de Informática y Salud,* ejemplar 122, 2017, p. 12, opina que: "En definitiva, el nuevo RGPD debe ser una oportunidad para seguir avanzando en proyectos de investigación biomédica que contemplen la reutilización de datos, o el uso de datos de salud "a gran escala", incluyendo las garantías adecuadas para asegurar el máximo beneficio de los pacientes, siempre bajo la supervisión de los comités de ética de investigación. Se ha de tener presente el mecanismo de coherencia del Reglamento Europeo, para que todas las autoridades estén alineadas en esta materia, con la finalidad de conseguir una adecuada armonización que otorgue seguridad jurídica y permita a nuestros investigadores mantener un liderazgo en el ámbito de consorcios paneuropeos de investigación biomédica presentes y futuros, buscando y respetando siempre un adecuado equilibrio entre la protección de datos de los participantes, y otros valores sociales como la salud pública, el interés público y la promoción de la investigación biomédica en el mayor beneficio de los pacientes".

[688] El art. 12 de la LIB sobre las funciones de los Comités de Ética de la Investigación.

[689] SERRANO PÉREZ, "La necesidad…", *op. cit*., p.6.

a la historia clínica de los pacientes debe constar de manera expresa previamente el visto bueno del Comité de Ética de la Investigación del hospital o centro sanitario (público o privado) concreto donde se esté realizando la investigación.

De igual modo, la ley sectorial debe regular la posibilidad de que los Comités de Ética de la Investigación científica pública que se realice con datos de salud o en la investigación con muestras biológicas, de manera excepcional puedan permitir su acceso sin existir consentimiento de los titulares de los mismos, cuando nos encontremos ante un estudio observacional de gran interés social, donde resulte imposible anonimizar los datos de salud y suponga a su vez, un mínimo riesgo para los titulares de los datos. Asimismo, establecer la necesidad legal de que los Comités de Ética de la Investigación determinen las condiciones específicas en función del tipo y fines de la Investigación científica (pública o privada) para el tratamiento de datos sin el consentimiento informado de los participantes, así como la obligatoriedad de que emita a un dictamen favorable en los casos en los que no exista consentimiento informado del paciente.

En este sentido, conviene subrayar que sobre la aplicación de las tecnologías del *big data* donde se traten cantidades masivas de datos de salud a gran escala que procedan de fuentes heterogéneas, resulta también de interés que la ley sectorial establezca que el Comité de Ética realice una evaluación previa y control al respecto a efectos de sustituir el consentimiento de los interesados[690]. Igualmente, la ley de protección de datos debe tener en consideración la posibilidad de establecer que en el caso estudios de investigación biomédica de interés público donde se requiera la utilización de datos masivos de salud identificativos donde no conste consentimiento de los titulares previamente deba existir autorización del Comité de Ética de la Investigación que será efectuada tras consulta planteada al mismo por parte de los responsables del tratamiento[691]. Por último, resulta de interés que la ley de protección de datos de salud regule aquellas situaciones en la que los Comités de Ética asistencial como órgano consultivo deban ser consultados por los profesionales sanitarios a los efectos de salvaguardar el deber de secreto profesional ante aquellas situaciones en la

[690]De conformidad con lo establecido en el art. 58 LIB.

[691] Según lo establecido en el art. 58.3 RGPD, donde se interpreta que la autoridad de control deba ser el Comité de Ética de la Investigación.

que deban comunicar de la información relevante de los datos de salud de los pacientes a terceros.

En síntesis, consta más que justificada la necesidad de una ley de protección de datos en el ámbito de la salud, pues como se ha podido apreciar a lo largo del presente trabajo, la normativa vigente de protección de datos entremezcla los datos personales con los datos de salud, siendo el resultado una normativa dispersa, confusa y con grandes complejidades a la hora de ser interpretada a por los profesionales de la sanidad en calidad de responsables y encargados del tratamiento, así como por la población en su conjunto, partiendo desde los propios juristas especializados en la materia hasta el interesado titular de los datos personales y de salud. Por ello, sin duda, una normativa de protección de datos de salud de aplicación en el contexto de la salud de la salud pública e investigación científica, que de manera clara y concisa regule la protección y el tratamiento de los datos de salud, será una decisión acertada y segura hacía la evolución de nuestro ordenamiento jurídico por parte del legislador, si legado el momento decide finalmente promulgarla.

A modo de clausura de este punto, conviene acentuar que para aquellas cuestiones generales de protección de datos tanto personales como de salud, a modo de ejemplo citar el régimen de sanciones e infracciones o las reglas generales para el consentimiento, entre otros, convendría que la ley sectorial propuesta en este trabajo se remitiera a la normativa general de protección de datos vigente, así como a las leyes sanitaras para aquellas cuestiones particulares de salud, todo ello en aras del principio de unidad jurídica y del principio de seguridad jurídica.

VIII. NIVEL DE PROTECCIÓN ADECUADO EN EL TRATAMIENTO TRANSFRONTERIZO DE LOS DATOS PERSONALES

Por último y, no menos importante, otra de las garantías del derecho de protección de datos es la del “nivel de protección adecuado” que la Directiva 95/46 cita de manera reiterada en los considerados (56) y (57), así como en los preceptos 25 y 26 de la misma, a fin de regular la situación de transferencia de datos personales a terceros países. No cabe duda que en el campo de la investigación cada vez son más frecuentes

las transferencias internacionales de datos tanto para el desarrollo de proyectos europeos como internacionales, que requieren del acceso y tratamiento de datos genéticos y de salud[692], por ello el legislador europeo, siendo consciente de ello, regula esta cuestión en el Reglamento, previamente abordada por el TJUE en el año 2015 en la Sentencia de 6 de octubre de 2015, asunto C-362/14 (caso Schrems) donde realiza la siguiente valoración:

Por un lado, el TJUE establece que el "nivel de protección adecuado" lleva implícito la exigencia de que la legislación interna o los compromisos internacionales del tercer país deben garantizar de manera efectiva "un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta." Por ende, es el ordenamiento jurídico del tercer país el que debe garantizar el nivel adecuado de protección, en caso contrario, si el ordenamiento jurídico del tercer país no pudiera garantizar en la practica una protección de los datos personales equivalente a la garantizada en la Unión el objetivo se vería frustrado y por tanto la transmisión de los datos personales al mismo sería nula y contraria a Derecho[693]. Por otro lado, el TJUE en la citada sentencia establece que la Comisión tiene la función y el deber de valorar las normas aplicables del derecho interno del tercer país o sus compromisos internacionales a efectos de declarar válida o no la adecuación, así como el deber de verificar el cumplimiento de las condiciones reguladas en las mismas, "debiendo atender esa institución (la Comisión)[694] a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país, conforme al artículo 25, apartado 2, de la Directiva 95/46"[695].

En relación con el tratamiento, el Reglamento diferencia entre tratamiento y tratamiento transfronterizo[696]. En primer término, el RGPD en el apartado segundo del

[692] *Vid.* RECUERDO LINARES, M., "Transferencias internacionales de datos genéticos y datos de salud con fines de investigación", *Revista de Derecho y Genoma Humano,* Núm. Extraordinario, 2019, p. 415.

[693] *Vid.* STJUE (Gran Sala) de 6 de octubre de 2015, asunto C-362/14 (caso Schrems), §§ 73 y 74.

[694] Aclaración añadida a efectos de no generar confusión en el lector.

[695] *Vid.* STJUE (Gran Sala) de 6 de octubre de 2015, asunto C-362/14 (caso Schrems), §§ 75.

[696] ÁLVAREZ RIGAUDIAS, C., "Transferencia de Datos Personales a terceros países y organizaciones internacionales (Arts. 44-50 RGPD. Arts. 40-43 y Disposición adicional quinta y decimotercera LOPGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la*

artículo 4 regula una enumeración exhaustiva de las diferentes operaciones que conllevan el tratamiento genérico de los datos personales, en concreto, destaca la "recogida, registros, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" operaciones que según establece el legislador pueden ser realizadas mediante procedimientos automatizados o no automatizados.

En segundo término, cuando nos encontramos ante actividades que se desarrollan en establecimientos sitos en más de un Estado miembro cuyo tratamiento de los datos personales es realizado bien, por un responsable, ya sea una persona física o jurídica, autoridad pública, servicio u otro organismo que, que solo o junto con otros, determine los fines y medios del tratamiento; o bien, por un encargado del tratamiento, entendiéndose por el mismo persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, de la Unión Europea, estaríamos ante un tratamiento transfronterizo siempre y cuando el responsable o el encargado está establecido en más de un Estado miembro de la Unión Europea.

Igualmente, debe indicarse que nos encontramos ante un tratamiento transfronterizo, cuando el tratamiento de datos personales es realizado en el contexto de las actividades de un responsable o encargado del mismo en la Unión, pero con un único establecimiento en un Estado miembro pero que sin embargo afecta sustancialmente o cabe la probabilidad que afecte sustancialmente a interesados en más

---

LOPDGDD, (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 570-71, aclara que: "El Reglamento mantiene en lo esencial el régimen de transferencias internacionales que estableció la Directiva 95/46/CE, aunque introduce una serie de cambios relevantes. Se articula en torno a los siguientes elementos…: - *Nivel adecuado:* De conformidad con el art. 45 del Reglamento, la Comisión Europea (la «Comisión») puede declarar la existencia de un nivel adecuado de protección respecto del país (tercero) de destino, de un territorio (lo que de facto la Comisión ya hizo en su momento al amparo de la Directiva 95/46/CE) así como respecto de (un) sector(es) especifico(s) en un país tercero o de una «organización internacional». – *Garantías y excepciones*: El Reglamento establece una serie de excepciones por las que es legítimo transferir los datos personales a países de nivel «no equiparable» y «no adecuado». Estas excepciones se refieren bien a ciertas garantías específicas (arts. 46 y 47) o a una lista tasada de excepciones (art. 49). – *Decisiones administrativas o judiciales de país tercero:* El art. 48 del Reglamento hace una referencia al supuesto de que la transferencia esté motivada en una decisión por un órgano administrativo o judicial no fundada en una ley UE (o del EM). – *Cooperación internacional:* El art. 50 del Reglamento regula el supuesto de cooperación internacional entre la Comisión y las autoridades de control".

de un Estado miembro. Consecuentemente, la situación de tratamiento transfronterizo viene marcada por la actividad desarrollada por el encargado o responsable del tratamiento, en concreto, bien por el existir varios establecimientos titularidad del encargado o responsable en diferentes Estados miembros, bien porque los interesados afectados por la actividad del encargado o responsable del tratamiento pertenezcan a diferentes Estados miembros, en virtud de lo establecido en el artículo 4. 23) del mismo.

En este sentido, la nueva regulación reconoce que el lugar de la administración central del tratamiento en la Unión debe ser el establecimiento principal de un responsable del tratamiento, excepto cuando nos encontremos ante situaciones donde las decisiones respecto a los fines y medios del tratamiento de los datos personales sean tomadas en otro establecimiento que el responsable tenga dentro de la Unión Europea, en este caso, será este otro establecimiento el principal. En concreto, el lugar de administración central vendrá determinado en base a criterios objetivos, implicando un ejercicio efectivo y real de actividades de gestión donde sean determinadas de manera estable las principales decisiones en relación con fines y medios del tratamiento, independientemente de que las actividades de tratamiento o el tratamiento de datos mediante presencia y utilización de medios técnicos y tecnologías sea realizado en el mismo lugar o distinto. En defecto de que el encargado del tratamiento careciese de un lugar de administración central, entonces será el lugar donde sean realizadas las principales actividades de este en la Unión Europea.

Por lo que respecta a aquellas situaciones que afectan tanto al encargado y como al responsable, la autoridad de control competente seguirá siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, siendo a su vez, la autoridad de control del encargado la autoridad control interesada, lo cual le permite participar en el procedimiento de cooperación establecido en el RGPD, excepto en aquellos casos donde el proyecto de decisión afecte únicamente al responsable.

En otros términos, cabe poner en cuestión el tratamiento de los datos personales mediante un grupo empresarial. Ante la presente situación donde nos encontremos con un grupo empresarial, constituido por una empresa que ejerce el control y empresas controladas, siendo la empresa controladora la que domine mediante participación financiera, propiedad, normas o poder de hacer cumplir las normas de protección de

datos personales, al resto de empresas, en este caso, el establecimiento principal de aquella empresa que ejerce el control y a su vez determine los fines y medios del tratamiento, será el establecimiento principal del grupo empresarial, sin embargo, en caso de que sea otra empresa la que determine los fines y medios, entonces será éste el establecimiento principal. Así pues, podemos deducir que el establecimiento principal en un grupo empresarial quedará afecto de aquella empresa que determine los fines y medios del tratamiento, independientemente de que sea la que ejerza el control o sea empresa contratada.

Debemos destacar que el artículo 45 del RGPD, permite la transferencia de datos a un tercer país u organización[697], siempre y cuando exista decisión favorable por parte de la Comisión Europea sobre la garantía de un nivel adecuado de protección en atención al respeto del tercer país al Estado de Derecho, los Derechos Humanos y las Libertadas Fundamentales, a la normativa jurídica interna sobre protección de datos, existencia dentro del tercer país de autoridades de control independientes, con capacidad de garantizar el cumplimiento de la normativa específica de protección de datos, así como la adhesión a convenios o acuerdos vinculantes en materia de protección de datos, especialmente al Convenio 108[698]. En caso de inexistencia de decisión favorable de la Comisión Europea, el responsable o el encargado del tratamiento de datos personales, únicamente puede transmitir los datos a un tercer país cuando este ofrezca garantías adecuadas y bajo la condición de que los interesados sean garantes de derechos exigibles y acciones legales efectivas.

En este extremo lo más significativo es que la ley de protección de datos de salud, además de tener en consideración los establecido en los artículos 44 y 45.1 del RGPD, prevea la posibilidad de transferir datos de salud por razones epidemiológicas ante amenazas graves a la salud de la población sin necesidad de que el interesado haya dado previamente explícitamente su consentimiento a la transferencia, ni que la Comisión se haya pronunciado sobre la adecuación del país preceptor para proteger los datos personales[699].

---

[697] A consecuencia de la doctrina asentada en la ya citada STJUE de 6 de octubre de 2015, asunto C-362/14, caso Schrems.

[698] Considerando 105 RGPD.

[699] Considerando 112 del RGPD y art. 49 RGPD.

En conclusión, la efectividad de las medidas jurídicas adecuadas dependen del efectivo cumplimiento de las garantías tecnológicas, donde el consentimiento del paciente pasa a segundo plano, siendo lo relevante el cumplimiento de las garantías técnicas, si no se cumplen las normas técnicas no se puede hacer de manera efectiva *big data*, jurídicamente es imposible, a mayor abundamiento si se trata de información sensible como es la de la salud que afecta a esfera privada del paciente o se genera un modelo de cumplimiento adecuado o no es factible desde un punto de vista jurídico – real realizar *big data*.

CAPÍTULO QUINTO

OPORTUNIDADES, LÍMITES Y DESAFÍOS DE LA TECNOLOGÍA *BIG DATA* EN EL ÁMBITO SANITARIO

I. OPORTUNIDADES DE LAS TECNOLOGÍAS *BIG DATA* EN EL SECTOR SANITARIO

En este capítulo centraremos nuestra atención en las oportunidades y retos de las tecnologías *big data* en el sector sanitario. De igual modo, en algunos epígrafes se hará referencia de manera conjunta al *big data* como a la Inteligencia Artificial debido a la estrecha vinculación que guardan ambos al resultar técnicas influentes en el tratamiento de los datos relativos a la salud en el sector sanitario, como se verá a continuación.

En la nueva era digital, con especial atención a los datos sanitarios, tanto en la industria tecnológica, como en el sector sanitario y en el jurídico constantemente se alude a las nuevas oportunidades, retos y desafíos que supone el *big data* en la sanidad y en la investigación, especialmente, en la investigación biomédica y farmacéutica. Todo

ello se deriva del hecho de que los datos sanitarios, tras ser analizados a través de algoritmos, aportan conocimiento e información de un gran valor que coopera a que la esfera sanitaria evolucione velozmente y de manera eficaz hacía una medicina predictiva, precisa y de calidad, aumentando el conocimiento en el sector de la Medicina y la Ciencia, suponiendo en consecuencia una mejora en el bienestar de la humanidad[700].

Así pues, ya en año 2012[701] la revista *Forbes* predijo en su artículo "The Next Revolution in Healthcare*"*[702], que el *big data* ofrecía una oportunidad a los innovadores y agentes que intervenían en el sector sanitario, al aumentar las posibilidades de obtener información más efectiva de los datos y menores tasas de mortalidad en los enfermos. De igual modo, el informe *Big data in digital Health[703]* suscrito por la Fundación *Rock*

[700] En este sentido, TRONCOSO REIGADA, *La protección de los datos personales*…, *op. cit.*, p. 1100, declara que: "Las tecnologías de la información y la comunicación son un instrumento muy positivo para la actividad sanitaria no en sí mismo consideradas, sino porque redundan en la mejora de la calidad asistencial de los pacientes". Asimismo, MARTIN URANGA, "El nuevo Reglamento Europeo de Protección de Datos: una oportunidad para avanzar…", *op. cit.*, p. 10, opina que: "La apuesta de la industria por la investigación clínica, por los pacientes y por la sociedad española en su conjunto, es una realidad que pone de manifiesto la apuesta que el sector desarrolla de forma coordinada con hospitales, centros de investigación, profesionales sanitarios y Administraciones públicas. Por ello, una interpretación restrictiva de la normativa de protección de datos, así como de determinadas normas de aplicación sectorial en las que incide dicha normativa, puede poner en peligro el trabajo realizado en los últimos años, dado que afectaría significativamente a la capacidad de los sistemas sanitarios europeos y de los investigadores para avanzar en investigación biomédica y aprovechar todo el potencial que las diferentes fuentes del *Big Data* (ensayos clínicos, historia clínica electrónica, registros de pacientes, receta electrónica etc…) ofrecen a las autoridades sanitarias, a los investigadores y, por supuesto, a los pacientes. No se puede ignorar que todo ello ayuda en la toma de decisiones de forma rápida y eficaz, a realizar análisis predictivos, así como a una mejora continua de los sistemas de trabajo y de la eficiencia en cuestiones tan sensibles como la asistencia sanitaria, con la finalidad de impulsar mejoras en el sistema sanitario y en su sostenibilidad". Asimismo, DE MONTALVO JÄÄSKELAÄINEN, "Una reflexión desde la teoría de los derechos fundamentales sobre el uso…", *op. cit.*, p. 45 señala que: "El *Big Data* ofrece en general y, especialmente, en el ámbito de la investigación en salud, muchas alternativas y oportunidades2. La explotación masiva de los datos de salud tradicionales e, incluso, su interrelación con los no tradicionales, va a permitir avanzar en la lucha contra las enfermedades y a favor de la prevención y predicción en unos términos que seguramente no van a encontrar parangón en la Historia de la Medicina y de la humanidad".

[701] Aunque fue en el año 2011 cuando Sir Tim Berners-Lee, el careador de la World Wide Web, dijo que los datos serían la nueva materia prima del siglo XXI, GARCÍA MEXÍA, P. y PERETE RAMÍREZ, C., "Internet, el RGPD y la LOPDGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, p. 852.

[702] RISKIN, D., "The Next Revolution in Healthcare", *Forbes,* 2012, [Documento sin paginación]. Documento disponible en: https://www.forbes.com/sites/singularity/2012/10/01/the-next-revolution-in-healthcare/#26f260d055cc (última consulta 22/01/19).

[703] Acceso web al informe: https://rockhealth.com/rock-report-big-data-healthcare/ (última consulta 23/07/18). Asimismo, el informe es comentado por POYATOS DÍAZ, J.M., "*Big Data* y el sector de la salud: el futuro de la sanidad", 2013, [Documento sin paginación]. Documento disponible en http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad (última consulta 22/01/19).

Health, establece diferentes motivos por los que el *big data* supone un cambio radical en la atención sanitaria y un gran sustento en la investigación biomédica: "(1) Investigación de soporte: genómica y más allá; (2) transformación de datos en información; (3) apoyo al autocuidado de las personas; (4) apoyo a los proveedores de cuidados médicos; (5) aumento del conocimiento y concienciación del estado de salud; (6) agrupamiento de los datos para expandir el ecosistema". A tales efectos según establece el citado informe es necesario combinar y agrupar una gran variedad de datos limitados a fin de mejorar resultados, destacando igualmente las siguientes áreas sanitarias que se verían favorecidas por los beneficios del *big data*:

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

Por ello, en el presente trabajo se defiende, entre otras, la tesis de que es necesaria una normativa sectorial sobre protección de datos de salud y de *big data*, pues no cabe duda que uno de los grandes retos de los legisladores estatales en los próximos años será el de garantizar la compatibilidad del tratamiento masivo de los datos sanitarios por medio de las tecnológicas *big data* (e incluso IA) a efectos de rentabilizar sus ventajas y beneficios para la mejora de la calidad de la vida de la humanidad y, a su vez, salvaguardar el derecho de protección de datos de los ciudadanos, siendo la única vía factible para conseguir la satisfacción de tal objeto el de la promulgación de una ley específica sobre la protección y el tratamiento de datos de salud, así como de medidas y garantías de aplicación de herramientas *big data* en proyectos de salud pública e investigación (biomédica y farmacéutica) de interés general.

A continuación, se analizará el cambio de la neutralidad de los datos sanitarios a ser grandes creadores de información y conocimiento con la aplicación de herramientas *big data*, haciéndose especial mención a su uso por parte de las compañías sanitarias, examinándose los actuales recursos y proyectos de *big data* más relevantes en el sector sanitario y en la investigación biomédica y farmacéutica.

1. DE LA NEUTRALIDAD DE LOS DATOS SANITARIOS A LA CREACIÓN DE CONOCIMIENTO E INFORMACIÓN

Actualmente, como se ha podido apreciar a lo largo del presente trabajo, el sector sanitario es uno de los sectores donde más valor aporta la aplicación de las tecnologías de *big data*, en España, tanto los organismos públicos como las entidades privadas de la investigación biomédica y asistencia sanitaria apuestan cada vez más por las herramientas *big data* en sus proyectos a efectos de sustraer información y conocimiento que garantice una medicina predictiva y de precisión, así como una asistencia sanitaria de calidad, además de obtener una mayor rentabilidad en términos económicos y temporales. De igual modo, no hemos de obviar el hecho de que tanto en los registros/ficheros de la Administración Pública sanitaria como de las entidades privadas se encuentran registrados una masividad de datos de salud que con la aplicación de las tecnologías de *big data* suponen un valor añadido para una sanidad eficiente, eficaz y de calidad[704].

Por ende, en el futuro las herramientas de *big data* serán esenciales para el desarrollo de proyectos de investigación biomédica y asistencia sanitaria, pues de un lado, es evidente que el *big data* supone una gran rentabilidad económica, puesto que

[704] DE MONTALVO JÄÄSKELAÄINEN, "Una reflexión desde la teoría de los…", *op. cit.*, p. 52, afirma que: "Especialmente en el ámbito de la salud, el *Big Data* muestra como todos estamos relacionados. Compartimos genes, exposiciones medioambientales, hábitos y comportamientos. De este modo, los datos obtenidos de un grupo de individuos pueden predecir la enfermedad y los patrones de evolución de otros grupos de individuo".

está demostrado que reduce costes y optimiza el gasto[705]. Al respecto, el *Informe de resultados big data en salud digital* indica que[706]:

"La potencialidad del uso de sistemas *big data* en el mundo de la salud podría ser enorme según los estudios consultados. Por ejemplo, algunas estimaciones en 2011 calculaban que las aplicaciones de *big data* en el sector sanitario podrían representar unos beneficios de hasta 250.000 millones de euros en los sistemas de salud públicos en Europa y de hasta 300.000 millones de dólares en Estados Unidos.

Otro posible indicador sobre el impacto que la aplicación de *big data* en salud podría tener en la economía puede estar relacionado con las iniciativas emprendedoras en relación a esta cuestión.

Así, la categoría de *big data* es la segunda que había recibido más inversión de capital riesgo en Estados Unidos en la primera mitad de 2015, sólo tras los *Wearables*, categoría con la que está íntimamente relacionada.

En relación con esto, la situación en España difiere de la que se observa en Estados Unidos, especialmente por lo que respecta a la profusión de iniciativas emprendedoras, menor en España, aunque parecida a la de los países de nuestro entorno más cercano".

---

[705] En este sentido, MOOIWEER, P. y SHOCKLEY, R., "Analítica de datos: El uso en el mundo real de *Big Data* en sanidad y ciencias de la vida. Cómo las organizaciones más innovadoras en sanidad y ciencias de la vida de la salud extraen valor de datos inciertos", *IBM Institute for Businees Value,* Julio 2013, p. 2, señalan que: "Para las compañías de ciencias de la vida, los datos son el motor de la función de investigación y desarrollo, así como de otras áreas esenciales como finanzas, marketing y gestión de riesgos. El factor que impulsa la optimización de los procesos en este sector es evidente: el desarrollo de un nuevo fármaco efectivo puede costar más de 1.900 millones de dólares; la globalización de la distribución de medicamentos trae consigo nuevas normas y un mayor escrutinio de la seguridad, efectividad comparada, ética y calidad3. Los datos serán igualmente esenciales para el futuro del sector de ciencias de la vida cuando éste busque mejorar los procesos de desarrollo clínico, actuar a partir de la información de los pacientes, pagadores y proveedores para promover el crecimiento y mejorar las relaciones en todo el ecosistema de sanidad y ciencias de la vida". Igualmente, MANYIKA, BROWN, DOBBS, ROXBURGH y BYERS, "*Big Data*: The next frontier…", *op. cit.,* señalan que el uso de las técnicas de *Big Data* en el sector sanitario podría representar unos beneficios de hasta 250.000 millones de euros los sistemas de salud públicos en Europa y de hasta 300.000 millones de dólares en Estados Unidos.

[706] Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p.39. Documento disponible en: https://www.ontsi.red.es/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf (última consulta 05/03/19).

Debido a ello, no es de sorprender que en el futuro se espere que de manera progresiva las entidades privadas y los organismos públicos inviertan gran parte de sus recursos económicos en proyectos que apliquen herramientas *big data*, a efectos de rentabilizar la actividad empresarial y profesional sanitaria al mínimo coste y máximo beneficio[707].

De otro lado, desde una perspectiva de la asistencia sanitaria e investigación biomédica de interés general, el uso de *big data* en el futuro resulta esencial para poder predecir, prevenir y personalizar la medicina hacía tratamientos personalizados que se adapten al paciente[708]. Así pues, en la actualidad el *big data* está siendo un valor añadido en el sector sanitario pues ofrece muchas y ventajosas posibilidades, tales como: el seguimiento de pacientes crónicos, la investigación genómica y la secuenciación del genoma, mejora en la atención personalizada al paciente, operativa clínica, medicina personalizada para todos, autopsias virtuales, monitorización remota de pacientes, mejoras en los procesos médicos, entre otros muchos sectores sanitarios a destacar[709].

---

[707] En este sentido, GARCÍA MEXÍA y PERETE RAMÍREZ, "Internet, el RGPD y la LOPDGDD…", *op. cit.,* p. 852, indican que: Las empresas son cada vez más conscientes de que el análisis de datos puede contribuir a mejorar notablemente sus procesos de toma de decisiones. Los datos son muy valiosos para ganar eficiencia, pues permiten entender mejor el comportamiento y pautas de consumo de los clientes, desarrollar productos y servicios mejor adaptados a sus necesidades y preferencias y crear vínculos más robustos para fidelizarlos e, incluso, predecir tendencias. Todo ello redunda, en última instancia, en mayores ventas y en un incremento de la innovación y competitividad. El análisis de datos ha comenzado también a generalizarse entre las pymes y administraciones públicas porque empieza a poder hacerse a costas más accesibles".

[708] De ello nos advierte GARCÍA BARBOSA, J., "La medicina del futuro pasa por *Big Data"*, octubre 2014, [Documento sin paginación]. Documento disponible en: https://empresas.blogthinkbig.com/la-medicina-del-futuro-pasa-por-big-data/ (última consulta 07/03/19) donde señala que la tecnología que utiliza los datos masivos será de gran alidada de la medicina del futuro o, "Medicina de las 4P: personalizada, predictiva, preventiva y participativa". Subraya el papel que esta nueva tecnología podrá desempeñar en cada uno de estos aspectos de la gestión clínica. Para sacar su máximo partido, "en la sanidad del futuro sería preciso capturar, almacenar y analizar todos los datos disponibles sobre ensayos clínicos, historiales médicos, secuenciación de ADN de pacientes, información procedente de redes sociales… Se debería disponer, por tanto, de una enorme base de datos compartida entre todos los hospitales y resto de actores del sector de la salud".

[709] Al respecto, NÚÑEZ, M., "Las asombrosas cifras de la mHealth", febrero 2014, [Documento sin paginación]. Documento disponible en: https://empresas.blogthinkbig.com/las-asombrosas-cifras-de-la-mhealth/ (última consulta 07/03/19) sobre los diez puntos fundamentales del informe "Análisis de la eSalud en España" de Ametic, señala que: "La aplicación de las TIC a la sanidad contribuye a mejorar los resultados en salud, así como la eficiencia del sistema y reduce de forma significativa el consumo de recursos sanitarios y los costes." […] "Se han conseguido logros como que 20 millones de españoles tengan historia clínica digital, y que el 70 por ciento de las recetas sean electrónicas, así como una amplia implantación de la radiología digital en nuestros hospitales". […] "Pero aún quedan muchos retos pendientes: no podemos hablar de historias clínicas integradas entre niveles, e interconectadas entre las diferentes comunidades autónomas y entre los sistemas públicos y privados de prestación sanitaria.

En el mismo sentido, el informe *eHealth (tecnología y medicina)*[710], señala algunas de las ventajas inmediatas: "1. Personalización del sistema sanitario; 2. Pronóstico y seguimiento de enfermedades en tiempo real sin que el paciente o usuario tenga que desplazarse; 3. Participación del ciudadano en temas de salud; 4. Seguridad del paciente en todas las etapas del proceso sanitario; 5. Integración de los sistemas sanitarios de distintos países, intercambio de información".

Asimismo, se ha de subrayar los beneficios que supone la aplicación de técnicas del *big data* en la propia gestión y administración del sistema sanitario (público y privado), así como su gran valor y aportación en la investigación y desarrollo científico, puesto que fundamentalmente ayuda a la determinación de causas de las enfermedades y agilizar el descubrimiento de tratamientos para las mismas[711].

Al respecto, el informe *Big data, el poder de los datos* de la Fundación Innovación Bankinter, señala que los profesionales mantienen que el *big data* contribuye a "reinventar el sistema sanitario", destacando en concreto que:

"La transformación del tradicional seguimiento periódico del enfermo en consulta a un proceso continuo en el que, a través de una plataforma digital o de una

---

Respecto a la receta electrónica hay también grandes diferencias y una evolución muy desigual en cuanto a prescripción y dispensación en las distintas CC.AA. Y en lo relativo a la cita previa sanitaria también quedan grandes retos por cubrir: multicanalidad, cita previa hospitalaria y en pruebas diagnósticas o servicios de valor añadido como la gestión de resultados y la orientación sanitaria". […] "Tanto para evitar el colapso del sistema como para ofrecer una sanidad moderna y adaptada a los nuevos tiempos es necesario que la inversión TIC en sanidad se intensifique. Las TIC son clave para garantizar la sostenibilidad del sistema sanitario: España es uno de los países más envejecidos del mundo, con una población mayor de 65 años superior al 25 por ciento y la cronicidad, debido en parte a este envejecimiento poblacional, representa cerca del 75 por ciento del gasto sanitario".

[710] GARCÍA CUMBRERAS, M.A., "eHealth (tecnología y medicina)", *Coddiinforme*, enero 2017, p.4. Documento disponible en https://coddii.org/wp-content/uploads/2017/01/Informe-e-Health-2.pdf

[711] Precisa al respecto LÓPEZ LÓPEZ, V., "*Big Data* sanitario: el acelerador del conocimiento y la decisión clínica", 4 de mayo 2015, [Documento sin paginación]. Documento disponible en https://empresas.blogthinkbig.com/big-data-sanitario-el-acelerador-del-conocimiento-y-la-decision-clinica/ (última consulta 08/03/19) que: "los profesionales sanitarios cada vez entienden mejor que puede suponer un cambio de paradigma en la práctica de la Medicina, y las empresas farmacéuticas quieren utilizarlo para diseñar medicamentos cada vez más efectivos y con menor coste de investigación. A su vez, las administraciones quieren comprobar la eficacia de los nuevos medicamentos en lo que se denomina *Real World Data*".

app, los profesionales pueden controlar minuto a minuto la evolución del paciente y realizar mediciones constantes"[712].

De igual modo, en el informe *Big data y Salud* elaborado por Media Planner y prodigioso Volcán en colaboración con Rache Farma y Siemens, donde se detallan algunas de las ideas fundamentales del *big data* para el futuro en el sector de la salud, se especifican varios proyectos reales llevados a cabo sobre *big data* sanitario como:

a) El proyecto *IBM Watson Health* (Sistema para computación cognitiva) cuyo objetivo es que "la tecnología Watson sirva como un servicio en *cloud* que permita a los hospitales médicos, aseguradoras e incluso potenciales pacientes a aprovechar su vasto almacenamiento de datos"[713] .

b) El proyecto *23andme-Google,* que usa los datos de ADN procedentes de las pruebas genéticas que realiza a sus clientes a través de muestras de saliva para proyectos de investigación y el desarrollo de nuevos fármacos.

c) El proyecto *PatientsLikeMe,* cuya finalidad es de guardar una copia completa de los datos de salud de personas afectadas por enfermedades graves o incurables. Los usuarios tienen acceso a una plataforma web donde pueden contar a los demás sus propias experiencias en relación con la enfermedad, síntomas del tratamiento, secuelas, opiniones… a cambio la web les ofrece herramientas analíticas de gran potencia y coste que hasta ese momento solo tenían acceso los investigadores. El proyecto se financia con la venta de los datos sanitarios agregados, anónimos y segmentados a las compañías farmacéuticas, y a la vez colabora con la mejora de la calidad de vida del paciente y con la investigación biomédica.

---

[712] SEYFERT-MARGOLIS, V., "Médicos y pacientes", en *Big Data. El poder de los datos*, Fundación innovación Bankinter, 2015, p.39. Documento disponible en: https://www.fundacionbankinter.org/documents/20183/42758/Publicaci%C3%B3n+Big+data/cc4bd4e9-8c9b-4052-8814-ccbd48324147

[713] Media Planner y Volcan, *Informe Big Data y Salud*, 2016, pp. 69-70. Documento disponible en: https://es.slideshare.net/AndresMacario2015/informe-big-data-y-salud?from_action=save (última consulta 16 de septiembre de 2018).

Igualmente, el citado informe detalla y explica de manera resumida algunos *wearables* o dispositivos electrónicos que registran información vital sobre la salud de los usuarios como el Fitbit, Reloj Apple, Propeller Health (GPS incorporado a un inhalador), Google X (nanopartículas para buscar cáncer) y, las lentillas inteligentes Google X, entre otros. Entre los proyectos desarrollados en España relacionados con *big data* en salud, se han de destacar los siguientes[714]:

De un lado, el proyecto *VISC+* de la Agencia de Calidad y Evaluación Sanitarias de Cataluña (Aqua), cuya finalidad era la de relacionar la información de salud de Cataluña una vez anonimizada y segura, a efectos de impulsar y facilitar la investigación, la innovación y la evaluación en el ámbito de la salud. Sin duda, un proyecto orientado al sector de la investigación y desarrollo científico (I+D+i) pertenecientes a la Administración pública, a fin de facilitar la investigación y aumentar la calidad de la asistencia sanitaria y mejorar la toma de decisiones y la capacidad de evaluar el sistema sanitario[715].

[714] *Vid.* al respecto Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, pp. 22 y ss.

[715]Sobre esta cuestión se pronuncia en su trabajo SERRANO PÉREZ, Mª M., "*Big Data* o la acumulación masiva de datos sanitarios: Derechos en riesgo en el marco de la sociedad digital", *Derecho y Salud,* Vol. 25, septiembre, extra 2015, pp. 63-64, indicando que: «En resumen, y tras el análisis realizado de diversas cuestiones relativas a la disposición normativa que recoge la forma jurídica del BD, podemos concluir que el encargo realizado a AQuAS para "medir, evaluar y difundir de forma pública y transparente los resultados en salud de los distintos actores que integran el servicio catalán de salud a través de gestión de la información sanitaria", resulta mejorable en aspectos fundamentales en orden a garantizar la protección de los sujetos de los que se recogen y tratan datos relativos a la salud. Las medidas de protección recogidas en el proyecto VISC+ resultan insuficientes para poder hablar de una protección elevada de los derechos de los ciudadanos, por lo que el riesgo del tratamiento de los datos sobre la salud por medio de este BD sanitario no aparece conjurado. Ello no significa, no obstante, que la acumulación masiva de datos en el contexto de la salud no deba realizarse y que mediante una mejora en los criterios de utilización de los datos y en los fines perseguidos, no pueda conseguirse una reutilización de los datos efectiva y eficaz. El BD introduce indudables beneficios que no deben ni pueden ignorarse, como tampoco la protección de los derechos de los sujetos cuyos datos son manejados. El equilibrio ha de lograrse a través de una regulación jurídica razonable y sensata». Igualmente, MARTÍNEZ MARTÍNEZ. R., "Big Data, investigación en salud y protección de datos personales: ¿Un falso debate?", *Revista Valenciana d'Estudis Autonòmics,* n.º 62, 2017, p. 253, señala que: "Las conclusiones del documento resultan particularmente valiosas y ofrecen ideas sobre como encauzar jurídicamente un proyecto sobre Big data. Pero ni el Documento, ni publicaciones posteriores, entraron en el detalle de las condiciones de uso fijadas por la Generalitat en la Memoria de VISC+, y en el documento sobre «Garantías éticas para el uso de los datos», ni en cómo se incorporaron o no las recomendaciones de la APDCAT. El resultado práctico fue ofrecer carnaza a todos aquellos dispuestos a entrar en un debate de buenos y malos, que fue el que finalmente triunfó llevando al fracaso el proyecto y cercenando toda posibilidad de desarrollos futuros por un buen periodo de tiempo".

De otro lado, el proyecto *SMUFIN (Somatic Mulations Finder)* que detecta de manera rápida y precisa los cambios genómicos causantes de la aparición y progresión de tumores e incluso analizando el genoma completo de un tumor y detectando sus mutaciones de manera rápida a la vez que son localizadas alteraciones que se encontraban ocultas, todo ello aplicando un innovador método *big data* desarrollado por investigadores españoles y promovido por Nature Biotechology[716].

Más recientemente, en el año 2019 la Universidad de Sidney desarrolló un proyecto donde a través de la forma facial de las personas se detectaban marcadores de salud fisiológica en más de 270 individuos de distintas etnias a fin de tener conocimiento de su masa corporal y la presión arterial[717]. Por otro lado, los investigadores del CNIO desarrollaron la herramienta *PanDrugs*, donde a través del análisis de los datos se prescriben medicamentos teniendo en consideración los datos genómicos del paciente[718]. Finalmente, mencionar los proyectos *Help4Mood*[719]*, Polen Control*[720]*, SAVANA*[721] y *Picto Connection*[722]*,* todos ellos de gran relevancia e impacto en España.

---

[716] Asimismo, *SMUFIN* ha sido dirigido por el grupo de genómica computacional del Barcelona Supercomputing Center – Centro Nacional de Supercomputación (BSN-CNS) en colaboración con otros grupos de investigación.

[717] *Vid.* documento web: "¿Cómo diagnosticar enfermedades a través de la forma del rostro?", Salud Digital. Disponible en: https://www.consalud.es/saludigital/94/como-diagnosticar-enfermedadesa- traves-de-la-forma-del-rostro_45763_102.html (Último acceso 11/11/20).

[718] *Vid.* https://www.cnio.es/noticias/publicaciones/un-nuevo-metodo-basado-en-analisis-de-datos-para-personalizar-el-tratamiento-del-cancer/ (última consulta 11/11/20).

[719] En este contexto, el Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 37, señala que: "Su objetivo es crear una herramienta de apoyo al tratamiento de la depresión mediante el seguimiento del paciente durante sus tareas diarias con una serie de sensores no intrusivos. La información que recogen los sensores se procesa y, a través de un agente virtual, el paciente recibe instrucciones y recomendaciones que le ayudan en el apoyo de su enfermedad. Por ejemplo, se podrían poner sensores en la cama del hogar del paciente y, en caso de detectarse una permanencia recostado no habitual o normal, se podría deducir que la persona con depresión está recayendo en la enfermedad y, consecuentemente, se podría llevar a cabo una intervención más inmediata".

[720] *Vid.* Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 38., donde establece que: "Este proyecto se basa en la combinación de aplicaciones para *smartphones* y el potencial de *Big Data* para prevenir o evitar los efectos de las patologías derivados de la profusión de polen en la atmósfera. Esta aplicación ha sido desarrollada conjuntamente por la Sociedad Española de Alergología e Inmunología Clínica (SEIAC) y los Laboratorios Almirall y realiza el seguimiento de la evolución sintomática en pacientes con alergia. Cada vez que se utiliza, el paciente describe sus síntomas y el sistema permite que el profesional médico pueda cruzar y relacionar dichos datos con los niveles polínicos existentes, lo cual supone un gran avance a la hora de establecer una relación entre síntomas y exposición a pólenes".

[721] Es una plataforma que analiza, resume y presenta de forma sencilla la información médica contenida en el conjunto de historias clínicas electrónicas para su reutilización en la práctica clínica en tiempo real.

Desde esta perspectiva, se puede apreciar que los usos del *big data* en la esfera sanitaria son múltiples, destacando su relevancia en los ensayos clínicos ya que por medio del *big data* de manera automática se seleccionan los pacientes para el ensayo clínico, en la efectividad de medicamentos y seguimientos de efectos adversos, en la evaluación de servicios sanitarios, en la vigilancia epidemiológica, en la predicción de hospitalización por patologías en base a factores externos (ambientales, poblacionales…), en la identificación de pacientes de alto riesgo, en la toma de decisiones de los médicos, en el análisis del estado de salud de un determinado territorio y, en el seguimiento de tendencias, en consecuencia, para poder obtener una información lo más eficaz posible y, poder avanzar así en *big data*, es necesario saber realizar las preguntas correctas.

Además, el *big data* sanitario supone una mejora en la gestión administrativa sobre los datos del ciudadano, donde la información que obtenemos resulta ser una gran herramienta a fin de adelantarse a la enfermedad y detectar necesidades, creándose así una medicina más precisa, a través de la información procedente de la tarjeta de identificación sanitaria, de la historia clínica, del Internet de las Cosas (*smartphones),* datos ambientales y de las casas, cuya finalidad es la de generar múltiples predicciones para distintas enfermedades o prevenir hábitos no saludables y caminar hacía la medicina de precisión, evaluando con esa información si lo que se hace es efectivo o no. Asimismo, apreciándose a su vez una reducción notable de los costes tras la aplicación

---

La idea es que cualquier médico, desde cualquier consultorio, por pequeño y distante que esté, puede tener una experiencia de consulta de opinión colectiva sobre cualquier problema clínico. Savana se basa en algoritmos de inteligencia artificial. *Vid.* Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 3.

[722]"Es un *software* de comunicación inteligente dirigido a personas que bien por un trastorno neurológico, una enfermedad o un accidente no pueden comunicarse o no lo pueden hacer de manera efectiva. Picto Connection parte de un análisis neuropsicológico del paciente a través de una serie de preguntas que puede responder tanto el padre del paciente, como el docente o el terapeuta. A partir de este análisis, se autogenera de manera automática una herramienta de comunicación en función de la patología y las necesidades de cada usuario. Es decir, la herramienta no sólo considera si el usuario tiene, por ejemplo, autismo, parálisis cerebral o ha sufrido un ictus, sino que además tiene en cuenta cada una de las necesidades específicas que desencadena cada uno de estos problemas: deficiencia visual, epilepsia, bajo nivel cognitivo, hipoacusia o hipercusia. Picto Connection también se basa en el uso de la inteligencia artificial y *Big Data* para poder hacer recomendaciones individualizadas basadas con el análisis de otros usuarios, incluso para poder analizar el comportamiento de un mismo usuario en el uso de la herramienta. El proyecto ha sido constituido como empresa con la ayuda de la incubadora Incubio (@incubio) situada en Barcelona. Picto Connection (@pictoconnection) ha sido premiado por la Fundación Vodafone por el concurso "Talento Joven" organizado en la Comunidad Valenciana y ha quedado como novena mejor aplicación del mundo en el concurso de los WSA-Mobile en inclusión social organizado por las Naciones Unidas", Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 38.

de las técnicas *big data*, a consecuencia de que cuanto mayor sea la gestión de la salud menores serán los gastos.

Por consiguiente, en el futuro se prevé que el *big data* sea cada vez más una tecnología más utilizada en el sector sanitario debido fundamentalmente a los amplios beneficios que resultan de su aplicación en los proyectos de asistencia sanitaria e investigación biomédica. En este sentido, como afirman MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGUADIAS:

"En particular, tecnológicamente, la conjunción del *cloud computing* y las herramientas de *machine learning* supone una revolución para la investigación científica. En efecto, permiten disponer de la experiencia acumulada durante lustros en petabytes de datos y son capaces de digerir datos no estructurados, desarrollar un análisis semántico automatizado, y tratar fuentes de todo tipo […] Distintas consultoras señalan el impacto de la tríada que integran *big data*, investigación retrospectiva y prospectiva con datos de salud y la "medicina de las 5 P": personalizada, predictiva, preventiva y participativa y poblacional"[723].

En este sentido, por un lado, resulta primordial que a efectos de que la sociedad pueda seguir avanzando y creciendo, a fin de garantizar un aumento del conocimiento y une mejora del bienestar social se ha de priorizar las inversiones en tecnologías, sobre todo en *big data* como una herramienta de interés general, sobre todo en el sector sanitario público y privado, que permita el desarrollo de estrategias nacionales de aplicación de tecnologías *big data*, donde se priorice la implantación de las mismas en aquellos casos de uso de interés general e incorpore un marco legal transparente y claro específico que tenga en consideración, entre otros, los principios asentados en relación con la ley sectorial propuesta en el presente trabajo.

Por otro lado, resulta fundamental para el crecimiento y desarrollo del país, sobre todo y ante todo en el sector de la sanidad, que en el futuro el sector público y privado invierta en recursos humanos especializados en TIC y en adaptar sus infraestructuras y servicios a las nuevas demandas tecnológicas y a los requisitos

[723] MARTÍNEZ MARTÍNEZ y ÁLVAREZ RIGAUDIAS, "El uso de datos con fines de investigación biomédica…", *op. cit.*, pp. 279-280.

necesarios en *big data*[724], así como a efectos de garantizar la sostenibilidad a medio plazo de la sanidad pública en países, que como el nuestro, donde va en creciente aumento los costes sanitarios debido al aumento del envejecimiento de la población.

En definitiva, el futuro de la sanidad se encuentra inevitablemente vinculado al análisis de grandes volúmenes de datos de salud procedentes de distintas fuentes. Así pues, por medio de la aplicación de técnicas *big data* se obtiene una información y conocimiento de gran valor que colabora en una potencial toma de decisiones en presencia del paciente, reducir dudas acerca del diagnóstico, predecir enfermedades, simplificar costes sanitarios, colaborar en la investigación biomédica, así como el acceso directo y automático a los datos del paciente por parte de cualquier facultativo médico independientemente del lugar donde se encuentre el centro de salud, además de todos los beneficios mencionados a lo largo del presente capítulo, siendo cada uno de ellos de interés común para la humanidad en su conjunto[725].

Por otro lado, como tendencia de futuro innovadora dimanante del *big data* es la globalización de los datos, donde el *big data* a través de las TIC y el IoT, facilita que se disponga de un mayor número de datos a través de sensores generando así mayor número de repositorios de datos, siendo estos la fuente principal de datos de las tecnologías *big data* a efectos de crear conocimiento e información.

---

[724]Como advierte GARCÍA BARBOSA, J., "La medicina del futuro pasa por *big data*", *cit.,* [Documento sin paginación], opina que: "en la actualidad se ha de superar algunos problemas como el de la barrera tecnológica, para el autor, la tecnología *Big Data* tiene que consolidarse todavía en el ámbito sanitario, por lo que cree necesario "que aumenten las inversiones públicas y privadas en este tipo de soluciones". No obstante, piensa que tal vez el factor más importante sea el humano, es decir, científicos de datos que sepan sacar provecho de la tecnología: "Es crucial contar con la presencia de analistas de datos expertos en el ámbito de la salud para que, a través del uso de tecnologías *Big Data*, puedan dar el soporte adecuado a los médicos en la toma de decisiones relativas a sus pacientes". *Vid.* GARCÍA BARBOSA, "La medicina del futuro pasa por *big data*", *op. cit.,* [Documento sin paginación].

[725] Al respecto, Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 29, señalan que: "La combinación de la genómica y el Big data apunta a que puede convertirse en una nueva revolución de la salud. (…) Estos cambios pueden ayudar a mejorar la toma de decisiones clínicas. Por ejemplo, mediante la aplicación de técnicas de Big data se puede predecir con un mayor nivel de certeza si un individuo es más propenso o no a desarrollar una patología en función de sus factores genéticos, permitiendo anticiparse al desarrollo de la misma. Por tanto, se tendería al nuevo paradigma de medicina preventiva, seleccionando, mediante la fármaco-genética, las medicaciones más eficaces para los pacientes. Por ejemplo, se calcula que, al ritmo actual, la cantidad de datos de genómica producidos diariamente se duplicará cada 7 meses. En 2025, esa cifra oscilará entre 2 y 40 exabytes por año, estima el equipo, en función de la tasa de duplicación y, en ese mismo año, se espera que 1.000 millones de personas tengan sus genomas completos secuenciados (Schatz, 2015)".

1.1. Análisis sobre el uso del *big data* por los organismos sanitarios

El informe ejecutivo de IBM sobre *Analítica de datos: El uso en el mundo real de big data en sanidad y ciencias de la vida,* suscrito por Peter Mooiweer y Rebecca Shockley ofrece un análisis exhaustivo sobre cómo las organizaciones más innovadoras en sanidad y ciencias de la salud extraen valor de datos inciertos, donde se indica en primer lugar, que el "*big data* plantea tanto retos como oportunidades para las compañías sanitarias y de ciencias de la vida", puesto que a pesar que en la actualidad las técnicas de *big data* en el sector sanitario están orientadas a resultados. No obstante, el futuro es incierto debido fundamentalmente a la incertidumbre dimanante de la normativa de protección de datos a nivel mundial, de los continuos cambios en la participación de los gobiernos, así como del propio adelanto de los "hábitos y demandadas" de los pacientes[726]. De igual modo, el citado informe advierte que las compañías sanitarias en la actualidad utilizan herramientas de *big data* de forma práctica[727] destacando a su vez, cinco conclusiones principales sobre cómo llevan a cabo las organizaciones proyectos de *big data*. En concreto, el informe concluye lo siguiente:

Por un lado, destaca que "el análisis de clientes (consumidores, pacientes, miembros) motiva las iniciativas *big data*"[728], es decir, según el informe *IMB* los principales motivos de las organizaciones sanitarias por los que aplican técnicas *big data* en sus proyectos se encuentran fundamentalmente orientados al cliente a efectos de disponer de un conocimiento más completo acerca de la salud de los pacientes, de los tratamientos, así como de sus necesidades financieras, todo ello con el objetivo de

[726] MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op.cit.,* p. 1.

[727]En este sentido, se precisa en MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.* ,pp. 2-3 que: "Aunque un porcentaje menor de compañías sanitarias y de ciencias de la vida está enfocado en entender estos conceptos (un 20% de éstas en comparación con el 24% de las organizaciones mundiales), la mayoría está o bien definiendo una hoja de ruta asociada a *Big Data* (un 50% de las compañías sanitarias y de ciencias de la vida, superando ligeramente al 47% del conjunto de empresas) o ya han emprendido pilotos e implementaciones de *Big Data* (un 30% frente al 28% de las grandes organizaciones)", indicando a su vez que: "Cuatro de cada cinco compañías sanitarias y de ciencias de la vida han comenzado a desarrollar una estrategia *Big Data* o están implantando actividades *Big Data*, dejando atrás a las empresas de otros sectores".

[728]MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.3, indica que: "casi la mitad de los proyectos *Big Data* emprendidos por compañías sanitarias y de ciencias de la vida están destinados a obtener resultados orientados al cliente y casi una cuarta parte está orientada a la gestión financiera y del riesgo".

ofrecer unos servicios más eficientes aprovechando las oportunidades del mercado al menor coste.

Por otro lado, el informe indica que "el *big data* requiere una infraestructura escalable y ampliable"[729], por medio de una base de información "integrada, escalable, ampliable y segura" a efectos de organizar el volumen, la variedad y la velocidad de los datos pues "los datos de una organización deben estar fácilmente disponibles y ser accesibles para las personas y los sistemas que los necesitan"[730]. Así pues, es sumamente importante una infraestructura de almacenamiento escalable y un almacén de alta capacidad a efectos de soportar un rápido crecimiento de los datos que de manera progresiva se registren en la organización, procurándose a su vez por medio de la aplicación de medidas idóneas garantizar la seguridad y la privacidad en la gestión de la información.

En tercer lugar, concluye que "los proyectos *big data* iniciales se concentran en obtener información de los almacenes de datos internos ya existentes"[731]. Por ende, los organismos sanitarios (públicos o privados) que aplican las nuevas tecnologías y cuentan con una infraestructura que le permite tener una gran capacidad de almacenamiento y gestión de sus datos internos ya existentes, podrán obtener a través del *big data* un conocimiento e información con mayor facilidad y eficiencia.

En cuarto lugar, se precisa que el "*big data* requiere sólidas capacidades analíticas"[732]. En concreto, MOOIWEER y SHOCKLEY afirman que debido a que el *big data* por sí mismo no aporta valor hasta que los datos no son analizados a efectos de solucionar retos relevantes de los proyectos de investigación biomédica y farmacéutica, se requiere la aplicación de sólidas herramientas de *software* por medio de analistas de

[729] MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.4.

[730] Según se indica en el estudio realizado por AA.VV., "Analytics: The widening divide: How companies are achieving competitive advantage through analytics", *IBM Institute for Business Value* and *MIT Sloan Management Review*, 2011 [Documento sin paginación]. Documento disponible en: http://www-935.ibm.com/ services/us/gbs/ thoughtleadership/ibv-analytics-widening-divide.html

[731] Así pues, señala MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.6, que: "Las compañías sanitarias y de ciencias de la salud concentran sus proyectos *Big Data* iniciales en transacciones, registro de datos y de audio, todos ellos fuentes internas de información clave".

[732] Se advierte en MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.7 que: "Las organizaciones sanitarias y de ciencias de la vida cuentan con una sólida base de capacidades analíticas, creadas para sustentar plataformas de *business intelligence* ".

TIC que tengan los conocimientos necesarios para utilizar las mismas incluidos en aquellos casos en los que se generen datos en tiempo casi real.

Finalmente, el mencionado informe indica que "la pauta actual de adopción de *big data* resalta las dudas de las compañías sanitarias y de ciencias de la vida, pero también afirma su interés"[733]. Por consiguiente, a efectos de adoptar el *big data*, las organizaciones destacan cuatro actividades fundamentales que ejecutan: (1) *Educar*, en el sentido, de crear conocimiento; (2) *Explorar*, es decir, desarrollar una estrategia y hoja de ruta en función de las necesidades y los retos de negocio; (3) *Implicar,* que conlleva aceptar *big data* por medio de iniciativas *big data* piloto para validar el valor y los requisitos y; (4) *Ejecutar*, esto es, implantar *big data* a gran escala con el despliegue de dos o más iniciativas *big data* y continuar el uso de análisis avanzados. En este sentido, MOOIWEER y SHOCKLEY, advierten que "para que los ejecutivos acepten la inversión en tiempo, dinero y recursos necesaria para generar valor empresarial a partir de *big data*, deben entender el valor de negocio potencial u obtenido"[734], aplicando el concepto "ejecutivo" de manera amplia, suponiendo en el sector sanitario de manera específica los organismos sanitarios (públicos o privados), facultativos sanitarios e investigadores que apliquen herramientas *big data* en la salud pública y en el desarrollo proyectos de investigación biomédica y farmacéutica de interés general.

Por último, como broche de cierre, examinaremos algunas de las empresas (organizaciones) más innovadoras de sanidad que aplican tecnologías *big data* en sus proyectos[735]: entre las más destacables, se encuentra la empresa Predyletics que analiza datos de pacientes a efectos de predecir futuros servicios de salud que mejoren la salud y a su vez reduzcan los costes de compañías de seguros y hospitales optimizando su rentabilidad. Por otro lado, la organización *(startup*) neoyorquina Flatiron Health cuenta con una excelente plataforma en la nube que analiza datos oncológicos en tiempo real, proporcionando estadísticas detalladas para hospitales y centros de investigación. A

[733] Igualmente, en MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.8 se indica que: "La mayoría de las compañías sanitarias y de ciencias de la vida están desarrollando estrategias o pilotos *Big Data*, pero casi una de cada diez ha comenzado a integrar esos análisis en sus procesos operativos".

[734] MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.9.

[735] En este sentido, ampliándose a los organismos públicos y privados referenciado en el capítulo dos del presente trabajo.

nivel nacional, se ha de mencionar la aplicación Conult@web promovida por la Consejería de Sanidad de la Comunidad de Madrid a efectos de facilitar el acceso a la información clínica sobre diferentes ámbitos sanitarios de los pacientes a los facultativos sanitarios, así como la identificación de patologías y analizar el debido cumplimiento del tratamiento por parte del paciente. Igualmente, citar la aplicación "Social Diabetes" que entre las de sus funciones principales se encuentra la de ajustar la dosis de insulina en tiempo real y cuantificar la cantidad de carbohidratos ingeridos y ejercicio físico realizado por el paciente.

1.2. Recursos y proyectos relevantes de *big data* aplicados en investigación biomédica y asistencia sanitaria

A continuación serán analizados algunos de los avances médicos más relevantes procedentes del *big data* sanitario llevados a cabo en la práctica de la medicina, a fin de confirmar lo que las nuevas corrientes sanitarias, jurídicas y tecnológicas vienen afirmando acerca del valor de los datos sanitarios, así como, la importancia de que los distintos actores de la esfera sanitaria puedan acceder a los mismos, siempre y cuando la circulación libre de los datos sanitarios se encuentre amparada, entre otros, por el principio de interés general.

A) Recursos *big data*

En junio de 2011, McKinsey Global Institute (MGI) publicó el informe *Big data: The Next Frontier for Innovation, Competition and Productivity*[736], donde destaca una serie de recursos de creación de valor del *big data* relacionados con el ámbito sanitario desde la esfera de la atención sanitaria y el comercio minorista en EE.UU., la administración del sector público en la Unión Europea y, desde la generación de datos

[736] McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition and Productivity,* Junio 2011. Dispone en:http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx (última consulta 22/03/19).

de geolocalización de personas y entidades. En suma, según establece el citado informe, el *big data* genera valor en el sector sanitario a través de las siguientes herramientas[737]:

En primer lugar, por medio de programas CER (*Comparative Effectiveness Research*) efectuando una investigación comparativa de los tratamientos aplicados a los pacientes, esto es, un análisis exhaustivo de los datos de salud de los pacientes con las mismas patologías en relación con los resultados de los tratamientos, así como de los costes de los mismos, se pueden identificar aquellos tratamientos más eficaces para los pacientes y a la vez que supongan menos costes.

En segundo lugar, a través de Sistemas de Soporte a las Decisiones Clínicas se consigue mejorar la calidad de las prescripciones por medio de las órdenes de tratamiento de los facultativos sanitarios registrados en estos sistemas. Así pues, tras análisis comparativo de las órdenes registradas, los sistemas alertan sobre errores relevantes o efectos adversos de los medicamentos, pudiéndose reducir las reacciones adversas y la tasa de error médicos, así como posibles negligencias médicas.

En tercer lugar, a través del Sistema de Creación de Transparencia de los Datos Médicos, donde a efectos de identificar y analizar las fuentes de variabilidad y de pérdidas en los procesos clínicos con el fin de optimizar los mismos, se analizan los datos operaciones y de rendimiento del proveedor a fin de crear mapas de procesos y cuadros de mando que permitan una transparencia informativa y mejoras en el rendimiento.

Por otro lado, por medio de Sistemas de Monitorización de Pacientes a Distancia, donde se recogen datos a tiempo real de pacientes con enfermedades crónicas como la diabetes, insuficiencia cardiaca congestiva e hipertensión, entre otras y, tras un análisis de los mismos se consigue controlar la evolución del paciente, vigilar el cumplimiento del tratamiento por parte del paciente, así como mejorar el tratamiento y la medicación de cara a un futuro. Asimismo, a través de la monitorización de pacientes a distancia se consigue reducir el ingreso del paciente en el hospital, disminuir el uso del servicio de urgencias, mejorar la focalización de la atención de enfermería a

[737] McKinsey Global Institute, *Big Data: The Next Frontier for Innovation, Competition and Productivity,* Junio 2011, pp.43-49.

domicilio, así como de las citas con el facultativo sanitario y, sobre todo, reducir un empeoramiento de la enfermedad que implique hospitalizar al paciente[738]. En este mismo sentido MOOIWEER y SHOCKLEY afirman que:

"La solución empelada por el hospital utiliza una nueva arquitectura de procesamiento de la información que permite tomar decisiones en tiempo casi real mediante el análisis continuo del flujo de datos gracias a sofisticados algoritmos específicos, por lo que constituye una plataforma flexible que puede adaptarse a una amplia variedad de necesidades de monitorización médica. Esto dota al personal clínico de la posibilidad sin precedentes de interpretar una gran cantidad de datos heterogéneos en tiempo real y detectar tendencias sutiles. El hospital complementa los conocimientos y la experiencia de los facultativos y el personal de enfermería con capacidades tecnológicas destinadas a ofrecer resultados más efectivos que los obtenidos con los dispositivos de monitorización por sí solos"[739].

Por último, otro recurso es el de la analítica avanzada aplicada a reconocer perfiles de pacientes que son propensos a desarrollar una determinada enfermedad a efectos de beneficiarse de un programa de atención preventiva.

De igual modo, el citado informe señala los siguientes recursos en los que las herramientas de *big data* aportan valor en el sector de la investigación científica y desarrollo en la industria farmacéutica:

Por un lado, a través del *modelo predictivo* se consigue reducir el tiempo de investigación en los ensayos clínicos agregando datos masivos a la investigación en las fases preclínicas y en fases iniciales del desarrollo de nuevos medicamentos, lo que permite crear modelos predictivos que anticipan conocer si el resultado final es eficaz y seguro, así como los posibles efectos secundarios del medicamento. Por otro lado, por medio de *herramientas y algoritmos estadísticos* se consigue mejorar el diseño de los

[738] Estos sistemas fundamentalmente usan tecnológicas que monitorizan el estado del corazón, remiten información sobre los niveles de glucosa en sangre, transmiten las instrucciones de los cuidadores, así como la tecnología chip-en-una-píldora que informa si el paciente está o no tomando la medicación.

[739] MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* p.5.

ensayos clínicos, donde a través de técnicas de minería de datos se seleccionan aquellos pacientes idóneos para el estudio del ensayo clínico, detectar los lugares donde existen un mayor número de casos, diseñar protocolos eficaces, seleccionar las indicaciones más eficaces del producto, diseñar el modelado comercial, analizar las posibilidades de aprobación regulatoria y, seleccionar al personal cualificado científico a fin de dirigir el proyecto, entre lo más destacado.

Tampoco debemos olvidarnos de otro recurso fundamental como es el del *análisis de los datos de ensayos clínicos*, donde tras la comercialización del producto en el mercado, se recogen en tiempo real los informes de reacciones adversas a fin de identificar nuevas indicaciones del fármaco o efectos adversos, lo que conlleva en consecuencia detección rápida y eficaz de aquellos casos excepcionales y minoritarios que no han sido descubiertos previamente en el ensayo clínico. Otra herramienta a destacar es el de la *medicina personalizada* por medio de *big data* donde a través del análisis de relaciones entre unas personas con una determinada genética y su respuesta ante determinados fármacos se desarrollan fármacos más eficaces, mejorando la atención sanitaria por medio de detección temprana de una enfermedad en determinados pacientes, de la búsqueda de terapias eficaces que se adapten a la enfermedad del paciente y de la adaptación de las dosificaciones del fármaco según sea el perfil molecular del paciente reduciendo efectos secundarios y mejorando la eficacia del fármaco. Por último, el informe cita el *análisis de patrones de enfermedades* por el que se identifican patrones y tendencias de enfermedades permitiendo una toma de decisiones estratégicas de inversión en I+D, moderar la demanda y los costes futuros, optimizando a su vez el desarrollo de actividades de I+D en las empresas farmacéuticas y ayudando a las mismas a la toma de decisiones sobre los recursos necesarios y eficientes.

Siguiendo el hilo conductor, otros de los usos a destacar del *big data*, procede del método *Real World Data* (RWD), que muestra la atención real dada a los pacientes en un contexto determinado, así como los resultados clínicos que en la práctica realmente se dan. Por ende, el RWD, permite identificar pacientes crónicos de riegos de descompensación, ayudar a la toma de decisiones clínicas en tiempo real y trasladar información directamente a los pacientes. Este método es comúnmente usado en la investigación clínica, farmacológica y epidemiológica, aportando grandes beneficios

para la humanidad. Un ejemplo de RWD, es la aplicación *Mini-Sentine* desarrollada por la Agencia de Medicamentos de los Estados Unidos, que permite detectar interacciones nuevas, efectos adversos de medicamentos y problemas de seguridad por los que se han retirado o modificado fármacos. Asimismo, por medio de los RWD se pueden comprobar en la práctica distintos tratamientos para una misma enfermedad en distintos pacientes, así como desarrollar indicadores sofisticados para comparar la atención dada a los pacientes por diferentes centros sanitarios y médicos, a fin de tomar medidas de mejora para una atención sanitaria de calidad.

B) Proyectos actuales que utilizan *big data* a efectos de mejorar la sanidad extrayendo valor de datos inciertos

A todo esto, debemos tener presente que el informe *Big data Healthcare Hype and Hope*[740], realiza un estudio exhaustivo de los proyectos reales que aplican tecnologías de *big data* extrayendo valor de los datos inciertos a efectos de mejorar la sanidad, así pues, el citado informe como indica PAINIAGUA[741] "explora con bastante precisión cómo *big data* se está convirtiendo en una creciente fuerza de cambio en el panorama sanitario". En concreto, en el informe se destacan diferentes modalidades de aplicación de las herramientas de *big data* en la atención sanitaria puestas en práctica en diversos proyectos reales:

De un lado, proyectos de investigación genómica y otras ramas de la investigación molecular[742]: Genoma Health Solutions, GNS Healthcare, DNAnexus, Appistry y NextBio, donde a través de aplicación de herramientas de *big data* se han identificado con gran rapidez y a menor coste perfiles genéticos o biomoleculares de personas propensas a padecer determinadas enfermedades a efectos de tratar a las mismas y tomar las medidas adecuadas de prevención por medio de la medicina personalizada, esto es, a través de nuevos medicamentos que eviten la enfermedad.

---

[740] FELDMAN, B., MARTIN, E.M. and SKOTNES, T., "*Big Data* Healthcare Hype and Hope*"*, 2012, [Documento sin paginación]. Documento disponible en: http://www.west-info.eu/files/big-data-in-healthcare.pdf (última consulta 25/03/19).

[741] PANIAGUA, S., "*Big Data* en sanidad para predecir, prevenir y personalizar", noviembre 2012, [Documento sin paginación]. Disponible en: http://www.sorayapaniagua.com/2012/11/12/big-data-en-sanidad-para-predecir-prevenir-y-personalizar/ (última consulta 27/03/19).

[742] *V.gr.,* proteótica, metabolónica, etc.

De otro lado, proyectos que transforman los datos en información y la información en datos por medio de la aplicación de tecnologías de *big data*, como Health Fidelity, que a través del procesamiento de lenguaje natural convierten el registro médico narrativo en datos a efectos que sean asimilados por una máquina o, como la tecnología Predixion Software, que efectúa análisis predictivo a fin de prevenir infecciones hospitalarias o enfermedades crónicas, así como identificar a aquellos pacientes con alto riesgo de ingreso. Otros de los proyectos que cita el informe, son los referentes al apoyo de autocuidado y colaboración de la ciudadanía, donde a través de aplicaciones móviles, como IBLueButton (de Humetrix) se permite el intercambio seguro y a gran velocidad información entre los pacientes y los facultativos sanitarios o, como la plataforma en la nube *Ginger.io* que recopila datos a tiempo real sobre el comportamiento de los pacientes a fin de ayudar a los facultativos sanitarios a tomar decisiones y ofrecer una asistencia sanitaria de calidad, sobre todo en las enfermedades crónicas. En general, por medio de aplicaciones móviles, el *big data* ofrece información a los pacientes sobre su estado de salud. Igualmente, el informe subraya aquellos proyectos que apoyan a las empresas sanitarias y a la mejora en la atención del paciente: OneHealth Solutions, Explorys o Humedica. En estos proyectos se aplican las técnicas *big data* en la gestión sanitaria a fin de mejorar la atención al paciente y reducir costes a través de la inteligencia de negocio en la gestión sanitaria, donde se calcula el rendimiento y se abordan nuevas formas de reembolso de los servicios sanitarios.

Evidentemente, como era de esperar, el informe también menciona aquellos proyectos que aumentan el conocimiento y resuelven problemas sanitarios por medio de la aplicación de tecnologías de *big data*. En concreto menciona: (1) Sproxil, que a través del big data identifica aquellos medicamentos falsificados a efectos de prevenir el fraude en la industria farmacéutica; (2) Asthmapolis, que es una aplicación móvil para los enfermos de asma que proporciona retroalimentación a efectos de controlar la enfermedad y que recoge datos de los posibles factores ambientales que afectan al asma, así como sus síntomas a través de inhaladores para el asma con sensores que controlan la hora y lugar de toma de la dosis y; (3) Sickweather LLC que por medio de las redes sociales (Facebook, Twitter) localiza brotes de enfermedades y ofrece previsiones a los usuarios. De igual modo, el informe hace referencia a los proyectos que agregan datos para construir un ecosistema mejor procedente de fuentes externas, donde a través del *big data* se efectúan nuevas tipologías de análisis y se responden a las preguntas de los

investigadores. Particularmente, el informe menciona el proyecto *Qualcomm Like* y el sistema *Watson* de IBM.

Igualmente, se ha de subrayar que a efectos de cultivar la adopción de *big data* en las organizaciones de salud, el informe ejecutivo de IBM sobre *Analítica de datos: El uso en el mundo real de big data en sanidad y ciencias de la vida*, establece algunas pautas a modo de recomendación, tales como: destinar los proyectos iniciales a obtener resultados orientados al cliente, definir una estrategia *big data* con un plan orientado al negocio, comenzar con datos existentes para obtener resultados a corto plazo, crear capacidades de análisis en función de las prioridades de negocio y crear un caso de negocio basado en resultados medibles[743].

En conclusión, como se ha podido apreciar tecnológicamente las herramientas *big data* significan una revolución en el ámbito de la salud como en la investigación científica, que "con la legislación adecuada, un alto grado de digitalización y un potente ecosistema de investigación en salud son elementos indispensables para abordar una investigación moderna de calidad"[744], especialmente en la medicina personalizada, predictiva, preventiva y participativa, pues permiten acceder a conocimiento e información procedentes de datos de salud no estructurados registrados tanto en fuentes propias el ámbito sanitario[745] como de la población y del ecosistema en general[746] por medio de un análisis sistemático automatizado de los mismos.

---

[743] *Vid.* MOOIWEER y SHOCKLEY, "Analítica de datos: El uso en el…", *op. cit.,* pp.9-11, advirtiendo al respecto MOOIWEER y SHOCKLEY que: "Tras cada una de estas recomendaciones se oculta un principio importante: los profesionales del negocio y de TI deben trabajar juntos durante todo el viaje hacia *Big Data*. Las soluciones *Big Data* más eficaces identifican en primer lugar los requisitos de negocio y luego adaptan la infraestructura, fuentes de datos, procesos y habilidades necesarios para sustentar esa oportunidad de negocio". Asimismo, el informe "El gran cuaderno de *Big Data*. Una guía práctica para emprender su primer proyecto de *Big Data*", de *Informatica.* Documento disponible en: https://docplayer.es/19123678-El-gran-cuaderno-del-big-data-una-guia-practica-para-emprender-su-primer-proyecto-de-big-data.html señala tres consejos fundamentales para conseguir que un proyecto de *Big Data* funciones: (1) Marcar objetivos claros y contener las expectativas; (2)Definir las métricas que demuestran el valor del proyecto; (3)Adoptar una estrategia en cuanto a las herramientas y la codificación manual. Igualmente, señala los siguientes motivos por los que fracasan algunos proyectos de *Big Data*: 1. Objetivos difusos; 2. Expectativas equivocadas; 3. Aumento de costes y retrasos del proyecto; 4. Incapacidad de escalar.

[744] Como sostienen MARTÍNEZ MARTÍNEZ y ÁLAVAREZ RIGUADAS, *op. cit.,* p. 279.

[745] Por ejemplo, el genoma del paciente.

[746] *V.gr.,* datos poblacionales, climáticos, sociodemográficos, etc.

1.3. Oportunidades del *big data* en la sanidad española

En España, el Instituto de Ingeniería del Conocimiento (IIC), ha desarrollado distintos proyectos sanitarios mediante la aplicación de técnicas *big data*[747]. El IIC, como es sabido, es un organismo privado de I+D+i que centra su actividad en la extracción de conocimiento a partir de la aplicación de las técnicas de *big data* a fin de optimizar procesos empresariales del sector de la banca, la salud, los medios sociales, la energía y la gestión del talento en Recursos Humanos. En este sentido, en el sector sanitario, el IIC ha centrado su atención en el desarrollado de proyectos predictivos que ayudan a anticipar necesidades sanitarias, colaborando con la toma de decisiones de los profesionales de la salud y, ofreciendo a los pacientes una atención médica eficaz. Todo ello a través de la aplicación de herramientas de *big data* en fuentes de datos heterogéneas como las historias clínicas, dispositivos de Telemedicina, pruebas clínicas, e incluso *wereables*, así como de datos procedentes de fuentes relacionadas con el *Real World Data* y con la medicina personalizada generadora de datos epidemiológicos, los nutricionales y los genómicos.

En consecuencia, se puede observar como el IIC tras la aplicación de técnicas propias del análisis de la información procedente de datos sanitarios, ha conseguido optimizar la gestión clínica asentando las pautas predictivas de utilización de los recursos sanitarios de forma más eficiente, así como el tratamiento y la atención al paciente por medio de una medicina personalizada. Este planteamiento resulta especialmente relevante por lo que se refiere a los avances médicos alcanzados por medio de la aplicación de las técnicas *big data*, dado que el IIC ha desarrollado en la práctica diversos servicios que han significado relevantes avances en medicina.

A) Análisis de algunos avances médicos relevantes a través de las técnicas *big data*

Por un lado, nos encontramos con el *Proyecto optimización de los servicios públicos sociales y sociosanitarios de teleasistencia* desarrollado a efectos de atender

[747] Consultado en web: http://www.iic.uam.es/soluciones/salud/ (27/04/20)

y/o prevenir las consecuencias de determinadas desigualdades sociales facilitando la integración social, optimizando a su vez la atención a la dependencia prediciendo una posible evolución y anticipándose a las necesidades de los pacientes dependientes a fin de atender ser atendidos eficazmente y mejorando a la calidad del servicio.

Así pues, por medio del desarrollo de modelos predictivos que predicen patrones de comportamiento y la aplicación de métodos algorítmicos propios de análisis de la información (*big data*), el IIC consigue optimizar la atención de los pacientes de dependencia a través del conocimiento real y la valiosa información extraída del análisis de los datos almacenados en sistemas de información muy heterogéneos como la atención primaria, atención especializada, farmacia, dispositivos terminales y periféricos, comentarios recogidos por los especialistas, variables sociales del patrón u otra procedencia, entre otros. Por tanto, una vez que son detectadas una serie de variables relevantes los pacientes en situación de dependencia son clasificados, siendo así optimizada la atención prestada. De igual modo, de los resultados obtenidos de los análisis se extraen reglas para emitir alertas y recomendaciones. El IIC ha colaborado a la mejorar de los servicios de las empresas de teleasistencia por medio del desarrollado de modelos predictivos de patrones de comportamiento en función de las características comunes y del análisis de datos procedentes de las causas de urgencia sanitaria, de atención permanente y de un seguimiento personalizado, así como de recordatorios de citas, toma de medicamentos o del soporte técnico.

Por otro lado, el IIC con el objetivo de proporcionar datos de gran utilidad práctica a los profesionales sanitarios destinados al establecimiento de protocolos, al diagnóstico temprano de enfermedades, al pronóstico de la evolución de enfermedades y a la planificación del tratamiento de los pacientes, ha desarrollado sistemas de alertas inteligentes. En concreto, el IIC ha desarrollado los siguientes sistemas de alertas:

En primer lugar, *Alzheimer´s Disease Medical Images Research Environment* (ADMIRE), que consiste en un sistema informático de alertas creado para dar soporte a los investigadores en sanidad, diagnóstico precoz, pronóstico y planificación del tratamiento de la Enfermedad de Alzheimer (EA). Este sistema desarrollado por expertos del IIC, de la Fundación Centro de Investigación de Enfermedades Neurológicas, de la Fundación Reina Sofía, de la Fundación Desarrollo de Imágenes

Médicas avanzadas y de la Universidad Rey Juan Carlos, permite evaluar el riesgo individual de padecer la enfermedad del Alzheimer, con un nivel de acierto superior al 90%. Así pues, por medio de datos numéricos anonimizados procedentes de imágenes de resonancia magnética, el sistema determina la fase de la enfermedad de Alzheimer en la que se encuentra el paciente, sugiriendo a su vez un diagnóstico individual acerca de la enfermedad y ofreciendo predicciones sobre la eficacia y uso de las distintas técnicas de resonancia magnética. Por medio de técnicas de analítica descriptiva y analítica predictiva de DIGNA, el sistema ADMIRE visualiza aquella información relevante procedente de las imágenes de resonancia magnética. Asimismo, también hace uso de técnicas de visualización, como las *Social Network Analysis* (SNA), a fin de proporcionar recomendaciones y alertas a los especialistas médicos. Asimismo, entre sus funcionalidades y beneficios, se ha de destacar las siguientes:

(1) Proporcionar al especialista avisos en los casos que el diagnóstico generado por el sistema no coincida con el indicado por el especialista.

(2) Generar informes que relacionan variables y su influencia en cada fenotipo y sus combinaciones.

(3) Permitir visualizar información acerca de aquellas variables importantes de los pacientes en cada fase de la enfermedad y efectuar análisis comparativos.

De igual modo, ADMIRE es un sistema que puede ser utilizado por todo tipo de profesionales y entidades destinadas al estudio y tratamiento de enfermedades neurodegenerativas y, a la promoción de la investigación multicéntrica y traslacional en demencias.

En segundo lugar, *Degenerative Neural Intelligent Alerts* (DIGNA), consiste en un sistema de alertas inteligentes que permite la creación de instancias para distintas patologías médicas, proporcionando apoyo a los profesionales sanitarios a la hora de establecer protocolos, diagnosticar enfermedades tempranas, pronosticar la evolución de una enfermedad concreta y planificar el tratamiento del paciente. En este sentido, su conocimiento (*know-how*) principalmente se basa en aplicar técnicas de analítica descriptiva a efectos de determinar posibles pronósticos a modo de recomendaciones y

establecer un sistema de alertas tempranas. Así pues, DIGNA recoge, procesa y visualiza información médica relevante procedente de diversas fuentes de datos, incorporando técnicas de visualización avanzada ayudando al facultativo médico a interpretar los resultados. En resumen, podemos destacar los siguientes beneficios del sistema de alertas DIGNA:

(1) Anonimización y seguridad. La información de los pacientes es anónima, accediéndose a la misma a través de la web de manera segura.

(2) Información clasificada. Los datos de los pacientes se encuentran clasificados mediante distintos filtros lo que garantiza una fácil localización.

(3) Previsión del diagnóstico. A través de la información médica del paciente es capaz de sugerir un posible y acertado diagnóstico de este.

(4) Avisos y actualización. Revisión de la información del paciente por medio de avisos y alertas proporcionados al especialista, actualizándose de manera automática el conocimiento cada vez que son cargados nuevos datos.

(5) Resumen gráfico. Por medio de un gráfico resume de manera detallada la información más relevante para un posterior diagnóstico o investigación sobre la enfermedad.

Lo más relevante es que en la práctica el sistema de alertas DIGNA se ha desarrollado como una herramienta automática, dotada de grandes capacidades de autoaprendizaje, así pues, en el estudio desarrollado por el Grupo de Demencia de la Comunidad de Madrid, donde fueron analizados cuatro grupos de pacientes (pacientes cognitivamente santos, con deterioro cognitivo leve tipo amnésico y tipo multidominio y, enfermos de Alzheimer), DIGNA proporcionó la siguiente información y conocimiento relevante:

- Evaluación del riesgo de cada paciente de pertenecer en un futuro a un grupo u otro.

- Selección automáticamente las 10 variables más importantes de las 238 variables involucradas en el estudio.

- Determinación – según el fenotipo del paciente – de las técnicas de resonancia más eficientes a fin de detectar diferencias relevantes entre los grupos de pacientes. Lo que permitió reducir el tiempo invertido en la realización de resonancia magnética.

Este instrumento puede ser empleado tanto por entidades públicas como privadas del sector sanitario, como pueden ser entre otras, los servicios sanitarios regionales, las farmacéuticas, los hospitales, los grupos de investigación biomédica, las unidades centradas en patologías específicas y las fundaciones de pro-salud. En tercer lugar, el IIC también ha desarrollado el Servicio de Segmentación de Pacientes Crónicos, donde a través del análisis de datos sanitarios se detectan variables a fin de clasificar los pacientes crónicos. Tal sistema por medio de la estratificación y segmentación de la población en niveles de riesgo y de modelos predictivos de pacientes de mayor riesgo, predice una posible evolución de los pacientes, así como un tratamiento de calidad, utilización de servicios y costes, puesto que la mayoría de los pacientes crónicos acuden con frecuencia de manera innecesaria a los costosos servicios de Atención Especializada cuando realmente únicamente requieren de un seguimiento rutinario desde Atención Primaria.

Así pues, puede mantenerse que el servicio de segmentación de pacientes crónicos es una herramienta con fines preventivos, puesto que a través del conocimiento obtenido de los datos procedentes de perfiles médicos se adelantan y predicen las necesidades de los pacientes y de los centros médicos, optimizando los recursos sanitarios. De tal modo, que si la población es segmentada por medio de patologías crónicas determinándose a su vez los distintos niveles de pacientes crónicos, se pueden obtener guías preventivas de actuación sobre aquel grupo de pacientes que presente mayor riesgo, consiguiéndose a su vez optimizar la calidad de vida y disminuir los reingresos en urgencias evitándose aquellos innecesarios que podrían controlarse por medio de revisiones periódicas en aquellos pacientes con una alta probabilidad de reingreso, lo que también conllevaría una notoria aminoración de los gastos sanitarios.

Por último, siguiendo con los sistemas desarrollados por el IIC por medio de la aplicación de las técnicas *big data*, se encuentra la herramienta de Análisis De Hiperfrecuentación en Atención Primaria, donde es fundamental el acceso a los datos clínicos del paciente a fin de diseñar estrategias proactivas y gestionar de manera óptima los recursos. En este caso nos encontramos ante una tipología de paciente concreta, que es aquel que acude a consulta doce o más veces al año, definido por la Sociedad Española de Médicos de Atención Primaria como "hiperfrecuentador".

El problema radica en que no todos aquellos pacientes que acuden doce veces o más a consultas de atención primaria son realmente hiperfrecuentadores, por ello, el IIC ha desarrollado un sistema que por medio de patrones de comportamiento de pacientes y de información retrospectiva sobre los mismos recogida en las bases de datos, permite determinar aquellos perfiles reales de pacientes hiperfrecuentadores, todo ello con el objetivo de diseñar estrategias proactivas que disminuyan el coste por paciente, puesto que según los análisis de la Sociedad Española de Médicos de Atención Primaria (SEMERGEN), en España los pacientes hiperfrecuentadores gastan de media, entre ocho y diez veces más recursos sanitarios que el resto de la población. Además, de suponer una mejora en la gestión de los centros de atención primaria y la atención recibida por los pacientes, sin que los servicios pierdan calidad y sin aumentar la carga de trabajo de los profesionales sanitarios. De este modo, una vez detectados los pacientes hiperfrecuentadores reales según su tipología y sintomatología, así como localizados los centros con mayor casos de pacientes de este tipo por medio de la técnica de análisis de hiperfrecuentación en atención primaria, dispondremos de información y conocimiento de gran valor que va a permitir una gestión eficaz del tratamiento, una mejora de la calidad del servicio, ampliar políticas de acción específicas y reducir notablemente el gasto sanitario.

B) Casos de éxito reales de la aplicación de herramientas *big data*

La medicina predictiva consigue dar a cada paciente lo que necesita, siendo así más efectivo, adelantándose a las necesidades evitándose enfermedades y daños multiorgánicos. Asimismo, con los ensayos clínicos ya no será necesario reclutar al

paciente o revisar manualmente las historias clínicas, puesto que a través de los mismos se hace un seguimiento automático del paciente.

Otras de las aportaciones importantes es la efectividad de medicamentos y seguimiento de efectos adversos, así como la evaluación de servicios sanitarios, una mayor vigilancia epidemiológica, una predicción más detallada acerca de hospitalizaciones por patologías en base de factores ambientales, poblaciones, así como una identificación de pacientes de alto riesgo, los médicos a través de la información adquirida con la aplicación de herramientas *big data* pueden tomar decisiones en la consulta. Igualmente, otras de las aportaciones importantes del *big data sanitario* es el análisis de estado de salud de una población o territorio, así como el seguimiento de tendencias. Es indudable que actualmente varios son los casos de éxito reales obtenidos a través de la práctica de técnicas *big data* en el sector sanitario. En concreto se han de destacar los siguientes:

a) Detección precoz de la sepsis

En España, más de 50.000 personas cada año sufren de la sepsis, lo que supone 104 casos por cada 100.000 habitantes, falleciendo 17.000 personas. A nivel europeo la cifra de personas afectadas por la citada enfermedad es de 3,4 millones de casos por año, falleciendo 700.000 personas. Por consiguiente, nos encontramos ante una enfermedad con un índice de mortalidad mayor que la de enfermedades como la de insuficiencia cardiaca, cáncer de mama, cáncer de colon y el VIH, produciéndose incluso trece veces más muertes que en los accidentes de tráfico. Por ende, con la aplicación de técnicas *big data*, la Unidad Multidisciplinar de Sepsis del Hospital Son Llàtzer de Palma de Mallorca, por medio de la cooperación de diferentes especialistas, internistas, médicos de urgencias, cirujanos, neumólogos, microbiólogos y farmacólogos, así con la cooperación del ICC, ha conseguido detectar la sepsis en fase temprana permitiéndole al médico actuar de manera inmediata y, llevar a cabo una personalización del proceso de manera individual para cada paciente.

En el caso de la sepsis, según los profesionales en medicina, es sumamente importante su detección precoz, puesto que nos encontramos ante una enfermedad hiperaguda, donde los primeros momentos de un paciente son de crucial importancia, ya que nos encontramos ante procesos tiempo-dependientes, donde el riesgo de mortalidad aumenta notablemente cuanto más se retrase el tratamiento, hasta el extremo, de que si se retrasa un tratamiento antibiótico en un paciente grave la mortalidad aumenta un 7% primero y, un 17% a la segunda hora. Todo ello debido a que la sepsis se da cuando una persona sufre una infección causada por bacterias, virus, hongos o parásitos, su cura depende de la brevedad en la que se actúe con un antibiótico que mate las bacterias en 24, 48 o 72 horas, permaneciendo la alteración de los órganos debido a que las células que están para proteger al organismo son las mismas que lo atacan, de tal modo, que el propio organismo se ataca defendiéndose de esa infección.

En suma, la detección temprana de la sepsis es crucial en el proceso de curación, puesto que un diagnóstico y tratamiento precoz supone disminuir el riesgo de mortalidad y de las secuelas. De lo contrario, si la detección de la sepsis se retrasa, aumenta de manera notoria el riesgo de mortalidad, disminuyendo la supervivencia un 7,6 % para cada hora de retraso en la administración de antibióticos. Igualmente, se ha de tener presente, que la detección temprana de la enfermedad supone una reducción de los recursos médicos, de la estancia hospitalaria y del uso de fármacos. A través de la aplicación de técnicas de *big data* en el sector sanitario, el hospital tiene como objetivo reducir un 14% la tasa de los falsos positivos y adaptar el sistema a las características de los enfermos sépticos.

b) Predicción de la evolución de esclerosis múltiple

La enfermedad de esclerosis múltiple es una enfermedad relevante que afecta aproximadamente a 47.000 pacientes en España y, 2.3 millones en el mundo, siendo la primera causa de invalidez neurológica en el adulto joven entre la edad de 20 y 40 años. Con el paso de tiempo la discapacidad va progresando y la calidad de vida se va degenerando, puesto que a los 10 años de padecer la enfermedad la mayoría de los enfermos dejan de trabajar.

Por medio de la aplicación del *big data* en el sector sanitario y la Inteligencia Artificial, son aplicados datos médicos que ayudan a los profesionales de Neurología para tratar la enfermedad a través del proyecto *Model MS* desarrollado por el Dr. Rafael Arroyo González, Jefe de Neurología del Hospital Quirónsalud Madrid y del Hospital Ruber Juan Bravo y por el Dr. Guillermo Izquierdo, Ex-presidente de la Sociedad Andaluza de Neurología y Coordinador de la Unidad de Esclerosis Múltiple del Hospital Vithas NISA en Sevilla. Se trata de un modelo matemático que predice la evolución de la enfermedad de los pacientes que la padecen, en base a datos en relación al mismo como: datos demográficos, datos en relación al progreso de la enfermedad (existencia o no de brotes), datos sobre el grado discapacidad del paciente, la resonancia magnética, si el paciente ha tenido o no tratamiento previo, se puede predecir la evolución de la enfermedad en el paciente o cómo ha de ser el tratamiento específico eficaz que debe seguir el paciente para su mejora y progreso. Así pues, a través de la base de datos que cuenta con 40.000 pacientes del proyecto *Model MS*, en aplicación de técnicas de *big data* e Inteligencia Artificial, se han descubierto algunas variables que no se tienen en cuenta habitualmente, se ha confirmado la relevancia de los últimos medicamentos del mercado, así como el hecho de que tratar a un paciente es siempre mejor que esperar a que evolucione, permitiendo, en suma, realizar un pronóstico adaptado a las características de los pacientes, resultando ser un ejemplo de medicina personalidad y de medicina predictiva, puesto que colabora a predecir cómo será la evolución de la enfermedad, el tratamiento idóneo para el paciente y los fármacos más eficaces[748].

c) Teleasistencia

Por medio de un análisis estructurado y automático de los datos procedentes de los servicios sociosanitarios a través de la aplicación de técnicas *big data*, es extraída una gran cantidad de información de gran valor que mejora tanto los distintos programas sociales como la gestión y eficacia del servicio. A todo ello habría que añadir el impacto y la importancia de las redes sociales, puesto que facilitan la interpretación

[748] *Vid.* Enlace web del *Instituto de Ingeniería del Conocimiento*: http://www.iic.uam.es/lasalud/big-data-ia-predecir-evolucion-esclerosis-multiple/ así como, video en YOUTUBE el siguiente enlace: https://www.youtube.com/watch?v=IuTjoZmg4PM

de las relaciones existentes, como pueden ser resultados de pruebas con la edad, sexo y estado civil, entre otros, del paciente. El método que seguir es el siguiente:

(1) Análisis de la información procedente de datos depositados en los servicios sanitarios.

(2) Estructuración de la información en distintos segmentos, grupos o tipología, añadiéndose a su vez grupos de riesgo.

Así pues, el beneficio resulta evidente, puesto que una mayor optimización de los servicios sociosanitarios de Teleasistencia equivale a una segmentación y clasificación de los pacientes que se encuentren en situación de dependencia, así como a predecir una evolución en el tratamiento, precipitarse a las necesidades del paciente mediante una atención y cuidado de mejor calidad a un menor coste.

d) Alertas de alergias

El presente caso de éxito ha sido llevado a cabo en el Servicio Madrileño de Salud (SERMAS), donde tras la aplicación de *big data*, se consigue obtener información y conocimiento de gran valor de los datos no estructurados sobre alergias registrados en la aplicación AP-MADRID del SERMAS. De igual modo, ha sido creado un repositorio central que permite el intercambio de información entre profesionales y centros médicos, encontrándose el mismo estructurado y normalizado en un sistema de alertas de alergias asociado a códigos SNOMED-CT, que permiten la identificación única e inequívoca tanto del contenido como del significado de los documentos clínicos.

En este sentido, el repositorio central permite a los profesionales intercambiar información, así como tener un acceso y conocimiento directo del significado de la misma, asegurándose una correcta interpretación. Además, es de crucial importancia para el paciente que un facultativo médico – independientemente del centro sanitario en el que sea atendido - pueda tener conocimiento de su estado alérgico, gracias a la estandarización accesible y univoca entre instituciones.

e) Detección de tendencias

Del mismo modo, es obvio que son destacables también y de gran relevancia en la esfera sanitaria las opiniones de los usuarios manifestadas de manera abierta y directa en las redes sociales. En este sentido, el Hospital Clínico San Carlos junto con el IIC, ha llevado a cabo con éxito en la práctica un proyecto consistente en un modelo lingüístico computacional desarrollado por algoritmos ad hoc cuya finalidad es la de escuchar las opiniones de los usuarios sobre sanidad en las redes sociales a efectos de detectar tendencias, grupos de conversación y posibles *influencers*. De este modo, se ha conseguido obtener información relevante de gran utilidad para atacar algunas enfermedades y preocupaciones de los ciudadanos, predecir las necesidades de la población, mejorar la asistencia médica, difundir información sobre salud pública y desarrollar programas preventivos eficaces y de calidad.

2. LA MEDICINA DE PRECISIÓN A TRAVÉS LAS TECNOLOGÍAS *BIG DATA* E INTELIGENCIA ARTIFICIAL

La Medicina de Precisión, también denominada Medicina Personalizada, junto con la Medicina Basada en la Evidencia, previamente estudiada en el capítulo dos del presente trabajo, es una de grandes oportunidades y aportaciones del *big data* en el sector sanitario. Así pues, a través de la aplicación de las técnicas de *big data* los facultativos sanitarios pueden tomar decisiones terapéuticas de forma personalizada, es decir, en función de las características propias de la enfermedad de cada paciente. En este sentido, por medio de la Medicina de Precisión se consigue que un porcentaje de pacientes con diferentes patologías reciban tratamientos personalizados específicos que se adapten a la enfermedad, cuyo resultado en consecuencia será más eficaz y a la vez, generando menor toxicidad que los tratamientos convencionales.

De igual modo, la Medicina de Precisión permite que los pacientes se beneficien de la inclusión de ensayos clínicos a efectos de evaluar la eficacia de los tratamientos, así como a la obtención de un mejor conocimiento acerca de la naturaleza de la enfermedad, información y conocimiento que posteriormente será compartido con otros investigadores y profesionales sanitarios especializados en la materia, generándose así

un conocimiento acerca de la enfermad concreta que ayuda al desarrollo de la ciencia y de la medicina[749]. En síntesis, la Medicina de Precisión impulsa la investigación clínica al concretar el porcentaje de pacientes con una determinada alteración que podrían beneficiarse de un tratamiento concreto, fermentándose a la vez el desarrollo de nuevos fármacos. No obstante, actualmente, la Medicina de Precisión continúa siendo un reto, como afirma la Sociedad Española de Oncología Clínica:

"[…] un reto necesario si queremos estar a la vanguardia de la investigación, que requiere de planes estratégicos nacionales que fomenten su implementación para evitar inequidades diagnósticas y terapéuticas en el territorio Nacional. Además, la implementación de esta estrategia debe venir acompañada de proyectos de investigación, indicadores de calidad, historias clínicas electrónicas que integren los datos de los pacientes y que permitan compartir la información generada, todo ello bajo un marco regulatorio que asegure el tratamiento de los datos y la confidencialidad de la información. Todo ello va a fomentar el conocimiento necesario que permitirá una mejor atención al paciente con cáncer"[750].

---

[749] En este sentido, MCCRAE. I., "Medicina de precisión", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, p.47, aclara que: "A la hora de decidir un tratamiento, el éxito a menudo tiene que ver con los estilos de vida y las circunstancias sociales y personales, como las motivaciones de un paciente y sus objetivos en la vida. La medicina de precisión no trata sólo de determinar que medicamentos son los más adecuados para tratar mejor las enfermedades de los pacientes sino también todo aquello que los pacientes deben hacer para mejorar su estado de salud a través de planes asistenciales individualizados que se adapten a su estilo de vida y las circunstancias sociales. Con el fin de ofrecer la asistencia sanitaria más eficaz, incluida la intervención temprana y la atención preventiva, es fundamental poder capturar y analizar todos los datos relevantes en la salud de las personas, incluyendo los determinantes sociales, económicos, familiares o medioambientales. Por ejemplo, los factores que pueden tener un impacto importante en los resultados en salud son: situación familiar o si viven solos, zona de residencia y accesibilidad a centros sanitarios, acceso a medios de comunicación social, etc. Tener acceso a este tipo de información puede condicionar las intervenciones que afectan a la calidad en la atención. Por ejemplo, diversos estudios han demostrado que los pacientes que viven solos tienen una probabilidad mucho mayor de reingreso hospitalario que los que conviven en familia. Si se identifican los pacientes que viven solos en el momento del alta hospitalaria, se pueden prevenir reingresos innecesarios mediante la adopción de medidas tales como las llamadas de seguimiento, monitorización a domicilio, visitas de trabajadores sociales o enfermeras gestoras de casos. Un ejemplo reciente aparecido en las noticias relacionado con factores sociales vinculados a la salud es un estudio que identificó que las personas jóvenes que utilizan más las redes sociales son más propensas a la depresión. La recopilación de datos como el uso de redes sociales para identificar a los pacientes en situación de riesgo es otro ejemplo de cómo este tipo de análisis puede aprovecharse para decidir las intervenciones y mejorar la asistencia sanitaria. Aun cuando los profesionales clínicos abordan preguntas acerca de las circunstancias sociales de un paciente y las reflejan en la historia clínica, no siempre se hace de forma estructurada y completa, lo que dificulta su aplicación a la hora de la toma de decisiones. Tradicionalmente, esta información importante no está recogida en los modelos de datos que dan soporte a la Historia Clínica Electrónica".

[750] Al respecto *visítese* el siguiente enlace web: https://seom.org/informacion-sobre-el-cancer/ique-es-la-medicina-de-precision

Por ende, es necesario que en el futuro a fin de mejorar y avanzar hacia una Medicina de Personalizada de calidad, se apliquen las tecnológicas de *big data* y la IA en los proyectos de investigación biomédica, puesto que es el método más viable – por no decir el único – para mejorar la toma de decisiones en la asistencia sanitaria y, crear medicamentos que garanticen un tratamiento eficaz y eficiente del paciente, siendo un instrumento esencial para ayudar a los profesionales sanitarios a mejorar los diagnósticos y tratamientos.

Al respecto el informe sobre *Diez temas candentes de la Sanidad Española* para 2013 elaborado por PWC, establece los siguientes elementos esenciales para el desarrollo de la Medicina Personalizada: "(1) implantación de formación reglada o programas de formación específicos para especialistas en genómica y proteómica; (2) comunicación y colaboración entre el sector sanitario, farmacéutico, biotecnológico y el mundo académico; (3) desarrollo de tecnología que permita el acceso a datos genómicos y proteómicos para investigación; (4) involucración de los gestores sanitarios; (5) sustitución de otras técnicas y uso compartido de recursos; (5) realización de estudios coste-eficacia rigurosos; (6) definición de criterios clínicos para la solicitud de pruebas; (7) regulación de la introducción de datos genómicos/proteómicos en la historia clínica electrónica y; (8) resolución de aspectos éticos y legales. En España, aunque hay iniciativas aisladas de interés, falta un plan nacional de impulso a la Medicina Personalizada"[751].

En concreto, la herramienta *big data* que hasta hace poco se aplicaba para conseguir las mejoras de la Medicina Personalizada era el *Machine Learning*[752]*,* sin embargo, en la actualidad los avances en computación han evolucionado hacía el aprendizaje profundo, conocido como el *Deep Learning*, dejando atrás la tecnología *Machine Learning*, herramienta que por ser esencial para el desarrollo de la Medicina Basada en la Evidencia continúa empleándose (aunque con menos frecuencia), ya que *Deep Learning* requiere de una gran capacidad de proceso. A través del *Deep Learning*

[751] PRICEWATERHOUSECOOPERS, *Diez temas candentes de la Sanidad Española*, 2013, p.13. Documento disponible en: https://www.pwc.es/es/publicaciones/sector-publico/assets/diez-temas-candentes-sanidad-2013.pdf (última consulta 02/04/20).

[752] POULLET, Y., *Le RGPD face aux défis de l´intelligence artificielle,* Larcier, Bruxelles, 2020, pp. 17-33.

se están produciendo grandes avances en Inteligencia Artificial (IA)[753], debido a que esta nueva herramienta utiliza modelos especiales de redes neuronales a efectos de identificar las múltiples unidades de información y su translación a aprendizaje y conocimiento, a pesar de que como se me ha mencionado anteriormente, esta nueva e innovadora tecnología necesita de una capacidad de proceso muy grande, cada vez más los desarrollos en *hardware* permiten alcanzar resultados visibles. Como indica CERROLAZA "La IA se aplica para entender mejor el desarrollo del cerebro, mejorar el diagnostico de pacientes con demencia, que hayan sufrido un ictus o daños cerebrales, o bien realizar diagnósticos en personas con enfermedades cardiovasculares"[754]. En consecuencia, desde una perspectiva de futuro, se prevé que la capacidad de proceso se pueda aumentar cada vez más hacía una computación cuántica, lo que significa que nos encontraremos ante un nuevo paradigma, esto es, ante ordenadores con capacidades de proceso mucho más superiores a las de hoy día.

Por consiguiente, si en el futuro tenemos ordenadores con capacidades de proceso mucho más grandes a las actuales, en los que podemos combinar algoritmos de tipo redes neuronales específicas de *Deep Learning*, obtendremos numerosas oportunidades acerca de la capacidad de las máquinas a fin de procesar información y extraer conocimiento a través de los datos, lo que provocaría a su vez un cambio en la Medicina Basada en la Evidencia, ya que con la capacidades propias del desarrollo de la inteligencia artificial, como señala el *Informe de resultados big data en salud digital,* se puede dar el salto de un paradigma de Medicina Basada en la Evidencia a un paradigma de medicina generadora de evidencia, "en donde el descubrimiento de los patrones ocultos mediante algoritmos de aprendizaje no supervisado pueda ofrecernos resultados totalmente desconocidos sobre las cuestiones biológicas y las relaciones de las de las mismas con los aspectos comportamentales y de entorno que abran la puerta a posibilidades ahora difíciles de imaginar"[755].

---

[753] Sobre la Inteligencia Artificial, Julio Mayol aclara que: "utilizando bases de datos heterogéneas, estructuradas y no estructuradas, pretendemos el uso secundario de «*Big Data*» para conseguir estratificar riesgos y predecir el desarrollo de enfermedades que suponen la mayor carga en nuestro país, intentando entender como la inflamación es la mayor causa de discapacidad en los países occidentales", *Vid.* https://juliomayol.com/tag/inteligencia-artificial/

[754] *Vid.* https://lab.elmundo.es/inteligencia-artificial/salud.html

[755] Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 70.

En la actualidad, resulta un reto que en el futuro aumenten considerablemente el número de directivos que adopten la tecnología del IA, no obstante, se ha de destacar que, España junto con Singapur y Finlandia, es el país que más esfuerzo y recursos está invirtiendo a fin de ampliar en el sector sanitario las aplicaciones desarrolladas por la IA[756], siendo en la actualidad la barrera principal la falta de personal cualificado y especializado para adoptar la IA en el sistema sanitario, puesto que los más significativo para una adaptación exitosa de la IA son las competencias personales[757]. A pesar de lo anterior, en el futuro se prevé que "[…] las organizaciones sanitarias serán capaces de posicionarse como líderes del mercado en cuanto a la aplicación de IA en la sanidad. Uno de los aspectos a tener en cuenta es que el poder transformador de estas tecnologías se fundamenta en hacer de la sanidad un servicio más asequible y productivo, en vez de simplemente buscar mejorarla"[758]. En términos generales, la IA conlleva un cambio de paradigma innovador en los procesos de gestión y funcionamiento de las empresas[759], así pues, como señala MARTÍNEZ MARTÍNEZ[760]:

"El proceso de digitalización creciente de los sectores público y privado, y las capacidades de analizar los datos mediante herramientas de *machine learning* gracias a las posibilidades de almacenamiento y proceso que ofrecen los entorno de cloud, favorecen la migración a un modelo de decisiones basadas en datos. La IA aporta aquí todo su valor, ya sea como herramienta de apoyo a la decisión humana asistida, ya sea como proceso automático que opera ofreciendo directamente servicios […] incluso

[756]Accenture consulting, *Inyección de inteligencia para el sector sanitario,* 2019, p.2, indica que: "En lo que se refiere a los niveles actuales de adopción, las cifras son prometedoras: más de uno de cada cuatro encuestados (27%) afirma que ya se está utilizando IA en algún ámbito de su organización. Aunque la mayor parte de los directivos del sector sanitario están todavía planificando sus proyectos de IA, algunos aseguran que se encuentran en una fase bastante avanzada. El 11% considera que la integración de IA en las operaciones es buena, aunque muchos solo utilizan una o unas pocas aplicaciones con esta tecnología" […] "Así, según los resultados de la encuesta, los directivos consideran que la IA ya está empezando a dar frutos, especialmente en ámbitos operativos. La mejora de la ciberseguridad (56% de los encuestados), la eficiencia operativa (56%), el aumento de capacidades analíticas (50%) y el recorte de costes (43%) son los beneficios más importantes", *op. cit.,* p.5 -7.

[757]Accenture consulting, *Inyección de inteligencia para el sector sanitario,* 2019, p.9.

[758] Accenture consulting, *Inyección de inteligencia para el sector sanitario,* 2019, p.11.

[759] McKinsey Global Institute, *How artificial intelligence and data add value to businesses*, 2018, [Documento sin paginación]. Documento disponible en: https://www.mckinsey.com/featured-insights/artificial-intelligence/how-artificial-intelligence-and-data-add-value-to-businesses (última consulta 12/04/20).

[760] MARTÍNEZ MARTÍNEZ, R., "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista Catalana de Dret Públic,* núm. 58, 2019, p.67.

situaciones de ineficiencia se conciben como oportunidades de mejora, y también lo es el amplio espacio sectorial susceptible de crecer de la mano de la IA".

De manera particular, en sanidad, Inteligencia Artificial implica la aplicación de tecnologías que amplían las capacidades humanas por medio de la utilización de máquinas inteligentes que pueden percibir, comprender, actuar y aprender a efectuar labores administrativos y clínicos[761], lo que ha generado la denominada *eHwalth* o salud electrónica[762].

En este sentido, entre las aplicaciones de IA del sector sanitario más utilizadas se destacan[763]: (1) el asistente robótico para cirugías donde el profesional sanitario puede operar al paciente sin necesidad de que se encuentren en el mismo espacio; (2) enfermeras virtuales, que asisten al paciente en cualquier momento y llevando un seguimiento virtual de su tratamiento; (3) Watson, el superordenador IBM que diagnostica las enfermedades de cáncer con una gran precisión, sugiriendo a su vez al profesional sanitario los tratamientos que mejor se adaptan al paciente[764] y (4) SARS-CoV-2, desarrollado por *BlueDod* un sistema de inteligencia artificial destinado a la detección de brotes de enfermedades infecciosas en todo el mundo y que, predijo el

[761] Accenture consulting, *Inyección de inteligencia para el sector sanitario,* 2019, p.2, precisa en su informe que: "Estas tecnologías abarcan el procesamiento del lenguaje natural, actores inteligentes, visión artificial, aprendizaje automático, sistemas expertos, *software* de análisis de datos (como IBM Watson Health), herramientas de diagnóstico basadas en datos, chatbots y reconocimiento de voz (como Alexa de Amazon o Siri de Apple en el mercado de consumo)".

[762]En este sentido señala NAVAS NAVARRO, S., "Salud electrónica e Inteligencia Artificial", en AA.VV., *Salud e Inteligencia Artificial desde el derecho privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19),* (Dir. Susana Navas Navarro), Comares, Granada, p.9, que: "Se puede definir la salud electrónica como el conjunto de servicios sanitarios prestados de forma telemática, empleando tecnologías de la información, de la comunicación y sistemas de inteligencia artificial que son compatibles e interoperables".

[763] MARTÍNEZ GARCÍA, D.N., DALGO FLORES, V.M., HERRERA LÓPEZ, J.L., ANALUISA JIMÉNEZ, E.I. y VELASCO ACURIO, E.F., "Avances de la inteligencia artificial en salud", *Dominio de las ciencias,* Vol. 5, núm. 3, julio 2019, pp. 609-610. Documento disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7154291

[764] Precisan MARTÍNEZ GARCÍA, DALGO FLORES, HERRERA LÓPEZ, ANALUISA JIM y VELASCO ACURIO, "Avances de la inteligencia…", *op. cit.,* p.610, que: "Watson también puede realizar un seguimiento individualizado de cada paciente a nivel genético. E incluso ya está identificando medicamentos nuevos y la relación entre medicamentos existentes. DeepMind, la división de investigación de inteligencia artificial de Google se ha aliado con el servicio nacional de salud británico. El objetivo de la compañía de Alphabet es crear una aplicación, Streams, que centraliza la información sobre un paciente. La gracia es que Streams puede generar alertas en base a esa información, permitiendo al profesional sanitario actuar con rapidez. Sentrian apunta aún más allá, el objetivo es prever cuándo una persona se puede enfermar. Así podrá tratarse incluso antes de que tenga que ir al hospital, reduciendo las asistencias a los centros hospitalarios. Para ello usa biosensores, y machine learning para analizar datos".

COVID-19[765], entre otros[766]y, más recientemente a causa de la COVID-19, se ha de citar la *start-up* VivaLNK, un sistema retomo multifuncional de control de pacientes[767].

Para terminar, se han de subrayar algunos de los riesgos que ofrecen las tecnologías y procesos desarrollados por la IA, apreciados por el grupo de trabajo sobre "Inteligencia Artificial y Desarrollo Humano" creado por la Cátedra de Privacidad y Transformación Digital Microsoft-Universitat de Valencia y, que igualmente cita MARTÍNEZ MARTÍNEZ[768]: (1) *Riesgo de discriminación digital*, en el sentido de que la IA puede discriminar entre países avanzados y no menos avanzados desde un punto de vista tecnológico y económico; (2) *Riesgo de discriminación laboral*, debido a que una de las consecuencias de la IA es que las máquinas pueden llegar a realizar los trabajos que desempeñan las personas, lo que supondría la expulsión de millones de personas del ámbito laboral; (3) *El impacto en el derecho a la educación*, puesto que el IA exige educar a las nuevas generaciones en una formación vinculada a herramientas de pensamiento computacional a efectos de que los estudiantes desde una edad temprana desarrollen habilidades para el uso del IA; (4) *El sesgo como riesgo*, en el sentido de que la toma de decisión basados en la IA depende del análisis por medio de algoritmos que se efectúe sobre los datos masivos, de tal modo que, si hay algún tipo de sesgo o error, debido a la mala calidad de los datos o a un mal funcionamiento material del algoritmo, puede originar discriminación social en la toma de decisión[769].

---

[765]Al respecto DOUGLAS HEAVEN, W., "Por qué la IA nos ayudará a combatir la próxima pandemia, pero no esta", *MIT Technology Review,* 2020, [Documento sin paginación]. Documento disponible en: https://www.technologyreview.es/s/12021/por-que-la-ia-nos-ayudara-combatir-la-proxima-pandemia-pero-no-esta, (última consulta 07/04/20) afirma que: "Parece ser que un sistema de inteligencia artificial (IA) vio venir al coronavirus (SARS-CoV-2). El 30 de diciembre, la compañía de inteligencia artificial BlueDot, que utiliza aprendizaje automático para detectar brotes de enfermedades infecciosas en todo el mundo, alertó a sus clientes, incluidos varios gobiernos, hospitales y empresas, sobre un inusual aumento de casos de neumonía en Wuhan (China). Nueve días más tarde, la Organización Mundial de la Salud lanzó el aviso oficial sobre lo que ahora todos conocemos como COVID-19".

[766] DOUGLAS HEAVEN, "Por qué la IA nos…"*, op. cit.*, [Documento sin paginación] indica que: "BlueDot no fue la única empresa que lo detectó. El servicio automatizado HealthMap del Hospital Infantil de Boston (EE. UU.) también notó esas primeras señales. Lo mismo ocurrió con el sistema de la compañía Metabiota. Resulta impresionante que la IA sea capaz detectar un brote en el otro lado del mundo, y todos sabemos que las alertas tempranas salvan vidas".

[767]NAVAS NAVARRO, "Salud electrónica…", *op. cit.,* p. 12.

[768]MARTÍNEZ MARTÍNEZ, "Inteligencia artificial desde…", *op. cit.,* pp. 68-72.

[769]En este sentido, MARTÍNEZ MARTÍNEZ, "Inteligencia artificial desde…", *op. cit.*, p. 69, cita algunos ejemplos reales: "a) En procesos de selección de personal o de evaluación de la calidad de la prestación laboral puede producir efectos discriminatorios; por ejemplo, fomentar despidos injustos. b) En el ámbito de la seguridad pública se ha demostrado la existencia de programas de asistencia que orientan el desarrollo de la actividad policial a la detención de minorías. c) Se ha denunciado que programas de

Igualmente, el Parlamento Europeo, se ha pronunciado sobre la baja calidad de los datos o los procedimientos, señalando que[770]:

"[…] podrían dar lugar a algoritmos sesgados, correlaciones falsas, errores, una subestimación de las repercusiones éticas, sociales y legales, el riesgo de utilización de los datos con fines discriminatorios o fraudulentos y la marginación del papel de los seres humanos en esos procesos, lo que puede traducirse en procedimientos deficientes de toma de decisiones con repercusiones negativas en las vidas y oportunidades de los ciudadanos, en particular los grupos marginalizados, así como generar un impacto negativo en las sociedades y empresas".

Sin embargo, a pesar de lo anterior, la IA actualmente en el sector sanitario es una herramienta de gran valor puesto que ayuda a los facultativos sanitarios a la toma de decisiones, acción que solo y únicamente podemos hacer las personas, la IA ayuda a la toma de decisiones por medio de procesos de analítica de datos masivos basados en algoritmos, pero no hemos de obviar que es una herramienta que colabora en la toma de decisiones y, que en ningún caso decide por nosotros, la última palabra siempre la tiene el profesional sanitario o, al menos así debería de ser[771].

En consecuencia, debido a las diversas oportunidades que ofrece la IA, se prevé que en el futuro sea una herramienta esencial junto con el *big data* a efectos de mejorar la asistencia sanitaria, la relación entre profesionales y pacientes, optimizar recursos y procedimientos, así como para optimizar los servicios por parte del personal de los

---

asistencia en procesos para obtener libertades condicionales en Estados Unidos operan sesgadamente favoreciendo la concesión de este derecho a personas de raza blanca. d) En el plano del derecho a la tutela judicial efectiva, están apareciendo, en el mercado, programas que son capaces de establecer el porcentaje de éxito que alcanzará una determinada demanda ante un determinado tribunal. Desde el punto de vista de la garantía del juez ordinario predeterminado por la ley, y de la independencia de criterio del juzgador en el ejercicio de la función jurisdiccional, resulta preocupante pensar que existan máquinas capaces de predecir un determinado resultado".

[770] Considerando m) 31 Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

[771] NAVAS NAVARRO, "Salud electrónica…", *op. cit.,* p. 11, aclara que: "Podría afirmarse que la aplicación de IA y, en particular, del *machine learning*, en el ámbito sanitario, puede servir, por un lado, como herramienta que propone, recomienda, analiza imágenes, distribuye recursos o actúa como segunda opinión para diagnóstico y tratamiento de enfermedades permaneciendo el control siempre en el profesional sanitario y, por otro lado, como sustituto de éste como puede ser un algoritmo de reconocimiento de imágenes que puede hacer el trabajo que, en la actualidad, desempeñan patólogos y radiólogos".

centros sanitarios, además de reducir costes en la mayoría de las áreas del sector sanitario[772].

II. LÍMITES Y RIESGOS DEL *BIG DATA* Y DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR DE LA SALUD

1. LÍMITES DEL *BIG DATA* EN EL SECTOR SANITARIO

De manera adicional a las oportunidades que ofrece la aplicación de *big data* en el sector sanitario, *sensu contrario* se ha de tener en consideración los límites y riesgos que continúan existiendo y que imposibilitan una idónea aplicación de las tecnologías *big data* en los proyectos reales de asistencia sanitaria, de investigación biomédica y desarrollo e innovación (I+D+i), así como de optimizar los beneficios y valores que el *big data* puede alcanzar a ofrecer en la prestación de servicios sanitarios y en la evolución de la medicina[773]. Así pues, resulta evidente que debido a que las fuentes de los datos de salud son dispares y diversas (estructurados, semiestructurados y no-estructurados) es necesario capturar, almacenar y analizar la totalidad de los datos

[772] *Vid.* Geriatricarea, *La Inteligencia Artificial será clave para mejorar la asistencia sanitaria*, febrero 2020, disponible en https://www.geriatricarea.com/2020/02/06/la-inteligencia-artificial-empieza-a-ser-una-realidad-en-el-sector-sanitario/, donde indica que: "El 80% de los líderes del sector sanitario creen que la Inteligencia Artificial jugará un papel fundamental en el desarrollo de los sistemas sanitarios, según indica la encuesta de la consultora Accenture. Estos datos arrojan que las expectativas que generan las nuevas tecnologías son altas. Este estudio determina que el 56% de los directivos encuestados esperan que la Inteligencia Artificial suponga una herramienta para optimizar las labores que realiza el personal de los centros sanitarios, así como una forma de mejorar la ciberseguridad de los sistemas informáticos del sector. Los encuestados atribuyen a la Inteligencia Artificial la posibilidad de mejorar la asistencia sanitaria, la relación entre profesionales y pacientes, la optimización de recursos y procedimientos, además de la reducción de costes en distintas áreas".

[773] Al respecto, como indica ACED FÉLEZ, E., "Protección de Datos y Transformación Digital en Sanidad", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, p. 39: "Esta acumulación de información digital también está sirviendo de acicate para nuevos proyectos de reutilización de la misma, para extraer nuevo conocimiento, para optimizar procedimientos, mejorar la calidad asistencial y abrir nuevas vías de investigación en las que el nuevo paradigma se llama big data, herramienta que promete grandes avances a unos costes reducidos. Pero cuando analizamos estas cuestiones nunca debemos olvidar que, al final, detrás de todos estos procesos que generan mejoras en la eficiencia; otorgan más control y autonomía a los pacientes; mejoran la calidad asistencial y promueven interesantes líneas de investigación, siempre están las personas; y personas en una situación en muchos casos vulnerable pues son pacientes y, por lo tanto, han acudido a los servicios sanitarios a buscar soluciones a sus problemas de salud. Por ello, siempre hemos de tener en cuenta los riesgos a los que se pueden someter a estar personas si no se tienen en cuenta desde el principio de cada nuevo proyecto que sus derechos han de ser salvaguardados y, en particular, su derecho a la privacidad y a la seguridad de sus datos personales".

disponibles y registrados[774] a efectos de rentabilizar al máximo las herramientas de *big data* en la sanidad del futuro.

Debido a lo anterior, lo idóneo es que finalmente el día de mañana el Sistema Nacional de Salud disponga de un registro central donde se encuentren almacenados todos los datos de salud de los pacientes a fin garantizar una circulación libre y directa entre los profesionales de la sanidad y los distintos centros sanitarios públicos de todo el territorio español.

No en vano de los avances evidentes del sistema sanitario a efectos de adaptar el mismo a las nuevas demandas tecnológicas y a la aplicación de las tecnologías de *big data*, siendo la historia clínica electrónica juntamente con la receta electrónica claros ejemplos de ello, actualmente continúan existiendo límites y riesgos que solventar tanto desde un punto de vista práctico como teórico-jurídico e incluso ético.

Por ello, a continuación, serán analizados los límites actuales de la aplicación de *big data* con perspectivas de futuro, teniéndose especialmente en consideración el estudio efectuado en el *Informe de resultados big data en salud digital*[775], así como otros aspectos relevantes que se pondrán en manifiesto.

En primer lugar, unos de los límites que en el presente impiden una aplicación efectiva de las herramientas de *big data*, dimana de la ineficacia e insuficiencia de los sistemas actuales de organización en el sector sanitario, al quedar los mismo obsoletos ante las exigencias propias de las TIC y, con ello de las tecnologías de *big data*. Por ello, se precisa de un sistema organizativo que permita compartir la información de manera completa, directa y homogénea entre los profesionales sanitarios y los centros de salud públicos habientes en todo el territorio nacional, de tal modo que se alcance una integración en un sistema sanitario global y centralizado[776].

---

[774] Ensayos clínicos, historiales médicos, secuenciación de ADN de pacientes o información procedente de redes sociales, entre otros muchos.

[775] *Vid.* Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 11 y ss.

[776] Actualmente, la LGC como instrumento de colaboración crea el órgano de coordinación denominado Consejo Interterritorial del Sistema Nacional de Salud (CISNS), definido en el art. 69 de la Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud es "el órgano permanente de coordinación, cooperación, comunicación e información de los servicios de salud, entre ellos y con la Administracion

Asimismo, de la mencionada necesidad de repositorios completos de datos – o si se prefiere, de un registro central – en el sistema sanitario, a efectos de llevar a cabo una idónea aplicación de las tecnológicas *big data*, será necesario igualmente la adaptación a las mismas desde distintos enfoques organizativos encaminadas hacia un nuevo modelo de atención sociosanitaria. Así pues, por un lado, se requiere mejorar la participación y colaboración el Sistema Nacional de Salud y el resto de los agentes de Asistencia Social; por otro lado, se ha de mejorar hacía una colaboración integradora entre la sanidad pública y la privada, así como entre los diferentes niveles de atención sanitaria. De igual modo, se requiere que dentro del mismo centro sanitario se comparta entre los profesionales sanitarios y entre los distintos departamentos, la información de los pacientes de manera homogénea y directa; por último, la relevancia de crear un marco de colaboración entre otros agentes privados de salud (compañías de seguros, empresas farmacéuticas, analistas de IT, entre otras)[777].

De manera similar, desde una perspectiva práctico – tecnológica también existen algunas limitaciones que se han de tener en consideración todas a causa de la relativa novedad de las herramientas *big data*, tales como: (1) falta de integridad entre los distintos sistemas sanitarios lo que genera una insuficiencia en la calidad de los datos; (2) falta de sistemas diseñados para un eficiente registro y almacenaje de datos a fin de agilizar información para una toma de decisiones en tiempo real y; (3) ausencia de proyectos completos, la mayoría de los proyectos actualmente continúan siendo proyectos piloto, es cuestión de tiempo que las citadas insuficiencias se solventen conforme en la práctica se vayan adaptando las infraestructuras internas y externas de los sistemas sanitarios a las exigencias del *big data*.

En último lugar, otras de las limitaciones proceden del propio mercado, pues actualmente continúan siendo escasos los profesionales especializados en análisis de *big data*, lo que en consecuencia provoca inevitablemente una lentitud en la implantación de tales tecnologías, dado que "es crucial contar con la presencia de analistas de datos

---

del Estado, que tiene como finalidad promover la cohesión del Sistema Nacional de Salud a través de la garantía efectiva de los derechos de los ciudadanos en todo el territorio del Estado". Igualmente, la LGC crea como órgano de apoyo científico-técnico del Sistema, el Instituto de Salud Carlos III, debiendo desarrollar sus funciones en coordinación con el CISNS y con otras Administraciones Públicas.

[777]Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 54.

expertos en el ámbito de salud para que, a través del uso de tecnologías *big data*, puedan dar el soporte adecuado a los médicos en la toma de decisiones relativas a sus pacientes"[778].

2. RIESGOS JURÍDICOS DE ACUERDO CON LA NORMATIVA VIGENTE DE PROTECCIÓN DE DATOS DEL *BIG DATA*

Desde una perspectiva jurídica, debido a que son diversos los derechos que se pueden ver en riesgo tanto del marco legal europeo como el nacional, motivo principal por el que en este trabajo se defiende la tesis de la necesidad de una ley sectorial de protección de datos de salud y de las herramientas *big data* aplicadas en el sector sanitario y en proyectos de investigación biomédica y farmacéutica de interés general, que garantice la privacidad del paciente y a su vez garantice la circulación libre de los datos de salud entre profesionales sanitarios, investigadores y organismos sanitarios (públicos o privados), así como terceros que promuevan y desarrollen proyectos de salud pública e investigación biomédica y farmacéutica de interés general[779].

Previamente, se ha de aclarar de que en un principio para los datos no personales procedentes de fuentes como la expansión del Internet de las Cosas, la Inteligencia Artificial y el aprendizaje automático y, por consiguiente, entre otros, datos agregados y anonimizados utilizados para análisis de datos a gran escala[780], así como para el

---

[778]Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 55.

[779] Al respecto, el Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*, p. 54, precisa que: "En este sentido, la mayoría de los profesionales consultados muestran una cierta insatisfacción con el actual marco normativo, hasta el punto de que para muchos de ellos, es la principal barrera a superar". Igualmente, GONZÁLEZ GONZÁLEZ, "Responsabilidad proactiva en los tratamientos…", *op. cit.,* p.116, aclara que: "Aplicando la terminología del mundo de la gestión de riesgos, puede afirmarse que el tratamiento masivo de datos personales tiene, por su propia naturaleza y según la forma en que se lleve a cabo, un impacto sobre los derechos de las personas afectadas y puede suponer un riesgo para las mismas, en el caso de que dicho tratamiento masivo de datos no cuente con medidas adecuadas para evitar o mitigar dichos riesgos. Tales medidas, dicho de una forma muy general, pueden pertenecer a diferentes categorías, como por ejemplo el establecimiento de límites legales, directrices organizativas o condiciones técnicas. Estas medidas suponen una delimitación, más o menos clara, de lo que se puede y lo que no se puede hacer. Pero, además, resulta necesario establecer también un marco ético de referencia respecto del tratamiento masivo de datos personales, que llegue un poco más allá de donde lleguen las medidas legales, organizativas y técnicas, estableciendo unos límites adicionales sobre los que se debe o no se debe hacer. Por lo tanto, nos encontramos ante el escenario, por otra parte habitual, de necesidad de ponderación entre los beneficios conseguidos y los riesgos que supone la aplicación de los tratamientos masivos de datos".

[780] Al respecto, el Considerando 9 del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europeo, establece que: "La expansión del «internet de las cosas», la inteligencia artificial y

tratamiento de datos en un sentido amplio incluyéndose el tratamiento de datos de distintos grados de intensidad, "desde el almacenamiento de datos [infraestructura como servicio (IaaS)] hasta el tratamiento de datos en plataforma [plataforma como servicio (PaaS)] o en aplicaciones [software como servicio (SaaS)]"[781] se ha de aplicar el Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europeo (en adelante Reglamento 2018/1807), cuyo objetivo fundamental es el de dar efecto al principio de libre circulación de datos no personales a través de las fronteras, garantizando a su vez la rápida supresión de los actuales requisitos de localización de datos, permitiendo, el tratamiento de datos en múltiples lugares en la Unión por motivos operativos y, "la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales"[782].

Sin embargo, como se ha podido observar a lo largo del presente trabajo la anonimización de los datos personales y, en concreto de los datos de salud no se puede garantizar completamente, existiendo altas probabilidades de reversibilidad de los datos sanitarios lo que conlleva en consecuencia poder recuperar la identificación del titular. Por ello, a lo largo del presente trabajo y, en concreto en este apartado, se defiende la tesis de la necesidad de una norma jurídica sectorial que además de regularizar de manera específica el derecho de protección de datos de salud, establezca medidas y garantías de obligado cumplimiento en los proyectos de investigación biomédica o farmacéutica de interés general que apliquen herramientas *big data*, a modo de código de autorregulación y otras buenas prácticas donde se incluyan mecanismos adecuados para la determinación de responsabilidad, la transmisión de responsabilidad entre servicios complementarios, así como otras medidas que serán analizadas a continuación. Evidentemente, esta ley sectorial no se vería afectada por el Reglamento 2018/1807, todo lo contrario, a pesar de las particularidades en lo referente a los datos relativos a la

el aprendizaje automático representan las principales fuentes de datos no personales, por ejemplo como resultado de su despliegue en procesos de producción industrial automatizada. Entre los ejemplos específicos de datos no personales se encuentran los conjuntos de datos agregados y anonimizados utilizados para análisis de datos a gran escala, los datos sobre agricultura de precisión que pueden ayudar a controlar y optimizar la utilización de plaguicidas y de agua, o los datos sobre las necesidades de mantenimiento de máquinas industriales. Si los avances tecnológicos hicieran posible transformar datos anónimos en datos personales, dichos datos se deben tratar como datos personales y, en consecuencia, se debe aplicar el Reglamento (UE) 2016/679".

[781] Considerando 17 Reglamento 2018/1807.

[782] Considerando 18 y Art. 1 Reglamento 2018/1807.

salud, sería una norma armonizadora e integradora del citado Reglamento 2018/1807, así como de la normativa de protección de datos vigente tanto en el ámbito europeo como nacional, tal y como se expuesto a lo largo del trabajo.

En concreto, uno de los riesgos legales dimana de la complejidad de disociar los datos personales de los datos no personales registrados, incluso siendo aplicadas técnicas de anonimización con el fin de convertir los datos personales en datos no personales[783], nos encontraríamos ante un riesgo si existe posibilidad alguna de revertir el proceso y de reidentificar a las personas físicas, pues en ese caso, continuarán siendo datos de carácter personal, de conformidad con el artículo 4.5 RGPD.

En consecuencia, ante la existencia de datos de carácter personal o ante la posibilidad de volver a ser datos de carácter personal, cualquier tratamiento y cesión de datos a terceros debe hacerse conforme a lo establecido en el RGPD[784]. Por otro lado, se ha de tener presente que la normativa vigente de protección de datos delega en los responsables del tratamiento la carga y responsabilidad de identificar los riesgos y de tomar las medidas adecuadas para atenuarlos, todo ello de conformidad con el principio de responsabilidad proactiva (*accountability*) analizado en capítulos anteriores, una de las bases fundamentales del RGPD es la de que los organismos (públicos o privados) en calidad de responsables del tratamiento tengan la obligación de ser proactivos a fin de acreditar que cumplen de manera efectiva y potencial las obligaciones exigidas en el artículo 5.2 del RGPD. De contrario, para el caso de que la información no incluya datos personales[785] deberá aplicarse el Reglamento (UE) 2018/1807 del Parlamento

[783] *Vid.* el Considerando 26 RGPD: "[…] los principios de protección de datos no deben aplicarse a la información anónima […] ni a los convertidos en anónimos […]. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

[784] Recordemos que la base jurídica del RGPD es la de garantizar y salvaguardar el derecho de protección de datos y el tratamiento de datos personales como un derecho fundamental de conformidad con el art. 8, apdo. 1, de la Carta de los Derechos Fundamentales de la Unión Europea y en el art. 16, apto. 1, del Tratado de Funcionamiento de la Unión Europea.

[785] *V.gr.,* datos industriales generados por máquinas o por procesos basados en tecnologías emergentes como la Internet de las Cosas, así como datos creados por la actividad humana, pero que no tienen la consideración de datos de carácter personal al no estar referidos en una persona identificada o identificable, *Vid.* GARCÍA MEXÍA y PERETE RAMÍREZ, "Internet, el RGPD y la LOPDGDD…", *op. cit.,* p. 854.

Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea[786].

Asimismo, el hecho de que decisiones sumamente importantes para la vida y el bienestar de las personas sean tomadas a través de la aplicación de tecnologías analíticas como el *big data*, dejando al margen la intervención humana puede suponer un riesgo en el uso y tratamiento masivo de datos, por ello el RGPD regula como base fundamental del derecho de protección de datos el principio de transparencia, exigiendo a los responsables del tratamiento la obligación de informar de manera clara y transparente a los titulares de los datos, sobre todo ante situaciones en las que se van a llevar a cabo decisiones automatizadas a través de herramientas *big data*, incluida la elaboración de perfiles, así como de la importancia y de las consecuencias que se pudieran generan directamente en el interesado a consecuencia del tratamiento, todo ello a tenor de los arts. 13.1 y 13.2 y art. 22.1 del REGP y, en igual sentido en el artículo 11.2c) de la LOPDGDD.

No en vano, debemos tener en consideración que existe el riesgo de que el consentimiento informado a través de contratos o políticas de privacidad transparentes y claras no siempre sea posible en el contexto del *big data*[787], debido a la imposibilidad por parte del responsable del tratamiento de poder cumplir con el principio de transparencia y con el principio de privacidad desde el diseño y por defecto, puesto que se puede dar la situación en la que surja *a posteriori* la necesidad del tratamiento de los datos con técnicas *big data*, a causa principalmente del rápido avance de la tecnología, del contexto social en el que se dé la situación por motivos de salud pública (*v.gr.,* la COVID-19) o, bien, se desarrolle el proyecto de investigación biomédica o farmacéutica de interés general. De igual modo, se ha de tener en consideración que no todos los

[786]DOUE L 303/59, de 28 de noviembre de 2018.

[787] En este sentido, el funcionamiento del big data, como señala DURÁN RUIZ, F.J., "Big Data aplicado a la mejora de los servicios públicos y protección de datos personales", *Revista de la Escuela de Posgrado,* núm. 12, junio 2017, p. 62: "[…] dificulta enormemente esta labor, puesto que los datos se mueven de un lugar a otro, de un receptor a otro de forma impredecible, y especialmente porque el valor que pueden tener los datos no se conoce ni se puede conocer en el momento en que son recogidos, convirtiendo el consentimiento en un «todo incluido» y desvirtuando o vulnerando entre otros principios esenciales de la protección de datos como el de calidad de los datos". Asimismo, GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos*, Agencia Española de Protección de Datos y Boletín Oficial del Estado, Madrid 2016, p. 73, señala que: "[…] la cadena de emisores y receptores de datos es potencialmente infinita, e incluye actores e instituciones cuyo rol y responsabilidades no están delimitados o comprendidos. Así, la cesión de datos puede llegar a ser relativamente oscura".

datos que son tratados a través de herramientas *big data* proceden de fuentes en las que los titulares han facilitado los datos de manera consciente, ya que pueden proceder de fuentes públicas, de sensores de dispositivos, o a través de métodos analíticos y algoritmos, entre otros.

Otro de los riesgos jurídicos a destacar en la normativa jurídica es el que dimana del consentimiento flexible o residual de los pacientes, lo que genera en consecuencia que ante la falta de transparencia o claridad normativa los distintos actores del sector sanitarios realicen una interpretación estricta o restrictiva de la norma[788].

Por otro lado, se ha de tener presente las posibles discrepancias que pueden surtir de los distintos Comités de Ética de la Investigación ante la evaluación de un mismo proyecto o por "inadecuación del modelo organizativo"

Los anteriores escenarios justifican con mayor criterio la necesidad de una ley sectorial de protección de datos de salud y de *big data*, a fin de que en la misma se regulen las medidas que deben respetar los responsables del tratamiento en el momento de aplicar tecnologías *big data* (indistintamente de que sea *a prior* o *posteriori* del consentimiento del titular) a fin de salvaguardar con máxima rigurosidad la privacidad del titular de los datos de salud, puesto tal y como señala DURÁN RUIZ:

"[…] la atención no puede estar tan centrada en el momento de prestación del consentimiento para el tratamiento de los datos y en los sistemas para prestar un verdadero consentimiento informado, sino que debe desplazarse al momento de la utilización efectiva de los datos"[789].

De igual modo, también se pronuncia sobre esta cuestión el *Código de Buenas Prácticas en protección de datos para proyectos de Big Data,* al señalar que:

---

[788] AUSTÍN, T., ANDREU MARTÍNEZ, B., VALERO TORRIJOS, J. y CAYÓN DE LAS CUEVAS, J., "Diez consideraciones ético-jurídicas en relación con la reutilización y big data en el ámbito sanitario", *Bioderecho.es,* N.º 12, 2020, p. 1.

[789] DURÁN RUIZ, "Big Data aplicado…", *op. cit.*, p.63.

"[…] la información al afectado se facilita en el momento de captación del dato, mientras que los tratamientos de Big Data, si por algo se caracterizan, es por su continuidad en el tiempo. De ahí la necesidad de implantar un sistema que facilite información sobre el modo y el procedimiento para el ejercicio de derechos, y que la misma sea de fácil acceso y localización por parte de los afectados"[790].

Debido a lo anterior, resulta primordial que la ley sectorial de protección de datos de salud y *big data*, como se ha visto en los capítulos anteriores, aborde y regule cuestiones como las anteriores, sobre todo, a fin de evitar posibles riesgos que pudieran darse ante situaciones en la que no sea posible un anonimización absoluta, irreversible y sin posibilidad de reidentificación, antes de ser sometidos los datos personales a técnicas *big data*, ya que en caso contrario, los datos seguirían siendo personales a los efectos del artículo 4.5 del RGPD.

Asimismo, se propone que la ley sectorial de manera paralela regule algunas de las medidas técnicas y de seguridad que resultaría de relevancia que fueran implantas por las organizaciones de sanidad e investigación (públicas o privadas) que desarrollen proyectos donde apliquen tecnologías y herramientas de *big data*, lo que vendrían a ser las medidas que el responsable del tratamiento debe ejecutar y comunicar a la autoridad de control desde el diseño del proyecto, y que cuya implantación a su vez la autoridad de control puede exigir al organismo responsable del tratamiento de los datos de salud en el proyecto concreto donde se emplee *big data* sanitario, en caso de apreciar su ausencia en la consulta previa que debe realizar el responsable del tratamiento antes de iniciar el proyecto, esto es, en el momento del diseño del mismo.

Por consiguiente, a efectos de garantizar la privacidad de los pacientes en los proyectos de *big data* sanitario, se estima conveniente que la ley sectorial tenga en cuenta que el responsable del tratamiento debe adoptar desde el diseño medidas de privacidad, tales como: minimizar todo lo posible la cantidad de los datos de salud, procesar al mayor nivel posible de agregación y con el mínimo detalle los datos de salud, ocultar y proteger la visibilidad de los datos de salud a los usuarios, proceder a la

[790] Agencia Española de Protección de Datos. *Código de buenas prácticas en protección de datos para proyectos Big Data*, p. 18. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (última consulta 15/02/2021).

separación de los datos personales en entornos separados y distribuidos, información previa trasparente a los interesados sobre el tratamiento y procesamiento de sus datos de salud en proyectos de *big data*, informar y facilitar el acceso a los procedimientos del ejercicio de sus derechos a los interesados, implar políticas de privacidad conforme a la normativa vigente de protección de datos que posteriormente se pueda demostrar a la autoridad de control y órganos jurisdiccionales.

En concreto, la AEPD[791] señala algunas técnicas o tecnológicas a fin de llevar a cabo de manera real las anteriores medidas de privacidad en cada una de las fases de la cadena de valor de los proyectos de *big data*, esto es, en la fase de adquisición, fase de recopilación, fase de análisis, fase de validación, fase de almacenamiento y fase de explotación[792]:

Medida de privacidad		Técnica/tecnología a aplicar
Minimizar o agregar	→	**Anonimización**
Ocultar o separar	→	**Cifrado**
Informar o controlar	→	**Control de Acceso**
Cumplir o demostrar	→	**Trazabilidad**

Igualmente, la ley sectorial debería hacer referencia a otras medidas técnicas citadas a lo largo del articulado del RGPD – además de las anteriores – tales como las medidas de responsabilidad proactiva, medidas de transparencia, consentimiento, monetización y control, que los organismos, públicos o privados, responsables del tratamiento de datos de salud en proyectos *big data* deberán implantar en la medida de lo posible. Por otro lado, conviene acentuar que el RGPD establece medidas de seguridad[793] a efectos de optimizar la confianza de los interesados, como son los

[791] Agencia Española de Protección de Datos. *Código de buenas prácticas en protección de datos para proyectos Big Data*, p. 29

[792] *Vid.* Anexo: Tabla 2. Resumen de las estrategias de privacidad más adecuadas para cada una de las fases que conforman la cadena de valor de *Big Data* diseñada por la AEPD.

[793] Arts. 40 a 43 del RGPD.

códigos de conducta en las organizaciones a efectos de facilitar la aplicación de la normativa vigente de protección de datos, así como mecanismos de certificación, sellos y etiquetas de protección de datos que permiten demostrar a terceros el cumplimiento de la normativa de protección de datos, siendo la privacidad un valor primordial en los proyectos de *big data*. Por ende, las citadas medidas han de ser igualmente tenidas en cuenta en la ley sectorial puesto que asegurar la confianza de los interesados debe ser objetivo principal tanto para el legislador como para las organizaciones (públicas o privadas) que desarrollen proyectos de investigación biomédica o asistencia sanitaria de interés público con aplicación de herramientas *big data*, sobre todo, a los efectos de hacer conscientes a los ciudadanos de los beneficios que reporta el *big data* en el sector sanitario.

En conclusión, la finalidad principal de lo podría regularse como una parte especial de la ley sectorial destinada a las medidas y garantías de protección de datos para proyectos de salud pública e investigación biomédica con aplicación de herramientas *big data*, es la de regular desde una perspectiva jurídica legal los deberes y obligaciones que las organizaciones (públicas o privadas) que lleven a cabo proyectos de *big data* sanitario deben respetar y cumplir a efectos de mejorar y afianzar la confianza de los interesados, así como asegurar el derecho de privacidad y a la protección de datos de los mismos, por medio de medidas y garantías, que – como se ha expuesto – obliguen a los responsables del tratamiento de *big data* llevar a cabo una metodología de protección de datos desde el diseño del proyecto. De igual modo, no hemos de obviar que, llegado el momento, debido a la complejidad de la materia, el legislador deberá tener en consideración la opinión de los profesionales involucrados[794] a los efectos de confeccionar una ley especial a medida y que se adapte a las exigencias presentes y futuras dimanantes del sector de la santidad, de la investigación biomédica y de las nuevas tecnológicas.

[794] Entiéndase por profesionales involucrados aquellos que pertenecen al sector sanitario, al de la investigación y a los especialistas en nuevas tecnológicas que desarrollan herramientas de *Big Data*, tanto del sector público como privado.

3. RIESGOS ÉTICOS DEL *BIG DATA* Y DE LA INTELIGENCIA ARTIFICIAL

Paralelamente y de manera aislada, a continuación, en este apartado se subrayan los riesgos éticos que conlleva la aplicación de herramientas de *big data* y la Inteligencia Artificial en el sector sanitario.

No obstante, además de aquellos riesgos propios de posibles vulneraciones a los derechos de intimidad y privacidad de los titulares de los datos procedentes de una mala praxis con los datos, analizados anteriormente en el presente trabajo, existen otros riesgos éticos relevantes y que hemos de tener en consideración. Así pues, resulta un hecho notorio que el *big data* y la IA conllevan un cambio en la prestación de servicios sanitarios, lo que implica a su vez un desigual acceso a las TIC por parte de aquellos colectivos vulnerables, con menos recursos económicos, hecho que repercute igualmente a los países avanzados y menos avanzados, pues las TIC requiere de inversiones económicas que no todos los ciudadanos pueden hacer frente, aunque cada vez están más al acceso de la población, en la actualidad todavía existen colectivos vulnerables que no pueden acceder a las mismas, bien por falta de recursos económicos, bien por falta de conocimientos en su manejo, en caso de ancianos o niños[795].

Por otro lado, la aplicación de las herramientas de *big data* y de la IA puede llegar a implicar un control excesivo por parte de los agentes del sector sanitario e incluso las empresas sobre los pacientes lo que puede conllevar a su vez una pérdida de autonomía y libertad de estos. Es evidente, que los datos masivos tras ser analizados aportan información y conocimiento, por lo que es imprescindible que esa información y conocimiento sustraído sea manejado por los agentes no únicamente conforme a la normativa vigente de protección de datos, sino también conforme a los principios de la moral y la ética, puesto que, de lo contrario, pondríamos en riego la autonomía y libertad de los titulares de los datos.

[795] Al respecto, SÁNCHEZ DEL CAMPO REDONET, A., "Inteligencia artificial y privacidad", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (Coord., J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 986-987, señala que: "[…] la discriminación provocada por el algoritmo puede ser una propiedad emergente y no intencionada derivada de la utilización del *software*, en lugar de una elección consciente de sus programadores y por ello puede ser extraordinariamente difícil identificar la fuente del problema […] hay una enorme falta de transparencia de las empresas en lo que al uso y métodos utilizados por los algoritmos se refiere porque las compañías entienden que son secretos industriales cuya difusión les perjudicaría seriamente".

Por ende, en el momento que la información y conocimiento sustraído sea destinada a fines exclusivamente económicos a efectos de garantizar a las empresas sanitarias y otros agentes anexos como compañías de seguros y entidades financieras a establecer o cambiar determinadas tendencias que puedan afectar a los ciudadanos, estaríamos ante un mal uso o un uso inmoral de las herramientas de *big data* y de la IA , que podría suponer un grave desequilibrio de poder entre las empresas y los pacientes, siendo estos en calidad de consumidores la parte débil o vulnerable[796]. Asimismo, desde una perspectiva jurídica, el RGPD es claro, puesto que, sobre el principio de limitación de la finalidad en relación con supuestos de tratamientos de datos de salud por razones de interés público, el Considerando (54) RGPD establece que: "[…] Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

De manera similar, un mal uso de la información y conocimiento sustraído de la aplicación de *big data* y de la IA puede generar en consecuencia estereotipos sociales lo que conllevaría implícitos problemas de exclusión social ante aquella parte de la sociedad que incumpliera los comportamientos sociales establecidos por las masas y, por tanto, deseables, que no tienen que ser necesariamente los mejores o correctos desde un punto de vista sanitario, ético o social[797]. Pues, es evidente que la denominada "dictadura de datos"[798] que crea ciertas patologías o estereotipos resulta en el mayor de los casos perjudicial para la sociedad, puesto que pondrían suponer una perdida confianza en las autoridades en salud, generando en consecuencia que la propia población le preste más interés a lo que dicta la tecnología que a la opinión de los propios profesionales, como podría ser el caso del uso de seguros médicos privados.

---

[796] Sobre esta cuestión, LERMAN, J., "*Big Data* and Its Exclusions", *Stanford Law Review* Online, 66 Stanford Law Review Online 55, SSRN, 2013, [Documento sin paginación] indica que: "millones de personas en todo el mundo permanecen en la periferia de los grandes datos. Así sus preferencias y necesidades están en riesgo de ser ignoradas en las decisiones que se basen en el *Big Data* y la inteligencia artificial".

[797] BAROCAS, S. and SELBST, A. D., "*Big Data*'s Disparate Impact", *104 California Law Review 671,* 2016, [Documento sin paginación]. Documento disponible en: https://ssrn.com/abstract=2477899 (última consulta 04/19/20) indican que el *Big Data* y los algoritmos pueden heredar o reflejar perjuicios y patrones de exclusión o ser el resultado de quienes han tomado decisiones anteriores.

[798]MAYER-SCHÖNBERGER, V. and CUKIER, K., "The Dictatorship of Data", *MIT Technology Review,* mayo 2013, [Documento sin paginación]. Documento disponible en: https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos (última consulta 04/22/20).

Igualmente, se ha de tener en cuenta que los expertos consideran que un mal uso del *big data* y la IA debido a un exceso de *biomonitorización* en la medicina preventiva y personalizada puede conllevar de manera negativa e indirecta a una pérdida de autonomía del paciente a la hora de decidir sobre su propia vida y salud, no debiéndose obviar por parte del facultativo sanitario que las tecnologías *big data* y la IA, son medios o herramientas cuya finalidad es ayudar y colaborar en la toma de decisiones, pero en ningún concepto a tomar la decisión de manera exclusiva sin tener en cuenta el criterio de otros profesionales sanitarios, así como la propia voluntad y autonomía del paciente.

Por último, señalar la propuesta del Parlamento Europeo en el año 2017 de un marco ético común sólido[799] o de máxima prudencia[800], así como de la necesidad de "evaluaciones periódicas sobre la representatividad de los conjuntos de datos y de examinar la exactitud e importancia de las predicciones, a efectos de combatir el peligro de "discriminación y sesgo algorítmicos"[801]. Asimismo, el Parlamento Europeo, afirma la necesidad de regular una "responsabilidad algorítmica, bajo la idea de que las normas científicas y éticas estrictas, son fundamentales"[802], destacando igualmente la necesidad

[799] Al respecto MARTÍNEZ MARTÍNEZ, "Inteligencia artificial desde…", *op. cit.*, p. 73, citando a European Commission's High-Level Expert Group on Artificial Intelligence, "Ethics guidelines for trustworthy *IA*", indica que: "En este sentido, el Grupo de Expertos de la Unión Europea para la Inteligencia Artificial11 ha recorrido un camino que ya habían abierto reguladores europeos como la Comisión Nacional de Informática y Libertades francesa, y el Supervisor Europeo de Protección de Datos, y ha identificado un elemento esencial para la ética de la IA. La ética de la inteligencia artificial debe ser una ética de la dignidad humana centrada en la garantía de los derechos fundamentales. Este enfoque nos permite una aproximación general al fenómeno de la IA, capaz de establecer una primera barrera jurídica al desarrollo de la tecnología, y funcional al modelo constitucional y democrático en el que debería desarrollarse. Permite situar la dignidad del ser humano en el centro y considerar una IA que no responda a criterios de mera eficiencia económica, sino que se centre en la función social de la inteligencia artificial y en el empleo de los datos para el bien común (Nadella, 2017: 146, 193). Por otra parte, este enfoque puede operar como un elemento de aplicación territorial del derecho en cada Estado y, a la vez, dinamizar el consenso de la comunidad internacional respecto del marco regulador de la IA".

[800] *Vid.* Considerandos 20 y 31 Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

[801] *Vid.* Considerando 20, Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

[802] *Vid.* Considerando 2, Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

de aplicar las normas éticas más elevadas ante el uso de macrodatos permitidos por el marco legal vigente[803].

No obstante, más recientemente, el día 19 de febrero de 2020 el Parlamento Europeo presentó sus estrategias en relación con los datos y la inteligencia artificial[804] a efectos de garantizar el desarrollo de la IA en beneficio de las personas y, sobre todo hacia una transformación digital en beneficio de todos, a efectos de dar soluciones digitales dando preferencia a las personas y, abriendo a su vez nuevas oportunidades las entidades privadas e impulsando el desarrollo de la tecnología[805]. En síntesis, para el desarrollo de esta estrategia digital, la Comisión Europea durante los próximos cinco años llevará a cabo las siguientes acciones principales: por un lado, diseñar el futuro digital de Europa por medio de una tecnológica cuya prioridad sea el beneficio de las personas, una economía justa y competitiva y, una sociedad abierta, democrática y sostenible. Por otro lado, apostando por la Excelencia y Confianza en la IA, por medio de un Libro Blanco[806] que fomentará el uso de forma segura de la IA, a través del aprovechamiento de los centros de investigación[807].

---

[803] *Vid.* Considerando 32, Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

[804] Fuente: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

[805] Al respecto la vicepresidenta ejecutiva para *Una Europa Adaptada a la Era digital* Margrethe Vesteger, indica que: «Queremos que todos los ciudadanos, todos los trabajadores, todas las empresas tengan una oportunidad justa de recoger los frutos de la digitalización. Eso puede suponer conducir de forma más segura o contaminar menos gracias a los vehículos conectados; o incluso salvar vidas mediante imágenes médicas controladas por inteligencia artificial que permitan a los médicos detectar enfermedades más rápidamente que nunca». Fuente: https://ec.europa.eu/commission/presscorner/detail/es/ip_20_273

[806] Desarrollando una estrategia europea de datos para situar a Europa como líder en la economía de datos, creando un auténtico espacio europeo y mercado único de datos para que fluyan libremente por toda la Unión Europea y entre sectores. Para ello la Comisión propondrá, la creación del marco regulador correcto en materia de gestión de los datos, apoyará el desarrollo de los sistemas tecnológicos y la siguiente generación de infraestructuras mediante inversiones en proyectos europeos de gran impacto sobre espacios de datos europeos e infraestructuras en la nube fiables y eficientes desde el punto de vista energético y finalmente, pondrá en marcha medidas sectoriales específicas, para construir espacios europeos de datos, por ejemplo, en relación con la fabricación industrial, el pacto verde, la movilidad o la salud. *Vid.* https://ec.europa.eu/info/files/communication-european-strategy-data_en

[807]Según la Comisión Europea, estas políticas y marcos permitirán que Europa implante tecnologías digitales punteras y refuerce sus capacidades de ciberseguridad, que desarrollará y proseguirá su propio camino para convertirse en una economía y una sociedad digitales competitivas a escala mundial, basadas en valores e inclusivas, al tiempo que continúa constituyendo un mercado abierto, colaborando estrechamente con sus socios internacionales. A lo largo de 2020 la Comisión presentará una norma de servicios digitales y un plan de acción europeo para la democracia, propondrá una revisión del Reglamento eIDAS (sobre identificación electrónica y servicios de confianza) y reforzará la ciberseguridad mediante la creación de una unidad informática conjunta, además de seguir avanzando en

III. DESAFÍOS DEL *BIG DATA* EN EL SECTOR SANITARIO

Por último, se ha de acentuar que actualmente el uso del *big data* en la sanidad continua en la actualidad siendo un reto principalmente por las siguientes causas: por un lado, la falta de expertos de analistas de TIC dentro del sector sanitario, por otro lado, algunos los sistemas e infraestructuras de la sanidad quedan obsoletas para una correcta implantación de las herramientas *big data*, lo que requiere grandes cambios estructurales tanto a nivel arquitectónico como de la organización del sistema, así como la toma de decisiones relevantes que puedan darse a consecuencia de la implantación de *big data*, como por ejemplo, el responsable del tratamiento, el lugar de almacenamiento, los datos afectos, entre otros, donde la normativa vigente de protección de datos tiene un papel relevante al respecto. Sobre esta cuestión Mayol señala seis retos más significativos de nuestro sistema sanitario en relación con el *big data*, en concreto: "(1) Extraer conocimiento de fuentes heterogéneas y complejas, a veces no estructuradas; (2) Comprender notas clínicas no estructuras en su contexto correcto; (3) Gestionar adecuadamente gran cantidad de datos de imagen clínica y extraer información útil para generar biomarcadores; (4) Analizar los múltiples niveles de complejidad que van desde los datos genómicos hasta los sociales; (6) Capturar los datos de comportamiento de los pacientes, a través de distintos sensores , con sus implicaciones sociales y de comunicación; (6) Evitar los problemas de privacidad y "*profiling*" que pueden generar riesgos para los individuos"[808].

---

la construcción de alianzas internacionales. Las inversiones requeridas se canalizarán desde los programas Digital Europe programme , the Connecting Europe Facility 2 y Horizon Europe, en concreto 15 mil millones de euros en IA y 2.500 millones de euros en el despliegue de plataformas de datos y aplicaciones de inteligencia artificial para el intercambio de datos confiable y eficiente en energía y las infraestructuras en la nube. *Vid.,* enlace web: https://www.dsn.gob.es/es/actualidad/sala-prensa/comisi%C3%B3n-europea-presenta-sus-estrategias-relaci%C3%B3n-con-digitalizaci%C3%B3n-datos

[808] MAYOL, J., "Los 6 retos del *Big Data* en la sanidad", enero 2015, [Documento sin paginación]. Documento disponible en: http://juliomayol.com/big-data-y-medicina-5p/ (último acceso 05/05/20).

1. DESAFÍOS DEL *BIG DATA* EN EL CONTEXTO ESPAÑOL

En España, del análisis de los datos aportados por el *Informe ÍNDICE SEIS* 2017, entre los principales retos del Sistema Nacional de Salud, se encuentra (1) poder atender en un futuro más inmediato a las exigencias de pacientes que actualmente a consecuencia de las TIC tienen mayor información y capacidad de decisión acerca de su propia salud, (2) dar una solución a la necesidad de garantizar una coordinación eficiente en las distintas áreas asistenciales y de atención al paciente, (3) otro de los retos es el referente al incremento del envejecimiento poblacional y de la prevalencia de enfermedades crónicas y, (4) el de incorporar e invertir en tecnologías avanzadas[809].

En consecuencia, según el último informe emitido por la Sociedad Española de Informática de la Salud (SEIS) sobre el estado de las TIC en la sanidad de española, en el año 2017 se destinaron 57.231.777 miles de euros al presupuesto global sanitario público asignado para el conjunto de las diecisiete Comunidades Autónomas. En concreto, se destinó la suma total de 695.593 miles de euros del presupuesto global a la inversión en TIC en todas las Comunidades Autónomas, lo que supone 1,22 % del presupuesto global, mismo porcentaje que en el 2016, donde más del 50% del total de gasto en TIC se reservó para la inversión en plataforma tecnológica, de lo que el 19% fue invertido en la contratación de servicios externos, seguido de un 8,2 % dirigido a comunicaciones de datos y un 8% de puestos de trabajo. Igualmente, el citado informe señala que el gasto en TIC por ciudadano en el 2017 fue de 15,09 euros y, en el 2016 de 14,60 euros, de lo que se deriva una variedad del 3,36 %[810].

En relación con las herramientas *big data* y los servicios *cloud*, el *Informe ÍNDICE SEIS* establece que, en el 2017 de las diecisiete Comunidades Autónomas, siete contaban con proyectos de *cloud computing*, lo que supone un 47 % del total, y seis tenían intención de implementarlo en ese año. Por otro lado, con relación al *big data*, en el 2017 fueron propuestos proyectos de gestión de datos en hasta once regiones, lo que supone un 73% del total[811].

---

[809] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2018, pp. 1-2. Documento disponible en: http://seis.es/indice-2017/ (último acceso 07/05/21).

[810] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2018, pp. 7-12.

[811] Sociedad Española de Informática de la Salud, *Índice SEIS 2017*, marzo 2018, p. 55.

Otros de los retos del *big data*, se ha de mencionar principalmente, por un lado, el de la exploración avanzada de los repositorios mediante *big data* a fin de proporcionar una gestión sanitaria de calidad al menor coste posible. Igualmente, otro de los retos relevantes y de urgencia a consecuencia del gran volumen de documentos clínicos escritos en formato no estructurado, es el de desarrollo de modelos de representación de información clínica a través de la creación de técnicas de procesamiento del lenguaje natural y la construcción automática de ontologías que representen el conocimiento clínico.

En cualquier caso, hay que subrayar que el sector sanitario tiene como reto el de aumentar las capacidades de las personas y el bienestar del ciudadano, objetivos que resultan imposibles de alcanzar con carácter inmediato por medio de la aplicación de técnicas de *big data* debido a la ausencia de una infraestructura en la mayoría de los organismos sanitarios (sobre todo de la Administración Pública) adaptada a las herramientas *big data* a fin de garantizar una gestión y tratamiento de los datos relativos a la salud eficaz y óptima, así como la ausencia de profesionales especializados en las nuevas tecnologías, todo ello debido principalmente a la falta de financiación en la estrategia de inversión de Salud Digital o, lo que es lo mismo, en las TIC SALUD[812].

En síntesis, a pesar de que son diversos y múltiples los retos que se pueden destacar[813], estimamos como fundamentales a fin de dar soporte a la transformación

[812] *Vid.* GARCÍA VIEIRA, F. J. y FERNÁNDEZ RANCAÑO, M., "Financiación de la Estrategia de Salud Digital", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 51-55.

[813] En este sentido, MARTÍNEZ MARTÍNEZ, "Big Data, investigación en salud y protección de datos personales: ¿Un falso debate?...", *op. cit.,* pp. 269-271, basándose en el trabajo *INFORMATION COMMISIONER'S OFFICE: Big data, artificial intelligence, machine learning and data protection. Version 2.0*, 2017. Disponible en https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf, destaca entre los retos del *big data*, los siguientes: A. Armar y formar éticamente a nuestros equipos de investigación; B. Disponer de políticas preventivas de análisis de riesgos; C. Delimitar la finalidad de la investigación; D. Garantizar una adecuada transparencia con el paciente y apostar por el consentimiento como elemento de legitimación de los tratamientos; E. Tratar adecuadamente cuando no evitar los supuestos que conduzcan a decisiones automatizadas; F. La publicación de resultados y la liberación de los datos deberían ser extremadamente cuidadosas con el cumplimiento normativo". Asimismo, PÉREZ CAMPILLO, L., "Una aproximación al *big data* y al *blockchain* sanitario y su implicación en la protección de datos personales", *Revista de Derecho y Genoma Humano,* Núm. Extraordinario, 2019, pp. 549-551, cita los siguientes retos: "i. La discriminación o dictadura de los datos; ii. La compatibilidad con el principio de finalidad, consentimiento y el continuo cambio […]; iii. La falta de autonomía invidual y de transparencia […]; iv. La anonimización no reversible". Igualmente, GUBBIOLI BELLECQ, "El valor de la información y el Big Data…", *op. cit.* pp. 40-41 señala los siguientes retos: "Institucionales: en un mundo globalizado, la obtención de la información de las distintas fuentes hará necesario que todos los estamentos

digital en el sector de la salud, por un lado, el diseño de nuevas arquitecturas y modelos tecnológicos en mejora de la calidad, la seguridad y la eficiencia de los servicios de salud destinada a un tratamiento de los datos de salud adaptado a la transformación digital, por otro lado, la formación de los profesionales[814] con el objeto de dotar a los mismos de competencias permitan una explotación adecuada de las capacidades potenciales de las TIC en el sector sanitario y, por último, un marco normativo específico que regule el tratamiento de los datos de salud, así como las medidas y garantías que se han de aplicar en los proyectos de investigación biomédica y farmacéutica que apliquen herramientas *big data* a fin de salvaguardar la privacidad de los pacientes, tal y como se defiende en el presente trabajo.

2. DESAFÍOS DEL *BIG DATA* EN EL CONTEXTO MUNDIAL: COVID-19

La crisis sanitaria generada por la COVID-19 a nivel mundial es un evidente ejemplo de los retos del *big data* tratados anteriormente, pues a través de la pandemia del coronavirus (COVID-19) hemos sido conscientes de relevantes carencias y

---

gubernamentales fomenten, en el marco de sus competencias, la colaboración e integración de los sistemas autonómicos y nacionales, para lograr proporcionar datos útiles, susceptibles de ser analizados para fines analíticos. En el ámbito nacional, será clave la labor que el Sistema Nacional de Salud pueda realizar para coordinar e integrar las distintas fuentes de información de los sistemas autonómicos. El valor del "Big Data" podría constituir, de hecho, una buena oportunidad de implementar una estrategia nacional para la generación de datos consistentes que hagan viable la explotación de datos; Técnicos: el constante aumento de la capacidad computacional y de almacenamiento de los sistemas, unido a la continua disminución de los costes, permite plantearse retos de análisis para conjuntos de datos inimaginables. Sin embargo, el reto técnico está en aspectos tales como la capacidad para compactar, filtrar y hacer consistentes los datos útiles de tal forma que puedan ser consultados, almacenados y comparados. Para superar este reto, serán cada vez más importantes aquellas plataformas tecnológicas que, empleando en la medida de lo posible los estándares establecidos, permitan un acceso a consistente a las fuentes de datos; Legales: la aplicación de las leyes de protección de datos y otras directivas europeas pueden suponer dificultades técnicas adicionales; Formativos: La implementación de un sistema de análisis de datos tiene como consecuencia la aparición de nuevos roles o adaptación de roles existentes con un foco formativo más orientado al tratamiento de grandes conjuntos de datos provenientes de distintas fuentes. Roles como los "Big Data Architects" deberán ser capaces de diseñar plataformas de consulta, almacenamiento y explotación de la información, que aseguren la transformación de los datos en información útil usable en el proceso de gestión o clínico. Además, otros roles existentes tendrán que formarse en nuevos sistemas para la gestión y consulta de datos, en el ámbito del desarrollo de *software*, los analistas de sistemas o los técnicos de sistemas".

[814] DEL RÍO SOLÁ y VAQUERO PUERTA, "El impacto de la transformación digital en el…", *op. cit.,* p. 106, opinan que: "Nuestro sistema de salud debe disponer de profesionales altamente cualificados y que lideren la incorporación de los nuevos procedimientos y servicios tecnológicos. Sin embargo, la situación de los recursos humanos relacionados con las tecnologías de la información y comunicación (TIC) en el sistema sanitario público es preocupante. En conocimiento de las TIC en salud es muy importante para avanzar en la transformación digital de la sanidad y garantizar la seguridad y disponibilidad de los servicios existentes".

problemas en el sistema actual de salud dimanantes del tratamiento de los datos de salud.

En primer lugar, se ha de hacer constar que, si la infraestructura del sistema sanitario hubiera estado adaptada de una manera eficaz y eficiente a las nuevas tecnologías permitiendo una correcta aplicación de las herramientas *big data*, la COVID-19 no hubiera tenido el grave impacto que ha generado, pues habríamos sido conocedores del virus antes de su surgimiento, lo que al menos, nos hubiera permitido tomar con antelación las medidas y decisiones más apropiadas para su prevención o, al menos para su control a fin de evitar el mayor número de fallecidos posibles y generar los menos daños posibles en la humanidad. Por tanto, si los distintos actores del sector sanitario hubieran tenido acceso abierto a un sistema de gestión de datos relativos a la salud estructurado tanto en la Administración Pública como en los distintos organismos privados vinculados al sector de la salud, que hubiera permitido una ágil y eficiente aplicación de las herramientas *big data,* tal vez se hubiera podido predecir la epidemia o, al menos tomar medidas con antelación a fin de prevenir el fuerte impacto que ha tenido en la realidad.

Sin embargo, en la actualidad nos encontramos con un sistema deficiente desde la Administración Pública pues no está preparado ni capacitado para adaptarse a los avances continuos tecnológicos[815], que carece a su vez de profesionales cualificados

[815]En este sentido, VALERO TORRIJOS y CERDÁ MESEGUER, "Transparencia, acceso y reutilización de la información ante la transformación digital del…", *op. cit.,* p. 105, señalan que: "Esta dimensión se ha puesto de manifiesto de manera especialmente curda durante la crisis generada por la pandemia del COVID-19, donde la falta de transparencia, la no disponibilidad de datos fiables y actualizados, así como la incapacidad de la Administración Pública de afrontar los desafíos planteados sin la colaboración del sector privado nos obligan a replantear el modelo de gestión". Asimismo, estos autores añaden que: "En definitiva, la necesidad de integrar sistemas de información pertenecientes a diferentes entidades sin una previa tarea de diseño y configuración más allá de las urgencias de la situación generada por la pandemia ha evidenciado la limitación del alcance del modelo puesto en marcha por lo que se refiere a las posibilidades y exigencias de la transparencia, en particular por lo que se refiere a la limitada disponibilidad de datos en formatos abiertos y reutilizables. Se trata de un problema de singular relevancia, ya que el valor añadido se genera, sobre todo, obteniendo datos proporcionados por diversas fuentes que, como sucede con las Administraciones sanitarias, deberían establecer mecanismos de coordinación en la gestión de la información que permitan dan respuestas adecuadas ante situaciones ordinarias y, asimismo, de singular gravedad como la que se ha vivido durante los últimos meses. Así pues, la urgencia y gravedad de la crisis ocasionada por el COVID-19 ha obligado a poner en marcha un modelo de gestión que no ha sido capaz de aprovechar, al menos en su diseño inicial, el potencial de la innovación tecnológica, lo que se ha terminado proyectando en las deficiencias de la puesta a disposición de los datos". VALERO TORRIJOS y CERDÁ MESEGUER, "Transparencia, acceso y reutilización de la información ante la transformación digital del…", *op. cit.,* p. 111-13. Igualmente, PALOMAR OLMEDA, A. y VÁZQUEZ GARRANZO, J., *La protección de la salud: la necesidad de recompension del sistema*

para una explotación adecuada de las tecnológicas *big data* el sector sanitario, aunque se ha de destacar países como China han podido tomar medidas de control del coronavirus gracias a las herramientas *big data* y a la Inteligencia Artificial[816], medidas que como indica Ortega Giménez "son impensable e irrealizables en el resto del mundo"[817], debido a las deficiencias en las infraestructuras de los sistemas sanitarios públicos y privados que impiden un control y gestión de calidad de los datos relativos a la salud a través aplicación de tecnológicas como el *big data* y la IA.

Desde un punto de vista de la sanidad pública, así como de la investigación biomédica y farmacéutica, la COVID-19 ha exigido un proceso de investigación inmediato lo que ha requerido de manera inevitable un acceso y tratamiento de los datos de salud de los ciudadanos por motivos de salud pública e interés general[818]. En principio, si aplicamos lo establecido en el RGPD, tanto los centros sanitarios (públicos y privados), así como los centros de investigación u otros organismos (públicos y privados), que requieran tratar y acceder a los datos de salud a fin de tomar medidas de salud pública e interés general para la población, así como para descubrir la vacuna o el tratamiento para el virus, estarán autorizados sin necesidad de solicitar previamente el consentimiento de los titulares de los datos personales, en especial, aquellos relativos a la salud, puesto como ha sido analizado anteriormente, el RGPD (y por ende, LOPDGDD) establece un límite al derecho de protección de datos así como flexibilidad en el consentimiento del interesado para el tratamiento de datos personales, de datos de

---

(Lecciones aprendidas durante la pandemia y propósito de enmienda), Thomson Reuters Aranzadi, Cizur Menor (Navarra), pp. 337-338, señala que: "Las consideraciones que acaban de hacerse nos sitúan ante un sistema fraccionado, con pocas o escasas referencias comunes que se ha visto sometido a una crisis de nivel o de consecuencias imprevisibles y de intensidad desconocida, ignorada, imprevista y, esencialmente, aguda. Un sistema que, como se ha visto, además no mantenía su nivel de crecimiento ni de incremento económico que le permitiera una subsistencia asistencial razonable y, finalmente y con visión de conjunto, un sistema que no crece ni en nivel infraestructural ni en nivel de personal, sino que mantiene sus esquemas de los últimos tiempos con un mayor nivel de inestabilidad y de rotación en las formas asistenciales que, ciertamente, merma su eficacia".

816 ORTEGA GIMÉNEZ, A., "COVID-19: Un desafío para la protección de datos de carácter personal", *Actualidad Jurídica Iberoamericana,* núm. 12 bis, mayo 2020*,* p. 862.

817 ORTEGA GIMÉNEZ, "COVID-19: Un desafío para la protección de datos…", *op. cit.,* p. 862.

818 Al respecto firma SARRIÓN ESTEVE, J., "La protección de la salud, la vida y la integridad física en tiempos de pandemia en la doctrina constitucional. A propósito del ATC 40/2020 del 30 de abril", *Actualidad Jurídica Iberoamericana,* N.º 14, 2021, pp. 1'28-1'29, que: "No hace falta, por tanto, acudir al tradicional principio de Salud Pública suprema lex esto, como una especie de principio de necesidad o de razón de Estado que pueda justificar o dar cobertura jurídica a aquellas limitaciones que son necesarias para proteger la salud y la vida de las personas, el bienestar y la salud común".

salud y de datos de localización con fines epidemiológicos, salud pública e investigación científica de interés general[819].

En consecuencia, cabría afirmar que la normativa de protección de datos vigente permite al responsable del tratamiento de los datos personales y de los datos de salud adoptar las decisiones y medidas necesarias a efectos de salvaguardar los intereses vitales de los ciudadanos, cumpliendo a su vez con sus obligaciones legales de protección de datos y garantizando los intereses esenciales de la salud pública. Así pues, la normativa de protección de datos contiene reglas que autorizan el tratamiento legítimo de datos personales en situaciones excepcionales como la provocada por el coronavirus, en la que existe una emergencia sanitaria a nivel mundial y, por consiguiente, de interés general[820]. En particular, el derecho fundamental de protección de datos no debe ser un obstáculo que limite la efectividad de las medidas que establezcan las autoridades estatales, en especial las sanitarias, a fin de salvaguardar la salud de los ciudadanos. Igualmente, se ha de subrayar que el art. 3 de la Ley Orgánica

[819] No en vano, ya aclaró la AEPD en su informe *El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios,* mayo de 2020, p.3 que: "Antes de implementar soluciones tecnológicas para enfrentarnos a la COVID-19 es imprescindible que éstas se encuentren integradas en el marco de una estrategia de medidas jurídicas y organizativas realistas, eficaces, basadas en criterios científicos, legítimas y proporcionales. La proporcionalidad se establece mediante un análisis del coste y el beneficio para la sociedad y los derechos y libertades del individuo. El beneficio tendrá que medirse en función de una menor propagación de la infección en términos globales, con la posibilidad de recuperar la libertad de acción, y una protección de la salud de los individuos. Los datos de salud tienen un alto valor, por lo que hay que prevenir que, aprovechando la incertidumbre que provoca una situación de emergencia, se produzcan abusos por parte de terceros que conduzcan a situaciones de pérdida de libertades, discriminación u otros daños en la situación personal de los ciudadanos". Disponible en: https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf (última consulta el 03/02/2021).

[820] En este sentido, DOMÍNGUEZ ÁLVAREZ, J.L., "¿Salud pública o protección de datos personales? Un difícil enfrentamiento en tiempos de Covid-19", *Archivamos: Boletín ACAL,* n.º 116, 2020, p.29, afirma que: "Por tanto, debe entenderse que la protección de datos personales no pretende obstruir o dificultar la realización de aquellos tratamientos de datos personales necesarios para la adopción de medidas eficaces frente a la Covid-19, sino todo lo contrario, lo que se persigue es la correcta aplicación de la regulación de un derecho fundamental, la protección de datos, que recordemos es el instituto básico para la plena eficacia y garantía del conjunto de derechos fundamentales reconocidos constitucionalmente, erigiéndose como piedra angular del Estado social y democrático de Derecho ante la (r)evolución digital. No se trata, en definitiva, de crear impedimentos poniendo como barrera infranqueable e inamovible la protección de datos personales, puesto que ello supondría un terrible error que podría exponer la integridad física de multitud de personas, sino más bien de potenciar la aplicación normal del viejo Estado de Derecho. Por ello, frente a quienes defienden la aplicación excepcional o incluso la inaplicación de la Ley en estos momentos difíciles, quienes analizamos con detenimiento el avance de los derechos de la privacidad abogamos por la más normal de sus aplicaciones, conscientes de que es imposible lograr una garantía cierta de salud pública sin salvaguardar unos elevados estándares de protección de datos personales, y lo más importante, sin la defensa de nuestra privacidad difícilmente podremos afrontar los procesos de reconstrucción social que están por venir en una sociedad que ha hecho de la tecnología y de la datificación masiva la principal fuente de prosperidad y desarrollo socioeconómico".

3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, señala como deber de colaboración de las operadoras basado en la seguridad pública, y en la competencia de las autoridades a efectos de "adoptar las medidas oportunas para el control de los enfermos", en el caso de la COVID-19, estas medidas serán fundamentalmente de control del virus en los pacientes infectados y hospitalizados a efectos de prevenir posibles contagios.

En concreto, el considerando 46 del RGPD[821] señala que, en situaciones como una epidemia, la base jurídica de los tratamientos puede fundamentarse tanto en el interés público como en el interés vital del interesado u otra persona física. Posteriormente, el art. 6.1., letra d) establece que el interés vital es suficiente motivo para un tratamiento lícito de los datos personales (en los que se han de incluir los relativos a la salud) a efectos de proteger a las personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría desde una punto de vista legal la licitud de las medidas adoptadas para tal fin, incluyéndose los datos personales (y de salud) que puedan ser identificables, pues es una de las circunstancias donde no es necesario el consentimiento. Por otro lado, de acuerdo con el artículo 6.3 RGPD, no es necesario que la base del tratamiento pro razón de interés vital haya de ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros aplicables al responsable del tratamiento, pues el citado precepto hace referencia únicamente a los tratamientos regulados para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, ambas referencias en las letras c) y e) del referido art. 6 RGPD[822].

Igualmente, se ha de destacar que para el tratamiento de datos de salud además de una base jurídica (art. 6 RGPD) es necesaria una circunstancia que sirva como excepción a la prohibición de tratamiento de los datos de salud, debido a ello, la AEPD

[821]Considerando (46) RGPD, establece que*:* "El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano".

[822] RODRIGUEZ AYUSO, J.F., "Responsabilidad proactiva de las administraciones públicas ante el Covid-19", *Actualidad Administrativa*, Nº 6, Sección Administración del siglo XXI, Junio 2020, pp. 12-15.

ha emitido un informe[823] dando respuesta jurídica a la licitud del tratamiento de los datos de salud por medio de lo establecido en el artículo 9.2 y art. 32 RGPD a fin de justificar el tratamiento lícito por parte del empleador de los datos de salud correspondientes a sus trabajadores a efectos de prevenir más contagios del virus.

Consecuentemente, de manera similar, consta justificado en el vigente marco normativo de protección de datos el tratamiento lícito de los datos de salud de los ciudadanos por parte de los centros de salud, públicos y privados, así como centros de investigación y otros organismos privados o públicos, cuyo fin sea el de adoptar medidas sanitarias de prevención de contagios del virus, así como de investigar y desarrollar un tratamiento que combata la COVID-19 por medio de la aplicación de herramientas *big data* sin necesidad de recabar previamente el consentimiento de los pacientes, de conformidad con lo establecido en el RGPD[824]. En concreto, el tratamiento lícito de los datos de salud de los pacientes para fines de salud pública e investigación biomédica en aplicación de herramientas *big data* a fin de ayudar a las autoridades sanitarias a la toma de decisiones sobre la adopción de medidas idóneas para hacer frente a la COVID-19, así como a las investigaciones científicas en búsqueda de un tratamiento para la cura del virus sin el consentimiento de los pacientes, constaría justificado de conformidad con los artículos 9.2 y 89 RGPD[825], por otro lado con el art. 6 RGPD[826], así como por el considerando 54 RGPD y, a tenor de la disposición

---

[823] Agencia Española de Protección de Datos, *Informe N/REF: 0017/2020*, de 12 de marzo 2020.

[824] Como indica MARTÍNEZ MARTÍNEZ, R., "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley,* núm. 38, Sección Ciberderecho, marzo 2020, p. 11, que: "Una interpretación sistemática de la normativa sobre protección de datos personales habilitaría en consecuencia, a todos aquellos tratamientos que resulten necesarios para conseguir los objetivos de salud pública. Y así lo ha señalado la AEPD en el *Informe N/REF: 0017/2020*, de 12 de marzo".

[825] De conformidad con los artículos 9.2 y 89 RGPD, se exime de responsabilidad – patrimonial o civil - imputable al responsable o encargo del tratamiento por posible vulneración de derechos fundamentales del titular de los datos, al profesional y centros sanitarios, público o privado al establecer que no es obligatorio por parte de los mismos solicitar el consentimiento del paciente en aquellos casos en los que los datos de salud se destinen para fines de medicina preventiva, por razones de interés público en el ámbito de la salud pública y, cuando el tratamiento es necesario con fines de archivo en interés público, findes de investigación científica o histórica o fines estadísticos.

[826] Al respecto, la Agencia Española de Protección de Datos, *Guía para pacientes y usuarios de la Sanidad*, 2019, p.4, efectuando una interpretación extensiva del art. 6 RGPD, detalla las siguientes finalidades: medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestación de los sistemas y servicios de asistencia sanitaria; por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios o la inspección de reclamaciones de los ciudadanos y; cuando el tratamiento es necesario para proteger

adicional decimoséptima de la LOPDGDD, en especial en el apartado segundo letra b) que autoriza a las autoridades sanitarias e instituciones públicas con competencias de salud pública a llevar estudios sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública y, en el apartado c) habilita al uso de datos con fines de investigación en salud pública sin consentimiento en circunstancias como una epidemia[827].

No obstante, a pesar de que la normativa vigente de protección de datos otorga cierta flexibilidad a los responsables del tratamiento de los datos en caso de necesidad a efectos de garantizar y salvaguardar la salud pública y el interés general, pudiendo existir como afirma MARTÍNEZ MARTÍNEZ las "bases jurídicas razonables para todos los posibles tratamientos"[828], sin embargo, la legislación actual no resulta suficiente a fin de dar respuesta a los problemas generados – y que se puedan generar en un futuro - en materia de protección de datos y del tratamiento de datos de salud sobre todo en lo que respecta a la implantación de técnicas y herramientas de *big data* e incluso de IA[829] de manera directa por parte del responsable de tratamiento de los datos o, indirecta a través de otros organismos públicos o privados, pues como indica ANDREU MARTÍNEZ:

---

intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento, o cuando lo solicite un órgano judicial.

[827] Asimismo, se ha de recordar la normativa española que permite el tratamiento de los datos personales sin el consentimiento: El artículo 26 de la Ley 14/1986, de 25 de abril, General de Sanidad, por el que se atribuye competencias a los servicios sanitarios ante la existencia de un riesgo inminente y extraordinario para la salud, en los siguientes términos; La Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) que habilita para el control de los enfermos; la Ley 33/2011, de 4 de octubre, General de Salud Pública, amén de garantizar el derecho fundamental a la protección de datos en su artículo 9, establece el deber de todas las personas de comunicar datos o circunstancias que pudieran constituir un riesgo o peligro grave para la salud. La colaboración con los servicios competentes resulta esencial para el logro de los objetivos que del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica. Por otra parte, si COVID 19 es una variante de SARS (en español: Síndrome Respiratorio Agudo Grave), figura entre las enfermedades de declaración obligatoria del Anexo I del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la red nacional de vigilancia epidemiológica; El párrafo segundo apartado c) de la disposición adicional decimoséptima sobre tratamientos de datos de salud de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, habilita al uso de datos con fines de investigación en salud pública sin consentimiento en circunstancias como una epidemia. *Vid.* al respecto MARTÍNEZ MARTÍNEZ, "Los tratamientos de datos personales en la crisis…", *op. cit.,* pp.10-11.

[828] MARTÍNEZ MARTÍNEZ, "Los tratamientos de datos personales en la crisis…", *op. cit.,* p.2.

[829] CAÑABETE PÉREZ, J., "Análisis de las aplicaciones para seguimientos de contactos COVID-19 en los países de Asia Oriental a la luz del Reglamento General de Protección de Datos", en AA.VV., *Salud e Inteligencia Artificial desde el derecho privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19),* (Dir. Susana Navas Navarro), Comares, Granada, pp. 217-236.

"[…] en la práctica está siendo problemática la aplicación de estas reglas en el uso de soluciones tecnológicas para la lucha contra la pandemia, lo que ha llevado a declaraciones restrictivas sobre su uso y a una gran confusión sobre su eficacia y seguridad"[830].

Por ello, con mayor motivo, en la presente situación de urgencia sanitaria, donde la COVID-19 está sometiendo a los profesionales de la sanidad e investigadores sanitarios a un proceso de investigación biomédica acelerada, resulte esencial la aplicación de herramientas de *big data* y de la IA, a efectos de agilizar los procesos y resolver problemas actuales[831], tales como, la saturación de líneas de atención o el análisis de pacientes infectados y hospitalizados y, sobre todo, el de hallar el tratamiento que ponga fin a la epidemia y predecir otros efectos adversos y colaterales que pudiera generar la COVID-19[832]. En este sentido, destacar que durante el estado de alama, en el

[830] ANDREU MARTÍNEZ, M.ª B., "Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19", *Actualidad Jurídica Iberoamericana,* núm. 12 bis, mayo 2020, p. 851.

[831] Precisa al respecto MARTÍNEZ MARTÍNEZ, "Los tratamientos de datos personales en la crisis…", *op. cit.,* pp.3-4 que: "existen otras necesidades cuya solución dependerá del tratamiento de datos personales, y del uso de la analítica de datos y de la inteligencia artificial. Se trata de servicios destinados a resolver problemas como, por ejemplo: ▪ Saturación de líneas de atención: a. En este sentido resulta posible definir criterios de asignación de un determinado valor de riesgo a una llamada mediante el cruce de datos sobre el origen de la llamada y los mapas de riesgos o mapas de infección que se hayan generado. b. El uso de *chatbots* sirve para atender al ciudadano y no saturar líneas de atención o 112, cuando se trata de casos leves o dudas principalmente. Pero el análisis de las conversaciones puede ofrecer una analítica de las emociones que asista al gestor de la llamada tanto en el modo de atención como en la identificación de riesgos no revelados por personas cuyas capacidades se encuentren limitadas. c. Habilitar teleconsultas permite que médicos y sanitarios en cuarentena que no pueden atender pacientes presencialmente, lo hagan telemáticamente y sirve, como están demostrando algunos modelos, para liberar recursos atendiendo las patologías más leves▪. Análisis de pacientes infectados y hospitalizados: a. El uso de Historias Clínicas Electrónicas para el seguimiento de pacientes, con técnicas de analítica de datos y metodologías decisionales basadas en inteligencia artificial ayudará hoy o en el futuro a identificar correlaciones relevantes y tomar decisiones sustentadas en datos. Pero ello implica el análisis de un lenguaje muy codificado, como el de la asignación de fármacos, junto con los elementos propios del lenguaje natural presentes en una historia clínica. b. Emplear redes neuronales para detectar coronavirus en imágenes en radiografías y TACS. Las redes neuronales requieren de entrenamiento con los datos que se vayan generando. Sea hoy o en el futuro, el estudio de aspectos como la comorbilidad, o la genética implican la necesidad de procesar historias clínicas de miles de personas. Finalmente, desde la experiencia investigadora puede intuirse la relevancia para el estudio retrospectivo de datos como por ejemplo los de carácter socioeconómico. Y no sólo esto, va a resultar imprescindible la generación de grandes lagos transnacionales de datos de salud anonimizados y de una intensa colaboración público-privada". Igualmente, ANTÓN JUÁREZ, I., "Big Data, Mobile Health aplications y colaboración empresarial: ¿Una combinación efectiva en tiempos de coronavirus?", en AA.VV., *Retos jurídicos ante la crisis del COVID-19*, (Dirs. Elena Atienza Macías y Juan Francisco Rodríguez Ayuso), Wolters Kluwer, Madrid, 2020, pp. 248-350.

[832] De ello nos advierte DOUGLAS HEAVEN, "Por qué la IA nos ayudará…", *op. cit.,* [Documento sin paginación], al indicar que: "Los datos también son esenciales para que la IA ayude a desarrollar tratamientos para una infección. Una técnica para identificar posibles candidatos a fármacos consiste en utilizar algoritmos de diseño generativo, que producen una gran cantidad de posibles

marco jurídico español, se publica la Orden SND/297/297/2020, de 27 de marzo, por la que se encomienda a la Secretaria de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por la COVID-19, donde se regulan posibles soluciones tecnológicas y aplicaciones móviles a efectos de recopilar datos para mejorar la asistencia sanitaria[833]. No obstante, debido a las limitaciones de la normativa vigente, ante tratamientos de grandes volúmenes de categorías especiales de datos personales en la COVID-19 lo que se exige es una seguridad reforzada del tratamiento por medio de implementación de "fuertes medidas destinadas a proteger la privacidad del interesado" [834] en vez de flexibilizar el acceso de los datos de salud por motivos de interés general y de salud pública.

---

resultados. Luego, solo haría que revisarlos para quedarse solo con aquellos que habría que analizar más detalladamente. Esta técnica se puede utilizar para buscar rápidamente a través de millones de estructuras biológicas o moleculares, por ejemplo. SRI International trabaja en una herramienta de IA de este tipo: mediante el aprendizaje profundo genera muchos nuevos candidatos a fármacos que los científicos pueden evaluar para determinar su eficacia. Esto representa una revolución en el descubrimiento de medicamentos, pero aún podrían pasar muchos meses antes de que un candidato prometedor se convierta en un tratamiento viable. En teoría, la IA también se podría usar para predecir la evolución del coronavirus. Inam imagina algoritmos de aprendizaje no supervisado que simulen todas las posibles rutas de la evolución. Entonces se podrían añadir posibles vacunas y ver si los virus mutan para desarrollar resistencia. "Esto permitirá a los virólogos estar unos pasos por delante de los virus y crear vacunas en caso de que ocurra alguna de estas mutaciones catastróficas", explica "No cabe duda de que se trata de una posibilidad fascinante, pero también remota. Todavía no disponemos de suficiente información sobre cómo muta el virus para poder simularlo, por ahora" en su trabajo.

[833] Al respecto, aclara RODRÍGUEZ AYUSO, J. F., "Cumplimiento de la normativa en materia de protección de datos personales en estado de alarma por parte de las Administraciones Públicas", en AA.VV., *Las respuestas del derecho a las crisis de salud pública*, (Dirs. Elena Atienza Macías y Juan Francisco Rodríguez Ayuso), Editorial Dikinson, Madrid, 2020, pp. 102-103 que: "En concreto, establece la necesidad de implementar una aplicación informática que permitirá al usuario la autoevaluación, con base en los síntomas médicos que comunique, de la probabilidad de que esté infectado por el COVID-19, ofrecerle información al respecto y proporcionarle consejos prácticos y recomendaciones a seguir según la evaluación, además de posibilitarle la geolocalización para verificar que se encuentra donde declara estar. Estas funcionalidades serán voluntaria, de modo que todo interesado que quiera someterse a ellas habrá de prestar su consentimiento explícito. El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento la Secretaría General de la Administración Digital (art. 28 RGPD y 33 LOPDGDD). También prevé el desarrollo de un asistente conversacional/chatbot para ser utilizado mediante aplicaciones de mensajería instantánea y que proporcionará información oficial, siendo necesario, igualmente, el consentimiento de quien plantee las dudas o consultas relacionadas con la crisis sanitaria. El responsable del tratamiento será el Ministerio de Sanidad y el encargado del Tratamiento será la Secretaría de Estado de Digitalización e Inteligencia Artificial mediante la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales".

[834] RODRÍGUEZ AYUSO, J.F., *Privacidad y coronavirus: aspectos esenciales,* Editorial Dikinson, Madrid, 2020, p. 162.

En suma, debido a la situación de crisis sanitaria generada por la pandemia de la COVID-19, desde un punto de vista legal es necesario un marco legislativo específico sobre el tratamiento de datos relativos a la salud que en cierto modo autorice a los diferentes actores del sector sanitario cuyo objetivo sea el de subsanar y/o prevenir problemas dimanantes de la COVID-19 aplicando herramientas *big data* o IA, un tratamiento lícito y directo de los datos de salud sin necesidad de requerirse para ello consentimiento de los pacientes, autorización e informe favorable de la autoridad de control de protección de datos o/y del Comité de Ética de la Investigación a efectos de acelerar los procesos de investigación biomédica y de toma de decisiones, pues como indica MARTÍNEZ MARTÍNEZ[835]:

"El Ordenamiento sitúa a las autoridades de protección de datos en una posición constitucional de significativa preeminencia y de juez último en muchos conflictos. Y esto puede producir un efecto paralizante poco conveniente en momentos en los que la protección del derecho fundamental a la vida y a la salud adquiere una relevancia primordial".

De manera que la COVID-19 ha significado un reto para el legislador español (e incluso europeo) que justifica la necesidad urgente de promulgar una ley sectorial sobre protección de datos de salud y *big data* sanitario, pues el Derecho debe tener en cuenta todas las situaciones posibles, es la única forma de constituir un ordenamiento jurídico completo y eficaz, con un mínimo de lagunas legales.

[835] MARTINEZ MARTINEZ, "Los tratamientos de datos personales en la crisis…", *op. cit.,* pp. 2-3, añadiendo que: "Esta situación de facto, que no *de iure*, implica una alta dependencia de todos los sectores respecto de los criterios que eventualmente fije el regulador caso por caso. Y la experiencia demuestra, al menos en nuestro país, algunas pautas que se vienen repitiendo de modo reiterado: 1. Las autoridades de control son reactivas. Esto es, responden a consultas específicas, o conflictos concretos. En raras ocasiones abordan cuestiones generales salvo en *guidelines*. 2. Cuando se definen criterios en sus guías —-elaboradas ya sea mediante recursos propios, ya mediante el recurso a la subcontratación de expertos--, no existe una consulta o debate público en la conformación de sus criterios. Esto afecta seriamente tanto a la calidad del resultado como la viabilidad de la implementación de recomendaciones muchas veces alejadas de la realidad material.3. El enfoque del regulador casi siempre opera desde el derecho fundamental a la protección de datos a la realidad, y casi nunca a la inversa. Y ello, no significa tan solo que se pierdan de vista elementos cruciales en los tratamientos de datos personales, sino también que se obvie en más de una ocasión la necesaria ponderación de derechos".

CONCLUSIONES

PRIMERA

Es un hecho evidente que la escritura, en especial, los textos clásicos y artículos científicos han sido y son fuentes principales de conocimiento e información y que, en parte, gracias a ellos la humanidad ha ido evolucionando a lo largo de la Historia.

Sin embargo, en la nueva era digital y con la conectividad global a través de las nuevas tecnologías y del Internet de las Cosas, los datos personales se han convertido también en grandes fuentes de conocimiento e información, en especial los datos de salud, pues consta acreditado que si los grandes volúmenes de datos sanitarios son recogidos, procesados y analizados por medio de la aplicación de herramientas *big data* de los mismos se puede sustraer información y conocimiento veraz y de gran valor en el ámbito sanitario y de la investigación biomédica y farmacéutica, entre otros.

SEGUNDA

En concreto, los datos sanitarios, tras ser analizados por medio de algoritmos con la aplicación de tecnologías *big data*, aportan conocimiento e información de gran valor que coopera a que el sector sanitario evolucione de manera eficaz y proactiva adelantándose a las enfermedades, encaminándose hacía una medicina predictiva, precisa, personalizada y de calidad. De igual modo, el *big data* gestiona a gran velocidad grandes volúmenes de datos, incluso no estructurados y, asimismo, permite crear modelos predictivos que sirven como base a los diferentes actores sanitarios en la toma de decisiones. En síntesis, el *big data* ofrece ventajas y beneficios en el sector de la asistencia sanitaria y de la investigación biomédica, entre las que cabe destacar: el seguimiento de pacientes crónicos, la investigación genómicas, mejora de atención personalizada, operativa clínica, medicina personalizada, autopsias virtuales, monitorización remota de pacientes, mejoras en los procesos médicos y, más recientemente está siendo de gran utilidad en la investigaciones llevadas a cabo para combatir la crisis de la COVID-19, entre otros.

TERCERA

Ahora bien, el surgimiento de las tecnologías ha generado inevitablemente una constante tensión entre las posibilidades de innovación que ofrece y las garantías jurídicas, en particular la normativa sobre protección de datos personales. En concreto, el escenario que existía previamente a las tecnologías y al Internet de las Cosas, tanto en la normativa jurídica como en las sentencias de los tribunales europeos y españoles, se basaba fundamentalmente en salvaguardar de manera radical el derecho de protección de datos y la intimidad de los ciudadanos, hasta el punto de prohibir o, al menos, limitar de manera drástica el uso de las tecnologías en caso de vulneración de la vida privada de las personas. El artículo 18.4 de nuestra Constitución es un ejemplo claro de este planteamiento al encargar al legislador que limitara el uso de la informática.

Sin embargo, conforme han ido evolucionado las tecnologías en la sociedad también han ido adaptándose el marco jurídico y, en particular, la normativa sobre protección de datos personales, siendo a su vez más consciente el legislador de sus beneficios sociales y de interés general, en especial de las herramientas *big data* en el sector sanitario y del valor de los datos de salud en la esfera de la medicina predictiva, de la investigación y de la asistencia sanitaria, como fuente de información y conocimiento de interés público. En este sentido, cabría afirmar que se ha producido de manera progresiva un cambio legislativo e interpretativo por parte de los tribunales en relación con el derecho de protección de datos, hacía una perspectiva jurídica más flexible y abierta a través de la regulación de nuevos principios y garantías.

CUARTA

Actualmente, en la normativa vigente de protección de datos tanto el legislador europeo como español han sido en cierto modo conscientes del importante valor de los datos de salud a pesar de que nos encontramos ante datos de especial protección por su contenido sensible, pues pertenecen a una de las esferas más íntimas de una persona: su salud. Así, la normativa actual, tanto estatal como europea, autoriza el tratamiento y acceso a los datos de salud de manera excepcional sin ser necesario el consentimiento del paciente en aquellas circunstancias de interés general y salud pública.

QUINTA

A pesar de que la vigente normativa europea de protección de datos le otorga una especial regulación a los datos de salud conforme a ciertas garantías, sin embargo, el RGPD, aun cuando establece ciertas singularidades para el tratamiento de datos en el ámbito de la salud, sin embargo utiliza conceptos de cierta ambigüedad y, asimismo, se basa en el establecimiento de principios generales cuya aplicación práctica en el caso concreto puede resultar problemática, en particular en el ámbito sanitario. Además, esta regulación europea, aun cuando establece concreciones y adaptaciones para el ámbito sanitario, deja en manos de los Estados la regulación de las concretas condiciones de licitud del tratamiento de estos datos más allá de la exigencia del consentimiento, lo que sin duda resulta especialmente problemático en el caso de España por cuanto, al margen de la previsión específica de la disposición adicional 17 LOPDPGDD, la mayor parte de las disposiciones específicas en el ámbito sanitario y de la salud pública son anteriores al propio RGPD.

En suma, la vigente normativa de protección de datos entremezcla la regulación de los datos personales en general con la regulación de los datos de salud en particular, bajo el intento de otorgar a estos un tratamiento lícito especial, generando tanto en los profesionales de la sanidad, como al resto de afectados por la normativa incluyendo a los propios titulares, confusiones, incertidumbre y, en consecuencia, inseguridad jurídica. Más aún, por lo que se refiere a la legislación estatal en materia sanitaria, al ser anterior al RGPD existe una cierta descoordinación que en última instancia genera incertidumbres y disfunciones a la hora de intentar poner en marcha proyectos e iniciativas que se basan en el uso de las tecnologías disruptivas.

Por ello, en el presente trabajo se defiende la necesidad de una ley sectorial sobre protección de datos de salud y del *big data* sanitario, como herramienta eficaz y eficiente para poner en valor todo el conocimiento que podría obtenerse a partir de los datos sanitarios. Así, por un lado, se ha de regular la protección de datos de salud de manera específica a fin de garantizar un tratamiento lícito de los datos de salud salvaguardando a su vez el derecho de protección de datos del titular. Por otro lado, ha de contemplar en su articulado las medidas y garantías que deben respetar los desarrolladores de proyectos de salud pública e investigación biomédica y farmacéutica

de interés general que apliquen tecnologías *big data*, que deberán implantar desde el diseño del proyecto a los efectos de afianzar la confianza de los titulares de los datos y asegurar el respeto de sus derechos.

SEXTA

En síntesis, como resultado del presente trabajo, se obtiene principalmente desde una perspectiva práctica el desarrollo del contenido mínimo de la citada ley sectorial donde se precisan las bases jurídicas esenciales para el tratamiento y protección de los datos de salud y de las medidas para una aplicación lícita de las herramientas *big data* en proyectos de investigación biomédica de interés general y de salud pública, a modo de propuesta de futuro para el legislador europeo y estatal. Todo ello, con la finalidad de solventar y dar respuesta desde una perspectiva jurídico-sanitaria a los problemas que se plantean (o pueden plantearse en un futuro cercano) con la actual normativa de protección de datos al resultar la misma insuficiente y confusa cuando se trata de supuestos de protección de datos de salud y del tratamiento de los mismos a través de la aplicación de tecnológicas, como el big data o, más recientemente, la Inteligencia Artificial.

SÉPTIMA

En concreto, en el presente trabajo se plantea que la regulación propuesta debería partir de una definición precisa sobre los datos relativos a la salud, así como de la expresión "interés público" e "investigación científica" a los efectos de proporcionar una normativa transparente, concisa y clara en lo que a su contenido respecta.

De igual modo, se considera apropiado que la ciada ley sectorial regule de manera específica aquellos principios fundamentales del tratamiento de datos de salud en relación con el interesado. Por otro lado, se estima como materia esencial a regular por parte de la ley específica la del consentimiento del interesado y legitimación para el tratamiento de datos de salud, donde se ha de perfilar las posibles situaciones de tratamiento lícito de los datos sin necesidad del consentimiento del paciente, haciendo especial referencia a los supuestos de investigación con muestras biológicas y

estableciendo asimismo como obligatorio el consentimiento del paciente, se apliquen o no técnicas de anonimización. Asimismo, se estima conveniente que la ley sectorial regule el tratamiento de datos de salud de personas fallecidas y de menores de edad, tomando como base lo establecido en la normativa vigente de protección de datos con las oportunas adaptaciones.

Por otro lado, se concreta que la ley sectorial recopile de manera taxativa entre su articulado medidas y garantías encaminadas a reforzar las garantías del tratamiento lícito de los datos sanitarios, destacándose, en otras, las siguientes: (1) la utilización de datos seudonimizados, datos anonimizados y datos personales (identificativos) en la investigación biomédica; (2) las situaciones en las que es necesaria la autorización de la autoridad de control para la realización de estudios epidemiológicos; (3) situaciones de obligado cumplimiento para los supuestos de divulgación de las publicaciones científicas donde se han manejado datos de salud; (4) en relación a la transferencias internacionales de datos de salud se estima necesario que la ley sectorial prevea distintas situaciones en las que se permita transferir datos de salud sin necesidad de que obre previamente consentimiento del interesado; (5) los procedimientos de ejercicio de los derechos propios vinculados a la protección de datos de carácter personal y circunstancias que excepcionen su ejercicio, haciéndose especial mención a la figura del Ministerio Fiscal en los procedimientos judiciales; (6) situaciones lícitas de acceso a la historia clínica y a la receta electrónica tanto por los distintos actores de la sanidad como por terceros, tanto de organismos públicos como privados; (7) medidas de seguridad haciéndose especial referencia a la instalación de cámaras de videovigilancia; (8) la figura del delegado de protección en organismos sanitarios públicos o privados; (9) la elaboración de la evaluación de impacto en la Protección de Datos por parte entidades sanitarias; (10) la regulación del Registro central de datos de salud y Registros de efectos adversos y protección de datos de salud; (11) igualmente se considera oportuno que, entre otros extremos, la ley regule el modo de acceso a la carpeta personal; (12) la regulación del derecho de información para el tratamiento de datos de salud del paciente; (13) el deber de secreto profesional de los responsables y encargados del tratamiento de datos de salud, así como sus excepciones (secreto compartido y secreto divulgado); (14) el acceso por parte de las autoridades de control a los datos de salud y el acceso a los datos de salud por parte del Ministerio Fiscal y de los defensores

del pueblo; (15) por último, se estima conveniente una regulación específica de las funciones de los Comités de Ética en el ámbito sanitario público y privado.

OCTAVA

Asimismo, resulta necesario que ley sectorial de datos de salud contenga una parte especial destinada a las medidas y garantías de protección de datos para los proyectos que se desarrollen en el ámbito de la investigación biomédica y de la asistencia sanitaria que apliquen herramientas *big data*. Por ende, se estima conveniente que en esta parte especial fundamentalmente se regulen:

Por un lado, las cuestiones legales de los tratamientos de *big data*, tales como: la obligación por parte de responsable y el encargado del tratamiento de ofrecer previamente al tratamiento de sus datos de salud una información clara, transparente y concisa a los interesados, así como aquellas situaciones en las que es obligado el consentimiento, los derechos de los que los interesados son titulares, particularmente en los tratamientos de *big data* y otras cuestiones relevantes, tales como el uso y reutilización de los datos disociados o el plazo de conservación de los datos de salud, entre otras que se desarrollarán a continuación.

Por otro lado, las garantías procedimentales, estableciendo los principios y aspectos fundamentales en los procedimientos de tratamiento de *big data*. Por último, resulta de interés que se contemplen las cuestiones técnicas y de seguridad donde se establezcan garantías a efectos de minimizar el alcance de los riesgos y de las amenazas que puedan darse particularmente en los procesos de anonimización, tal y como sucede con la reidentificación de los titulares de los datos o, asimismo, el uso del *cloud computing*, donde se han de aplicar mayores medidas de seguridad adaptadas a la singularidad de este tipo de supuestos.

NOVENA

Otro de los resultados que se desprende del presente trabajo es el estudio de los límites y riesgos que imposibilitan una aplicación correcta e íntegra de las herramientas *big data* en los proyectos reales de investigación biomédica o farmacéutica y de desarrollo e innovación (I+D+i). En estos casos, la necesidad de capturar, almacenar y analizar la totalidad de los datos disponibles y registrados a efectos de rentabilizar al máximo las herramientas de *big data* en la sanidad del futuro determinan que los actuales sistemas de organización en el sector sanitario sean inadecuados, sin que puedan obviarse los riesgos legales actuales y, asimismo, los limites dimanantes del propio mercado.

De igual modo, otra de las consecuencias es que, desde una perspectiva ético-jurídica, la aplicación de las herramientas *big data* y de la IA en el sector sanitario conlleva implícitos riegos relevantes. En concreto puede implicar desigual acceso a las TIC por parte de aquellos colectivos vulnerables con menos recursos económicos, un control excesivo por parte de los agentes del sector sanitario, públicos o privados, sobre los pacientes que, en última instancia, podrían afectar a su pérdida de autonomía y libertad, lo que conllevaría en consecuencia, un mal uso de la información y conocimiento sustraído del *big data* y de la IA. Por tanto, se podrían generar desequilibrios entre las empresas y pacientes, estereotipos sociales de exclusión social a causa de la denominada *dictadura de datos*, así como un exceso de *biomonitorización* en la medicina preventiva y personalizada lo que puede conllevar una pérdida del poder de decisión del paciente. En todo caso, hemos de entender que las herramientas *big data* y la IA, son medios e instrumentos que ayudan y colaboran con los facultativos sanitarios e investigadores, pero que en ningún concepto los sustituyen.

DÉCIMA

En definitiva, no parece que exista duda acerca del papel que corresponde actualmente a los datos de salud en tanto grandes fuentes de información y conocimiento inestimable tanto en el sector sanitario como de la investigación biomédica pudiendo generar, en consecuencia, una mejora del bienestar de la población

y la consecución de relevantes fines de interés público. En este sentido, no es de extrañar afirmar que en un futuro próximo se conviertan en los "libros" del mañana como nueva fuente de conocimiento en la humanidad, por lo que limitar injustificadamente desde una perspectiva jurídica el acceso y tratamiento de los datos de salud a los diferentes actores sanitarios supondría obstaculizar la evolución del conocimiento científico - sanitario y, por ende, de la humanidad.

Por ello, la normativa sectorial que se propone en el presente trabajo se defiende fundamentalmente la idea de permitir desde un punto de vista jurídico tanto a los a los centros sanitario (públicos y privados) así como a los distintos actores de la sanidad y de la investigación, un acceso y tratamiento lícito de los datos de salud de los pacientes, sin necesidad de que obre previamente su consentimiento, siempre y cuando se adopten las garantías adecuadas, sea para fines de salud pública y proyectos de investigación biomédica de interés general que apliquen herramientas *big data* u otras tecnologías.

UNDÉCIMA

Por último, cabe plantearse la posibilidad de que la ley sectorial de protección de datos de salud y herramientas *big data* regule otros usos secundarios de los datos de salud teniendo en cuenta el interés público que subyace de los mismos y su potencial valor económico. A este respecto, cabría considerar que a través de los mismos se pudiera obtener un posible ingreso patrimonial (*v.gr.* tasa) que permita financiar los servicios públicos, de tal modo que se deja entreabierta la propuesta de otra vía de financiación por parte de la Administración Pública, lo que le va a permitir al Estado acceder a mejores soluciones y más avanzadas en aquellos proyectos y servicios públicos destinados a satisfacer los intereses generales.

En todo caso, se ha de tener como referencia jurídica fundamentalmente, entre otras, por un lado, la Propuesta de Reglamento del Parlamento Europeo y del el Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos) y la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, donde se establece de manera concreta la posibilidad de que las Administraciones Públicas

puedan cobrar tasas por permitir la reutilización de categorías de datos (Considerando 20 y art. 6). Y, por otro lado, el Reglamento 2018/1807 de aplicación también a las autoridades y organismos de Derecho público (Considerando 13), así como la normativa vigente (europea y estatal) de protección de datos personales, todo ello a los efectos de abordar un planteamiento integrador y armonizador de la normativa vigente teniendo en cuenta las reformas inmediatas que se puedan aprobar a corto y medio plazo.

BIBLIOGRAFÍA

AA.VV., "¿Cómo diagnosticar enfermedades a través de la forma del rostro?", *Salud Digital*. Disponible en: https://www.consalud.es/saludigital/94/como-diagnosticar-enfermedadesa- traves-de-la-forma-del-rostro_45763_102.html (Último acceso 11/11/20).

AA.VV., "Analytics: The widening divide: How companies are achieving competitive advantage through analytics", *IBM Institute for Business Value* and *MIT Sloan Management Review*, 2011 [Documento sin paginación]. Documento disponible en: http://www-935.ibm.com/ services/us/gbs/ thoughtleadership/ibv-analytics-widening-divide.html

AA.VV., *Guía Rápida de Protección de Datos. Aplicación del RGPD,* Francis Lefebvre, Madrid, 2018.

AA.VV., *La Ética y el Derecho ante la biomedicina del futuro,* Universidad de Deusto, Bilbao, 2006.

AA.VV., *Retos jurídicos ante la crisis del COVID-19*, (Dirs. Elena Atienza Macías y Juan Francisco Rodríguez Ayuso), Wolters Kluwer, Madrid, 2020.

ABELLÁN- GARCÍA SÁNCHEZ, F., "El consentimiento informado, la intimidad y la confidencialidad de los datos del paciente en los ensayos clínicos: con especial referencia a las obligaciones en materia de protección de datos", en AA.VV., *Ensayos clínicos en España: aspectos científicos, bioéticos y jurídicos,* (Coords. J. Sánchez Caro y F. Abellán-García Sánchez), Comares, Granada, 2006, pp. 87-116.

ABERASTURI GORRIÑO, U., *La protección de datos en la sanidad*, Thomson Reutores – Aranzdi, Cizur Menor, 2013.

ACED FÉLEZ, E., "Protección de Datos y Transformación Digital en Sanidad", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 39-39.

ALBALADEJO, M., *Derecho Civil. I. Introducción y Parte General*, Edisofer, Madrid, 2009.

ALFONSECA MORENO, M., "La máquina de Turing", *Revista de didáctica de las matemáticas,* núm. 43-44, 2000, pp. 165-168.

ALONSO DE MAGDALENO, M.I. y GARCÍA GARCÍA, J., "Crowdsourcing: la descentralización del conocimiento y su impacto en los modelos productivos y de negocio", *Cuadernos de Gestión,* Vol. 14, núm. 2, 2014, pp. 33-49. Documento disponible en: http://www.redalyc.org/articulo.oa?id=274332765002 (última consulta 12/08/18).

ÁLVAREZ -CIENFUEGOS SUÁREZ, J.M., *La defensa de la Intimidad de los Ciudadanos y la Tecnología Informática,* Aranzadi, Navarra, 1990.

ÁLVAREZ RIGAUDIAS, C., "Transferencia de Datos Personales a terceros países y organizaciones internacionales (Arts. 44-50 RGPD. Arts. 40-43 y Disposición adicional quinta y decimotercera LOPGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 279-287.

ÁLVAREZ RIGAUDIAS, C., "Tratamiento de datos de salud", en AA.VV., en *Reglamento General de Protección de Datos. Hacía un nuevo modelo europeo de privacidad* (Dir. J. L. Piñar Mañas), Editorial Reus, Madrid, 2016, pp. 171-186.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M., "La aplicación de la firma electrónica y la protección de datos de la salud", *Actualidad Informática Aranzadi,* núm. 39, 2001, pp. 3-3.

AMAGO, F., *Diccionario LIB Innovación,* LID, Madrid, 2010.

ANDERSON, CH., "The end of theory: the data deluge makes the scientific metohd obsolete", *Wired,* 2008 [Documento sin paginación]. Documento disponible en: https://www.wired.com/2008/06/pb-theory/ (última consulta 17/01/18).

ANDREU MARTÍNEZ, Mª B. y PLANA ARNALDOS, Mª C., "El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica",* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 131-151.

ANDREU MARTÍNEZ, Mª. B., "Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19", *Actualidad Jurídica Iberoamericana,* núm. 12 bis, mayo 2020, pp. 848-859.

ANDREU MARTÍNEZ, Mª.B., PARDO LÓPEZ, Mª M. y ALARCÓN SEVILLA, V., "Hacia un nuevo uso de los datos de salud", *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia,* Vol. 3, núm. 1, 2017, pp. 161-171.

ANTÓN JUÁREZ, I., "Big Data, Mobile Health aplications y colaboración empresarial: ¿Una combinación efectiva en tiempos de coronavirus?", en AA.VV., *Retos jurídicos ante la crisis del COVID-19*, (Dirs. Elena Atienza Macías y Juan Francisco Rodríguez Ayuso), Wolters Kluwer, Madrid, 2020, pp. 343-363.

APARICIO SALOM, J., "Derechos del interesado (Arts. 12-19 RGPD. Arts. 11-16 LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Ed. Wolters Kluwer, Madrid, 2019, pp. 345-385.

APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Persona*, Aranzadi, Cizur Menor, 2002.

APARICIO SALOM, J., *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal*, Ed. Aranzadi, Cizur Menor, 2002.

ARIAS POU, M., "Definiciones a efectos del Reglamento General de Protección de datos", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, pp. 115-134.

ARIAS POU, M., "Definiciones a efectos del Reglamento General de Protección de datos", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, pp. 115-134.

ARROYO YANES, L.M., "El derecho de Autodeterminación Informativa frente a las Administraciones Públicas (Comentario a la STC 254/1993, de 20 de julio)", *Revista Andaluza de Administración Pública,* núm. 16, 1993, págs. 119 y ss.

ASHTON, K., "That `Internet of ThinGC´ Thing", *RFID Journal,* 2009*,* [Documento sin paginación]. Disponible en: http://www.rfidjournal.com/articles/view?4986 (última consulta 12/03/18).

AUSTIN, T. y ANDREU MARTÍNEZ, Mª. B., "Ética y protección de datos de salud en contexto de pandemia. Una referencia especial al caso de las aplicaciones de rastreo de contactos", *Enrahonar: an international journal of theoretical and practical reason*, núm. 65, 2020, pp. 47-56.

AUSTÍN, T., ANDREU MARTÍNEZ, B., VALERO TORRIJOS, J. y CAYÓN DE LAS CUEVAS, J., "Diez consideraciones ético-jurídicas en relación con la reutilización y big data en el ámbito sanitario", *Bioderecho.es,* N.º 12, 2020, pp. 1-4.

BALAGUERÓ, T., "Del Dataware House al Data Lake", *Deusto Formación. Planeta Formación Universitaria,* enero 2018, [Documento sin paginación]. Documento disponible en: https://www.deustoformacion.com/blog/gestion-empresas/dataware-house-data-lake (última consulta 25/02/18).

BALAGUERÓ, T., "Del Dataware House al Data Lake", *Deusto Formación. Planeta Formación Universitaria,* enero 2018, [Documento sin paginación]. Documento disponible en: https://www.deustoformacion.com/blog/gestion-empresas/dataware-house-data-lake (última consulta 25/02/18).

BALAGUERÓ, T., "Qué es la minería de datos en *Big Data*. *Deusto Formación",* noviembre 2017, [Documento sin paginación]. Documento disponible en https://www.deustoformacion.com/blog/gestion-empresas/que-es-mineria-datos-big-data (última consulta 02/04/18).

BALLBÉ MALLOL, M., "Concepto de dominio público", *Revista Jurídica de Cataluña,* núm. 5, 1945, pp. 25 y ss.

BALLISTA CASTILEJOS, A., "Conocimientos de los profesionales acerda de la ley de la protección de datos", en AA.VV., *Intervención e investigación en contextos clínicos y de la salud,* (Comps. M. M. Moreno Jurado, M.M. Simón Márquez, A.B. Barragán Martín, A. Martos Martínez et al.)*,* ASUNIVEP, Madrid, 2019, pp. 323-330.

BAROCAS, S.; SELBST, A. D., "*Big Data*'s Disparate Impact", *104 California Law Review 671,* 2016, [Documento sin paginación]. Documento disponible en: https://ssrn.com/abstract=2477899 (última consulta 04/19/20).

BARRAL, I., "Datos relativos a la salud e historia clínica: la confidencialidad de los datos medicos", en AA.VV. *Proteccion de datos personales en la Sociedad de la información y la vigilancia,* (Coord. M. R. Llácer Matacás), La Ley, Madrid, 2011, pp. 352-368.

BARRANCO FRAGOSO, R., "¿Qué es Big Data? Todos formamos parte de ese gran crecimiento de datos", *IBM*, junio 2012, [Documento sin paginación]. Documento disponible en: https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/ (última consulta 03/06/18).

BARRERA, L., GONZÁLEZ F., VALENZUELA, J. y CEDEÑO, M., *Impacto de las TICS en la Salud,* [Documento sin paginación]. Disponible en: http://www.neopuertomontt.com/InformaticaMedica/lasticsenelsectorsalud.pdf (última consulta 02/15/18).

BARRERA, L., GONZÁLEZ F., VALENZUELA, J. y CEDEÑO, M.: *Impacto de las TICS en la Salud* [Documento sin paginación]. Disponible en: http://www.neopuertomontt.com/InformaticaMedica/lasticsenelsectorsalud.pdf (última consulta 10/01/20).

BENITO TOVAR, M. A. y ÁLVAREZ SALAZAR, E., "Plataforma centralizada de logos del Ib-Salut", *Revista de la Sociedad Española de Informática y Salud,* núm.122 2017, pp. 18-21.

BERMEJO FRAILE, B., *Epidemiología clínica aplicada a la toma de decisiones en medicina,* Gobierno de Navarra, 2001.

BERROCAL LANZAROT, A. I., "La protección de datos relativos a la salud y la historia clínica", *Revista de la Escuela de Medicina Legal*, núm. 18, Octubre, 2011, pp. 11-44. Disponible en: http://webs.ucm.es/centros/cont/ descargas/documento30950.pdf (última consulta 12/12/20).

BIZER, CH., HEATH, T. and BERNERS-LEE, T., "Linked Data - The Story So Far", *Tomheath,* 2009, [DOCUMENTO SIN PAGINACIÓN]. Documento disponible en: http://tomheath.com/papers/bizer-heath-berners-lee-ijswis-linked-data.pdf (última consulta 22/01/18).

BOYD, D., "Critical questions for *Big Data*", *Journal Information, Communication & Society,* vol. 15, núm. 5, 2012, pp. 663-679. Documento disponible en https://people.cs.kuleuven.be/~bettina.berendt/teaching/ViennaDH15/boyd_crawford_2012.pdf (última consulta 11/01/18).

BRABHAM, D.C., "Crowdsourcing as a Model for Problem Soving: An Introduction and Cases", *Convergence,* Sage Publications, Vol. 14, núm. 1, 2008, p.76. Documento disponible en: http://sistemas-humano-computacionais.wdfiles.com/local--files/capitulo%3Aredes-sociais/Crowdsourcing-Problem-solving.pdf (última consulta 08/08/18).

BRENT, D.R., "En la era de la información: información, tecnología y estudio del comportamiento", *Documentación De Las Ciencias De La Información*, vol. 13, 1980, pp. 53-72.

BRITO IZQUIERDO, N., "Recursos, responsabilidad y sanciones (Arts. 77-84 RGPD. Arts. 63-78 LOPDGDD)" en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 663-713.

BRUECKNER, R., "Where Dig *Big Data* Come From", *InsideBIGDATA*, núm. 3, febrero 2013, [Documento sin paginación]. Disponible en: https://insidebigdata.com/2013/02/03/where-did-big-data-come-from/ (última consulta 02/07/18).

BRYANT, R.E., KATZ, R.H. and LAZOWSKA, E.D., "Big-Data Computing: Creating revolutionary breakthroughs in commerce, science, and society: A white paper prepared for the Computing Community Consortium committee of the Computing Research Association", *CCC-Led White Papers,* 2008, [Documento sin paginación]. Documento disponible en: http://cra.org/ccc/resources/ccc-led-whitepapers/ (última consulta 16/01/18).

CÁLIZ CÁLIZ, R., et al, *El derecho a la protección de datos en la historia clínica y la receta electronica,* Aranzadi Thomson Reuters, Navarra, 2009.

CALVO GALLEGO, F.J., "Test genéticos y vigilancia de la salud del trabajador", *Revista Digital de Seguridad y Salud en el Trabajo,* núm. 1, 2008, pp. 1-18.

CANTERO RIVAS, R., "La historia clínica: naturaleza y regimen jurídico", AA.VV., *El derecho a la protección de datos en la historia clínica y la receta electrónica* (Coord., R. Cáliz Cáliz), 2009, pp. 201-218.

CAÑABETE PÉREZ, J., "Análisis de las aplicaciones para seguimientos de contactos COVID-19 en los países de Asia Oriental a la luz del Reglamento General de Protección de Datos", en AA.VV., *Salud e Inteligencia Artificial desde el derecho privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19),* (Dir. Susana Navas Navarro), Comares, Granada, pp. 203-237.

CARRILLO LÓPEZ, M., "Los ámbitos del derecho a la intimidad en la sociedad de la comunicación", en AA.VV., *El derecho a la privacidad en el nuevo entorno tecnológico,* XX Jornadas de la Asociación de Letrados del Tribunal Constitucional, Ed. Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pp. 11-70.

CASAS BAAMONDE, M.E., "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal Constitucional", *20 años de protección de datos en España. Agencia Española de Protección de datos,* 2015, pp. 91-126. Documento disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5156606 (última consulta 12/11/18).

CASTELLS M., *La Sociedad Red. Volumen I. La era de la información: economía, Sociedad y cultura*, Alianza Editorial, Madrid, 1997.

CERDÁ MESEGUER, J.I., "La proteccion de datos santiarios en la administración de justiciar" en AA.VV., *Era digital, Sociedad y Derecho,* (Coord. Arrabal Platero y otros), Tirant lo Blanch, Valencia, pp. 559-568.

CERVERA NAVAS, L., "El nuevo modelo europeo de protección de datos de carácter personal", EN AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 71-77.

CÓRDOBA GARCÍA, F., "La privacidad genética: Concepto, fundamentos y consecuencias", en AA.VV., *Nuevos conflictos sociales. El papel de la privacidad,* (Coords. E. Anarte Borrado, F. Moreno Moreno y C.R. García Ruíz), Ed. Iustel, 2015, Madrid, pp. 21-46.

CORRAL SASTRE, A., "El régimen sancionador en materia de protección de datos en el Reglamento general de la Unión Europea", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, pp. 571-586.

COSTA HERNANDIS, R., "Responsabilidad del responsable del tratamiento (Art. 24 RGPD. Art. 28 LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 409-419.

COTINO HUESO, L. "La regulación del uso de medios electrónicos en la difusión activa de información pública y el ejercicio del derecho de acceso", en AA.VV., *La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho,* (Dir. I. Martín), Instituto Nacional de Administración Pública, Madrid, 2017, pp. 397-432.

COTINO HUESO, L., "*Big data* e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata. Revista Internacional de Éticas Aplicadas*, núm. 24, 2017, pp. 131-150.

COTINO HUESO, L., "Inteligencia artificial, *big data* y aplicaciones contra el Covid y la privacidad y protección de datos", *Internet, Derecho y Política*, núm. 31, 2020, pp. 1-17.

COX, M. and ELLSWORTH, D., "Application controlled demand paging for out of core visualization", *ProceedinGC of the 8th IEEE Visualization ´97 Conference*, 1997, pp. 235 - 244. Documento disponible en https://www.evl.uic.edu/cavern/rg/20040525_renambot/Viz/parallel_volviz/paging_outofcore_viz97.pdf (última consulta febrero 2018).

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

CUETO PÉREZ, M., *Responsabilidad de la Administracion en la Asistencia Sanitaria*, Ed. Tirant Monografías, Valencia, 1997.

CUKIER, K., "Data, data everywhere", *The Economist,* febrero 2010, [Documento sin paginación]. Documento disponible en: http://www.economist.com/node/15557443 (última consulta 17/01/18).

DA CRUZ, F., "Columbia University Computing History", *German Hollerith,* 2011, [Documento sin paginación]. Disponible en: http://www.columbia.edu/cu/computinghistory/hollerith.html(última consulta 04/11/17).

DAVARA DAVARA, M.A., *La protección de datos en Europa: principios, derechos y procedimientos*, Ed. Universidad de Comillas, Madrid, 1998.

DAVENPORT, T. and PRUSAK, L., "Diferencia Entre Dato, Información y Conocimiento", *Gestión del conocimiento,* 1999, [Documento sin paginación]. Documento disponible en: http://www.gestiondelconocimiento.com/conceptos_diferenciaentredato.htm (última consulta 12/03/17).

DE LA SERNA BILBAO, M. N.; FONSECA FERRADIS, F., "El acceso a la historia clínica; el alcance del derecho", en AA.VV., *Los retos del Estado y la Administracion del siglo XXI: libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo,* (Coords. L.J. Parejo Alonso y J. Vida Fernández) Vol. 2, Tomo 2, Tirant lo Blanch, Valencia, 2017, pp. 2271-2320.

DE LECUONA RAMÍREZ, I., "El valor y el precio de los datos personales de salud en la Sociedad digital", en AA.VV., *El cuerpo diseminado: estatuto, uso y disposicion de los biomaterials humano,* (Coords. R. García Manrique y M.E. Beltrás Pedreira), Thomson Reuters-Aranzadi, Cizur Menor, 2018, pp. 171-19.

DE LORZA GONZÁLEZ, J.R., "Modificaciones al régimen de protección de datos de carácter personal: el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la nueva Ley Orgánica de protección de Datos de Carácter Personal (SP/DOCT/70071)", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, pp. 719-732.

DE MIGUEL BERIAIN, I. y DE LORENZO Y APARICI, R., *Claves prácticas sanitarias. Datos genéticos y relativos a la salud,* Francis Lefebvre, Madrid, 2020.

DE MIGUEL SÁNCHEZ, N., "Datos de carácter personal relativos a la salud: una obligada remisión a la normativa del sector sanitario", en AA.VV., *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, (Dir. A. Troncoso Reigada), Civitas, Madrid, 2010, pp. 708-734.

DE MIGUEL SÁNCHEZ, N., "Investigación y protección de datos de carácter personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *Revista Española de Protección de Datos,* núm. 3, 2006, pp. 143-201.

DE MIGUEL SÁNCHEZ, N., *Secreto médico, confidencialidad e información sanitaria,* Ed. Marcial Pons, Madrid.

DE MIGUEL SÁNCHEZ, N., *Tratamiento de datos personales en el ámbito sanitario: intimidad "versus" interés público,* Ed. Tirant lo blanch, Valencia, 2004.

DE MONTALVO JÄÄSKELAÄINEN, F., "Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del *Big Data"*, *Revista de Derecho Político,* núm. 106, septiembre-diciembre, 2019, pp. 43-75.

DE SOLA POOL, I., "Tracking the Flow of Information", *Science,* vol. 221, agosto 1983, pp. 609-613.

DE TORRES VIGUERA, A., "Ética médica y tercera edad. Confidelidad de los datos clínicos y consentimiento informado", en AA.VV., *Actas de las Primeras Jornadas de problemas legales sobre tutela, asistencia y protección a las personas mayores,* (Coords., J.M. Gonález Porras y I. Gallego Domínguez), Cajasur, Obra Social y Cultura, España, 2001, pp. 317-330.

DEL RÍO SOLÁ, M.L y VAQUERO PUERTA C., "El impacto de la transformación digital en el sector sanitario"*, Revista Española de Investigaciones Quirúrgicas*, REIQ 2019, Vol. XXII, núm. 3, pp. 105-107.

DELGADO CARRAVILLA, E. y PUYOL MONTERO, J., *La implantación del nuevo Reglamento General de Protección de Datos de la Unión Europea,* Tirant lo Blanch, Valencia, 2018.

DEVENS MILLER, R., *Cyclopaedia of Commercial and Business Anecdotes*. *Comprising Interesting Reminiscences and Facts, Remarkable Traits and Humors of Merchants, Traders, Bankers Etc. in All Ages and Countries*, Ed. D. Appleton and Company, London, 1865.

DEVLIN, B.A. and MURPHY, P.T., "An architecture for a business and information system", *IBM Systems Journal,* vol. 27, núm. 1, febrero 1998, pp. 60-80. Documento disponible en: http://www.9sight.com/pdfs/EBIS_Devlin_&_Murphy_1988.pdf (última consulta 02/02/18).

DÍAZ DE LEÓN CASTAÑEDA, CH., "¿Qué es la salud electrónica ("e-Salud")?", *Infotec.* [Documento sin paginación]. Disponible en https://www.infotec.mx/es_mx/infotec/que_es_salud_electronica_esalud, (última consulta 25/02/20).

DÍAZ DÍAZ, E., "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones*", Revista Aranzadi Doctrinal*, agosto 2016, núm. 6/2016 parte Estudio, pp. 155-190.

DÍAZ GARCÍA, E., "La entrada en vigor del Reglamento Europeo de Protección de Datos como obstáculo a la investigación", *DS Derecho y Salud,* Vol. 28, Extraordinario XXVII Congreso 2018, pp. 231-238.

DIEZ-PICAZO, L. y GULLON, A., *Sistema de Derecho Civil*, Editorial Tecnos, Madrid, 2016.

DÍEZ-PICAZO, L., y GULLÓN, A., *Sistema de Derecho Civil*, Tecnos, Madrid, 2012.

DOMÍNGUEZ ÁLVAREZ, J.L., "¿Salud pública o protección de datos personales? Un difícil enfrentamiento en tiempos de Covid-19", *Archivamos: Boletín ACAL,* n.º 116, 2020, pp. 26-29.

DONOSO ABARCA, L., "Tratamiento de datos de salud. Condiciones de legitimidad de los usos secundarios de los datos personales por las entidades de salud", en AA.VV., *Hacia una Justicia 2.0: actas del XX Congreso Iberoamericano de Derecho e Informática: [Salamanca, 19-21 de octubre 2016],* (E. Y. Monive Cortés et al), Ratio Legis, Madrid, 2016, pp. 81-94.

DOUGLAS HEAVEN, W., "Por qué la IA nos ayudará a combatir la próxima pandemia pero no esta", *MIT Technology Review,* 2020, [Documento sin paginación]. Documento disponible en: https://www.technologyreview.es/s/12021/por-que-la-ia-nos-ayudara-combatir-la-proxima-pandemia-pero-no-esta, (última consulta 07/04/20).

DUFF, A.S., *Information Society Studies,* Ed. Routledge, London, 2000.

DURÁN RUIZ, F.J., "Big Data aplicado a la mejora de los servicios públicos y protección de datos personales", *Revista de la Escuela de Posgrado,* núm. 12, junio 2017, pp. 33-74.

ETRERos HUERTA, J.J., "Historia clínica electrónica", AA.VV., *El Derecho a la Protección de Datos en la Historia clínica y la Receta electrónica,* (Coord., R. Cáliz Cáliz), Thomson Reuters-Aranzadi, Cizur Menor, 2009, pp.181-200.

FAYYAD, U., PIATESTSKY-SHAPIRO, G. and SMYTH P., "From Data Mining to Knowledge Discovery in Databases*" Al Mazine.* Vol. 17, núm. 3, 1996, pp. 37-54. Documento disponible en: file:///Users/leticialatorreluna/Downloads/1230-Article%20Text-1227-1-10-20080129.pdf (última consulta 23/09/18).

FAYYAD, U.M., PIATESKY – SHAPIRO, G., SMYTH, P. and UTHURUSAMY, R., *Advances in knowledge and Data Mining.* Ed. AAAI/MIT Press, Cambridge (Massachussets), 1996.

FELDMAN, B., MARTIN, E.M. and SKOTNES, T., "*Big Data* Healthcare Hype and Hope*"*, 2012, [Documento sin paginación]. Documento disponible en: http://www.west-info.eu/files/big-data-in-healthcare.pdf (última consulta 25/03/19).

FERNÁNDEZ ACEVEDO, R., *Las concesiones administrativas de dominio público,* Thomson-Civitas, Navarra, 2007.

FERNÁNDEZ HIERRO, J.M., *Sistema de responsabilidad médica,* Editorial Comares, Granada, 2007.

FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas,* Civitas Ediciones, Madrid, 2003.

FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas,* Ed. Civitas Ediciones, Madrid, 2003.

FUENTES ESCOBAR, A., "Algunas cuestiones relevantes en el tratamiento de la LOPDGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 141-168.

GALÁN CORTÉS, J. C., "Relevancia jurídica de la historia clínica", *Salud Rural,* Vol. 14, núm. 7, 1997, pp. pp. 83-89.

GAMERO CASADO, E. y FERNÁNDEZ RAMOS, S., *Manual básico de Derecho Administrativo,* Editorial Tecnos, Madrid, 2019.

GARBERÍ LLOBREGAT, J., *Los procesos civiles de protección del honor, la intimidad y la propia imagen*, Bosch, Barcelona, 2007.

GARCÍA BARBOSA, J., "La medicina del futuro pasa por *Big Data"*, octubre 2014, [Documento sin paginación]. Documento disponible en: https://empresas.blogthinkbig.com/la-medicina-del-futuro-pasa-por-big-data/ (última consulta 07/03/19).

GARCÍA CAMPOS, J., ORTEGA DÍAZ, E. y HERNÁNDEZ SÁNCHEZ, S., "Ciencias de la salud basadas en le evidencia: hechos y reflexiones para la práctica clínica", *El Peu,* núm. 29, 2009, pp. 208-214.

GARCÍA CUMBRERAS, M.A., "eHealth (tecnología y medicina)", *Coddiinforme*, enero 2017, p.4.

GARCÍA GARCÍA, J.J., "Epidemiología clínica. Qué y para qué", *Revista Mexicana de Pediatría,* vol. 66, núm. 4, 1999, pp. 169-173.

GARCÍA MAHAMUT, R. (Ed.), *Hacia un derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.

GARCÍA MEXÍA, P. y PERETE RAMÍREZ, C., "Internet, el RGPD y la LOPDGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 851-872.

GARCÍA MEXÍA, P., *Derechos y libertades, Internet y TICs*, Ed. Tirant lo Blanch, Valencia, 2014.

GARCÍA VIEIRA, F. J. y FERNÁNDEZ RANCAÑO, M., "Financiación de la Estrategia de Salud Digital", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 51-55.

GARCÍA-MONCÓ, A., "A propósito del régimen jurídico-financiero del patrimonio de las Administraciones Publicas", en AA.VV. *El régimen jurídico general del Patrimonio de las Administraciones Públicas. Comentarios a la Ley 33/2003, de 3 de noviembre,* (Dir. J.F. Mestre Delgado), El consultor de los Ayuntamientos y de los Juzgados, Madrid, 2004, pp. 205-232.

GARCÍA-RIPOLL MONTIJANO, M., "El consentimiento al tratamiento de datos personales", en AA.VV., *Protección de datos personales,* (Coord. I. González Pacanowska), Asociación de profesores de Derecho Civil, Tirant lo Blanch, Valencia, 2020, pp.79-159.

GARCÍA, R., "El Reglamento General de Protección de Datos y su aplicación en el ámbito sanitario", *I+S Revista de la Sociedad Española de Informática y Salud,* núm. 127, febrero 2017, pp. 13-20.

GARRIGA DOMINGUEZ, A., "La protección de los datos de carácter personal en el ámbito sanitario. Usos de la historia clínica", en AA.VV., *Historia clínica y protección de datos personales. Especial referencia al registro obligatorio de los portadores del VIH,* (Dirs. A. Garriga Dominguez, y S. Álvarez González), Dykinson, Madrid, 2011, pp. 11-50.

GERVÁS, J., "Historia clínica: al limitar el acceso se mejora el proceso", *Actualización en Medicina de Familia,* vol. 11, núm. 7, 2015, pp. 312, 373. Documento disponible en: https://amf-semfyc.com/web/article_ver.php?id=1448 (última consulta 15 de octubre 2019) (última consulta 08/04/19).

GIL GONZÁLEZ, E., "Directrices del Grupo de Trabajo del Artículo 29 sobre el consentimiento en el Reglamento General de Protección de datos", AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva LO3/2018 y Reglamento (UE). Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, pp. 703-710.

GIL GONZÁLEZ, E., *Big Data, privacidad y protección de datos,* Agencia Española de Protección de Datos y Boletín Oficial del Estado, Madrid, 2016.

GÓMEZ ÁLVAREZ, F.J., "La cesión de datos de carácter personal al proceso penal: en especial los datos relativos a la salud", en AA.VV., *Cesión de datos personales y evidencias entre procesos penales y procedimientos administrativos sancionadores o tributarios,* (Coord., S. Oubiña Barbolla), Thomson Reuters-Aranzadi, Cizur Menor, 2017, pp. 607-646.

GÓMEZ PIQUERAS, C., "Disociación/anonimización de los datos de salud", *Revista Derecho y Salud,* vol. 18. núm. 1, 2009, pp. 43-56.

GÓMEZ PIQUERAS, C., "La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", en AA.VV., *El derecho a la protección de datos en la historia clínica y la receta electrónica,* (Coord. R. Cáliz Cáliz et al.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, pp. 127-160.

GÓMEZ SÁNCHEZ, Y., "Datos de salud como datos especialmente protegidos", en AA.VV., *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, (Dir. A. Troncoso Reigada), Ed. Civitas, Madrid, 2010, pp. 647 – 671.

GONZÁLEZ FUSTES, G., "TEDH – Sentencia de 04.12.2008, S. y Marper c. Reino Unido, 30562/04 y 30566/04 – Articulo 8 CEDH – Vida privada – Injerencia en una sociedad democrática – Los límites del tratamiento de datos biométricos de personas no condenadas", *Revista de Derecho Comunitario Europeo,* núm. 33, Madrid, mayo/agosto 2009, pp. 619-633. Documento disponible en: http://www.cepc.gob.es/publicaciones/revistas/revistaselectronicas?IDR=4&IDN=679&IDA=27523 (última consulta 12/12/18).

GONZÁLEZ GARCÍA, L., "Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos", *Derecho y Salud,* Vol. 24, núm. Extra. 1, 2014, pp. 287-298.

GONZÁLEZ GONZÁLEZ, P.A., "Responsabilidad proactiva en los tratamientos masivos de datos", *Dilemata,* núm. 24, 2017, pp. 115-129.

GONZÁLEZ LEÓN, C., "Privacidad e historia clínica electronica: la autonomía del paciente y el ejercicio de los derechos ARCO", en AA.VV., *En torno a la privacidad y la protección de datos en la Sociedad de la información,* (Coords. J.P. Aparicio Vaquero y A. Batuercas Caletrío)*,* Comares, Granada, 2015, pp. 27-68.

GONZÁLEZ MURUA, A.R., "Comentario a la S.T.C. 254/1993, de 20 de julio. Algunas Reflexiones en torno al Artículo 18.4 de la Constitución y la Protección de Datos Personales", *Revista Vasca de Administración Pública,* núm. 37, 1993, pp. 227-270.

GONZÁLEZ NAVARRO, F., "El derecho de la persona física a disponer de los datos de carácter personal que le conciernen", *Revista Jurídica de Navarra,* núm. 22, 1996, pp. 17-60.

GONZÁLEZ PÉREZ, J., *Los derechos reales administrativos,* 2ª ed., Civitas, Madrid, 1989.

GOST GARDE, J., "Gestión sanitaria y tecnológica de la información", *XX Congreso Nacional de la Sociedad Española de Anatomía Patológica*, 2001, pp. 37 -57. Documento disponible en: http://www.conganat.org/SEIS/informes/2001/PDF/2Gost.pdf (última consulta 17/05/19).

GOST GARDE, J., *Gestión sanitaria y tecnológica de la información,* 2001, pp. 37 -57. Disponible en: http://www.conganat.org/SEIS/informes/2001/PDF/2Gost.pdf (última consulta 03/03/20).

GRAU, J., "Smart Data: el tamaño no siempre importa", *AUSAPE*, marzo 2016 [Documento sin paginación]. Documento disponible en: http://www.scl-consulting.com/wp-content/uploads/2016/03/smart-data.pdf (última consulta 03/05/18).

GRIMALT SERVERA, P., "La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y libertades en internet", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica,* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 65-87.

GRIMALT SERVERA, P., *La protección civil de los derechos al honor, a la intimidad y a la propia imagen*, Iustel, Madrid, 2007.

GRIMALT SERVERA, P., *La responsabilidad civil en el tratamiento automatizado de datos personales,* Comares, Granada, 1999.

GUAZZELLI, A., "Predicciones sobre el futuro, parte 2: Técnicas de modelado predictivo", *IBM developerWorks*, diciembre 2012, [Documento sin paginación]. Documento disponible en: https://developer.ibm.com/es/technologies/predictive-analytics/articles/ba-predictive-analytics3/ (última consulta 03/10/18).

GUAZZELLI, A., "Predicciones sobre el Futuro. Parte 1: ¿Qué es la Analítica predictiva?", *IBM developerWorks,* noviembre 2012, [documento sin paginación]. Documento disponible en: https://developer.ibm.com/es/technologies/predictive-analytics/articles/ba-predictive-analytics1/ (última consulta 01/10/18)

GUBBIOLI BELLECQ, J., "El valor de la información y el Big Data", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 40-41.

GUICHOT REINA, E., "La responsabilidad patrimonial de los poderes públicos", en AA.VV.., *Lecciones de Derecho Administrativo. Parte General, Volumen II,* (Coord. C. Barrero Rodríguez), Editorial Tecnos, Madrid, 2017, pp. 217-256.

GUICHOT REINA, E., *Datos personales y Administración Pública,* Editorial Aranzadi, Cizur Menor, 2005.

GUTIÉRREZ BARRENENGOA, A., "La historia clínica como prueba en el Proceso Judicial por responsabilidad médica", en AA.VV., *Responsabilidad médica civil y penal por presunta mala práctica profesional,* (Coord. O. Monje Balmaseda), Ed. Dykinson, Madrid, 2012, pp. 323-334.

H. ELÍA, R., "El incendio de la biblioteca de Alejandría por los árabes: una historia falsificada", *Byzantion Nea Hellán,* núm. 32, 2013, pp. 37-69. Documento disponible en: https://scielo.conicyt.cl/pdf/byzantion/n32/art02.pdf (última consulta 15/08/18).

HERAS, R., "RGPD: Evaluación de impacto", *I+S Revista de la Sociedad Española de Informática y Salud,* núm. 127, Febrero 2017, pp. 24-27.

HEREDERO HIGUERAS, M., *La directiva comunitaria sobre la protección de datos de carácter personal*, Aranzadi, Pamplona, 1997.

HERNÁNDEZ MARTÍN, A., "Breve historia del *Big Data", Archivamos*, núm. 97, Marzo, 2015, pp. 41-44.

HERNÁNDEZ MARTÍNEZ CAMPELLO, C., "La Ley 41/2002 y la normative sobre protección y tratamiento de datos de carácter personal relativos a la salud", AA.VV., *Autonomía del paciente, información e historia clínica: (estudios sobre la Ley 41/2002, de 14 de noviembre),* (Coords. E. Lizarraga Bonelli y P. González Salinas), 2004, pp. 161-224.

HERNÁNDEZ MEDRANO, I., "La sanidad ante el mundo del Big Data", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 42-44.

HERRÁN ORTIZ, A.I., "A propósito de la Ley Orgánica de Protección de Datos Personales y los problemas sobre su inconstitucionalidad", en AA.VV., *Quince años de Encuentros sobre Informática y Derecho (1987-2002)* (Coord. M.A. Davara Rodriguez), Tomo II, Ed. Universidad Pontificia de Comillas, Instituto de Informática Jurídica, Madrid, 2002, pp. 77-107.

HERRÁN ORTIZ, A.I., "El derecho fundamental del paciente a la proteccion de los datos sanitarios en la legislación española", en AA.VV., *Los avances del derecho ante los avances de la medicina,* (Coords. S. Biosca Adrother, F. De Montalvo Jääskeläinen, M.R. Corripio Gil-Delgado y A.B. Veiga Copo), Editorial Aranzadi, Cizur Menor, pp. 819-836.

HERRÁN ORTIZ, A.I., *La violación de la intimidad en la protección de datos personales,* Ed. Dykinson, Madrid, 1999.

HERRERO TEJEDOR, F., *Honor, intimidad y propia imagen,* Ed. Colex, Madrid, 1990.

HOPP, W. J. and SPEARMAN, M. L., "To Pull or Not to Pull: What is the Question?", *Manufacturing & Service Operations Management (M&SOM)*, vol. 6, núm. 2, 2004, pp. 133-148. Documento disponible en: https://pubsonline.informs.org/doi/pdf/10.1287/msom.1030.0028 (última consulta 11/11/18)

HOSSAIN, L., PATRICK, J.D. and RASHID, M.A., *Enterprise Resource Planning: Global Opportunities and Challenges,* Ed. Idea Group Publishing, Estados Unidos, 2002.

HOWE, J., "The Rise of Crowdsourcing", *Wired Magazine.*Junio, 2006 [Documento sin paginación]. Documento disponible en: https://www.wired.com/2006/06/crowds/ (última consulta 07/09/18).

HOWE, J., *Crowdsourcing: Why the Power of the Crowd Is Driving the Future of Business*, Three Rivers Press, Nueva York, 2008.

IBÁÑEZ PRADAS, V. y MODESTO ALAPONT, V., "Introducción a la medicina basada en la evidencia", *Cirugía Pedriatica,* Vol. 18, núm. 2, 2005, pp. 55-60. Documento disponible en: https://www.secipe.org/coldata/upload/revista/CirPed18.55-60.pdf (última consulta 02/02/19).

IBM100, *Pioneering Speech Recognition,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/speechreco/ (última consulta 21/12/17).

IBM100, *Relational Database,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com (última consulta 21/12/17).

INMON, W. H., *Building the Data Warehouse,* Ed. John Wiley and Sons, Nueva York, 1993, p. 31.

IRABURO, M., "Confidencialidad e intimidad*", An. Sist. Sanit. Navar.*, Vol. 29, Suplemento 3, 2006, pp. 49-59.

JOVE VILLARES, D., "Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización"*, Revista Derecho y Salud*, núm. 1, 2017, pp. 55-66.

JOYANES AGUILAR, L., *Big Data. Análisis de grandes volúmenes de datos en las organizaciones.* Ed. Marcombo, Barcelona, 2014.

JUANE SÁNCHEZ, M. (Coord.), *Lecciones de derecho sanitario*, Servizo de Publicacións, Universidad da Caruña, 1999.

JUNQUERA, L.M., BALADRÓN, J., ALBERTOS, J.M. y OLAY, S., "Medicina basada en la evidencia (MBE). Ventajas" *Controversias en Cirugía Oral y Maxilofacial: Parte 1. Revista Española Cirugía Oral y Maxilofacial,* núm. 25, 2013, pp. 265-272.

LACORT, B., "La Financiación de la Estrategia de Salud Digital", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 56-59.

LACRUZ BERDEJO, J. L., *Elementos de Derecho Civil. I. Parte General,* vol. II, *Personas*, Dykinson, Madrid, 2010.

LAFUENTE BENACHES, M., *La concesión de dominio público (Estudio especial de la declaración de caducidad),* Montecorvo, Madrid, 1988.

LANEY, D., "3D Data Management: Controlling Data Volume, Velocity, and Variety", *Application Delivery Strategies, Meta Group Inc*., 6 de febrero 2001, [Documento sin paginación]. Documento disponible en: https://bloGC.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (última consulta 11/10/17).

LARIOS RISCO, D. (Coord.) y et al., *Tratado de Derecho sanitario,* Thomson-Reuters Aranzadi, Cizur Menor, 2013.

LARIOS RISCO, D., "La historia clínica como conjunto de datos especialmente protegidos", en AA.VV., *El derecho a la protección de datos en la historia clínica y la receta electrónica,* (Coord., R. Cáliz Cáliz et al.), 2009, pp. 161-180.

LARIOS RISCO, D., *Guía Práctica de Derechos de los Pacientes y de los Profesionales sanitario,* Thomson-Reuters Aranzadi, Cizur-Navarra, 2016.

LASCUARAÍN SÁNCHEZ, J.A. (Coord.), *Manual de Introducción al Derecho Penal,* 1ª ed., Agencia Estatal Boletín Oficial del Estado, Madrid, 2019.

LÁZARO GÓNZALEZ, I.E., "Confidencialidad de los datos sanitarios del menor versus obligación de los padres de proteger a los hijos", en AA.VV., *Los avances del derecho ante los avances de la medicina,* (Coords. S. Adroher Biosca, F. De Montalvo Jääskeläinen, M.R. Corripio Gil-Delgado y A.B. Veiga Copo), Aranzadi Thomson Reuters, Navarra, 2008, pp. 401-50.

LERMAN, J., "*Big Data* and Its Exclusions", *Stanford Law Review* Online, 66 Stanford Law Review Online 55, SSRN, 2013, [Documento sin paginación].

LESK, M., "How much information is there in the world?", *Tenopi,* 1997, [Documento sin paginación]. Disponible en: http://www.lesk.com/mlesk/ksg97/ksg.html (última consulta 23/11/17).

LIEBOWITZ, J. and BECKMAN, T., *Knowledge Organizationes: What every manager should know,* CRC Press, Estados Unidos, 1998.

LIMAN, P. and VARIAN, H.R., "How much information?", *Regents of the University of California,* 18 de octubre de 2000, [Documento sin paginación]. Documento disponible en: http://www2.sims.berkeley.edu/research/projects/how-much-info/ (última consulta 10/10/17).

LOMAS HERNÁNDEZ, V., "Principales Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales desde la Perspectiva Sanitaria", *I+S: Revista de la Sociedad Española de Informática y Salud,* núm. 134, 2019, pp. 7 – 11.

LOMBARTE, A. y GARCÍA MAHAMUT, R. (Coords.), *Hacia un derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015.

LÓPEZ -IBOR MAYOR, V., "Los límites al derecho fundamental a la autodeterminación informativa en la Ley española de protección de datos (LORTAD)", *Actualidad Informática Aranzadi,* núm. 8, 1993, pág. 1 y ss.

LÓPEZ ALONSO, F.J., "¿Cómo abordar un análisis de riesgos en un tratamiento de datos de carácter personal sujeto al Reglamento General de Protección de Datos?", AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, pp. 711-718.

LÓPEZ ÁLVAREZ, L.F., "La responsabilidad del responsable", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J.L. Piñar Mañas), Ed. Reus, Madrid, 2016, pp. 275-294.

LÓPEZ CALVO, J. (Coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos,* Wolters Kluwer, Madrid, 2018.

LÓPEZ CALVO, J., "Reglamento Europeo de Protección de Datos: ejes relevantes", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, pp. 609-678.

LÓPEZ CARMONA, F.J., "e-Salud, confidencialidad y seguridad de la información en el ámbito sanitario", en AA.VV., *Estudios sobre administraciones públicas y protección de datos personales: I Encuentro entre Agencias Autonómicas de Protección de Datos Personales: celebrado el día 2 de noviembre de 2004 en la Sede de la Universidad Carlos III de Madrid, organizada por la Agencia de Protección de Datos de la Comunidad de Madrid,* (Coord., A. Troncoso Reigada), Agencia de Protección de Datos, Madrid, 2006, pp. 95-101.

LÓPEZ GARRIDO, D. y MARTÍN PALLÍN, J. A., "La informática: un riesgo incontrolado", *Revista Vasca de Administración pública,* núm. 20, 1988, pp. 201-218.

LÓPEZ LÓPEZ, V., "*Big Data* sanitario: el acelerador del conocimiento y la decisión clínica", 4 de mayo 2015, [Documento sin paginación]. Documento disponible en https://empresas.blogthinkbig.com/big-data-sanitario-el-acelerador-del-conocimiento-y-la-decision-clinica/ (última consulta 08/03/19).

LÓPEZ RUIZ, C.G., "La figura del delegado de protección de datos (DPO)", en AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva LO3/2018 y Reglamento (UE). Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, 2018, pp. 695-701.

LÓPEZ RUÍZ, C.G., "La figura del delegado de protección de datos (DPO)", AA.VV., *Guía de Protección de Datos y Garantía de Derechos Digitales: nueva Ley Orgánica 3/2018 y Reglamento (UE9. Comentarios doctrinales, Normativa, Formularios y Esquemas*, Editorial Jurídica Sepín, Madrid, pp. 695-701.

LÓPEZ ULLA, J.M., "El derecho de acceso a la información pública que contenga datos personales: en particular, los datos relativos a la salud", en AA.VV., *Comentario a la ley de transparencia, acceso a la información pública y buen gobierno*, (Dir. Troncoso Reigada, A.), Civitas, Madrid, 2017, pp. 1079-1111.

LUCAS MURILLO DE LA CUEVA, P., *El derecho a la autodeterminación informativa,* Ed. Tecnos, Madrid, 1990.

LUCAS MURILLO DE LA CUEVA, P., *Informática y protección de datos personales. Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de datos de carácter personal*, Centro de Estudios Constitucionales, Madrid, 1993.

LUHN, H.P., "A *Business Intelligence* System", *IBM Journal*, Vol. 2-4, Octubre 1958, pp. 314-319. Disponible en http://altaplana.com/ibmrd0204H.pdf (última consulta 15/01/18).

MÁLAGA RODRÍGUEZ, G. y SÁNCHEZ MEJÍA, A., Medicina Basada en la Evidencia: aportes a la práctica médica actual y dificultades para su implementación, *Rev. Med. Hered,* Vol. 20, núm. 2, 2019, pp. 103 – 109. Documento disponible en: http://www.scielo.org.pe/pdf/rmh/v20n2/v20n2tr1.pdf

MANTERO, A., "Regulating big data. The guidelines of the council of europe in the context of the european data protection framework", *Computer Law & Security Review*, Vol. 33, Issue 5, October 2017, pp. 584-602.

MANYIKA, J., BROWN, B.M. DOBBS, R., ROXBURGH, CH. and BYERS, A. H., "*Big data*: The next frontier for innovation, competition, and productivity", *McKinsey Global Institute*, junio 2001, [Documento sin paginación]. Documento disponible en: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation (última consulta 15/11/17).

MARR, B., "A Brief History of *Big Data* Everyone Should Read", *World Economic Forum,* Febrero 2015, [Documento sin paginación]. Disponible en: https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/ (última consulta 03/01/18).

MARTENS, CH., "BI at age 17", *Computerworld,* octubre 2006, [Documento sin paginación]. Documento disponible en: https://www.computerworld.com/article/2554088/business-intelligence/bi-at-age-17.html (última consulta 22/02/18).

MARTÍN DELGADO, I., "El acceso electrónico a los servicios públicos: hacia un modelo de Administración digital auténticamente innovador", en AA.VV., *Sociedad Digital y Derecho,* (Dirs. T. de la Quadra y J.L. Piñar), Boletín Oficial del Estado, Madrid, 2018, pp. 179-201.

MARTÍN JIMÉNEZ, R., "Evaluación de impacto en la Protección de Datos: Paralelismos", *I+S: Revista de la Sociedad Española de Informática y Salud,* núm. 134, 2019, pp. 24-26.

MARTÍN MORENO, J.M., "Epidemiología y respeto a la confidencialidad sobre los datos personales: a propósito de una propuesta de Directiva europea", *Gaceta Sanitaria*, Vol. 8, núm. 45, 1994, pp. 317-320.

MARTIN URANGA, A., "El nuevo Reglamento Europeo de Protección de Datos: una oportunidad para avanzar en investigación biomédica con las garantías adecuadas para los pacientes", *I + S: Revista de la Sociedad Española de Informática y Salud,* ejemplar 122, 2017, pp. 10-12.

MARTÍNEZ GARCÍA, D.N., DALGO FLORES, V.M., HERRERA LÓPEZ, J.L.; ANALUISA JIMÉNEZ, E.I. y VELASCO ACURIO, E.F., "Avances de la inteligencia artificial en salud", *Dominio de las ciencias,* Vol. 5, núm. 3, julio 2019, pp. 603-613.

MARTÍNEZ MARTÍNEZ, R y ÁLVAREZ RIGAUDIAS, C., "El uso de datos con fines de investigación biomédica (Arts. 9 y 89 RGPD. Art. 9, Disposición adicional decimoséptima, Disposición final novena y Disposición transitoria sexta LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 279-287.

MARTÍNEZ MARTÍNEZ, R., "El derecho a la vida privada en España", en AA.VV., *El debate sobre la privacidad y seguridad en la red: Regulación y mercados,* (Coords. J. Pérez Martínez y Badía y Liberal)*,* Ed. Ariel, Barcelona, 2012.

MARTÍNEZ MARTÍNEZ, R., "El derecho fundamental a la protección de datos: perspectivas", *Monográfico "III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas". Revista de Internet Derecho y Política.* Núm. 5, 2007, pp. 47-61. Documento disponible en: https://www.researchgate.net/publication/28178556_El_derecho_fundamental_a_la_proteccion_de_datos_perspectivas (última consulta 11/11/18).

MARTÍNEZ MARTÍNEZ, R., "Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo", *Revista Catalana de Dret Públic,* núm. 58, 2019, pp. 64-81.

MARTÍNEZ MARTÍNEZ, R., "Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública", *Diario La Ley,* núm. 38, Sección Ciberderecho, marzo 2020, [Documento sin paginación]. Documento disponible en: https://diariolaley.laleynext.es/dll/2020/03/27/los-tratamientos-de-datos-personales-en-la-crisis-del-covid-19-un-enfoque-desde-la-salud-publica (último acceso 22/05/20).

MARTÍNEZ MARTÍNEZ. R., "Big Data, investigación en salud y protección de datos personales: ¿Un falso debate?", *Revista Valenciana d´Estudis Autonômics,* n.º 62, 2017, pp. 235-280.

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

MARTÍNEZ USEROS, E., "Improcedencia de servidumbre sobre dominio público", en AA.VV., *Estudios dedicados al profesor García Oviedo con motivo de su jubilación*, Escuela de Estudios Hispanoamericanos, Sevilla, 1954, pp. 137-176.

MARTOS DÍAZ, N., "Principios (Ars. 6-11 RGPD. Arts. 4-10 LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 333-343.

MARTOS DÍAZ, N., "Principios (Ars. 6-11 RGPD. Arts. 4-10 LOPDGDD)", en VV.AA., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. López Calvo, J.), Wolters Kluwer, Madrid, 2019, pp. 333-343.

MÁS, B., ACOSTA, Y. y BATISTA, M., "Visualización de la gestión del conocimiento en diferentes objetos de estudio: ayuda para la investigación-acción. Primera Parte", *Ciencias de la Información,* Vol. 40, núm. 3, 2009, pp. 3-12.

MAYER-SCHÖNBERGER, V y CUKIER, K., *Big Data. La revolución de los datos masivos*, Ed. Turner, Madrid, 2013.

MAYER-SCHÖNBERGER, V. and CUKIER, K., "The Dictatorship of Data", *MIT Technology Review,* mayo 2013, [Documento sin paginación]. Documento disponible en: https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos (última consulta 04/22/20).

MAYOL, J., "Los 6 retos del *Big Data* en la sanidad", enero 2015, [Documento sin paginación]. Documento disponible en: http://juliomayol.com/big-data-y-medicina-5p/ (último acceso 05/05/20).

MCCRAE. I., "Medicina de precisión", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 45-50.

MEDRANO, J. y PACHECO, L., "Historia clínica electrónica y confidencialidad", *Rev. Asoc. Esp. Neuropsiq*., vol. 35, núm. 126, 2015, p. 249. Documento disponible en: doi: 10.4321/S0211-57352015000200001 (última consulta 03/04/19).

MEJÍA ROCHA, M.I. y COLÍN SALGADO, M., "Gestión del conocimiento y su importancia en las organizaciones*", Trilogía. Revista Ciencia, Tecnología y Sociedad,* núm. 9, julio – diciembre, 2013, pp. 25-35.

MENASALVAS, E.; GONZALO, C. y RODRÍGUEZ-GONZÁLEZ, A., "*Big Data* en Salud: retos y oportunidades" *Economía Industrial,* núm. 405, 2017, pp. pp. 87 – 97. Documento disponible en: http://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/405/MENASALVAS,%20GONZALO%20Y%20RODR%C3%8DGUEZ.pdf, (última consulta 29/09/18).

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", *Revista de Derecho y Genoma Humano,* Núm. Extraordinario, 2019, pp. 205-232

MERINO MOLINS, V., "La responsabilidad patrimonial de la Administracion en el ámbito de la sanidad", *Actualidad Administrativa,* n.º 6, 2003, pp. 135-162.

MILLÁN CALENTI, R.A., "Los flujos de información en el tratamiento de los datos en la HCE: La distinción entre responsable del fichero y encargado del tratamiento, análisis de supuestos. La cesión a terceros de la información contenida en las historias clínicas, análisis de supuesto", en AA.VV., *El Derecho a la protección de datos en la historia clínica y la receta electrónica*, (Coord. R. Cáliz Cáliz et al.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, pp. 321-344.

MIR PUIGPELAT, O., *La responsabilidad patrimonial de la Administracion sanitaria*, Civitas, Madrid, 1991.

MIRALLES LÓPEZ, R., "Derecho de portabilidad (Art. 20 RGPD. Art. 17, 95 LOPDGDD", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 387-395.

MIRALLES LÓPEZ, R., "Desvinculación datos personales: seudonimización, desidentificación y anonimización", *I + S: Revista de la Sociedad Española de Informática y Salud,* ejemplar 122, 2017, pp. 7-9.

MITCHELL, T.M., *Machine Learning*, McGraw-Hill, Nueva York, 1997.

MOGOLLÓN GONZÁLEZ, S., "¿Existe de verdad la anonimización? El grupo del artículo 29 de Protección de Datos no lo pone fácil", *Noticias Jurídicas,* Conocimiento, Artículos doctrinales, Julio 2014, [Documento sin paginación]. Documento disponible en: https://www.audea.com/existe-de-verdad-la-anonimizacion-el-grupo-del-articulo-29-de-proteccion-de-datos-no-lo-pone-facil/ (último acceso 20/12/18).

MOLINA FÉLIX, L.C. y RIBERO, S., "Descubrimiento conocimiento para el mejoramiento bovino usando técnicas de *Data Mining*", *Actas del IV Congreso Catalán de Inteligencia Artificial*, Barcelona, 2001, pp. 123-130.

MOLINA FÉLIX, L.C., "Data Mining: torturando a los datos hasta que confiesen*"*, 2002, [Documento sin paginación]. Documento disponible en: http://www.uoc.edu/web/esp/art/uoc/molina1102/molina1102.html (última consulta 02/03/18).

MONLEÓN GETINO, A., "El impacto del *Big Data* en la información. Significado y utilidad", *Historia y comunicación social,* vol. 20, núm. 2, 2015, pp. 427-445.

MOOIWEER, P. and SHOCKLEY, R., "Analítica de datos: El uso en el mundo real de *Big Data* en sanidad y ciencias de la vida. Cómo las organizaciones más innovadoras en sanidad y ciencias de la vida de la salud extraen valor de datos inciertos", *IBM Institute for Businees Value,* julio 2013 [Documento sin paginación].

MORAES, R., "Big Data v/s Smart Data. Desde la cantidad a la calidad", *Gerencia*, julio 2014 [Documento sin paginación]. Documento disponible en http://www.emb.cl/gerencia/articulo.mvc?xid=3503&sec=12 (última consulta 28/04/18).

MORRIS, R.J.T. and TRUSKOWSKI, B.J., "The Evolution of Storage Systems", *IBM Systems Journal,* núm. 1, julio 2003, pp. 205-217.

NAVAS NAVARRO, S., "Salud electrónica e Inteligencia Artificial", en AA.VV., *Salud e Inteligencia Artificial desde el derecho privado. Con especial atención a la pandemia por SARS-CoV-2 (covid-19),* (Dir. Susana Navas Navarro), Comares, Granada, pp. 1-50.

NIETO GARRIDO, E., "Derecho a indemnización y responsabilidad", en AA.VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, (Dir. J. L. Piñar Mañas), Ed. Reus, Madrid, 2016, pp. 555-570.

NIGRO, H.O., XODO, D., CORTI, G. y TERREN, D., "KDD (Knowledge Discovery in Databases): Un proceso centrado en el usuario" *Red de Universidades con Carreras en Informática (RedUNCI*), 2004, p. 55. Documento disponible en: http://sedici.unlp.edu.ar/handle/10915/21220 (última consulta 24/09/18).

NONAKA, I. and TAKEUCHI, H., *The knowledge creating company.* Ed. Oxford University PRess, Nueva York, 1995.

NONAKA, I.; TAKEUCHI, H., *La organización creadora de conocimiento. Cómo las compañías japonesas crean la dinámica de la innovación.* Ed. Oxford, México, 1995.

NÚÑEZ, M., "Las asombrosas cifras de la mHealth", febrero 2014, [Documento sin paginación]. Documento disponible en: https://empresas.blogthinkbig.com/las-asombrosas-cifras-de-la-mhealth/ (última consulta 07/03/19).

O'CALLAGHAN MUÑOZ, X., "Personalidad y derechos de la personalidad (honor, intimidad e imagen) del menor, según la Ley de Protección del Menor", *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía*, núm. 4, 1996, pp. 1247-1251.

O´REILLY, T., "What is Web 2.0?", *O´Reilly Media*, 2005, [Documento sin paginación]. Documento disponible en: http://www.oreilly.com/pub/a//web2/archive/what-is-web-20.html (última consulta 01/01/18).

OBIOLS, A., "¿Qué es un Data Scientist?", *InLab FIB talent & tech UPC,* 2015, [Documento sin paginación]. Documento disponible en: https://inlab.fib.upc.edu/es/blog/que-es-un-data-scientist (última consulta 05/03/18).

OLAVSRUD, T., "12 *Big Data* Predictions for 2014", *CIO from IDG,* 2011, [DOCUMENTO SIN PAGINACIÓN]. Documento disponible en: https://www.cio.com/article/2369764/big-data/132163-12-Big-Data-Predictions-for-2014.html (última consulta 19/01/18).

OLIVER MORA, M. y IÑIGUEZ RUEDA, L., "El uso de las tecnologías de la información y la comunicación (TIC) en los centros de salud: la visión de los profesionales en Cataluña, España", *Interface (Botucatu)*, Vol. 21, núm. 63, 2007, pp. 945-955. Documento disponible en: https://doi.org/10.1590/1807-57622016.0331 (última consulta 03/02/20).

OLSON, M., "HADOOP: Scalable, Flexible Data Storage and Analysis", *Connecting Innovation and Intelligence IQT QUARTERLY,* Vol. 1, núm. 3, 2010, pp. 14-18. Documento disponible en: https://blog.cloudera.com/wp-content/uploads/2010/05/Olson_IQT_Quarterly_Spring_2010.pdf (última consulta 01/10/18).

ORDÁS ALONSO, M., "Intimidad, secreto médico y protección de datos sanitario", en AA.VV., *Razonar sobre Derechos,* (Coord. J.A. García Amado), Ed. Tirant lo Blanch, Valencia, 2016, pp. 773-834.

OROZCO PARDO, G., Protección de datos relativos a la salud y derecho a la información clínica, en AA.VV., *Nuevos conflictos sociales: el papel de la privacidad,* (Coords. E. Anarte Borrallo, F. Moreno Moreno, F. y C.R. García Ruíz), Iustel, Madrid, 2015, pp. 119-144.

ORTEGA GIMÉNEZ, A. (Dir.), *Problemas que el COVID-19 plantea en el trinomio protección de datos, transparencia y movilidad. Aportación de soluciones prácticas desde la Ciencia Jurídica,* Aranzadi, Navarra, 2021.

ORTEGA GIMÉNEZ, A., "COVID-19: Un desafío para la protección de datos de carácter personal", *Actualidad Jurídica Iberoamericana,* núm. 12 bis, mayo 2020, pp. 860-867.

ORTEGA GIMÉNEZ, A., "El impacto del Reglamento General de Protección de Datos de la Unión Europea y de la LOPDGDD en el regimen jurídico de las transferencias internacionales de datos de carácter personal", en AA.VV., *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales,* (Eds. R. García Mahamut y B. Tomás Mallén), Tirant lo Blanch, Valencia, 2019, pp. 393-418.

ORTEGA GIMÉNEZ, A., "Tratamiento ilícito internacional de datos personales, reglamento general de protección de datos y derecho internacional privado. Cuestiones de competencia judicial internacional y de determinación de la ley applicable", en AA.VV., *Era Digital, Sociedad y Derecho* (Dir. O. Fuentes Soriano), Tirant lo Blanch, Valencia, 2020, pp. 521-544.

ORTEGA GIMÉNEZ, A., *Las aplicaciones del Big Data en el ámbito asegurador y el tratamiento legal de sus datos. Una perspectiva desde el derecho internacional privado,* Fundación Mapfre, Madrid, 2019.

ORTÍ VALLEJO, A., *Derecho a la intimidad e informática (Tutela de la persona por el uso de los ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada),* Ed. Comares, Granada, 1994.

ORTIZ DE ZÁRATE, A., "Open Data el valor de los datos", *Alorza.net*., junio 2016 [Documento sin paginación]. Documento disponible en: https://es.slideshare.net/alorza/open-data-el-valor-de-los-datos (última consulta 12/04/18).

PALACIOS PALACIOS, P., "Protección de datos en el sector sanitario: el acceso a la historia clínica", en AA.VV., *Derecho y nuevas tecnologías,* (Coords. M. Escudero González, A.I. Herrán Ortiz, A.I. et al), Universidad de Deusto, Navarra, 2011, pp. 265-274.

PALOMAR OLMEDA, A., *Protección de la salud la necesidad de recomposición del sistema,* Aranzadi, Navarra, 2021.

PANIAGUA, S., "*Big Data* en sanidad para predecir, prevenir y personalizar", noviembre 2012, [Documento sin paginación]. Disponible en: http://www.sorayapaniagua.com/2012/11/12/big-data-en-sanidad-para-predecir-prevenir-y-personalizar/ (última consulta 27/03/19).

PARDO LÓPEZ, Mª M., "No sólo protección de datos personales en internet: de los conceptos jurídicos híbridos, las categorías mutantes y otras evoluciones en curso", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica,* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 89-112.

PAREJO ALFONSO, L., "La *suma divisio* de las cosas. Las cosas públicas: el patrimonio de las administraciones y el dominio público", en AA.VV., *Derecho de los bienes públicos,* (Dirs. A. Palomar Olmeda y L. Parejo Alfonso), Aranzadi, Navarra, 2013, pp. 49-100.

PAREJO GAMIR, R., "Transmisión y gravamen de concesiones administrativas", *Revista de Administración pública,* núm. 107, 1985, pp. 7-78.

PARIENTE DE PRADA, I., "Los datos de Salud en el Nuevo Reglamento Europeo de Protección de Datos", *I + S: Revista de la Sociedad Española de Informática y Salud,* ejemplar 122, 2017, pp. 13-14.

PASCUAL, P., "¿Cuáles son las diferencias entre *Big Data* y *Data Science*?", *PiperlabK,* diciembre 2017 [Documento sin paginación]. 5 diciembre. Documento disponible en: https://piperlab.es/2017/12/05/diferencias-entre-big-data-data-science/ (última consulta 03/03/18).

PEREIRA ÁLVAREZ, M., "El tratamiento de los datos en las HCE y las medidas de seguridad: una aproximación desde el punto de vista técnico. Especial referencia al nuevo Reglamento de desarrollo de la LOPD", en AA.VV., *El Derecho a la Protección de Datos en la Historia clínica y la Receta electrónica* (Coord. R. Cáliz Cáliz et al.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, pp. 305-320.

PÉREZ CAMPILLO, L., "Una aproximación al *big data* y al *blockchain* sanitario y su implicación en la protección de datos personales", *Revista de Derecho y Genoma Humano,* Núm. Extraordinario, 2019, pp. 547-567.

PÉREZ GÓMEZ, J. M., "El concepto de dato de salud y otras categorías afines de datos en el proyecto de Reglamento Europeo de Protección de Datos", *Actualidad de Derecho Sanitario,* núm. 225, 2015, pp. 297-308.

PÉREZ GÓMEZ, J. M., "Especialidades en el sector sanitario" en AA.VV., *La adaptación al nuevo marco de protección de datos tras la RGPD y la LOPDGDD,* (Coord. J. López Clavo), Wolters Kluwer, Madrid, 2019, pp. 873-902.

PÉREZ GÓMEZ, J.M., "Especialidades en el sector sanitario" En AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* (Coord., J. López Calvo) Wolters Kluwer, Madrid, pp. 873-902.

PÉREZ LUÑO, A.E., "La protección de los datos personales de carácter sanitario", en AA.VV., *Derechos humanos y protección de datos personales en el Siglo XXI: homenaje a Cinta Castilloo Jiménez,* (Coord. Sánchez Bravo, A.A.), Punto Rojo Libros, Sevilla, 2014, pp. 113-153.

PÉREZ LUÑO, A.E., "Nuevos derechos fundamentales en la era tecnológica: la libertad informática", *Anuario de Derecho Público y Estudios Políticos,* núm. 2, 1989, pp. 639-669.

PÉREZ ROYO, J., *Curso de Derecho constitucional,* 8ª Ed., Marcial Pons, Madrid, 2002.

PÉREZ SANTONJA, T., GÓMEZ PAREDES, L., ÁLVAREZ MONTERO, S., CABELLO BALLESTEROS, L. y MOMBIELA MURUZABAL, M.T., "Historia clínica electrónica: evolución de la relación médico-paciente en la consulta de Atención Primaria", *Semergen,* vol. 43, núm. 3, 2016 pp. 175-181. Documento disponible en: http://dx.doi.org/10.1016/j.semerg.2016.03.022 (última consulta 12/03/20).

PÉREZ-LUÑO ROBLEDO, E. C., "El "habeas data" sanitario: análisis de la jurisprudencia constitucional", en AA.VV., *FODERTICS 6.0: los nuevos retos del Derecho ante la era digital,* (Coord. F. Bueno de la Mata), Comares, Madrid, 2007, pp. 107-113.

PÉREZ, S.C. y FERNÁNDEZ. N., "Apoyo para la toma de decisiones", *Cátedra de gestión de datos UTN-F.R.M.* 3er. Año, 2006, [Documento sin paginación]. Documento disponible en http://www.edutecne.utn.edu.ar/sistemas-informacion/sist-info.htm (última consulta 01/03/18).

PINEDO GARCÍA, I., "Historia clínica electronica: cuestiones prácticas y legales desde la perspectiva de la protección de datos de carácter personal", en AA.VV., *Derecho y nuevas tecnologías,* (Coords. A. I. Herrán Ortiz, A. Emaldi Cirión y M. Enciso Santocildes)*,* Universidad de Deusto, Navarra, 2011, pp. 289-302.

PINEDO GARCÍA, I., "Protección de datos sanitarios: la historia clínica y sus accesos", *Revista CESCO de Derecho de Consumo,* núm. 8, 2013, pp. 306-318.

PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad,* Reus, Madrid, 2016.

PIÑAR MAÑAS, J.L., "La protección de datos: nuevos desafíos", en AA.VV., *España constitucional (1978-2018): trayectorias y perspectivas,* Vol. 5, Tomo 5, Madrid: Centro de Estudios Políticos y Constitucionales, (Dir. B. Pendás García), Centro de Estudios Políticos y Constitucionales, España, 2018, pp. 4489-4502.

PIÑAR MAÑAS, J.L., "El objeto del nuevo Reglamento Europeo de Protección de Datos", en AA.VV., *Derecho administrative e integración europea: estudios en homenaje al profesor José Luis Martínez López-Muñiz*, (Coords. J.L. Laguna de Paz, J.L., I. Sanz Rubiales, I. e I. De los Mozos Touya), Reus, Madrid, 2017, pp. 337-348.

PLANA ARNALDOS, Mª C., "Los datos personales como contraprestación", en AA.VV., *Protección de datos personales,* (Coord. I. González Pacanowska), Asociación de profesores de Derecho Civil, Tirant lo Blanch, Valencia, 2020, pp. 561-618.

PONCE DE LEÓN, A., "La evolución humana. Un conocimiento integrador", *Innovación educativa,* vol. 18, núm. 77, 2018, pp. 57-69.

POQUET CATALÁ, R., "La difícil conjugación del deber de protección de datos de carácter personal y la vigilancia de la salud", en AA.VV., *Actas Congreso Prevencionar 2017,* (Dir. A. Sánchez-Toledo Ledesma), Seguridad y Bienestar, Madrid, 2017, [Documento sin paginación]. Documento disponible en: file:///C:/Users/lety2/Downloads/Dialnet-ActasCongresoPrevencionar2017-722910.pdf (última consulta 22/03/20).

POULLET, Y., *Le RGPD face aux défis de l´intelligence artificielle,* Larcier, Bruxelles, 2020.

POWER, D.J., "A Brief History of Decision Support Systems"*, DSSResources.COM*, 2007, [DOCUMENTO SIN PAGINACIÓN]. Disponible en: http://dssresources.com/history/dsshistory.html (última consulta 18/02/18).

POYATOS DÍAZ, J.M., "*Big Data* y el sector de la salud: el futuro de la sanidad", 2013, [Documento sin paginación]. Documento disponible en http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad (última consulta 22/01/19).

PRESS, G., *A Very Short History Of Big Data,* Forbes, 2013, [Documento sin paginación]. Disponible en: https://www.forbes.com (última consulta 08/01/18).

PRESTON, P., "Choosing and installing the right ERP solution", *TechTarget,* 1999, [DOCUMENTO SIN PAGINACIÓN]. Documento disponible en: http://www.computerweekly.com/feature/Choosing-and-installing-the-right-ERP-solution (última consulta 10/10/17).

PUENTE ESCOBAR, A., "Informes y sentencias relevantes*", 8ª Sesión Abierta de la AEPD. Gran Auditorio Ramón y Cajal*, junio 2016 [Documento sin paginación]. Documento disponible en: https://docplayer.es/69057697-Informes-y-sentencias-relevantes-agustin-puente-escobar-abogado-del-estado-jefe-del-gabinete-juridico.html (última consulta 31/05/19).

PUYOL MONTERO, J., *Aproximación jurídica y Económica al Big Data,* Ed. Tirant lo Blanch, Madrid, 2015.

PUYOL MONTERO, J., *Guía divulgativa del Reglamento General de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018.

PUYOL MORENO, J., "Una aproximación a *big data"*, *Revista de Derecho UNED,* núm. 14, 2014, pp. 471 – 505. Documento disponible en: http://e-spacio.uned.es/fez/eserv/bibliuned:RDUNED-2014-14-7150/Documento.pdf (última consulta 02/08/19).

QUINTANA MARTÍNEZ, V., "Ley de protección de datos en el paciente en las instituciones sanitarias", en AA.VV., Actualización en salud para la mejora de la calidad de vida, (Comps. M.M. Molero Jurado, A.B. Barragán Martín, A. Martos Martínez, M.M. Simón Márquez, N.F. Oropesa Ruíz, M. Sisto, B.M. Tortosa Martínez y A. González Moreno), Vol. II, Asociación Universitaria de Educación y Psicología (ASUNIVEP), España, 2019, pp. 615-620.

QUINTANILLA, M.A., *Tecnología: un enfoque filosófico y otros ensayos de filosofía de la tecnología,* Fondo de Cultura Económica, México, 2005.

RALLO LOMBARTE, A., "Hacia un sistema europeo de protección de datos: las claves de la reforma", *RDP*, Núm. 85, 2012, pp. 15-56.

RAMÍREZ NEILA, N.M., "Accesos legítimos a las historias clínicas electrónicas", en AA.VV., *El Derecho a la Protección de Datos en la Historia clínica y la Receta electrónica*, (Coord. R. Cáliz Cáliz et al.), Thomson Reuters-Aranzadi, Cizur Menor, 2009, pp. 289-304.

RAMIRO AVILÉS, M.A., "Reutilización con fines de investigación en materia de salud y bomédica de datos persoanels recogidos con anterioridad a la entrada en vigor a esta ley", en AA.VV., *Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relacion con el RGPD),* (Dirs. M. Arenas Ramiro y A. Ortega Giménez), Editoral Jurídica Sepin, Madrid, 2019, pp. 492-493.

RAMIRO AVILÉS, M.A., "Tratamiento de datos de salud", en AA.VV., *Protección de datos: Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relacion con el RGPD),* (Dirs. M. Arenas Ramiro y A. Ortega Giménez), Editoral Jurídica Sepin, Madrid, 2019, pp. 459-467.

RAMÓN MORENO, J. R., "Crowdsourcing creativo o la democratización del talento", marzo 2012, [Documento sin paginación]. Documento disponible en: http://www.marketingnews.es/varios/opinion/1064265028705/crowdsourcing-creativo-democratizacion-talento.1.html (última consulta 09/09/18).

RASHID, M.A., HOSSAIN, L. and PATRICK, J.D., "The Evolution of ERP Systems: A Historical Perspective", *Idea Group Publishing,* 2002, pp. 1-16. Documento disponible en: https://faculty.biu.ac.il/~shnaidh/zooloo/nihul/evolution.pdf (última consulta 15/10/17).

REALE, G. y ANTISERI, D., *La Historia del Pensamiento Filósofico y Científico. Tomo I,* Editorial Herder, Barcelona, 1988.

REBOLLO DELGADO, L. y SERRANO PÉREZ, Mª M., *Manual de protección de datos*, 3.ª Ed., Dykinson, Madrid, 2019.

REBOLLO DELGADO, L., "Derechos de la personalidad y datos personales", *Revista de Derecho Público,* núm. 44, 1998, pp. 143-206.

REBOLLO DELGADO, L., *El Derecho Fundamental a la Intimidad,* Ed. Dykinson, Madrid, 2005.

RECUERDO LINARES, M., "Transferencias internacionales de datos genéticos y datos de salud con fines de investigación", *Revista de Derecho y Genoma Humano,* Núm. Extraordinario, 2019, pp. 413-433.

RISKIN, D., "The Next Revolution in Healthcare", *Forbes,* 2012, [Documento sin paginación]. Documento disponible en: https://www.forbes.com/sites/singularity/2012/10/01/the-next-revolution-in-healthcare/#26f260d055cc (última consulta 22/01/19).

RIVERO ORTEGA, R., *El expediente administrativo. De los legajos a los soportes electrónicos*, Thomson Aranzadi, Cizur Menor, 2007.

RODRÍGUEZ AYUSO, J. F., "Cumplimiento de la normativa en materia de protección de datos personales en estado de alarma por parte de las Administraciones Públicas", en AA.VV., *Las respuestas del derecho a las crisis de salud pública*, (Dirs. Elena Atienza Macías y Juan Francisco Rodríguez Ayuso), Editorial Dikinson, Madrid, 2020, pp. 89-106.

RODRIGUEZ AYUSO, J.F., "Responsabilidad proactiva de las administraciones públicas ante el Covid-19", *Actualidad Administrativa*, Nº 6, Sección Administración del siglo XXI, Junio 2020, pp. 1-17.

RODRÍGUEZ AYUSO, J.F., *Figuras y responsabilidades en el tratamiento de datos personales,* JB Bosch, Barcelona, 2019.

RODRÍGUEZ AYUSO, J.F., *Garantía administrativa de los derechos del interesado en materia de protección de datos personales,* JB Bosch, Barcelona, 2021.

RODRÍGUEZ AYUSO, J.F., *Privacidad y coronavirus: aspectos esenciales,* Editorial Dikinson, Madrid, 2020.

RODRÍGUEZ GÓMEZ, D., "Modelos para la creación y gestión del conocimiento: una aproximación teórica", *Educar*, núm. 37, 2006, p. 27, pp. 25 – 39.

RODRÍGUEZ LÓPEZ, P., *Derecho Administrativo Patrimonial: comentario a la Ley 33/2003, del Patrimonio de las Administraciones Públicas, Tomo I,* Bosch, Barcelona, 2005.

RODRÍGUEZ LÓPEZ, P., *Responsabilidad patrimonial de la Administración en materia sanitaria*, Atelier, Barcelona, 2007.

ROGERS, S., "Top 10 Trends in *Business Intelligence* and Analytics for 2011", *Enterprise Management EMA BloGC,* 2011 [Documento sin paginación]. Documento disponible en: http://bloGC.enterprisemanagement.com/shawnrogers/2011/01/11/top-10-trends-in-business-intelligence-and-analytics-for-2011/ (última consulta 10/01/18).

ROMEO CASABONA, C. M.ª y otros, *La Ética y el Derecho ante la biomedicina del futuro,* Universidad de Deusto, Bilbao, 2006.

ROVIRI VIÑAS, A., "Reflexiones sobre el derecho a la intimidad en relacion a la informática, la medicina y los medios de comunicación", *Revista de Estudios Políticos,* núm. 77, 1992, pp. 259 y ss.

ROYO V. y MÉLER, N., "Multas impuestas por la AEPD en aplicación del RGPD: motivos y cuantías", *Diario La Ley*, 5 de septiembre, 2019, pp. 1-4.

RUBÍ PUIG, A., Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD*, Revista de Derecho Civil,* vol. V, núm. 4, octubre-diciembre 2018, pp. 53-87.

RUIZ MIGUEL, C., "El derecho a la protección de datos de los datos personales en la Carta de los Derechos Fundamentales de la Unión Europea: análisis crítico", *Revista de Derecho Comunitario Europeo,* núm. 14, 2003, pp. 7-43.

SACKETT, D.L., STRAUS, S.E., RICHARDSON, W. S., GLASZIOU, P. and HAYNES, R. B., *Medicina Basada en la Evidencia: como practicar y enseñar la MBE (3ª Ed.),* Ed. Elsevier España, Madrid, 2005.

SAN SEGUNDO ENCINAR, J.M. (Dir.), *Big data en salud digital*, Fundación Vodafone, Ed. Minetad, Red. Es., Madrid, 2017.

SÁNCHEZ BRAVO, A., *La protección del derecho a la libertad informática en la Unión Europea*, Ed. Secretariado de Publicaciones de la Universidad de Sevilla, Sevilla, 1998.

SÁNCHEZ CARAZO, C., "El derecho a la confidencialidad y a la información de los datos sanitarios", en AA.VV., *La libertad de información: gobierno y arquitectura de Internet,* L. Corredoira y Alfonso: III Seminario -Complutense de Telecomunicaciones e Información, Madrid, 2001, pp. 237-243.

SÁNCHEZ CARO, J. y ABELLÁN, F., *Imprudencia y negligencia en la profesión sanitaria,* Comares, Granada, 2001.

SÁNCHEZ CARO, J., "La historia clínica gallega: un paso importante en la gestión del conocimiento", *Derecho y salud,* vol. 18, núm. 1, 2009, pp. 57-86.

SÁNCHEZ DEL CAMPO REDONET, A., "Inteligencia artificial y privacidad", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 983-995.

SÁNCHEZ ORS, C., "El Delegado de Protección de Datos (Arts. 37-39 RGPD. Arts. 34-37 LOPDGDD)", en AA.VV., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, (Coord. J. López Calvo), Wolters Kluwer, Madrid, 2019, pp. 851-872.

SANTOS MORÓN, MªJ., "Tratamiento de datos, sujetos implicados, responsabilidad proactiva", en AA.VV., *Protección de datos personales,* (Coord. I. González Pacanowska), Asociación de profesores de Derecho Civil, Tirant lo Blanch, Valencia, 2020, pp. 23-77.

SAQUERO RODRÍGUEZ A., DE LA TORRE, I. y DURANGO PASCUAL, A., "Análisis de aspectos de interés sobre privacidad y seguridad en la historia clínica electrónica", *RevistaeSalud.com,* vol. 7, núm. 27, 2011, pp. 1-8.

SARAN, C., "Putting ERP in the cloud", *Computer Weekly*, 2010, [Documento sin paginación]. Documento disponible en: http://www.computerweekly.com/news/1280092536/Putting-ERP-in-the-cloud (última consulta 17/01/18).

SARRIÓN ESTEVE, J. y BENLLOCH DOMÈNECH, C., "Protección de los datos clínicos relativos a la propia salud", en AA.VV., *La protección de la salud en tiempos de crisis: nuevos retos del bioderecho en una* sociedad plural (Dirs. A. Fernández-Coronado González y S. Pérez Álvarez), Tirant lo Blanch, Valencia, 2014, pp. 331-359.

SARRIÓN ESTEVE, J., "La protección de la salud, la vida y la integridad física en tiempos de pandemia en la doctrina constitucional. A propósito del ATC 40/2020 del 30 de abril", *Actualidad Jurídica Iberoamericana,* N.º 14, 2021, pp. 1026-1039.

SARRIÓN ESTEVE, J., "Las novedades de la nueva normativa de protección de datos y su aplicación a los ensayos clínicos de menores", *DS: Derecho y Salud,* Vol. 27, 2017, pp. 229-237.

SCHMIDT, E., "Eric Schmidt at Techonomy", *Techonomy,* 2010, [DOCUMENTO SIN PAGINACIÓN]. Documento disponible en http://www.techonomy.com/.

SCHROECK, M., SHOCKLEY, R., ROMERO-MORALES, D. y TUFANO, P., "Analytics: el uso de *Big Data* en el mundo real. Cómo las empresas más innovadoras extraen valor de datos inciertos. Informe Ejecutivo", *IBM Global Business Services Business Analytics and Optimisation y la Escuela de Negocios Saïd en la Universidad de Oxford*, 2012, [Documento sin paginación]. Documento disponible en: ftp://ftp.software.ibm.com/la/documents/swg/es/analytics/IBM_Analitica_uso_de_Big_Data_en_mundo_para_sector_servicios_financieros.pdf (última consulta 19/03/18).

SERRANO PÉREZ, Mª M., "La necesidad de una ley de protección de datos en salud", *Bioderecho.Es,* núm. 8, 2018, pp. 1-6.

SERRANO PÉREZ, Mª. M., "Salud pública, epidemiología y protección de datos" en AA.VV., *Tratado de Derecho Sanitario,* (Coord. Larios Risco et al.), Editorial Aranzadi, Navarra, 2013, pp. 1091-1113.

SERRANO PÉREZ, Mª M., SÁNCHEZ NAVARRO, C. y ZURRIAGA LLORENS, C., "A modo de reflexión y crítica en torno a la propuesta de reglamento europeo de protección de datos y algunas de las enmiendas presentadas en relación con la epidemiología y la salud", *Derecho y Salud,* vol. 23, núm. extraordinario, 2013, pp. 285-293.

SERRANO PÉREZ, Mª M., "*Big Data* o la acumulación masiva de datos sanitarios: Derechos en riesgo en el marco de la sociedad digital", *Derecho y Salud,* Vol. 25, septiembre, extra. 2015, pp. 51-64.

SERRATO MARTÍNEZ, L., "El régimen legal de acceso a la historia clínica y sus garantías", *Revista Jurídica de Castilla y León,* núm. 17, 2009, pp. 177-215.

SIEGEL, E., *Analítica predictiva. Predecir el futuro utilizando Big Data*, Ed. Anaya, Madrid, 2014.

SILVANI, L., *Historia de la Filosofía,* Editorial Optima, Barcelona, 2003.

SOCHE LÓPEZ, S., "Metodología para el modelamiento de datos basado en Big Data, enfocados al consumo de tráfico (voz-datos) generado por los clientes", *Especialización en Gerencia Integral de Proyectos,* Universidad Militar Nueva Granada Bogotá, 2016, p. 5. Documento disponible en: https://core.ac.uk/download/pdf/143452539.pdf

STAMFORD, C., "Gartner EXP Worldwide Survey of More than 1,500 CIOs Shows IT Spending to Be Flat in 2009, *Gartner,* enero 2009, [Documento sin paginación]. Documento disponible en: Available from: https://www.gartner.com/newsroom/id/855612 (última consulta 21/01/18).

STANTON, J., *An introduction to Data Science,* Ed. Syracuse University, Nueva York, 2012.

SUAREZ RUBIO, S. M.ª., *Constitución y privacidad sanitaria*, Tirant lo Blanch, Valencia, 2015.

SUERO SALAMANCA, J.A., "Comentarios a la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre", 2001, pp. 1-10. Documento disponible en: http://www.madrid.org/usupadron/legislacion/protdatos/protecciondatos.pdf (última consulta 22/08/18).

SVEIBY, K., *The new organizatonial wealth: managing and measuring intangible assets,* Ed. Berret – Koelher Publishers, San Francisco,1998.

TASCÓN, M., "Introducción: *Big Data*. Pasado, presente y futuro". *Telos: Cuadernos de comunicación e innovación,* núm. 95, 2013, pp. 47-50.

TERRIBAS I SALA, N., "Confidencialidad de datos sanitarios: de la norma a la práctica médica", en AA.VV., *Los avances del derecho ante los avances de la medicina,* (Cords. S. Adroher Biosca, F. De Montalvo Jääskeläinen, M.R. Corripio Gil-Delgado y A.B. Veiga Copo), Aranzadi Thomson Reuters, Navarra, 2008, pp. 791-806.

TITO HUAMANÍ, P.L., "Gestión del conocimiento: un nuevo paradigma organizacional", *Gest. Terc. Milen*, núm. 9, octubre, 2002, [Documento sin paginación]. Documento disponible en: https://sisbib.unmsm.edu.pe/bibvirtual/Publicaciones/administracion/v05_n9/gestion_conocimiento.htm# (última consulta 19/03/17)

TIWANA, A., *The Knowledge Management Toolkit,* Ed. Prentice Hall, Upper Saddle River, 2002.

TJOMSLAND, I.A., "To Digest of Papers: The Gap between MSS Products and User Requirements*", Fourth IEEE Symposium on Mass Storage System*s, abril 1980, pp. 15-17.

TOMÁS-VALIENTE LANUZA, C., "La vulneración de la intimidad en el ámbito de los datos sanitarios: algunos supuestos problemáticos desde la óptica penal" en AA.VV., *La Salud: intimidad y libertades informativas,* (Coord. Tomás-Valiente Lanuza, C.), Tirant lo Blanch, Valencia, 2006, pp. 243-276.

TORRES GARCÍA, T.F., "Responsabilidad patrimonial de la administración sanitaria", en AA.VV., *Lecciones de Derecho Sanitario* (Coord. M. Juane Sánchez), Ed. Servizo de Publicacións, Cataluña, 1999, pp. pp. 569-594.

TRONCOSO REIGADA, A., "Autoridades de control independientes" en AA.VV., *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, (Dir. J.L. Piñar Mañas), Ed. Reus, Madrid, pp. 461-512.

TRONCOSO REIGADA, A., "Hacia un nuevo marco jurídico europeo de protección de datos personales", *REDE*, núm. 43, 2012, pp. 25-184.

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", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada,* núm. 49, Julio-Diciembre 2018, pp. 187-266.

TRONCOSO REIGADA, A., "La confidencialidad de la historia clínica", *Cuadernos de Derecho Público,* Núm. 27, 2006, pp. 45-147.

TRONCOSO REIGADA, A., *La protección de datos personales. En busca del equilibrio,* Tirant lo Blanch, Valencia, 2010.

VALDUCIEL, V., "La aplicación del Reglamento General de Protección de Datos en el Sector Salud de Datos", *Revista de la Sociedad Española de Informática y Salud,* núm. 122, 2017, pp. 15-17.

VALERO TORRIJOS J. y LÓPEZ PELLICER, J.A., "Algunas consideraciones sobre el derecho a la protección de datos personales en la actividad administrativa", *RVAP,* núm. 59, 2001, pp. 255-288.

VALERO TORRIJOS, J. y CERDÁ MESEGUER, J.I., "Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos de COVID-19", *Eunomía. Revista en Cultura de la Legalidad,* núm. 19, octubre 2020 – marzo 2021, pp. 103-126.

VALERO TORRIJOS, J. y PARDO LOPEZ, M.M. "Institutional Backing and PSI Reuse: Is the EU Going Too Far or Just Going in the Wrong Way?", *Masaryk University Journal of Law and Technology (MUJLT)*, vol. 6, núm. 3, 2012, 455-470.

VALERO TORRIJOS, J., "Acceso, reutilización y gestión avanzada de la información en el ámbito de la Administración sanitaria: implicaciones jurídicas desde la perspectiva de la innovación tecnológica", en AA.VV., *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información,* (Coords. J. Valero y M. Fernández), Thomson Reuters Aranzadi, Cizur Menor, 2016, pp. 631-667.

VALERO TORRIJOS, J., "De la digitalización a la innovación tecnológica: valoración jurídica del proceso de modernización de las administraciones públicas españolas en la última década (2004-2014)", *Internet, Derecho y Política*, núm. 19, 2014, pp. 117-129.

VALERO TORRIJOS, J., "La exigencia legal de formatos abiertos y reutilizables en la gestión de la contratación pública", en AA.VV., *Transparencia, innovación y buen gobierno en la contratación pública*, (Dirs. M. Fernández y M.F. Gómez), Tirant lo Blanch, Valencia, 2019, pp. 49-74.

VALERO TORRIJOS, J., "La necesaria reconfiguración de las garantías jurídicas en el contexto de la transformación digital del sector público", en AA.VV., *Sociedad digital y Derecho* (Ed. T. de la Quadra y J.L. Piñar), Boletín Oficial del Estado, Madrid, 2018, pp. 375-396.

VALERO TORRIJOS, J., "Las quiebras en internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado", en AA.VV., *La protección de los Datos Personales en Internet ante la Innovación Tecnológica,* (Coord. J. Valero Torrijos), Editorial Aranzadi, Cizur Menor (Navarra), 2013, pp. 25-63.

VÁZQUEZ DE CASTRO, E., "Titularidad y responsabilidad en la economía del dato", *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 46, 2018, p.52.

VIGUERAS PAREDES, P., "Intimidad, confidencialidad y protección de la información sanitaria. Estudio práctico del acceso al aplicativo Selene por facultativos del Servicio Murciano de Salud", *Revista Bioderecho.es,* Núm. 6, 2017, pp. 1-20.

VIGUERAS PAREDES, P., "La historia clínica: acceso, disponibilidad y seguridad", *Revista Bioderecho.es*, núm. 6, 2017, pp. 1-20.

VILARIÑO PINTOS, E. "Los derechos de la persona en el ámbito de las tecnologías de la información", en AA.VV., *El derecho a la intimidad y a la privacidad y las Administraciones Públicas,* (Dir. D. Bello Janeiro), Ed. Escola Galega de Administración Pública, Santiago de Compostela, 1999.

VILASALU SOLANA, M., "Derecho de intimidad y protección de datos personales", en AA.VV., *Derecho y nuevas tecnologías,* (Coord. Peguera Poch, M.), Universitat Oberta de Catalunya, Editorial UOC, España, 2005, pp. 93-140.

VILASALU SOLANA, M., "El Reglamento general de protección de datos (Reglamento 2016/679): aspectos clave", en AA.VV., *Derecho de Internet,* Universitat Oberta de Catalunya, Editorial UOC, España, 2017.

VILASALU SOLANA, M., "Las exigencias de información en el RGPD y en la LO 3/2018 de Protección de Datos y garantía de los derechos digitales. ¿contribuyen a la formación de un consentimiento de mejor calidad?", en AA.VV., *El Reglamento General de Protección de Datos: un enfoque nacional y comparado. Especial referencia a la LO 3/2018 de Protección de Datos y garantía de los derechos digitales,* (Eds. R. García Mahamut y B. Tomás Mallén), Tirant lo Blanch, Valencia, 2019, pp. 209-236.

VILASALU SOLANA, M., "Privacidad, redes sociales y el factor humano", en AA.VV., *Derecho y redes sociales*, (Coord. A. Rallo Lombarte y R. Martínez Martínez), Civitas, Madrid, 2010, pp. 55-82.

VILLASECA, M., "El Delegado de Protección de Datos", *I+S Revista de la Sociedad Española de Informática y Salud,* núm. 127, Febrero 2017, pp. 21-23.

VILLAVERDE MENÉNDEZ, I., "Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", *Revista Española de Derecho Constitucional,* núm. 41, 1994, pp. 187 y ss.

YANES, L.M., "El derecho de Autodeterminación Informativa frente a las Administraciones Públicas (Comentario a la STC 254/1993, de 20 de julio)", *Revista Andaluza de Administración Pública,* núm. 16, 1993, pp. 119 y ss.

ZAVALA DE GONZÁLEZ, M.M., *Derecho a la Intimidad*, Ed. Abeledo-Perrot, Buenos Aires, 1982, pp. 29-29.

TABLA NORMAS CITADAS

Deontológico de la Profesión de Enfermería (Madrid, 14-7-1989, corregido y ratificado en resolución 2/1998).

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 probidad y las comunicaciones electrónicas).

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.

Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.

Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p.29).

Directiva 95/46/CE del Parlamento europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos a efectos.

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

Instrucción 1/1995, de 1 de marzo de la AEPD, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito, BOE núm. 54, de 4 de marzo de 1995.

Instrucción 1/1996, de 1 de marzo de la AEPD, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios, BOE núm. 62, de 12 de marzo de 1996.

Instrucción 1/1998, del 19 de enero, de la AEPD relativa al ejercicio de los derechos de acceso, rectificación y cancelación, BOE núm. 25, de 29 de enero de 1998.

Instrucción 2/1995, de 4 mayo, de la AEPD, sobre medidas que granizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal, BOE núm. 110, de 9 de mayo de 1995.

Ley 14/1986, de 25 de abril, General de Sanidad.

Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud

Ley 30/1979, sobre extracción y trasplante de órganos.

Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Ley 55/2003, de 16 de diciembre, del Estatuto Marco del personal estatutario de los servicios de salud.

Ley 58/2003, de 17 de diciembre, General Tributaria.

Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

Ley de Expropiación forzosa de 1954.

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, BOE núm. 298, de 14 de diciembre de 1999.

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

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

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, BOE núm. 262, de 31 de octubre de 1992.

Orden de 26 de octubre de 2011, de Galicia, que específica los criterios técnicos y/o científicos para el acceso a la historia clínica a efectos epidemiológicos y de salud pública (DOG de 16- 11-2011).

Orden por la que se aprueba el Reglamento General para el Régimen, Gobierno y Servicio de las Instituciones Sanitarias de la Seguridad Social, de 19 de julio de 1972.

Orden SAS/3470/2009, de 16 de diciembre, por la que se publican las directrices sobre estudios posautorización de tipo observacional para medicamentos de uso.

Orden SSI/445/2015, de 9 de marzo, por la que se modifican los anexos I, II y III del Real Decreto 2210/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica, relativos a la lista de enfermedades de declaración obligatoria, modalidades de declaración y enfermedades endémicas de ámbito regional.

Propuesta de Reglamento del Parlamento Europeo y del el Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos),

Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los Ensayos Clínicos con Medicamentos, los Comités de Ética de la Investigación con medicamentos (CEIm) y el Registro Español de Estudios Clínicos (RD-ECM).

Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

Real Decreto 1372/1986, de 13 de junio, por el que se aprueba el Reglamento de Bienes de las Entidades Locales.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, BOE núm. 17, de 19 de enero de 2008.

Real Decreto 1723/2012, de 28 de diciembre, por el que se regulan las actividades de obtención, utilización clínica y coordinación territorial de los órganos humanos destinados al trasplante y se establecen requisitos de calidad y seguridad.

Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas por el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio. BOE núm. 49 de 26 de febrero de 2000.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, BOE núm. 106, de 4 de mayo de 1993.

Real Decreto 831/2010, de 25 de junio, de garantía de la calidad asistencial de la prestación a la interrupción voluntaria del embarazo.

Real Decreto Legislativo 1/2015, de 24 de julio, por el que se aprueba el texto refundido de la Ley de garantías y uso racional de los medicamentos y productos sanitarios.

Recomendación núm. R (97) 5 del Consejo de Europa sobre la protección de datos médicos de 13 de febrero de 1997.

Reglamento (CE) 45/2001, del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Reglamento (CE) N.º 133/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31,12,2008, p. 70).

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 (Reglamento general de protección de datos).
Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea.
Reglamento (UE) 536/2014 del Parlamento Europeo y del Consejo de 16 de abril de 2014 sobre los Ensayos Clínicos de Medicamentos de uso humano (RUE-ECM).
Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).
Texto Refundido de la Ley Reguladora de las Haciendas Locales.
Tratado Constitutivo de la Comunidad Europea.
Tratado de Funcionamiento de la Unión Europea.
Tratado de Lisboa por el que se modifican el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea (2007/ C 306/01).

TABLA JURISPRUDENCIA

SSTC 290 de 30 de noviembre.

SSTC 292/2000 de 30 de noviembre.

SSTC 94/1998, de 4 de mayo.

SSTC 99/2002, de 6 de mayo.

SSTS 04-02-02

SSTS 29-03-1988

SSTS de 25 de abril de 1994.

STC 115/2000, de 5 de mayo.

STEDH de 25 de febrero de 1997, caso Z. c. Finlandia (Rec. Núm. 9/1996).

STEDH de 4 de diciembre de 2008, caso S. and Marper v. The United Kingdom.

STJUE (Gran Sala) de 16 de diciembre de 2008, asunto C-73/07 (caso Satakunnan Markkinapörssi y Satamedia)

STJUE de 6 de noviembre de 2003, asunto C-101/01 (caso Lindqvist).

STJUE (Gran Sala) de 13 de mayo de 2014, asunto C-131/12 (caso Google).

STJUE (Gran Sala) de 29 de junio de 2010, asunto C-28/08 (caso Comisión/Bavarian Lager).

STJUE (Gran Sala) de 6 de octubre de 2015, asunto C-362/14 (caso Schrems).

STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz).

STJUE (Sala Cuarta) de 17 de octubre de 2013, asunto C-291/12 (caso Schwartz).

STJUE (Sala Segunda) de 19 de octubre de 2016, asunto C-582/14 (caso Breyer).

STJUE (Sala Tercera) de 1 de octubre de 2015, asunto C-201/14, (caso Bara)

STJUE (Sala Tercera) de 24 de noviembre de 2011, asunto C-70/10 (caso Scarlet).

STJUE de 24 de noviembre de 2011, ASNEF y FECEMD, C-468/10 y C-469/10, Rec. p. I-12181.

STJUE de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, Rec. p. I-11063.

STS de 29 de mayo de 2007.

TSJ Navarra Sentencia núm. 111/2012 de 8 febrero.

Sentencia del Tribunal Supremo 532/2015, de 23 de septiembre.

Sentencia del Tribunal Supremo, Sala de lo Contencioso-Administrativo, de 20 de febrero 2012.

Sentencia núm. 532/2015 del Tribunal Supremo, Sala de lo Penal, Sección 1ª, de 23 de septiembre.

Sentencias de la Audiencia Provincial de Palma de Mallorca de 26 de enero y 16 de febrero de 2015.

Sentencia del Tribunal Supremo de 18 de octubre de 2012.

TABLA INFORMES, DOCUMENTOS Y PROYECTOS

Accenture consulting, *Inyección de inteligencia para el sector sanitario*, 2019. Documento disponible en: https://www.accenture.com/_acnmedia/pdf-97/accenture-health-ai-survey-spanish.pdf (última consulta 03/04/20).

Bebea González, I., Martínez Fernández, A. y Rey Moreno, C., *Guía de la Cooperación Española para la incorporación de las TIC en las intervenciones de Salud en la Cooperación para el Desarrollo,* Agencia Española de Cooperación Internacional para el Desarrollo, Departamento de Cooperación Sectorial y de Género, Área de Salud, 2012. Disponible en: https://www.aecid.es/galerias/que-hacemos/descargas/GUIA_TICs_SALUD.pdf (última consulta 23/02/20).

Agencia de Calidad del Sistema Nacional de Salud e Instituto de Información Sanitaria, *Historia Clínica Digital en el Sistema Nacional de Salud. Conjunto mínimo de datos de Informes Clínicos*, 2018. Documento disponible en: http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/CMDIC.pdf (última consulta 27/07/18).

Agencia Española de Protección de Datos, *Código de buenas prácticas en protección de datos para proyectos Big Data*, p. 18. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (última consulta 15/02/2021).

Agencia Española de Protección de Datos, *El uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios*, 2020.

Agencia Española de Protección de Datos, *Guía de Privacidad desde el Diseño*, 2019. Documento disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Agencia Española de Protección de Datos, *Guía para pacientes y usuarios de la Sanidad*, 2019. Disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

Agencia Española de Protección de Datos, *Guía para una evaluación de impacto en la protección de datos personales,* 2019. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Agencia Española de Protección de Datos, *Informe 0073/2010. Gabinete jurídico*, 2010. Disponible en: https://www.aepd.es/es/documento/2010-0073.pdf

Agencia Española de Protección de Datos, *Informe N/REF 36/2020 sobre los procesos de reconocimiento facial empleados para la realización de evaluaciones,* 2020.

Agencia Española de Protección de Datos, *Informe N/REF: 0017/2020*, de 12 de marzo 2020.

Agencia Española de Protección de Datos, *Informes jurídicos n.º 0248/2005, n.º 167/2005, n.º 656/2008, n.º 171/2008, n.º 283/2008, n.º 471/2008, n.º 617/2008, n.º 584/2009 y n.º 0054/2010*.

Agencia Española de Protección de Datos, *Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4),* 2019. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf (última consulta 05/03/20).

Bebea González, I., Martínez Fernández, A. y Rey Moreno, C., *Guía de la Cooperación Española para la incorporación de las TIC en las intervenciones de Salud en la Cooperación para el Desarrollo,* Agencia Española de Cooperación Internacional para el Desarrollo, Departamento de Cooperación Sectorial y de Género, Área de Salud, 2012. Disponible en: https://www.aecid.es/galerias/que-hacemos/descargas/GUIA_TICs_SALUD.pdf (última consulta 23/02/20).

Big Data international campus, *Data Mining vs Big Data*, febrero 2017, [Documento sin paginación]. Documento disponible en http://www.campusbigdata.com/big-data-blog/item/82-data-mining-vs-big-data (última consulta 02/04/18).

Big Data International Campus, *Data Mining vs Big Data*, febrero 2017, [Documento sin paginación]. Documento disponible en http://www.campusbigdata.com/big-data-blog/item/82-data-mining-vs-big-data (última consulta 02/04/18).

Centro Nacional de Excelencia Tecnológica en salud, *¿Qué es la Telesalud y la Telemedicina?,* 2017, [Documento sin paginación]. Disponible en: https://www.gob.mx/salud/cenetec/acciones-y-programas/que-es-la-telesalud-y-la-telemedicina (última consulta 02/03/20).

Comisión Central de Deontología de la Organización Médica Colegial de España y la Comisión Permanente del Consejo General de Colegios Oficiales de Médicos, *Decálogo de la Historia Clínica,* 2017. Disponible en: http://www.comalmeria.es/sites/default/files/noticias/docs/decalogo_sobre_historia_clinica.pdf

Comisión de Recursos Humanos del Sistema Nacional de Salud, *Protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en ciencias de la salud,* 2016. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-1200

Comité Europeo de Protección de Datos, *Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19,* 2020. Disponible en: https://edpb.europa.eu/our-work-tools/our-documents/ohjeet/guidelines-042020-use-location-data-and-contact-tracing-tools_es

Comité Europeo de Protección de Datos, *Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto Versión 2.0* adoptadas el 20 de octubre de 2020. Disponible en: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_es

Computer Sciences Corporation, *Big data Just Beginning to Explode*, Visually, 2012, [Documento sin paginación]. Documento disponible en: https://visual.ly/community/infographic/technology/big-data-just-beginning-explode (última consulta 17/01/18).

Consejería de Sanidad de la Junta de Castilla y León, *Guía de intimidad, confidencialidad y protección de datos de carácter personal*. Disponible en: http://www.enfermerialeon.com/docs/comision_deo/GuiaConfidencialidadDatosJCyL.pdf

Cosello de bioética de Galicia, *Ética en el acceso y en el uso de la documentación clínica: reflexiones y recomendaciones*, 2017. Disponible en: https://extranet.sergas.es/catpb/Docs/cas/Publicaciones/Docs/AtEspecializada/PDF-2669-es.pdf

El Confidencial, *Un matemático andaluz desconocido es el mejor cientofco de datos del mundo*, 2013. Documento disponible en: https://www.elconfidencial.com/tecnologia/2013-12-19/un-matematico-andaluz-desconocido-es-el-mejor-cientifico-de-datos-del-mundo_67675/ (última consulta 22/03/18).

EPB 603 Sistemas de Conocimiento, *Metodología para el Desarrollo de Proyectos en Minería de Datos CRISP-DM*, 2007, pp. 1-12. Documento disponible en: http://www.oldemarrodriguez.com/yahoo_site_admin/assets/docs/Documento_CRISP-DM.2385037.pdf (última consulta 25/09/18).

EPB 603 Sistemas de Conocimiento, *Metodología para el Desarrollo de Proyectos en Minería de Datos CRISP-DM*, 2007, pp. 1-12. Documento disponible en: http://www.oldemarrodriguez.com/yahoo_site_admin/assets/docs/Documento_CRISP-DM.2385037.pdf (última consulta 25/09/18).

Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*. Documento disponible en: https://www.ontsi.red.es/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf (última consulta 05/03/19).

Equipo de Trabajo de la Fundación Vodafone España y Red.es, *Informe de resultados Big Data en salud digital*. Documento disponible en: https://www.ontsi.red.es/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf (última consulta 05/03/19)

Feldman, B., Martin, E.M. and Skotnes, T., *Big Data Healthcare Hype and Hope*, 2012. Disponible en: http://www.west-info.eu/files/big-data-in-healthcare.pdf

Fundación de Ciencias de la Salud, *Intimidad, confidencialidad y secreto. Guías de ética en la práctica médica,* 2015, [Documento sin paginación]. Documento disponible en: https://www.cgcom.es/sites/default/files/guia_confidencialidad.pdf (última consulta 23/11/19).

Fundación Innovación Bankinter., *Big data. El poder de los datos*, 2015. Documento disponible en: https://www.fundacionbankinter.org/documents/20183/42758/Publicaci%C3%B3n+Big+data/cc4bd4e9-8c9b-4052-8814-ccbd48324147

Fundación Rock Health, *Big data in digital Health*, 2012. Documento disponible en: https://rockhealth.com/rock-report-big-data-healthcare/ (última consulta 23/07/18).

Fundación Salud 2000, *Informe del experto núm. 12 Acceso a la historia clínica con fines de investigación. Estado de la cuestión y controversias*, julio 2015.

Fundación Salud, "Acceso a la historia clínica con fines de investigación. Estado de la cuestión y controversias", *Informe del expert núm. 12*, 2015. Documento disponible en: https://www.fundacionmercksalud.com/wp-content/uploads/2017/06/12_Informe_Experto_datosHistoria_Cl%C3%ADnicas_WEB_.pdf

García Cumbreras, M.A., "eHealth (tecnología y medicina)", *Coddiinforme*, enero, 2017. Documento disponible en https://coddii.org/wp-content/uploads/2017/01/Informe-e-Health-2.pdf

Gost Garde, J., *Gestión sanitaria y tecnológica de la información,* 2001, pp. 37 -57. Disponible en: http://www.conganat.org/SEIS/informes/2001/PDF/2Gost.pdf (última consulta 03/03/20).

Grupo de Trabajo Artículo 29, *Annex: Health data in apps and devices,* 2015. Disponible en: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (última consulta 05/12/20).

Grupo de Trabajo del artículo 29, *Dictamen 05/2014 sobre técnicas de anonimización, (0829/14/ES WP216)*, 2014. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

Grupo de Trabajo del artículo 29, *Dictamen 3/2012, sobre la evolución de las tecnologías biométricas,* 2012.

Grupo de Trabajo del artículo 29, *Dictamen 6/2013 sobre protección de datos en la reutilización de la información del sector público*, 2013. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/wp242rev01-es.pdf

Grupo de Trabajo del Artículo 29*, Directrices sobre la evaluación de impacto relativa a la protección de datos (eipd) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679 (documento WP248)*, 2017. Documento disponible en: https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

Grupo de Trabajo del artículo 29, *Documento de Trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME) (Documento WP131)*, 2007. Disponible en: https://www.apda.ad/sites/default/files/2018-10/wp131_es.pdf

GTI, Software & Networking., *5 Diferencias entre Big Data y Business Intelligence,* 2015 [documento sin paginación]. Documento disponible en: http://noticias.gti.es/productos/5-diferencias-entre-big-data-y-business-intelligence/ (última consulta 25/02/18).

GTI, Software & Networking., *5 Diferencias entre Big Data y Business Intelligence,* 2015 [documento sin paginación]. Documento disponible en: http://noticias.gti.es/productos/5-diferencias-entre-big-data-y-business-intelligence/ (última consulta 25/02/18).

IBM100, *Pioneering Speech Recognition,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/speechreco/ (última consulta 21/12/17).

IBM100, *Relational Database,* [Documento sin paginación]. Disponible en: http://www-03.ibm.com (última consulta 21/12/17).

Informática, *El gran cuaderno de Big Data. Una guía práctica para emprender su primer proyecto de Big Data.* Documento disponible en: https://docplayer.es/19123678-El-gran-cuaderno-del-big-data-una-guia-practica-para-emprender-su-primer-proyecto-de-big-data.html

Iniciativa Aporta, Ministerio de Economía y Empresa, a través de la Entidad Pública Empresarial Red.es, y en colaboración con el Ministerio de Política Territorial y Función Pública, *Datos abiertos y sanidad: contexto tecnológico, actores implicados y marco jurídico.* Documento disponible en: https://datos.gob.es/es/documentacion/datos-abiertos-y-sanidad-contexto-tecnologico-actores-implicados-y-marco-juridico

Instituto de Ingeniería del Conocimiento, *Las 7V del Big Data: características más importantes,* 2016, [Documento sin paginación]. Documento disponible en: http://www.iic.uam.es/innovacion/big-data-caracteristicas-mas-importantes-7-v/#viabilidad (última consulta 05/03/18)

Instituto de Salud Carlos III, *Imagen médica. Informe de vigilancia tecnológica,* Noviembre 2015. Documento disponible en https://fipse.es/sites/default/files/documentos/documento/2017/04/16/20151130_informe_vtimagenmedica.pdf (última consulta 18/08/18).

McCrae., "Medicina de precisión", *I+S Revista de la Sociedad Española de Información y Salud,* núm. 118, septiembre 2016, pp. 45-50.

McKinsey Global Institute, *Big data: The Next Frontier for Innovation, Competition and Productivity*, junio 2011, [Documento sin paginación]. Dispone en:http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx (última consulta 22/03/19).

McKinsey Global Institute, *How artificial intelligence and data add value to businesses*, 2018, [Documento sin paginación]. Documento disponible en: https://www.mckinsey.com/featured-insights/artificial-intelligence/how-artificial-intelligence-and-data-add-value-to-businesses (última consulta 12/04/20).

Media Planner y Volcan, *Informe big data y Salud*, 2016. Documento disponible en: https://es.slideshare.net/AndresMacario2015/informe-big-data-y-salud?from_action=save (última consulta 02/02/19).

Ministerio de Economía y Empresa, *TIC y salud: aplicaciones móviles, redes sociales e iniciativas pública*, Red.es*,* [Documento sin paginación]. Documento disponible en: http://www.red.es/redes/es/magazin-red/reportajes/tic-y-salud-aplicaciones-moviles-redes-sociales-e-iniciativas-publicas (última consulta 22/09/18).

Ministerio de Sanidad y Política Social, *Las TIC en el Sistema Nacional de Salud. El programa Sanidad en línea,* enero 2010. Disponible en: https://www.mscbs.gob.es/profesionales/hcdsns/TICS/TICS_SNS_ACTUALIZACION_ES_2010.pdf (Última consulta 10/01/20).

Ministerio de Sanidad y Política Social, *Las TIC en el Sistema Nacional de Salud. El programa Sanidad en línea,* 2010. Disponible en: https://www.mscbs.gob.es/profesionales/hcdsns/TICS/TICS_SNS_ACTUALIZACION_ES_2010.pdf (Última consulta 10/01/20).

Ministerio de Sanidad, Consumo y Bienestar Social, *Sistema HCDSNS Historia Clínica Digital del Sistema Nacional de Salud,* 2018. Documento disponible en: https://www.msssi.gob.es/profesionales/hcdsns/contenidoDoc/WEB_Informe_de_Situacion_HCDSNS_Julio_2018.pdf (Consultado 21/07/18).

Ministerio de Sanidad, Proyecto de Historia Clínica Digital en el Sistema Nacional de Salud. Disponible en: https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf

Mooiweer, P. and Shockley, R., "Analítica de datos: El uso en el mundo real de *big data* en sanidad y ciencias de la vida. Cómo las organizaciones más innovadoras en sanidad y ciencias de la vida de la salud extraen valor de datos inciertos", *IBM Institute for Businees Value,* julio 2013.

Open Data Charter, Carta *Internacional de los Datos Abiertos. Principios*, octubre 2015 [Documento sin paginación]. Documento disponible en https://opendatacharter.net/principles-es/ (última consulta 14/04/18).

Power data. Especialistas en Gestión de datos, *Data Warehouse: todo lo que necesitas saber sobre el almacenamiento de datos*, [Documento sin paginación]. Documento disponible en: https://www.powerdata.es/data-warehouse (última consulta 27/02/18).

PriceWaterhouseCoopers, *Diez temas candentes de la Sanidad Española*, 2013. Documento disponible en: https://www.pwc.es/es/publicaciones/sector-publico/assets/diez-temas-candentes-sanidad-2013.pdf

Proyecto Visc+. Documento disponible en: http://aquas.gencat.cat/ca/projectes/visc/documental.

Schroeck, M., Shockley, R., Romero-Morales, D. y Tufano, P., "Analytics: el uso de big data en el mundo real. Cómo las empresas más innovadoras extraen valor de datos inciertos. Informe Ejecutivo", *IBM Global Business Services Business Analytics and Optimisation y la Escuela de Negocios Saïd en la Universidad de Oxford*, 2012. Documento disponible en: ftp://ftp.software.ibm.com/la/documents/swg/es/analytics/IBM_Analitica_uso_de_Big_Data_en_mundo_para_sector_servicios_financieros.pdf

Sinnexus. Business Intelligence Informática Estratégica, *Datamart*, 2016, [Documento sin paginación]. Documento disponible en: http://www.sinnexus.com/business_intelligence/datamart.aspx (último acceso 02/03/18).

Sinxus. Business Intelligence Informática EstratégicaNE, *Datawarehouse*, 2016, [Documento sin paginación]. Documento disponible en: http://www.sinnexus.com/business_intelligence/datawarehouse.aspx (última consulta 27/02/18).

Smart Open Services For European Patients, *Stockholm: epSOS.* Documento disponible en: https://www.itu.int/net4/wsis/stocktaking/projects/Project/Details?projectId=1399467257 (última consulta 11/06/18).

Sociedad Española de Informática de la Salud, *Índice SEIS 2017,* marzo 2018. Documento disponible en: http://seis.es/indice-2017/ (última consulta 10/07/18).

Sociedad Española de Informática de la Salud, *Manifiesto en defensa de la confidencialidad y el secreto médico,* Gac Sanit, Vol. 17, núm. 4, 2003, pp. 337-339.

Sociedad Española de Salud Pública y Administración Sanitaria, *Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD*, 2017 Disponible en: https://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd/

Soft Computing And Intelligent Information System, *Sistemas Inteligentes para la Gestión de la Empresa,* 2015-2016, [Documento sin paginación]. Documento disponible en: http://sci2s.ugr.es/sites/default/files/files/Teaching/GraduatesCourses/SIGE/Tema01-SIGE-Introduccion%20a%20la%20Ciencia%20de%20Datos%20-%202015-16.pdf (última consulta 06/03/18).

Subdirección General de Información Sanitaria e Innovación. Área de receta Electrónica del SNS (Coord. Subdirección General de Tecnología de la Información), *Interoperabilidad de receta electrónica en el Sistema Nacional de Salud*, Dirección General de Salud Pública, Calidad e Innovación. Ministerio de Sanidad, Servicios Sociales e Igualdad.

Subdirección General de Información Sanitaria e Innovación. Área de receta Electrónica del SNS (Coord. Subdirección General de Tecnologías de la Información), *Interoperabilidad de receta electrónica en el Sistema Nacional de Salud,* Dirección General de Salud Pública, Calidad e Innovación. Ministerio de Sanidad, Servicios Sociales e Igualdad. Documento disponible en: https://www.msssi.gob.es/profesionales/recetaElectronicaSNS/Doc_Bas_Proyect_Interop_RESNS_v2.1.pdf (Última consulta 1/08/18).

Tribunal de Justicia de la Unión Europea, *Comunicado de prensa n.º 117/15, de 6 de octubre de 2015, Sentencia en el asunto C-362/14, Maximillian Schrems/Data Protection Commissioner,* 2015.

Universia España, ¿Qué es Machine Learning y cómo se usa en Big Data?, septiembre 2017, [Documento sin paginación]. Documento disponible en: http://noticias.universia.es/ciencia-tecnologia/noticia/2017/09/12/1155659/machine-learning-como-usa-big-data.html (última consulta 04/03/18).

World Health Organization, "Essential health technologies", *Geneva: WHO*, 2011 [Documento sin paginación]. Documento disponible en: http://www.who.int aspx (última consulta 17/06/18).

World Health Organization, “Essential health technologies”, *Geneva: WHO*, 2011 [Documento sin paginación]. Documento disponible en: http://www.who.int aspx (última consulta 17/06/18).

ANEXO

Tabla 1.- Algoritmos utilizados en el aprendizaje automático (ML).
MONLEÓN GETINO, A., "El impacto del *Big Data* en la información. Significado y utilidad", *Historia y comunicación social,* vol. 20, núm. 2, 2015, *pp. 438-439*

Tipo de aprendizaje	Descripción	Ejemplos
Aprendizaje supervisado	El algoritmo utilizado produce una función que establece una correspondencia entre las entradas y las salidas deseadas del sistema. Este tipo de aprendizaje puede llegar a ser muy útil en problemas de investigación biológica, biología computacional y bioinformática.	Programa informático que clasifica el mail como " spam" o "no spam" Este es un problema de clasificación, donde el sistema de aprendizaje trata de etiquetar (clasificar) una serie de vectores utilizando una entre varias categorías (clases). La base de conocimiento del sistema está formada por ejemplos de etiquetados realizados anteriormente por el usuario.
Aprendizaje no supervisado	Todo el proceso de modelado se lleva a cabo sobre un conjunto de ejemplos formado tan sólo por entradas al sistema. No se tiene información sobre las categorías previas. El algoritmo tiene que ser capaz de reconocer patrones para poder etiquetar las nuevas entradas.	Un robot que minimiza la energía consumida en función de lo que indican los sensores que posee (temperatura, estado de la batería, etc)
Aprendizaje semisupervisado	Este tipo de algoritmos combinan los algoritmos anteriores para poder clasificar de manera adecuada. Se tiene en cuenta los datos marcados y los no marcados.	Algún dispositivo que permitiera una mezcla de los dos tipos anteriores.
Aprendizaje por refuerzo	El algoritmo aprende observando el mundo que le rodea. Su información de entrada es la retroalimentación que obtiene del mundo exterior como respuesta a sus acciones. Por lo tanto, el sistema aprende a base de ensayo-error. Hay un supervisor que da información al agente sobre si lo está haciendo bien o mal, pero no exactamente lo que debe hacer.	Robot experto que aprende del mundo exterior en base a ensayo-error.

Transducción	Similar al aprendizaje supervisado, pero el algoritmo no construye de forma explícita una función, ya que los datos no tienen etiqueta, estan sin clasificar. Se pretende pronosticar las categorías de los futuros ejemplos basándose en los ejemplos de entrada, sus respectivas categorías y los ejemplos nuevos al sistema.	Análisis automático de texto, aplicaciones de la bioinformática.
Aprendizaje multi-tarea o multiinstancia	Éste algoritmo implica la resolución simultánea de distintas tareas; en particular, el aprendizaje de una tarea se ve mejorado y completado por el aprendizaje común con otras tareas relacionadas con la primera	Imputación de datos incompletos y clasificación de patrones mediante aprendizaje multitarea

Tabla 2. Resumen de las estrategias de privacidad más adecuadas para cada una de las fases que conforman la cadena de valor de big data. Agencia Española de Protección de Datos. *Código de buenas prácticas en protección de datos para proyectos Big Data,* p. 29.

FASE BIG DATA	ESTRATEGIA	IMPLEMENTACIÓN
Adquisición y recolección	Minimizar	• Seleccionar antes de adquirir • EIPD
	Agregar	• Anonimización en la fuente origen
	Ocultar	• Herramientas de cifrado • Herramientas de enmascaramiento de datos
	Informar	• Transparencia - Comunicación al interesado
	Controlar	• Mecanismos para recabar consentimiento
Análisis y validación	Agregar	• Técnicas de anonimización
	Ocultar	• Herramientas de cifrado
Almacenamiento	Ocultar	• Herramientas de cifrado • Mecanismos de autenticación y control de acceso
	Separar	• Almacenamiento distribuido / descentralizado
Explotación	Agregar	• Técnicas de anonimización
Todas las fases	Cumplir / Demostrar	• Definición de políticas • Trazabilidad de las acciones • Herramientas de cumplimiento