LÍMITES Y RIESGOS DEL *BIG DATA* Y DE LA INTELIGENCIA ARTIFICIAL EN EL SECTOR DE LA SALUD*

Leticia Latorre Luna

Abogada y Doctora en Derecho
Universidad de Murcia

SUMARIO

RESUMEN

El presente trabajo se centra en el estudio de los límites y riesgos jurídicos 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), así como en el análisis de los riesgos éticos de la aplicación de las herramientas *big data* y de la inteligencia artificial en el sector sanitario, como es el del control excesivo por parte de los agentes del sector sanitario, públicos o privados, sobre los pacientes que podría 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 inteligencia artificial.

PALABRAS CLAVE

Big data, inteligencia artificial, datos de salud, riesgos jurídicos, riesgos éticos.

ABSTRACT

This paper focuses on the study of the legal limits and risks that prevent the correct and complete application of big data tools in real biomedical or pharmaceutical research and development and innovation (R&D&I) projects, as well as on the analysis of the ethical risks of the application of big data and artificial intelligence tools in the healthcare sector, such as excessive control by public or private health sector agents over patients, which could affect their loss of autonomy and freedom, leading to a consequent misuse of the information and knowledge obtained from big data and artificial intelligence.

KEYWORDS

Big data, artificial intelligence, health data, legal risks, ethical risks.

** Trabajo postulado al Premio Derecho y Salud 2024.*

I. LÍMITES DEL *BIG DATA* Y LA INTELIGENCIA ARTIFICIAL EN EL SECTOR SANITARIO

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 suponen el *big data* y la inteligencia artificial 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[1].

Así pues, ya en el año 2012[2] la revista *Forbes* predijo en su artículo "The Next Revolution in Healthcare"[3], 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*[4] suscrito por la Fundación *Rock Health*, establece diferentes motivos por las 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* y la inteligencia artificial a fin 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

1 En este sentido, TRONCOSO, A. (2010): *La protección de datos personales. En busca del equilibrio.* Tirant lo Blanch, p. 1100, afirma 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, A. (2017): «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.* 112, 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, F. (2019). "Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del *Big Data". Revista de Derecho Político.* (106), 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".

2 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. *Vid.* GARCIA, P. y PERETE, C. (2019): «Internet, el RGPD y la LOPDGDD». En J. Calvo (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Wolters Kluwer, p. 852.

3 RISKIN, D. (2012): «The Next Revolution in Healthcare». *Forbes* (https://www.forbes.com/sites/singularity/2012/10/01/the-next-revolution-in-healthcare/#26f260d055cc).

4 Acceso web al informe: https://rockhealth.com/rock-report-big-data-healthcare/. Asimismo, el informe es comentado por POYATOS, J.M. (2013): «*Big Data* y el sector de la salud: el futuro de la sanidad» (http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad).

medidas y garantías de aplicación de herramientas *big data* en proyectos de salud pública e investigación (biomédica y farmacéutica) de interés general.

De manera adicional a las oportunidades que ofrece la aplicación de *big data* y la inteligencia artificial 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[5]. 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 disponibles y registrados[6] 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.

A pesar de los evidentes avances del sistema sanitario con el objetivo de adaptar el mismo a las nuevas demandas tecnológicas y a la aplicación de las tecnologías de *big data* e inteligencia artificial, siendo la historia clínica electrónica y la receta electrónica claros ejemplos de ello, actualmente continúan existiendo en la práctica diversos límites y riesgos tanto desde una perspectiva jurídica como ética.

Por ello, a continuación, serán analizados los límites actuales de la aplicación de *big data* y de la inteligencia artificial con perspectivas de futuro, teniéndose especialmente en consideración el estudio efectuado en el *Informe de resultados big data en salud digital*[7], así como otros aspectos relevantes que se pondrán en manifiesto.

En primer lugar, unos de los límites que en la actualidad impiden una aplicación efectiva de las herramientas de *big data* y la inteligencia artificial, 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* y la inteligencia artificial. 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[8].

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* y la inteligencia artificial, 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

5 Al respecto, como indica ACED, E. (2016): «Protección de Datos y Transformación Digital en Sanidad». *I+S Revista de la Sociedad Española de Información y Salud.* (118), 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".

6 Ensayos clínicos, historiales médicos, secuenciación de ADN de pacientes o información procedente de redes sociales, entre otros muchos.

7 *Vid.* EQUIPO DE TRABAJO DE LA FUNDACIÓN VODAFONE ESPAÑA Y RED.ES (2017): *Informe de resultados Big Data en salud digital*. 11 y ss. (https://www.ontsi.es/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf).

8 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 Administración 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.

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)[9].

De manera similar, desde una perspectiva práctico – tecnológica también existen algunas limitaciones que se han de tener en consideración a causa de la relativa novedad de las herramientas *big data* y la inteligencia artificial, 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* y la inteligencia artificial.

En último lugar, otras de las limitaciones proceden del propio mercado, pues actualmente continúan siendo escasos los profesionales especializados en análisis de *big data* y en la inteligencia artificial, 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 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"[10].

II. RIESGOS JURÍDICOS DE ACUERDO CON LA NORMATIVA VIGENTE DE PROTECCIÓN DE DATOS DEL *BIG DATA* Y DE LA INTELIGENCIA ARTIFICIAL

Desde una perspectiva jurídica, son diversos los derechos que se pueden ver en riesgo tanto en el marco legal europeo como en 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* e inteligencia artificial 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[11].

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[12], así como para el 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)]"[13] 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"[14].

Sin embargo, la anonimización de los datos personales y, en concreto de los datos de salud no se

9 EQUIPO DE TRABAJO DE LA FUNDACIÓN VODAFONE ESPAÑA Y RED.ES (2017: 54).

10 EQUIPO DE TRABAJO DE LA FUNDACIÓN VODAFONE ESPAÑA Y RED.ES (2017: 55).

11 LATORRE, L. (2021): «Salud pública y *big data*: COVID-19. Reflexión jurídica sobre la normativa de datos de salud y de aplicación de herramientas *big data* en el ámbito de la investigación biomédica y de la asistencia sanitaria». *Revista Derecho y Salud.* 31 (2021-1), 12-19.

12 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 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".

13 Considerando 17 Reglamento 2018/1807.

14 Considerando 18 y Art. 1 Reglamento 2018/1807.

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, 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 y la transmisión de responsabilidad entre servicios complementarios[15]. 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 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.

En concreto, uno de los riesgos jurídicos 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[16], 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[17]. 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*) analizamos que 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[18] deberá aplicarse 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 Europea[19].

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.

15 Al respecto, EQUIPO DE TRABAJO DE LA FUNDACIÓN VODAFONE ESPAÑA Y RED.ES (2017: 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, P.A. (2017): «Responsabilidad proactiva en los tratamientos masivos de datos». *Dilemata.* (24), 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".

16 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".

17 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.

18 *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.* GARCIA, P. y PERETE, C. (2019: 854).

19 DOUE L 303/59, de 28 de noviembre de 2018.

De igual modo, se ha de tener en consideración un evidente riesgo en el consentimiento informado a través de contratos o políticas de privacidad, dado que este tipo de contratos con cláusulas aparentemente transparentes y claras no siempre es posible su aplicación en el contexto del *big data*[20], a consecuencia de 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.,* 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 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[21].

Por otro lado, se ha de tener presente las posibles discrepancias que pueden surgir de los distintos Comités de Ética de la Investigación ante la evaluación de un mismo proyecto o por "inadecuación del modelo organizativo".

Por ello, resulta necesario de una ley sectorial de protección de datos de salud y de *big data*, donde 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"[22].

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:

> "[…] 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"[23].

Debido a lo anterior, resulta primordial que la ley sectorial de protección de datos de salud y *big data*, 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 tenor 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

20 En este sentido, el funcionamiento del big data, como señala DURÁN, F.J. (2017): «Big Data aplicado a la mejora de los servicios públicos y protección de datos personales». *Revista de la Escuela de Posgrado.* (12), 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, E. (2016). *Big Data, privacidad y protección de datos.* Agencia Española de Protección de Datos y Boletín Oficial del Estado, 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".

21 AGUSTÍN, T, ADNREU, B., VALERO, J. y CAYÓN DE LAS CUEVAS, J. (2020): «Diez consideraciones ético-jurídicas en relación con la reutilización y big data en el ámbito sanitario». *Bioderecho.es.* (12), p. 1.

22 DURÁN, F.J. (2017:63).

23 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2015): *Código de buenas prácticas en protección de datos para proyectos Big Data*, 18. (https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf).

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, con la finalidad 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 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[24] 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:

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[25] a efectos de optimizar la confianza de los interesados, como son los 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 fin 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[26] 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.

III. 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

24 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2015:19).

25 Arts. 40 a 43 del RGPD.

26 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.

que conlleva la aplicación de herramientas de *big data* y la inteligencia artificial en el sector sanitario.

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 inteligencia artificial conllevan un cambio en la prestación de servicios sanitarios, lo que implica a su vez un desigual acceso a las Nuevas Tecnologías por parte de aquellos colectivos vulnerables, con menos recursos económicos, hecho que repercute igualmente en los países avanzados y menos avanzados, pues las Nuevas Tecnologías requieren 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[27].

Por otro lado, la aplicación de las herramientas de *big data* y de la inteligencia artificial pueden 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.

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 inteligencia artificial, 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[28]. 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 inteligencia artificial 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[29]. Pues, es evidente que la denominada "dictadura de datos"[30] que crea ciertas patologías o estereotipos resulta en el mayor de los casos perjudicial para la sociedad, puesto que pondrían suponer una perdida de 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.

Igualmente, se ha de tener en cuenta que los expertos consideran que un mal uso del *big data* y la inteligencia artificial debido a un exceso de *biomonitorización* en la medicina preventiva y personalizada puede conllevar de manera negativa e indirecta

27 En este sentido, SÁNCHEZ DEL CAMPO, A. (2019): «Inteligencia artificial y privacidad». En J. López (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Wolters Kluwer, 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".

28 Sobre esta cuestión, LERMAN, J. (2013): «*Big Data* and Its Exclusions». *Stanford Law Review.* 66, (https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-and-its-exclusions/) 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".

29 BARROCAS, S. and SELBST, A.D. (2016): «*Big Data*'s Disparate Impact». *104 California Law Review 671* (https://ssrn.com/abstract=2477899) 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.

30 MAYER-SCHÖNBERGER, V. and CUKIER, K. (2013): «The Dictatorship of Data». *MIT Technology Review* (https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos).

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.

En el año 2017 ya el Parlamento Europeo desarrolló un marco ético común sólido[31] o de máxima prudencia[32], haciendo hincapié en 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"[33]. Asimismo, el Parlamento Europeo, afirmó en su día la necesidad de regular una "responsabilidad algorítmica, bajo la idea de que las normas científicas y éticas estrictas, son fundamentales"[34], destacando igualmente la necesidad de aplicar las normas éticas más elevadas ante el uso de macrodatos permitidos por el marco legal vigente[35].

En consecuencia de lo anterior, como se puede apreciar el Parlamento Europeo ha ido planteando durante todo este tiempo sus propias estrategias legales en relación con los datos y la inteligencia artificial[36] a efectos de garantizar el desarrollo de la inteligencia artificial en beneficio de la sociedad y, sobre todo hacia una transformación digital en beneficio de todos, a fin 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[37]. 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 inteligencia artificial, por medio de un Libro Blanco[38] que fomentará el uso de forma segura de la inteligencia artificial, a través del aprovechamiento de los centros de investigación[39].

31 Al respecto MARTÍNEZ, R. (2019): «Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo». *Revista Catalana de Dret Públic.* (58), 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. 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".

32 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)).

33 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)).

34 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)).

35 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)).

36 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

37 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

38 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

39 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

Por último y, no menos importante, se ha de destacar otros de los riesgos éticos que plantean las herramientas *big data* y la inteligencia artificial dimanante de la necesidad de educar en valores morales a la sociedad en su conjunto y, en especial a las entidades especializadas en el análisis de datos sanitarios, así como los centros sanitarios y de investigación tanto públicos como privados y a sus facultativos sanitarios sobre el uso de este tipo de herramientas, dado que un mal uso o, si se prefiere, un uso amoral y/o ilícito del *big data* y de la inteligencia artificial podría conllevar grandes problemas en la práctica sanitaria, tanto para el paciente como para la sanidad pública en general.

Para ello, es necesario que los Comités de Ética estén formados por especialistas con una amplia capacidad de aplicar y adaptar los valores propios de la ética tradicional en la nueva era tecnológica, así como de crear – en la medida de lo posible – una "nueva ética" cuya finalidad sea la de evitar nuevos problemas morales que pudieran surgir a causa de un mal uso del *big data* y de la inteligencia artificial en el ámbito sanitario, así como de dar solución y una respuesta a los problemas actuales, dado que la ética tradicional en la mayoría de los casos resulta insuficiente.

IV. CONCLUSIONES

En definitiva, como se ha podido apreciar en el presente trabajo, se pueden dar diversos 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 límites 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 inteligencia artificial en el sector sanitario conlleva implícitos riegos relevantes. En concreto puede implicar desigual acceso a las Nuevas Tecnologías 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 inteligencia artificial. 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 inteligencia artificial, son medios e instrumentos que ayudan y colaboran con los facultativos sanitarios e investigadores, pero que en ningún concepto los sustituyen.

Nos encontramos ante deficiencias que incrementan las dificultades a la hora de plantear el uso de tecnologías de *big data* e inteligencia artificial, 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 embargo, como se ha apreciado no se regulan cuestiones jurídicas ni éticas de gran relevancia, lo que conlleva ante la incertidumbre a una interpretación restrictiva y limitativa por parte del propio responsable del tratamiento – 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, de ahí la necesidad de una ley sectorial de protección de datos de salud y de las herramientas *big data* e inteligencia artificial 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.

informática conjunta, además de seguir avanzando en 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

V. BIBLIOGRAFÍA

ACED, E. (2016): «Protección de Datos y Transformación Digital en Sanidad». *I+S Revista de la Sociedad Española de Información y Salud.* (118), 39-40.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. (2015): *Código de buenas prácticas en protección de datos para proyectos Big Data*, 1-40. (https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf).

AGUSTÍN, T, ADNREU, B., VALERO, J. y CAYÓN DE LAS CUEVAS, J. (2020): «Diez consideraciones ético-jurídicas en relación con la reutilización y big data en el ámbito sanitario». *Bioderecho.es.* (12), 1-3.

BARROCAS, S. and SELBST, A.D. (2016). «*Big Data*'s Disparate Impact». *104 California Law Review 671* (https://ssrn.com/abstract=2477899).

DE MONTALVO, F. (2019). «Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del *Big Data*». *Revista de Derecho Político.* (106), 43-75.

DURÁN, F.J. (2017). «Big Data aplicado a la mejora de los servicios públicos y protección de datos personales». *Revista de la Escuela de Posgrado.* (12), 33-74.

EQUIPO DE TRABAJO DE LA FUNDACIÓN VODAFONE ESPAÑA Y RED.ES (2017): *Informe de resultados Big Data en salud digital*. 1-86. (https://www.ontsi.es/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf)

GARCIA, P. y PERETE, C. (2019): «Internet, el RGPD y la LOPDGDD». En J. Calvo (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Wolters Kluwer, 851-872.

GIL, E. (2016). *Big Data, privacidad y protección de datos.* Agencia Española de Protección de Datos y Boletín Oficial del Estado, 145 páginas.

GONZÁLEZ, P.A. (2017). «Responsabilidad proactiva en los tratamientos masivos de datos». *Dilemata.* (24), 115-129.

LATORRE, L. (2021). «Salud pública y *big data*: COVID-19. Reflexión jurídica sobre la normativa de datos de salud y de aplicación de herramientas *big data* en el ámbito de la investigación biomédica y de la asistencia sanitaria». *Revista Derecho y Salud.* 31 (2021-1), 6-21.

LERMAN, J. (2013). «*Big Data* and Its Exclusions». *Stanford Law Review.* 66, (https://www.stanfordlawreview.org/online/privacy-and-big-data-big-data-and-its-exclusions/).

MARTIN, A. (2017). «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.* 112, 10-12.

MARTÍNEZ, R. (2019). «Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo». *Revista Catalana de Dret Públic.* (58), 64-81.

MAYER-SCHÖNBERGER, V. and CUKIER, K. (2013): «The Dictatorship of Data». *MIT Technology Review* (https://www.technologyreview.es/s/3564/la-dictadura-de-los-datos).

POYATOS, J.M. (2013): «*Big Data* y el sector de la salud: el futuro de la sanidad» (http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad).

RISKIN, D. (2012): «The Next Revolution in Healthcare». *Forbes* (https://www.forbes.com/sites/singularity/2012/10/01/the-next-revolution-in-healthcare/#26f260d055cc).

SÁNCHEZ DEL CAMPO, A. (2019): «Inteligencia artificial y privacidad». En J. López (Corrd.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD.* Wolters Kluwer, 983-995.

TRONCOSO, A. (2010). *La protección de datos personales. En busca del equilibrio.* Tirant lo Blanch, 1990 páginas.