ASPECTOS ÉTICOS, LEGALES Y SOCIALES DEL USO DE LA INTELIGENCIA ARTIFICIAL Y EL BIG DATA EN SALUD EN UN CONTEXTO DE PANDEMIA

ETHICAL, LEGAL AND SOCIETAL ISSUES OF THE USE OF ARTIFICIAL INTELLIGENCE AND BIG DATA APPLIED TO HEALTHCARE IN A PANDEMIC

Itziar de Lecuona
Universidad de Barcelona, Barcelona, España
itziardelecuona@ub.edu

Recibido: octubre de 2020
Aceptado: noviembre de 2020

Palabras clave: Inteligencia artificial, Big Data, Apps, investigación e innovación en salud, intimidad y datos personales, comités de ética de la investigación.
Keywords: Artificial Intelligence, Big Data, Apps, healthcare research and innovation, privacy and personal data, Research Ethics Committees.

Resumen: Ante el uso de la inteligencia artificial, el Big Data y el desarrollo de Apps en salud en situación de pandemia por COVID-19, se analizan las consecuencias que para la libertad y la intimidad tiene la tendencia a la mercantilización de datos personales y la "economía de la atención" promovida por las *big tech*; la amenaza que supone la "discriminación algorítmica" y la acumulación indiscriminada de datos. Se trata de cuestiones cuyo análisis filosófico-jurídico requiere indagar previamente sobre aspectos técnicos de especial complejidad para así construir una reflexión sólida acerca de las cuestiones bioéticas de las tecnologías emergentes.

Abstract: Faced, as we are, with the use of artificial intelligence, Big Data and the development of healthcare Apps in the COVID-19 pandemic, the article analyses the consequences for freedom and privacy of the trend towards the commodification of personal data and the "attention economy" promoted by big tech; the threat posed by "algorithmic discrimination", and the indiscriminate accumulation of data. These are issues whose philosophical and legal analysis requires us, as a previous step, to look into especially complex technical aspects in order to construct a sound body of thought on bioethical issues in the emerging technologies.

1. La pandemia por covid-19 y su impacto en la investigación y la innovación en salud

Actualmente buena parte de la investigación e innovación en salud que se desarrolla en los centros de investigación y hospitalarios públicos y privados en nuestro contexto, utiliza tecnologías emergentes como la inteligencia artificial y la analítica de datos masivos (*Big Data*). Se trata de identificar patrones de comportamiento para predecir conductas y mejorar así la toma de decisiones mediante el desarrollo de algoritmos.[1] Para ello, es preciso acceder y tratar conjuntos de datos, entre los que se incluyen los datos personales.

La Unión Europea promueve una sociedad digital guiada por el dato[2] para crear un mercado único digital competitivo que permita el liderazgo en el plano internacional. Esta es una apuesta económica y científica que incluye una medicina más personalizada, así como la mejora de los sistemas sanitarios para que sean más eficientes y permitan un envejecimiento activo y saludable.[3] Esta decisión política también permite poner de manifiesto las tensiones que se generan entre el interés colectivo y los intereses particulares entorno a los datos personales. Sería maleficente no aplicar las tecnologías emergentes y no utilizar datos personales en beneficio de las personas y de la sociedad, y más aún en situación de pandemia por COVID-19, de ahí que sea necesario ponderar derechos e intereses. La pandemia ha intensificado los debates sobre la protección de la intimidad y ha generado una falsa dicotomía entre seguridad y protección de los datos personales que nada ayuda a un tratamiento adecuado de los derechos e intereses en juego.

Los intereses de la ciencia y de la tecnología no deben prevalecer sobre los del individuo[4]. Es necesario analizar las implicaciones éticas, legales y sociales del uso de tecnologías emergentes y datos personales, pero también las cuestiones técnicas aparejadas. Así será posible avanzar en el desarrollo de pautas que permitan que derechos como la intimidad o la toma de decisiones libre e informada se protejan en los entornos altamente digitalizados del ámbito de la salud.

Estas tecnologías se nutren de conjuntos de datos -entre ellos, datos personales-[5],

1. La Real Academia de la lengua española define "algoritmo" como un "Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema." Real Academia Española: Diccionario de la lengua española, 23.ª ed. Última consulta 30 de octubre de 2020, disponible en: https://dle.rae.es

2. Comisión Europea, *Communication on data-driven economy* COM(2014)442 final Última consulta 30 de octubre de 2020, disponible en:https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-442-EN-F1-1.Pdf

3. Comisión Europea, *Programa Marco de Investigación HORIZONTE 2020* Última consulta 30 de octubre de 2020, disponible en:https://ec.europa.eu/programmes/horizon2020/en

4. Art. 2.: "Primacía del ser humano. El interés y el bienestar del ser humano deberán prevalecer sobre el interés exclusivo de la sociedad o de la ciencia." *Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), Consejo de Europa, Oviedo, 4 de abril de 1997*. Última consulta 30 de octubre de 2020, disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168007cf98

5, "Son categorías especiales de datos aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, los datos genéticos

almacenados en su mayoría en bases de datos, como las que contienen historias clínicas, bajo criterios de calidad y seguridad.[6] Así, el objetivo es combinar distintos conjuntos de datos procedentes de diferentes bases, entre las que se incluyen repositorios dedicados exclusivamente a investigación.[7] Junto a las historias clínicas informatizadas cabe también la posibilidad de combinar esta información con la que proviene de otras fuentes y plataformas que pueden recoger datos personales en tiempo real. Conviene tener en cuenta que hoy la emisión, recopilación y almacenamiento de datos personales es constante, bien sea de forma voluntaria o involuntaria por parte de su titular.

Para ayudar a identificar el problema pueden ponerse algunos ejemplos de uso de tecnologías emergentes y tratamiento de datos personales en procesos de creación y transferencia de conocimiento en salud como: a) el desarrollo de sistemas de predicción y gestión de la pandemia por COVID-19; y b) las *Hackatones* o retos para desarrollar algoritmos en las que participan terceros, fundamentalmente especialistas en informática y ciencia de los datos, que normalmente compiten por un premio. Estos retos pueden ser el preludio de proyectos de investigación punteros orientados a la detección de síntomas y la predicción de enfermedades. La investigación y la innovación que se lleva a cabo actualmente, y en particular por COVID-19, dista mucho de aquella para la que se establecieron pautas y requisitos tras la Segunda Guerra Mundial[8]. Aquella estaba fundamentalmente centrada en el desarrollo de medicamentos y productos sanitarios de uso humano, con el ensayo clínico como paradigma. Hoy, la industria farmacéutica cierra acuerdos millonarios con empresas dedicadas a la genética

y biométricos, datos relativos a la salud y la vida sexual o las orientaciones sexuales de una persona física" (art. 9)

Reglamento 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). R. (UE) 2016/679 (27 abril 2016).

6. Véanse la Historia Clínica compartida (HC3) de Cataluña https://salutweb.gencat.cat/ca/ambits_actuacio/linies_dactuacio/tecnologies_informacio_i_comunicacio/historia_clinica_compartida/ y el Programa de historia clínica informatizada en atención primaria de Cataluña (eCAP) https://salutweb.gencat.cat/ca/ambits_actuacio/linies_dactuacio/tecnologies_informacio_i_comunicacio/ecap/ Última consulta 30 de octubre de 2020.

7. Por ejemplo, el Sistema de Información para el desarrollo de la Investigación en Atención Primaria de Cataluña (SIDIAP), Última consulta 30 de octubre de 2020, disponible en: https://www.sidiap.org/index.php/es

8. ASOCIACIÓN MÉDICA MUNDIAL, *Declaración de Helsinki: principios éticos para las investigaciones médicas en seres humanos*. Adoptada por la 18ª Asamblea Médica Mundial, Helsinki, Finlandia, junio 1964 y enmendada por la 29ª Asamblea Médica Mundial, Tokio, Japón, octubre 1975 35ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983 41ª Asamblea Médica Mundial, Hong Kong, septiembre 1989 48ª Asamblea General Somerset West, Sudáfrica, octubre 1996 52ª Asamblea General, Edimburgo, Escocia, octubre 2000 Nota de Clarificación, agregada por la Asamblea General de la AMM, Washington 2002 Nota de Clarificación, agregada por la Asamblea General de la AMM, Tokio 2004 59ª Asamblea General, Seúl, Corea, octubre 2008 64ª Asamblea General, Fortaleza, Brasil, octubre 2013 y NATIONAL COMMISSION FOR THE PROTECTION OF HUMAN SUBJECTS OF BIOMEDICAL AND BEHAVIORAL RESEARCH, *The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research*, U.S.A, 1979.

directa al consumidor[9] para acceder a bases de datos personales, que incluyen datos de salud, información genética, datos sociodemográficos e incluso gustos y preferencias. Estas bases de datos han sido creadas con fines comerciales para predecir el riesgo a padecer enfermedades de base genética, pero también pueden informar sobre los ancestros[10] o incluso emplearse para encontrar a familiares y delincuentes. Este supuesto ejemplifica cómo los negocios e iniciativas sobre datos personales son exponenciales, y también permite cuestionar si los titulares de los datos personales tienen el control sobre estos[11] en la era digital, lo que pone de manifiesto la necesidad de articular mecanismos para asegurar la transparencia. Precisamente, uno de los mayores retos de nuestro tiempo es controlar los usos secundarios de los datos personales, los usos no deseados y aquellos que puedan dar lugar a discriminaciones, especialmente aquellas encubiertas.

Asimismo, en el ámbito hospitalario se prueban y aplican sistemas de inteligencia artificial para analizar y aprender de las historias clínicas informatizadas con el fin de mejorar los procesos asistenciales. Asistimos hoy al auge del desarrollo de Apps de salud para, por ejemplo, evaluar síntomas o para identificar posibles positivos por COVID-19 y rastrear a sus contactos como herramientas de apoyo en el marco de la salud pública, con no pocas dudas acerca de su fiabilidad y seguridad[12]. Estos dispositivos digitales de salud forman parte del llamado internet de las cosas y *mHealth*[13] en el ámbito de la salud, en el que distintos dispositivos, que también incluyen diversos sensores y vestibles o ***wearables***, permiten la conectividad entre sí y una monitorización constante de las personas. Los titulares de los datos personales que alimentan a

9. Instrumento de Ratificación del Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), hecho en Oviedo el 4 de abril de 1997. Última consulta 30 de octubre de 2020, disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-20638. El Convenio de Oviedo contiene disposiciones específicas relativas a la genética (artículos 11 a 14), en particular, las pruebas genéticas de predicción y las intervenciones en el genoma humano. Véase también: Consejo de Europa, *Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes,* CETS No.203, hecho en Estrasburgo el 11 de noviembre de 2008. Última consulta 30 de octubre de 2020, disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/203

10. "GlaxoSmithKline strikes $300 million deal with 23andMe for genetics-driven drug research", CNBC, 25 de julio de 2018, Última consulta 30 de octubre de 2020, disponible en: https://www.cnbc.com/2018/07/24/glaxosmithkline-23andme-team-up-on-genetics-driven-drug-research.html

11. Tutton, R., Prainsack, B. "Enterprising or altruistic selves? Making up research subjects in genetics research", *Sociology of Health & Illness*, 2011, Vol. 33, núm. 7 pp. 1081-1095. doi:10.1111/j.1467-9566.2011.01348.x

12. Manifiesto en favor de la transparencia en desarrollos de software públicos, septiembre de 2020, última consulta 30 de octubre de 2020, disponible en: https://transparenciagov2020.github.io/

13. La OMS define *mHealth* como "la práctica médica y de salud pública apoyada por dispositivos móviles, como teléfonos móviles, dispositivos de vigilancia de pacientes, asistentes digitales personales (PDA) y otros dispositivos inalámbricos."

Organización Mundial de la Salud, *Global Observatory for eHealth series*, vol.3 Suiza, 2011. Última consulta 30 de octubre de 2020, disponible en: https://www.who.int/goe/publications/goe_mhealth_web.pdf

estos sistemas que utilizan tecnologías emergentes son a su vez destinatarios, en su mayoría, de los resultados de estos procesos.

Las Apps así como otras intervenciones y desarrollos en el ámbito de la salud, deben ser probadas en entornos controlados mediante la participación de personas o el uso de datos personales para que sean validadas antes de su utilización de forma generalizada. Aplicaciones y dispositivos que estarán a disposición del consumidor, y para los que se reclaman sistemas de certificación que garanticen que sus creadores merecen la confianza de los usuarios finales que, como se ha indicado anteriormente, se nutren de los datos de éstos[14]. Se persigue así obtener el sello de calidad de los algoritmos, que depende en buena parte de la reputación de las entidades en las que éstos se prueban y comprueban, y de la calidad de los datos que manejan. Son numerosas las iniciativas que llaman a las puertas de grandes hospitales y centros de investigación de referencia para obtener el aval ético de sus fórmulas algorítmicas. Estas propuestas han aumentado considerablemente durante la pandemia por COVID-19. Especialmente Apps que tienen como objetivo recopilar datos mediante el formato encuesta solicitando numerosos datos personales. Son ejemplos los sistemas digitales para evaluar síntomas y también encuestas para proveer soporte emocional. Así, tanto la investigación tradicional como la innovación que tiene que validarse con datos personales, son evaluadas por los correspondientes comités de ética de la investigación acreditados por los departamentos de salud de las Comunidades Autónomas, establecidos para analizar los aspectos metodológicos, éticos, legales y sociales de los proyectos de investigación, pero no la innovación en salud.

Debido a la cantidad de información personal almacenada y al desarrollo de tecnología para combinarla, hemos dejado de ser datos aislados para convertirnos en conjuntos de datos personales candidatos a ser explotados por parte de distintos actores con intereses diversos, y potencialmente en conflicto. Hoy la posibilidad de reidentificar a una persona con datos como el sexo, el código postal y la fecha de nacimiento es muy elevada[15]. Esta situación exige que se establezcan medidas técnicas y organizativas para que el uso de las tecnologías con determinados fines en salud no permitiera la reidentificación de las personas, es decir, la no atribución de personalidad[16]. Esta es una cuestión

14. En este sentido véase por ejemplo el proyecto de investigación NESTORE: financiado por el Programa Marco de Investigación Horizonte2020 de la Unión Europea para desarrollar un sistema de consejo virtual para un envejecimiento activo. Última consulta 30 de octubre de 2020, disponible en: https://cordis.europa.eu/project/id/769643/es

15. Sweeney, L., "Simple Demographics Often Identify People Uniquely". Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000. Última consulta 30 de octubre de 2020, disponible en: https://dataprivacylab.org/projects/identifiability/paper1.pdf

16. En la mayoría de los casos la seudonimización debería exigirse por defecto. Se entiende por seudonimización el "tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable. Real Academia Española: Diccionario de la lengua española, 23.ª ed. Última consulta 30 de octubre de 2020, disponible en: https://dle.rae.es

técnica que es crucial para comprender el fenómeno al que se enfrenta la sociedad digital. Por las razones aducidas, no es posible garantizar el anonimato. Tampoco serían válidos buena parte de los procesos y protocolos de información y consentimiento informado asentados en esta garantía de anonimización[17]. De otra forma, se genera una falsa seguridad asentada en una cláusula ya obsoleta como es la anonimización.

En el contexto europeo se ha transitado de un sistema analógico a otro digital sin llevar a cabo un debate social informado sobre las consecuencias del desarrollo y aplicación de la investigación y la innovación orientada a la monitorización de la conducta de las personas a través de entornos digitales. Las citadas tecnologías evolucionan a una velocidad sin precedentes. Esta rapidez impide una reflexión pausada sobre los beneficios y los riesgos de cada una de las tecnologías emergentes, así como decidir qué iniciativas se priorizan y con qué fines e impacto social. Si bien es cierto que los ritmos de producción normativa y de los procesos de creación y aplicación del conocimiento no son los mismos, se produce cierta parálisis en la aplicación de las normas[18].

En 2018 los medios revelaron que la consultora Cambridge Analytica contribuyó a que Donald Trump ganara las elecciones de 2016, mediante la manipulación de la intención de voto de aproximadamente 50 millones de personas a través de las redes sociales. El objetivo era influir en los perfiles considerados más vulnerables[19]. Este caso ejemplifica una de las prácticas de nuestro tiempo, la elaboración de perfiles que consiste en cualquier forma de tratamiento de los dato personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en la persona o le afecte significativamente de modo similar, y que está regulada por el Reglamento General de Protección de Datos, permitiéndola en determinadas circunstancias. Los desafíos tecnológicos representan también un reto para la libertad humana no sea anulada[20].

2. La tendencia a la explotación y a la mercantilización de los datos personales

No cabe duda de que los datos personales son el oro de nuestro tiempo y el interés por acceder a ellos es creciente, también porque el acceso a estos permite

17. De Lecuona, I., "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)", *Gaceta Sanitaria*, 2018, Vol. 32. Núm. 6, pp. 576-578. DOI: 10.1016/j.gaceta.2018.02.007

18. Rodotà, S., *La vida y las reglas; Entre el derecho y el no derecho*, Editorial Trotta, Madrid, 2010

19. The Cambridge Analytica Files, The Guardian, 17 de marzo de 2018. Última consulta 30 de octubre de 2020, disponible en: https://www.theguardian.com/news/series/cambridge-analytica-files

20. Harari, Y.N., "Los cerebros hackeados votan", *El País*, 6 de enero de 2019. Última consulta 30 de octubre de 2020, disponible en: https://elpais.com/internacional/2019/01/04/actualidad/1546602935_606381.html

abrir innumerables posibilidades de tratamiento y aplicación, incluidos modelos de negocio en salud. La iniciativa pública y privada centra su atención en la información personal, por lo que esta informa de sus titulares, pero también, por lo que puede predecir, si se destinan suficientes recursos humanos y materiales y se formulan las hipótesis adecuadas. Por estas razones, en el ámbito de la salud es preciso evitar oportunistas que accedan a los datos personales con intereses espurios alejados del bien común o del interés colectivo que habilitaría a tratarlos[21].

Es necesario evitar mercados de datos disfrazados de investigación e innovación en salud que aumenten las desigualdades existentes y la discriminación[22], y que permitan el lucro de terceros mediante la monetización de datos personales[23]. Estos posibles mercados de datos personales vestidos de buenas intenciones, como puede ocurrir a propósito de la pandemia por COVID-19, deben ser identificados con urgencia. Puede afirmarse que existe una falta de comprensión de las implicaciones que tiene el nuevo paradigma digital asentado en la utilización de tecnologías emergentes y la explotación intensiva de datos personales para la dignidad de las personas y sus derechos y libertades fundamentales. Existe una profunda desafección por los datos personales que puede tener efectos perversos en el sistema de investigación e innovación en salud. El uso de los datos personales no puede resultarnos indiferente. En la sociedad digital, todos somos relevantes. Es necesario crear ontologías[24] para mejorar la toma de decisiones y éstas necesitan numerosos conjuntos de datos. Nuestra información y nuestra identidad digital es objeto de deseo para la iniciativa pública y privada.

El acceso a datos personales confiere un poder extraordinario a terceros, bien sea la iniciativa pública o privada, sobre los titulares de estos y pueden dar lugar a usos no deseados, y a discriminaciones, algunas de ellas encubiertas. Por otra parte, el "solucionismo tecnológico"[25] que entiende la aplicación de tecnología *per se* como solución a los problemas y retos de nuestro tiempo, y el ajetreo que provoca la velocidad a la que se desarrolla la tecnología digital[26], banalizan el uso de datos

21. De Lecuona, I., "La tendencia a la mercantilización de partes del cuerpo humano y de la intimidad en investigación con muestras biológicas y datos (pequeños y masivos)", en Casado, M. (Coord.), *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016, pp. 267-296.

22. Casado, M. (Coord.), *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016. Reeditado por Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2018. Última consulta 30 de octubre de 2020, disponible en: http://diposit.ub.edu/dspace/bitstream/2445/116007/1/9788447541195.pdf y García Manrique, R. (Coord.), *El cuerpo diseminado. Estatuto, uso y disposición de los biomateriales humanos*, Editorial Aranzadi, Cizur Menor, 2018.

23. De Lecuona, I. "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)", *Gaceta Sanitaria*, 2018, Vol. 32. Núm. 6, pp. 576-578. DOI: 10.1016/j.gaceta.2018.02.007

24. Casanovas, P. et al, *AI Approaches to the Complexity of Legal Systems. Complex Systems, the Semantic Web, Ontologies, Argumentation, and Dialogue*, volume 6237, Springer, 2010.

25. Morozov, E., *La locura del solucionismo tecnológico*. Katz-Clave intelectual, Madrid, 2015.

26. Wajcman, J., *Esclavos del tiempo: Vidas aceleradas en la era del capitalismo digital*, Paidós, Barcelona, 2017.

personales y el significado de la intimidad y la confidencialidad en nuestra sociedad. Si bien la intimidad debería tratarse como un valor esencial y un bien común a proteger, la tendencia es a entender la información personal como moneda de cambio que puede ofrecerse al mejor postor, sin atender a los usos y las consecuencias que pudieran tener para su titular y para las generaciones futuras. La utilización de información genética es un magnífico ejemplo.

En nuestro contexto, el sistema de investigación se asienta en los principios de solidaridad y altruismo. Así, las personas donan muestras biológicas y datos personales[27] para que el aumento de conocimiento, las intervenciones y los tratamientos que se desarrollen reviertan en beneficio de la sociedad y de las generaciones futuras, entendiendo que las personas no siempre obtendrán provecho de manera directa. Además, dado que buena parte de la investigación que se lleva a cabo está financiada mediante el pago de impuestos, esta debe revertir en beneficio del interés colectivo y el bien común.

La tendencia a la mercantilización de datos personales también se despliega en el uso de muestras de biológicas de origen humano[28]. Estas están almacenadas en biobancos públicos y privados para avanzar en la medicina traslacional y regenerativa. Estos repositorios que están regulados en España desde el año 2007, también están en el punto de mira de iniciativas privadas, especialmente los biobancos públicos, en los que se recogen muestras biológicas humanas de alto valor científico donadas por las personas de forma altruista y solidaria. Los biobancos y, en particular, los de carácter público no pueden estar a merced de las reglas del mercado y no están exentos de prácticas mercantilistas.

Es necesario identificar prácticas mercantilistas vestidas de buenas intenciones también en el ámbito de los biobancos. Un ejemplo es el interés por el acceso a muestras biológicas humanas almacenadas en estos repositorios por parte de empresas, solicitando estas el monopolio para su "posicionamiento" a cambio de publicaciones en revistas de reconocido prestigio o mediante acuerdos económicos que conducen a la venta de muestras biológicas en el extranjero[29]. Estas prácticas son lo opuesto a la integridad científica y degradan la confianza de la sociedad en la ciencia. Se trata de propuestas que están permitidas en países donde la iniciativa pública no cubre determinadas necesidades en investigación en salud y

27. Véase por ejemplo la Ley 14/2007, de 3 de julio, de Investigación biomédica. Última consulta 30 de octubre de 2020, disponible en: https://www.boe.es/eli/es/l/2007/07/03/14

28. Rubio, A., "Sujeto, cuerpo y mercado. Una relación compleja." en Casado, M. (Coord.), *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016. Reeditado por Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2018. Última consulta 30 de octubre de 2020, disponible en: http://diposit.ub.edu/dspace/bitstream/2445/116007/1/9788447541195.pdf

29. De Lecuona, I., "La tendencia a la mercantilización de partes del cuerpo humano y de la intimidad en investigación con muestras biológicas y datos (pequeños y masivos)", en Casado, M. (Coord.), *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016, pp. 267-296. Sevillano, E., "Mi tumor se vende en el extranjero", *El País*, 25 de julio de 2016. Última consulta 30 de octubre de 2020, disponible en: https://elpais.com/politica/2016/07/24/actualidad/1469369527_015224.html

atención sanitaria y que siguen políticas neoliberales. Aquello que está permitido en otros lugares no puede aceptarse en nuestro contexto. La globalización de las prácticas mercantilistas sobre muestras biológicas de origen humano y los datos personales asociados no justifica que deban permitirse, precisamente porque torpedea los cimientos del sistema investigador. Estas prácticas deben ser identificadas por parte de los actores que toman decisiones en los procesos de creación y aplicación del conocimiento y para ello se requiere un profundo conocimiento de las cuestiones científicas, pero también del marco ético y legal aplicable en una sociedad de mercado en la que el precio sustituye fácilmente al valor de las cosas. Se trata de maniobras sutiles que además juegan con los requisitos del propio sistema científico, que pueden ser vistas como fortalezas o debilidades, en el que los investigadores están abocados fundamentalmente a publicar los resultados de su investigación y a atraer financiación para llevar a cabo sus proyectos también en beneficio de la institución en la que trabajan.

Así, el avance del conocimiento científico, y su aplicación, tiene lugar en ambientes muy competitivos, con equipos interdisciplinares, de distinta procedencia geográfica y culturalmente diversos, y en los que "publicar o morir" y las reglas del mercado se imponen[30]. Un ejemplo más a considerar es la faceta emprendedora que se le exige al académico-investigador para transferir al mercado los resultados de su investigación y que sean valorizados mediante la financiación de fondos de inversión o de capital-riesgo, entre otras fórmulas. Este requisito viene impuesto por las agencias de acreditación del sistema universitario y de investigación de los Estados, provocando en numerosas ocasiones efectos no deseados en los procesos de creación de conocimiento científico[31].

Y es cierto que la brecha entre la sociedad y la ciencia es cada vez mayor. Una situación paradójica puesto que parecería que hoy el ciudadano dispone de más información que antes para someter a escrutinio el avance de conocimiento científico y tecnológico y sus aplicaciones[32]. En la aplicación de las tecnologías emergentes y el uso datos personales y que incluye el desarrollo de dispositivos de salud, predomina la opacidad propia de los negocios digitales[33]. Esta situación debe evitarse para transitar hacia un modelo que permita la gobernanza de los datos y el acceso a la información de forma transparente.

La pandemia por COVID-19 ha puesto de manifiesto que Europa no tiene infraestructuras públicas suficientes que permitan un sistema de gestión de datos sólida y eficaz. Además, tanto los Estados miem-

30. Sandel, M., *Lo que el dinero no puede comprar*, Editorial Debate, España, 2013.

31. Casado, M., Patrão Neves, M., De Lecuona, I., Carvalho, A., Araújo, J., *Declaración sobre integridad científica en investigación e innovación responsable*, Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2016. Última consulta 30 de octubre de 2020, disponible en: http://www.bioeticayderecho.ub.edu/es/declaracion-sobre-integridad-cientifica-en-investigacion-e-innovacion-responsable

32. Casado, M., Puigdomènech, P. (Coords.) *Documento sobre los aspectos éticos del diálogo entre ciencia y sociedad*, Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2018. Última consulta 30 de octubre de 2020, disponible en: http://www.bioeticayderecho.ub.edu/sites/default/files/documents/doc_ciencia-sociedad.pdf

33. Pasquale, F., *The black box society: the secret algorithms that control money and information Cambridge*, Massachusetts; London, England: Harvard University Press, Boston, 2015.

bros como la Unión Europea dependen excesivamente de las grandes tecnológicas fundamentalmente norteamericanas, centradas en extraer valor de los datos y no en crear valor[34]. Estas empresas a las que recurre tanto la iniciativa pública como privada para la prestación de servicios tienen, como es lógico, objetivos distintos a la investigación e innovación en salud, e interés en acceder a los conjuntos de datos, especialmente los de carácter personal. Un interés que difiere del que pueda tener un médico o un investigador. El modelo de negocio de las *bigtech* se basa en el acceso a datos personales para su explotación y monetización. Hoy se debaten los perniciosos efectos que ha generado la "economía de la atención" [35] promovida fundamentalmente por el impero GAFAM (Google, Apple, Facebook, Amazon y Microsoft por sus siglas en inglés), que ha abierto un pujante mercado de servicios basado en la explotación de datos personales y del que somos dependientes, voluntaria e involuntariamente. Pocas veces se reconoce que el auge de GAFAM ha sido posible porque los Estados han creado las infraestructuras necesarias mediante el pago de impuestos de los contribuyentes. Internet y el GPS son ejemplos y los gobiernos deben garantizar que un valor que se ha creado colectivamente esté al servicio del bien común[36]. Las Apps para la identificación de positivos y el rastreo de contactos deben ser consideradas como un ejemplo de nuevos servicios e infraestructuras públicas digitales al servicio del bien común y del interés colectivo, y deben diseñarse, probarse y aplicarse desde la máxima transparencia. Desafortunadamente en el caso español no ha sido así. La App RADAR COVID es un claro ejemplo de opacidad y falta de transparencia. Esta App recomendada por el gobierno español para la identificación de posibles positivos y el rastreo de sus contactos no ha sido objeto de un debate social informado acerca de su diseño, validación e implementación. Se han revelado importantes brechas de seguridad con elevado impacto para la intimidad de los usuarios y no se han llevado a cabo las correspondientes evaluaciones para identificar riesgos para los tratamientos de datos personales. Tampoco se ha liberado el código de programación en los repositorios en abierto habilitados a tal efecto para poder entender su lógica e identificar problemas, ni el expediente de contratación pública que incluye una prueba piloto en la Gomera a la que tampoco se ha podido acceder a pesar de varias peticiones ciudadanas a través del portal de transparencia y de grupos de expertos asesores ministeriales sobre COVID-19[37]. El gobierno ha esgrimido que publicar esta información podría dañar intereses comerciales para INDRA[38], la empresa beneficiaria y

34. Mazzucato, M., *El estado emprendedor*. RBA Libros, Barcelona, 2014.

35. Patino, B., *La civilización de la memoria de pez*. Alianza Editorial, Madrid, 2020 y Zuboff, S., *The age of surveillance capitalism*, PublicAffairs, Nueva York, 2019.

36. Mazzucato, M., "Preventing Digital Feudalism", *Social Europe*, 9 de octubre de 2019, Última consulta 30 de octubre de 2020, disponible en: https://www.socialeurope.eu/preventing-digital-feudalism

37. Pérez, J, "La 'app' Radar Covid ha tenido una brecha de seguridad desde su lanzamiento", *El País*, 22 de octubre de 2020, Última consulta 30 de octubre de 2020, disponible en: https://elpais.com/tecnologia/2020-10-22/la-app-radar-covid-ha-tenido-una-brecha-de-seguridad-desde-su-lanzamiento.html

38. Véase la Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el

que, por ello, mantiene su confidencialidad. Conviene tener en cuenta esta App formaría parte de las nuevas infraestructuras públicas en materia de salud pública al servicio de los ciudadanos y financiada por estos mediante el pago de impuestos, y que ha costado 330.537,52 euros[39].

El software, las Interfaces de Programación de Aplicaciones (APIs), las nubes y los servicios que se usan en el ámbito biomédico son, en su mayoría, propiedad de las *bigtech.* Es alarmante que no existan nubes propias desarrolladas por y para los sistemas sanitarios públicos que permitan, como se ha indicado, la interoperabilidad en condiciones seguras, ni tampoco nubes académicas donde compartir los datos de investigación[40]. Este vacío y retraso con respecto a la iniciativa privada condiciona el acceso y la utilización de los datos, y obliga a exigir a los Estados garantías que aseguren la intimidad y la confidencialidad de los datos, así como a establecer las condiciones para el control de estos por sus titulares. Las primeras reacciones para romper el dominio del imperio GAFAM se produjeron justo antes de la pandemia por COVID-19. En febrero de 2020, la Unión Europea presentó su estrategia digital y el Libro Blanco sobre Inteligencia Artificial[41]. Meses antes, Angela Merkel había alertado de la situación de dependencia de las *big tech* afectando a la competitividad europea[42].

No contar con un sistema sólido para la gestión de datos que permita el acceso, la interoperabilidad y la reutilización de datos, incluidos los datos personales,[43] es un obstáculo para la ciencia y para la toma de decisiones políticas. Los datos personales objeto de tratamiento deben ser fiables, de calidad, y almacenarse de formar segura, permitiendo su trazabili-

Ministerio de Sanidad, acerca de la aplicación «Radar COVID».

39. Manifiesto en favor de la transparencia en desarrollos de software públicos, septiembre de 2020, Última consulta 30 de octubre de 2020, disponible en: https://transparenciagov2020.github.io/

40. Grupo De Trabajo Multidisciplinar Covid-19 del Ministerio de Ciencia e Innovación, *Informe sobre datos e información en la epidemia COVID-19 y propuestas para la evolución digital del sistema de salud*, octubre de 2020.

41. Comisión Europea, *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data,* Bruselas, 19 de febrero de 2020 COM(2020) 66 final. Última consulta 30 de octubre de 2020, disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066

Comisión Europea, *White Paper on Artificial Intelligence - A European approach to excellence and trust* Brussels, 19 de febrero de 2020, COM(2020) 65 final Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

42. Pellicer, L. "Europa ultima un plan para dar la batalla en el negocio de los datos", *El País,* 17 de noviembre de 2019. Última consulta 30 de octubre de 2020, disponible en: https://elpais.com/economia/2019/11/16/actualidad/1573926886_318836.html

43. Comisión Europea, *Turning Fair into reality*, Brussels, 2018. Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_0.pdf

Comisión Europea, Directorate-General for Research & Innovation H2020 Programme, *Guidelines on FAIR Data Management in Horizon 2020,* de 26 de julio de 2016. Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf

dad. Los datos personales y, en particular, los datos de salud, no pueden estar al alcance de cualquiera. Por ello, existen no solo obligaciones jurídicas, sino también éticas y deontológicas para garantizar la más elevada protección[44].

Los efectos que la monetización de la información personal y de la propia intimidad no se proyectan únicamente sobre individuos, sino también sobre sociedades y democracias. La acumulación de datos por defecto y sin fines determinados que define a la sociedad digital hace tambalear los principios de protección de datos como la proporcionalidad y la minimización del dato. Esta quiebra de los esquemas tradicionales también ocurre en investigación, puesto que los presupuestos sobre los que se asienta la evaluación de los proyectos no se cumplen. Se debe revertir esta tendencia a la acumulación y a la monetización de datos personales, que pueden llegar a considerarse como un activo tóxico para entender lo que la economía digital representa para la intimidad[45].

3. Sesgos y discriminación algorítmica

En el desarrollo y aplicación de las tecnologías el riesgo cero no existe, y como sociedad debemos determinar el umbral de riesgo que estamos dispuestos a asumir. Si bien esta es una cuestión obvia, se torna compleja en el ámbito de las tecnologías emergentes, puesto que determinadas aplicaciones de la inteligencia artificial generan cajas negras que no permiten su inteligibilidad. Estas plantean retos para la toma de decisiones sobre si aplicar aquella inteligencia o no y cómo podrá justificarse el resultado cuando parte del proceso no puede explicarse, si bien el resultado final conduce a una decisión que genera más beneficios que riesgos[46].

Los algoritmos discriminan por razón de raza o de género[47]. Los medios de comunicación han revelado ejemplos de iniciativas para desarrollar algoritmos que han sido abandonadas porque las decisiones resultantes, que pretendían mejorar las tomadas por los humanos, eran discriminatorias. El caso de la inteligencia artificial de Amazon para seleccionar al mejor candidato fue sonado. Jeff Bezos, dueño de la compañía, anunció que no ofrecería este servicio porque sistemáticamente el algoritmo nunca priorizaba a una mujer como candidata, aunque tuviera el mejor currículum[48].

Los sesgos que incorpora la inteligencia artificial deben ser corregidos para que no se perpetúen, y para evitar la discriminación algorítmica[49]. Los sistemas de aprendizaje profundo, que pueden llegar

44. Martínez Montauti, J. *La relación médico-paciente*, Edicions i publicacions de la Universitat de Barcelona, Barcelona, 2018.

45. Véliz, C., *Privacy is Power*, Bantam Press, Londres 2020.

46. *Barcelona Declaration for the proper development and usage of Artificial Intelligence in Europe* Última consulta 30 de octubre de 2020, disponible en: https://www.iiia.csic.es/barcelonadeclaration/

47. O'Neil, C., *Armas de destrucción matemática*, Capitán Swing Libros, Madrid, 2018.

48. Dastin, J., "Amazon abandona un proyecto de IA para la contratación por su sesgo sexista", *Reuters,* 14 de octubre de 2018, Última consulta 30 de octubre de 2020, disponible en: https://fr.reuters.com/article/amazon-com-contratacion-ia-idESKCN1MO0M4

49. Baroni, M.J., "Las narrativas de la inteligencia artificial", *Revista de Bioética y Derecho*, 2019, pp. 5-28. Última consulta 30 de octubre

a tomar decisiones por sí mismos, deberían contar con datos de calidad y eliminar los sesgos. Tendrían además que ser revisados y corregidos por el humano con carácter previo a su aplicación, pero también durante su desarrollo. Los expertos en inteligencia artificial alertan que es necesario integrar los aspectos éticos desde el diseño de las intervenciones. Y convienen en que es crucial analizar el conjunto de datos que nutre a los sistemas de inteligencia artificial y limpiar aquellos datos antes de poner en marcha la intervención. Recientemente, ingenieros, informáticos y científicos de los datos, entre otros perfiles técnicos, reclaman formación específica en ética y en protección de los datos personales y que tradicionalmente no estaban contempladas en sus planes docentes. Se trata de tomar decisiones equitativas y determinar la responsabilidad sobre el algoritmo.

Es habitual caer en el error de que no existe suficiente normativa para tratar los retos que plantea toda nueva tecnología desde la perspectiva ética, legal y social. Para las tecnologías emergentes, como la inteligencia artificial y la analítica de datos masivos, existe una regulación jurídica transversal sobre protección de datos como es el Reglamento General de Protección de Datos, que establece una serie de principios, derechos y garantías. En los últimos tiempos se han elaborado guías y pautas para este ámbito que deben ser analizadas y que aportan los referentes sobre los que asentar la protección de las personas frente al uso de las tecnologías emergentes y la utilización de datos personales. En particular, conviene considerar la Guía del Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (2019) que se acompaña de una metodología cimentada en la Carta Europea de Derechos Fundamentales para que las organizaciones públicas y privadas, incluyendo también a la pequeña y mediana empresa, puedan evaluar el estado de la cuestión[50]. La estrategia europea se centra así en una inteligencia artificial confiable[51],centrada en el humano; fundamentada en el respeto por los derechos humanos y los valores a respetar en Europa; y que debe seguir los principios de beneficencia y no maleficencia, el respeto por la autonomía de los humanos, la justicia y la explicabilidad. El Grupo de Expertos de Alto Nivel se refiere específicamente a las asimetrías que se pueden generar en cuanto a la información de la que puedan disponer los distintos actores como por empleadores y empleados etc., y reclama atención hacia aquellas situaciones que puedan comprometer los de-

de 2020, disponible en: https://revistes.ub.edu/index.php/RBD/article/view/27280

50. En la Unión Europea, el Grupo de Expertos de Alto Nivel Sobre Inteligencia Artificial publicó en abril de 2019 las *Pautas para una Inteligencia Artificial confiable.* que incluye una evaluación desde el enfoque de valores y respeto por los derechos humanos para el desarrollo de aplicaciones de inteligencia artificial. Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

51. Comisión Europea, *Communication to the commission. European Commission digital strategy*. A digitally transformed, user-focused and data-driven Commission, Brussels, 21.11.2018 C(2018) 7118 final. Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/info/sites/info/files/strategy/decision-making_process/documents/ec_digitalstrategy_en.pdf y Comisión Europea, *White Paper on Artificial Intelligence: A European approach to excellence and trust*, Brussels, 19.2.2020 COM(2020) 65 final. Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

rechos de los colectivos y personas más vulnerables por el uso de la inteligencia artificial.

Por su parte, el Consejo de Europa ha efectuado aportaciones relativamente recientes y del todo relevantes para la protección de datos personales en cuanto al tratamiento automatizado de datos y ante la inteligencia artificial y el Big Data. El resultado es aplicable a otras tecnologías emergentes, como la biometría o la realidad virtual, que también se utilizan en los procesos de investigación e innovación en salud. La *Guía para la protección de las personas con respecto al tratamiento de datos de carácter personal en el mundo Big Data* (2017)[52] y la *Guía sobre Inteligencia Artificial y Protección de Datos* (2019)[53], fueron elaboradas por el Comité Consultivo del Convenio para la protección de las personas en relación con el procesamiento de datos de carácter personal. Interesa analizar aquí específicamente las aportaciones sobre la vigilancia algorítmica precisamente para evitar discriminaciones, incluidas aquellas encubiertas por razón de los algoritmos. El objetivo del Consejo de Europa es proporcionar un conjunto de medidas para ayudar a que gobiernos, desarrolladores, fabricantes y proveedores de servicios de inteligencia artificial se aseguren de que sus aplicaciones no socavan la dignidad y los derechos humanos, especialmente al derecho a la intimidad y la confidencialidad de los datos personales.

Según las Pautas, las aplicaciones de la inteligencia artificial se refieren a sistemas basados en inteligencia artificial, pero también a software y dispositivos que aportan nuevas y valiosas soluciones para dar respuesta a los retos de nuestro tiempo en diversos campos. Un ejemplo es el sector salud y el uso de sistemas predictivos como ya se ha visto. El Consejo de Europa incide en que ante las consecuencias que pueden tener las aplicaciones de inteligencia artificial, la protección de la dignidad humana y la salvaguardia de los derechos humanos y las libertades fundamentales deben preservarse. Situación especialmente relevante en el caso de que la inteligencia artificial sirva como herramienta de apoyo para para tomar decisiones. Así, este desarrollo debe estar fundamentado en los principios de licitud, equidad, limitación del propósito, proporcionalidad, privacidad desde el diseño y por defecto, responsabilidad, rendición de cuentas, transparencia, seguridad de los datos y gestión de riesgos. Se hace hincapié también en que la innovación responsable es necesaria en inteligencia artificial, no solo desde el punto de vista de los derechos individuales, sino también teniendo en cuenta su posible impacto en valores éticos y sociales y en el funcionamiento de las democracias. Asimismo, las aplicaciones de inteligencia artificial deben permitir el control del tratamiento de los datos por parte de los interesados.

En las orientaciones para desarrolladores, fabricantes y proveedores de servicios de inteligencia artificial, se hace hincapié en

52. Consejo de Europa, *Guidelines on Big Data* adopted by the Consultative Committee of the Council of Europe´s data protection convention (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108), Estrasburgo, 2017. Última consulta 30 de octubre de 2020, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a

53. Consejo de Europa, *Guidelines on Artificial Intelligence and Data Protection*, Estrasburgo, 2019. Última consulta 30 de octubre de 2020, disponible en: https://www.coe.int/en/web/artificial-intelligence/-/new-guidelines-on-artificial-intelligence-and-data-protection

adoptar un enfoque orientado al respeto por los valores consensuados desde el diseño de los productos y las intervenciones, de manera que sean conformes con los instrumentos jurídicos internacionales y, en particular, con aquellos elaborados por el Consejo de Europa. Debe adoptarse además un enfoque precautorio basado en la prevención del riesgo y su mitigación. El enfoque del diseño basado en el respeto por los derechos humanos debe aplicarse en todas las fases del tratamiento de datos y evitar potenciales sesgos, incluidos aquellos ocultos o no intencionados, el riesgo de discriminación u otros impactos adversos en los derechos y libertades fundamentales de los titulares de los datos personales. Los desarrolladores de inteligencia artificial deben evaluar la calidad, naturaleza, origen y el volumen de datos personales usados. Deben reducir la cantidad de datos tratados durante el proceso de desarrollo, para eliminar aquellos que sean redundantes o considerados como marginales. Esta acción también aplicaría a las etapas de entrenamiento de los sistemas y para poder hacer el seguimiento para determinar la exactitud del modelo mientras es alimentado con nuevos datos. Para minimizar la cantidad de datos personales a usar se recomienda recurrir a datos sintéticos, esto es, aquellos generados por modelos de datos que se han creado de datos reales.

La evaluación de las posibles consecuencias negativas de la inteligencia artificial en los derechos y libertades fundamentales recae en los citados actores, y se aconseja que existan medidas de prevención y minimización de riesgos en su desarrollo. Los riesgos que la utilización de datos y modelos algorítmicos descontextualizados puede tener en las personas afectadas y en la sociedad deben ser también tenidos en cuenta en el desarrollo y uso de aplicaciones de inteligencia artificial[54]. Se contempla la posibilidad de crear o consultar a comités de expertos independientes en distintos ámbitos, y se anima a trabajar en colaboración con instituciones académicas independientes. Esta colaboración puede ayudar a contribuir a un diseño de inteligencia artificial que incorpore los valores éticos y sociales e identifique posibles sesgos. En cuanto a los citados comités, estos pueden tener una función clave en áreas en las que la transparencia y la participación de los interesados sean más difíciles debido a los intereses en conflicto. La evaluación del riesgo sobre los datos personales objeto de tratamiento debe incluir formas de participación para que las personas y los colectivos afectados puedan estar representados.

En el ámbito de la inteligencia artificial los productos y servicios deben diseñarse para asegurar el derecho de las personas a no ser objeto de decisiones automatizadas que les afecten de forma significativa, y sin haber tomado en consideración su punto de vista. Es necesario generar confianza en el usuario en las aplicaciones de inteligencia artificial y para ello, tanto los desarrolladores, como los fabricantes y los proveedores de servicios deberían preservar la libertad para decidir sobre el uso de estas aplicaciones de los destinatarios y para ello es necesario proporcionar alternativas a estas. Los desarrolladores, fabricantes y proveedores de servicios de inteligencia artificial deberían adoptar formas

54. Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial de la Unión Europea, *Pautas éticas sobre inteligencia artificial*, Bruselas, 2019. Última consulta 30 de octubre de 2020, disponible en: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence

de vigilancia algorítmica para promover la rendición de cuentas de todos los actores implicados a lo largo del ciclo de vida de estas aplicaciones, de tal forma que sea posible cumplir con la normativa aplicable en materia de protección de datos y derechos humanos. Los titulares de los datos deben ser informados acerca de si interactúan con una aplicación de inteligencia artificial y obtener información sobre el razonamiento subyacente al procesamiento de datos de la inteligencia artificial que se les aplique y las consecuencias de la lógica explicada. Debe garantizarse el derecho de oposición a tratamientos basados en tecnologías que influyan en opiniones y en el desarrollo personal de los individuos.

Las orientaciones para legisladores y responsables políticos incluidas en las Pautas establecen que el respeto del principio de rendición de cuentas, la adopción de procedimientos de evaluación de riesgos y el desarrollo de códigos de conducta y mecanismos de certificación ayuda a mejorar la confianza en los productos y servicios de inteligencia artificial mediante. Además, en los procesos de contratación pública para desarrolladores, fabricantes y proveedores de servicios de inteligencia artificial se deben establecer obligatoriamente deberes específicos sobre transparencia, evaluación previa del impacto de los tratamientos de datos en los derechos y libertades fundamentales y mecanismos de vigilancia algorítmica sobre los potenciales efectos adversos y las consecuencias de las aplicaciones de inteligencia artificial. Se insta a las autoridades a que se doten de los recursos necesarios para hacer el correspondiente seguimiento. No se debe depender en exceso de estas tecnologías y es necesario preservar la intervención humana en los procesos de toma de decisiones. También es necesario fomentar la cooperación entre las autoridades de supervisión de protección de datos y otros organismos que tengan competencias relacionadas con la inteligencia artificial. Las personas, los grupos y otros interesados deben ser informados y participar activamente en el debate sobre el desarrollo y aplicación de la inteligencia artificial. Estos pueden contribuir a determinar el lugar que ocupa la inteligencia artificial en la dinámica social y en la toma de decisiones.

Los legisladores y los responsables políticos deben invertir recursos en educación y alfabetización digital para que las personas puedan mejorar su comprensión sobre los efectos de las aplicaciones de inteligencia artificial. Además, los legisladores y responsables políticos deben fomentar la capacitación y formación de los desarrolladores de inteligencia artificial para que éstos también entiendan las implicaciones que tiene sobre individuos y sociedades. Es necesario apoyar la investigación sobre inteligencia artificial desde el enfoque de los derechos humanos.

4. Acumulación de datos por defecto y analítica de datos masivos

Es conocida la historia del supermercado norteamericano Target y la invasión que provocó su algoritmo en la intimidad de una familia debido a que el padre supo que su hija adolescente estaba embarazada por los cupones de descuentos para toallitas que le llegaron a su buzón[55]. El

55. Duhigg, C., "How companies learn your secrets" *The New York Times Magazine*, 16 de febrero de 2012, Última consulta 30 de octubre

Big Data implica un cambio de paradigma y pone en entredicho los principios de protección de datos precisamente porque el desarrollo de la citada tecnología está condicionado al acceso y explotación de grandes cantidades de datos. Se rompen las tradicionales reglas del juego porque la tendencia es a acumular datos por defecto para luego establecer las hipótesis o las preguntas a las que se quiere dar respuesta[56]. En el mundo digital el principio de proporcionalidad y de minimización de los datos no encajan. Si bien existen varias definiciones, el ***Big Data*** se refiere a que tecnológicamente es posible recoger, procesar y extraer nuevo conocimiento que permita hacer predicciones a través del tratamiento de grandes cantidades de datos, que proceden de diversidad de fuentes y a mayor velocidad[57]. Esta tecnología serviría para mejorar la toma de decisiones. El *Big Data* se refiere también a la analítica de datos masivos.

Las *Pautas para la protección de las personas en relación con el procesamiento de datos personales en contextos Big Data*, fueron elaboradas por el Comité Consultivo del Convenio para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal, y publicadas en enero de 2017. Los retos planteados por el tratamiento de datos masivos motivaron al Comité a redactar estas Pautas, con el objetivo de aportar un marco de principios y guías para que los Estados pudieran desarrollar las políticas y las medidas apropiadas para hacer efectivos los principios y las disposiciones del Convenio para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal[58] en el contexto del Big Data. La sociedad digital que tiende a acumular conjuntos de datos por defecto, y entre ellos datos personales, necesita referentes como los aportados por el Consejo de Europa, en un momento de cambio normativo, puesto que el Reglamento General de Protección de Datos es de aplicación desde mayo de 2018. Es preciso articular un marco de principios y procedimientos que permitan avanzar en el uso de las tecnologías emergentes en el ámbito de la investigación e innovación en salud. Las Pautas del Consejo de Europa pueden contribuir a identificar un marco de principios y a desarrollar acciones en salud como complemento al citado Reglamento.

El Big Data puede aportar valor e innovación a la sociedad, mejorar la productividad, la actividad del sector público y también la participación social. La analítica de datos masivos representa una ventaja, pero también una amenaza para la protección de los datos de carácter personal, dado que se nutre en buena parte de datos personales. Por ello, el objetivo de las Pautas es recomendar medidas que los

de 2020, disponible en: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

56. En este sentido véase Llácer, M.R., Casado, M., Buisán, L., *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública,* Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2015. Última consulta 30 de octubre de 2020, disponible en: http://www.bioeticayderecho.ub.edu/es/documento-sobre-bioetica-y-big-data-de-salud-explotacion-y-comercializacion-de-los-datos-de-los

57. Las Pautas definen Big Data en el apartado III sobre terminología.

58. Consejo de Europa, *Convention for the protection of individuals with regard to the processing of personal data*, hecho en Estrasburgo en 1981 y que fue modificado en 2018. Última consulta 30 de octubre de 2020, disponible en: https://www.coe.int/en/web/data-protection/convention108/modernised

Estados, los responsables y los encargados del tratamiento de datos puedan tomar para prevenir los posibles impactos negativos del uso del Big Data sobre las personas. Estos riesgos para los derechos de los individuos se refieren principalmente al sesgo potencial que deriva del análisis de los datos, la infravaloración de las implicaciones legales, sociales y éticas del uso de Big Data y a la marginación de las personas afectadas en los procesos de toma de decisiones que impide su participación efectiva. Se trata de asegurar la protección de la autonomía de las personas mediante el derecho a controlar su información personal y el procesamiento de sus datos personales. Un derecho que debe ser analizado detenidamente en el contexto del Big Data y que implica que las instituciones, los legisladores y los responsables políticos, así como los responsables y encargados del tratamiento de datos deben involucrarse en la compleja tarea de evaluar el impacto y los riesgos del uso de estos, y no dejar esa protección circunscrita al mero control individual.

El primero de los principios recogidos es el uso de datos ético y socialmente consciente, que responde a la necesidad de encontrar el equilibrio entre los intereses implicados en el procesamiento de los datos personales. La posibilidad de hacer predicciones a través del uso del Big Data que sirvan para la toma de decisiones obliga a los responsables y los encargados de tratamiento a analizar el impacto de los procesamientos de datos en sus titulares. Este debe hacerse desde una perspectiva amplia que tenga en cuenta los aspectos éticos y las implicaciones sociales de tal forma que sea posible proteger y garantizar los derechos y libertades fundamentales. El desarrollo y aplicación del Big Data no pueden entrar en conflicto con los valores éticos consensuados ni tampoco pueden perjudicar intereses sociales, valores, normas ni derechos reconocidos.

Las Pautas aconsejan la creación *ad hoc* o el recurso a comités de ética ya establecidos para que identifiquen aquellos valores éticos a preservar, en el caso de que de la evaluación del impacto de los tratamientos de datos personales en contextos Big Data se detecte un elevado riesgo. Estos comités deben ser independientes y objetivos, y deben estar formados por personas que, por su competencia, experiencia, y cualificación profesional, garanticen su correcto funcionamiento. Se observa la tendencia a la creación de comités y comisiones interdisciplinares para poder tratar adecuadamente los retos que la ciencia y la tecnología plantean. Parece que estos pueden adaptarse de manera ágil a los nuevos escenarios para evaluar y asesorar.

Hacen falta políticas de prevención y las evaluaciones de riesgo. Se aplica así un enfoque precautorio para tratar la protección de datos personales y que son tarea de los responsables de los tratamientos. Estas políticas están en consonancia con los principios de prevenir y minimizar los impactos potenciales del tratamiento de datos personales en los derechos fundamentales. La evaluación de los riesgos se debe hacer con carácter previo, pero también a lo largo de todo el ciclo de vida de las tecnologías que impliquen tratamiento de datos personales e involucrar a diferentes perfiles profesionales que puedan analizar los diferentes impactos, incluyendo las dimensión legal, social, ética y técnica, así como introducir en estos procesos de evaluación a personas o grupos potencialmente afectados. El uso del Big Data puede afectar a individuos y grupos

y, por ello, es necesario que se garantice la equidad y la no discriminación.

Los usos del procesamiento de datos deben ser legítimos y no exponer a los individuos a riesgos mayores de los contemplados por los objetivos iniciales. Además, los resultados de las evaluaciones de riesgo deben ser accesibles públicamente, con las pertinentes salvaguardas que disponga la ley. El enfoque desde el diseño se despliega en las diferentes etapas del procesamiento de datos masivos con el objetivo de minimizar su uso, evitar sesgos ocultos y el riesgo a que tengan lugar discriminaciones. Además, se incide en el desarrollo de medidas para garantizar la seudonimización de tal forma que se reduzca el riesgo que el tratamiento de datos puede representar para las personas.

El consentimiento libre, específico, informado e inequívoco debe estar basado en la información proporcionada al titular de los datos de acuerdo con el principio de transparencia. La información debe incluir el resultado del proceso de evaluación antes descrito. El consentimiento no se considera libre si existe un desequilibrio de poder entre la persona afectada y el responsable del tratamiento. Este último es quien debe demostrar que esta asimetría no existe. Los controladores y los encargados de tratamiento tienen que facilitar las condiciones técnicas para que las personas puedan reaccionar ante un tratamiento de datos que se considere incompatible con los fines inicialmente establecidos y que puedan revocar el consentimiento prestado.

Ante la posibilidad de reidentificar a las personas, es obligación del responsable del tratamiento llevar a cabo una evaluación de esta probabilidad teniendo en cuenta el tiempo, el esfuerzo y los recursos que se necesitan con respecto a la naturaleza de los datos, el contexto en el que se usan, la disponibilidad de tecnologías que permitan reidentificación de las personas afectadas y los costes. El responsable del tratamiento debe demostrar la pertinencia de las medidas adoptadas para asegurar de forma efectiva la no atribución de personalidad a los titulares de los datos. Para prevenir posibles reidentificaciones es necesario aplicar medidas técnicas además de revisar las obligaciones legales y contractuales, y llevar a cabo revisiones periódicas teniendo en cuenta los avances tecnológicos al respecto.

La intervención humana en decisiones apoyadas por la analítica de datos masivos es necesaria. Las decisiones que se tomen en aplicación de esta tecnología deben evitar descontextualizar la información y tienen que ser transparentes en cuanto a los razonamientos en los que se basan. Si las decisiones resultantes pueden afectar a la persona o tener efectos legales, a petición del interesado, quien toma las decisiones debe aportar evidencias del proceso de razonamiento llevado a cabo, y las consecuencias que pudiera tener para el afectado. Asimismo, quien toma las decisiones es libre de no confiar en el resultado de las recomendaciones proporcionadas por la aplicación de la analítica de datos masivos. Cuando existan indicios de los que se pueda presumir que ha habido directa o indirecta discriminación basada en el análisis de Big Data, los responsables y encargados de tratamiento de los datos deben demostrar la ausencia de discriminación. Las personas afectadas por una decisión basada en Big Data tienen derecho a impugnarla ante la autoridad competente.

La iniciativa pública y privada debería establecer políticas sobre datos abiertos y

datos personales, puesto que estos datos en abierto se pueden utilizar para inferir información sobre individuos y grupos. En el caso de que los responsables adopten políticas de acceso abierto, la evaluación del impacto antes descrita debe prestar especial atención a las consecuencias de combinar diferentes datos que provengan de distintos conjuntos de datos, nuevamente por el riesgo de reidentificación. Finalmente, el Consejo de Europa vuelve sobre la educación y la alfabetización digital, necesarias para contribuir a que las personas puedan comprender adecuadamente las implicaciones de los usos del Big Data. La alfabetización digital debe considerarse como una competencia esencial.

5. Los comités de ética de la investigación como mecanismos de protección de las personas en investigación e innovación en salud ante el uso de tecnologías emergentes

Asentados en la sociedad digital guiada por el dato como decisión política europea es preciso revisar planteamientos y requisitos para contribuir al desarrollo de pautas para evaluar adecuadamente la investigación e innovación en salud que utiliza tecnologías emergentes y datos personales. La ética de la investigación ha sido y sigue siendo una de las temáticas que definen a la bioética como disciplina[59]. El origen de la bioética está estrechamente vinculado a la creación de los comités de ética de la investigación que se conciben como instancias para ponderar los derechos e intereses en juego desde la independencia que les debe caracterizar[60]. Los comités de ética de la investigación son órganos interdisciplinares con el cometido de proteger los derechos de las personas participantes en investigación y de aquellas que estén implicadas, bien porque donan sus muestras biológicas o porque ceden sus datos personales. Entre estos derechos se sitúa también la libertad de investigación, como principal estímulo para el avance del conocimiento científico y su aplicación. Así, los comités de ética de la investigación regulados por ley hace décadas[61] y sin los que no es posible avanzar en investigación, pues de ellos depende la aprobación de los proyectos, se convierten en actores fundamentales del sistema de investigación y también de la innovación aparejada en salud. Su dictamen previo y favorable es *conditio sine qua non* para que puedan desarrollarse los citados proyectos en centros hospitalarios y de investigación públicos y privados[62]. En Europa conviven distintas fórmulas: los comités de ética de

59. López Baroni, M.J., *El origen de la bioética como problema*, Editorial de la Universitat de Barcelona, Barcelona, 2016.

60. JONSEN, A., *The Birth of Bioethics,* Oxford University Press, 2003, ANNAS, G.J., "Ethics committees: from ethical comfort to ethical cover", *The Hastings Center Report,* Vol. 21, Núm. 3, 1991, pp.18 a 21.

61. Ley 25/1990, de 20 de diciembre, del Medicamento (Derogada) y 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.

62. Ley 14/2007, de 3 de julio, de Investigación biomédica y 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 y el Registro Español de Estudios Clínicos.

la investigación pueden ser de carácter nacional, regional, pero también cabe la posibilidad de que cada centro de investigación cuente con su propio comité de ética de la investigación o se adscriba a uno ya creado. Todos ellos deben estar acreditados por el organismo correspondiente, previo cumplimiento de una serie de requisitos y condiciones[63].

Inicialmente los comités de ética de la investigación se crearon para evaluar ensayos clínicos con medicamentos y productos sanitarios, para luego analizar otros tipos de investigaciones que, por sus características, también plantean la necesidad de encontrar un equilibrio entre el avance del conocimiento científico, el interés investigador y la protección de las personas. En los últimos tiempos evalúan también, como se ha descrito, proyectos de investigación e innovación que utilicen tecnologías emergentes como la inteligencia artificial, el Big Data, y en los que se desarrollen de dispositivos y Apps de salud. Los intereses de la ciencia, de la tecnología y de la sociedad no deben prevalecer sobre los del individuo. Para ello, los comités de ética de la investigación deben analizar la validez científica de las propuestas, su valor social y ponderar los derechos e intereses en juego.

La pandemia por COVID-19 ha provocado un aluvión de proyectos para desarrollar tratamientos e intervenciones como vacunas y medicamentos pero también han sido numerosas las propuestas de sistemas de predicción y gestión de la COVID-19 utilizando sistemas de inteligencia artificial, datos masivos y biometría, como se ha descrito. El SARS-COV-2 ha puesto a prueba también a los comités de ética de la investigación que trabajan a destajo y que deben decidir sobre qué investigaciones priorizar debido a su validez científica y valor social. Los comités de ética de la investigación han tenido que articular procedimientos para dar una rápida respuesta a los investigadores sin abandonar el análisis exhaustivo de los aspectos metodológicos, éticos, legales y sociales de las propuestas. Es posible, que en muchos casos lo hayan hecho sin precedentes, pues la investigación que aplique inteligencia artificial o Big Data no tiene suficiente andadura todavía como para tener una casuística que permita identificar con claridad las cuestiones más complejas y los posibles vacíos. Se ha puesto de manifiesto que la composición no es la adecuada, faltan expertos en estas tecnologías capaces de identificar los problemas y los retos y llevar a cabo una adecuada evaluación; no hay suficientes recursos humanos y materiales en las secretarías técnicas, cuando la investigación es el pilar del sistema y se traduce en poder, en conocimiento, y en un apoyo económico para las instituciones nada despreciable. Las pautas y procedimientos de trabajo no responden a las necesidades actuales pero sobre todo, falta un marco teórico que permita a los agentes implicados entender las cuestiones que luego deben ser objeto de análisis. Ese marco teórico está por hacerse y por ello, se siguen aplicando viejos referentes a problemas nuevos pero arrastrando viejas inercias en cuanto al funcionamiento de los comités de ética de la investigación que provocan numerosos desajustes.

Así, puede decirse que el modelo evaluador de la investigación e innovación en salud es ineficaz debido a que los principios,

63. Véase a título de ejemplo el Decreto 406/2006, de 24 de octubre, por el que se regulan los requisitos y el procedimiento de acreditación de los comités de ética de investigación clínica.

los requisitos y los procedimientos que se establecieron después de la segunda mitad del siglo XX en investigación ya no son aplicables en su mayoría. Y es que, como se ha constatado, el paradigma digital asentado en la explotación intensiva de datos personales mediante el recurso a tecnologías emergentes y su convergencia ha provocado que principios y garantías clásicas como la proporcionalidad, la anonimización y los protocolos de información y consentimiento informado hayan quedado desfasados en el paradigma digital[64]. Es un hecho que la digitalización tiende a la acumulación de conjuntos datos por defecto, situación que rompe también con el principio de minimización del dato en investigación. Se aplican pautas y protocolos de la evaluación analógicos al contexto actual que es digital en su conjunto. Los comités de ética de la investigación no están consiguiendo adaptarse al paradigma digital, y al cambio que supone asentar los procesos de investigación e innovación en salud en la explotación intensiva de conjuntos de datos personales generando no pocas disfunciones y una falsa seguridad que podría esconder mercados de datos disfrazados de investigación e innovación.

Los comités de ética de la investigación deben analizar cuestiones con profundas implicaciones para las personas, incluidas las generaciones futuras. Este trabajo pone de manifiesto que es acuciante estudiar las implicaciones éticas de la toma de decisiones automatizada, la equidad de los algoritmos y la calidad de los datos que se utilizan para alimentarlos; la responsabilidad de los actores implicados en los procesos de investigación e innovación en salud cuando se utilizan tecnologías emergentes y datos personales; el valor que se le otorga a los datos personales (y no el precio) en la sociedad digital guiada por el dato anteriormente descrita y en la que debería primar el bien común y no favorecer intereses espurios; y sobre nuevas fórmulas de gobernanza digital. Estas cuestiones puramente bioéticas necesitan un análisis doctrinal, pero también una respuesta práctica que permita a los comités de ética de la investigación contar con recomendaciones y pautas para una adecuada evaluación de los proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales[65].

Los comités de ética de la investigación deben proteger a las personas a través de la salvaguarda de sus datos personales y asegurar la intimidad y la confidencialidad de sus titulares. Además, deben promover y garantizar el ejercicio de la autonomía para tomar decisiones de manera libre e informada, evitar la discriminación,

64. Pérez, G., "Peligros del uso de los big data en la investigación en salud pública y en epidemiología", *Gaceta Sanitaria*, vol. 30, núm. 1, pp. 66-68, DOI: 10.1016/j.gaceta.2015.09.007 y De Lecuona, I., "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)", *Gaceta Sanitaria*, 2018, Vol. 32. Núm. 6, pp. 576-578. DOI: 10.1016/j.gaceta.2018.02.007

65. ATIENZA, M., "Juridificar la bioética", edición digital a partir de *Isonomía: Revista de Teoría y Filosofía del Derecho,* núm. 8 (abril 1998), pp. 75-79. Última consulta 30 de octubre de 2020, disponible en: http://www.cervantesvirtual.com/obra/juridificar-la-biotica-0/ y De Lecuona, I. (Coord.), *Pautas para evaluar proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales*, Observatorio de Bioética y Derecho de la Universitat de Barcelona, octubre 2020, Barcelona. Última consulta 30 de octubre de 2020, disponible en: http://www.bioeticayderecho.ub.edu/sites/default/files/documents/doc_eval-proyectos.pdf

también aquella encubierta, así como garantizar la equidad y la transparencia. El equilibro que los comités de ética de la investigación deben alcanzar entre maximizar los beneficios y minimizar los riesgos incluye también tratar adecuadamente los datos personales[66].

Integrar nuevos miembros o asesores en tecnologías emergentes, especialmente a científicos de datos y a expertos en técnicas de seudonimización debería ser una prioridad para los comités de ética de la investigación. También deben incorporar al Delegado de Protección de Datos, figura establecida por la normativa de protección de datos personales para asesorar de forma independiente en el análisis de los riesgos que los tratamientos de datos puedan provocar en la intimidad y la confidencialidad de los datos personales de los afectados[67]. Ante los riesgos del tratamiento de datos personales en contextos altamente digitalizados para la intimidad y la confidencialidad de los datos, los comités de ética de la investigación deben actuar de forma coordinada con los servicios legales y las áreas de tecnologías de la información y la comunicación de la institución correspondiente[68]. Los comités de ética de la investigación también deber incorporar el enfoque de gestión de los riesgos sobre los tratamientos de datos personales para revisar que se desarrollan medidas técnicas y organizativas suficientes para asegurar que se protege la intimidad de las personas afectadas a través del tratamiento de datos personales propuesto.

6. Conclusiones

La explotación intensiva de datos personales obliga a repensar la forma en la que se investiga e innova mediante el recurso a las tecnologías emergentes y el uso de datos personales. Conviene revisar el modelo de evaluación y desarrollar un marco de principios y procedimientos que permitan analizar adecuadamente los aspectos metodológicos, éticos, legales y sociales de los proyectos de investigación e innovación en salud en la sociedad digital. Es preciso desarrollar una ética de la investigación y de la innovación para el siglo XXI en la que la protección de las personas se efectúe a través de la salvaguarda de los datos personales. Se necesitan nuevas fórmulas de gobernanza sobre los datos personales, que permitan la parti-

66. De Lecuona, I. "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)" *Gaceta Sanitaria*, Vol. 32. Núm. 6, pp. 576-578. 2018. DOI: 10.1016/j.gaceta.2018.02.007 Última consulta 30 de octubre de 2020, disponible en: https://www.gacetasanitaria.org/es-evaluacion-los-aspectos-metodologicos-eticos-articulo-S0213911118300864

67. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disposición adicional decimoséptima, letra g se establece: "El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica, deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial" y h) "en el plazo máximo de un año los CEI deberán integrar entre sus miembros un delegado de protección de datos, o un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados."

68. Véase European Data Protection Supervisor, *Flowcharts and Checklists on Data Protection* , 2020. Última consulta 30 de octubre de 2020, disponible en: https://edps.europa.eu/sites/edp/files/publication/flowcharts_and_checklists_on_data_protection_brochure_en_1.pdf

cipación de todos los implicados, y que sitúen en el centro a los participantes, a quienes proveen los datos, sus titulares, y que son, en buena parte también sus destinatarios. Los datos forman parte de la intimidad de las personas pero también deberían entenderse como bien común a proteger. Un valor social en alza.

El consentimiento informado, tal y como lo conocemos, no parece suficiente para garantizar el adecuado tratamiento de los datos personales y se hace necesario exigir transparencia y rendición de cuentas en los procesos de generación y transferencia de conocimiento en el ámbito de la salud. El desarrollo y aplicación de las tecnologías emergentes afecta a individuos, a grupos de personas, pero también se ha puesto de manifiesto aquí que puede tener consecuencias no deseadas sobre democracias por condicionar la libertad de las personas y afectar a las generaciones futuras.

Europa debe evitar la excesiva dependencia de las grandes tecnológicas estadounidenses y promover el desarrollo de infraestructuras públicas propias para la gestión de los datos personales en investigación e innovación en salud. La economía de la atención no puede inundar los territorios reservados a la creación de conocimiento científico ni deshacer sus salvaguardas. Esta situación obliga a repensar la función del Estado y de las grandes tecnológicas en el siglo XXI, y reconocer que, en estos momentos, tras años de digitalización intensiva, el individuo todavía no tiene el control sobre sus datos personales a no ser que se produzca un cambio en la concepción de la intimidad. Esta debe considerarse como un bien común a proteger además de un derecho fundamental. Se debe evitar el lucro sobre los datos personales. Su mercantilización debería estar prohibida.

El principio de prohibición de lucro sobre los datos personales debería ser impuesto por los Estados y desarrollar acciones para que los diversos actores contaran con mecanismos para evitar que intereses espurios accedan a datos personales, en particular, en el ámbito de la salud y que además estos se moneticen. Las prácticas mercantilistas sobre el cuerpo humano y los datos personales invisibilizan los pilares sobre los que asienta el sistema de salud, que son el altruismo y la solidaridad. Los resultados de la explotación controlada y con fines determinados previamente establecidos, deben revertir en beneficio de las personas, bien sea mediante tratamientos o intervenciones o mediante el aumento del conocimiento generalizable sin un beneficio directo para los cesionarios de estos. La utilización del Big Data y la inteligencia artificial no pueden obviar la aplicación de los principios de protección de datos ni debilitarlos. Es perentorio evitar los sesgos y la discriminación algorítmica y la acumulación indiscriminada de datos por defecto o por si acaso por la elevada afectación de derechos y libertades fundamentales. Se debe evitar el abuso de los datos personales y cualquier tipo de discriminación derivada de su tratamiento, incluida aquella encubierta.

Los principios de protección de datos a aplicar en el uso de tecnologías emergentes y datos personales de salud son: licitud, lealtad y transparencia; limitación del propósito; minimización del dato; exactitud y actualización; almacenamiento limitado e integridad y confidencialidad. Asimismo, deben aplicarse los principios de privacidad desde el diseño y privacidad por defecto, para determinar las medidas técnicas y organizativas necesarias para asegurar la protección de datos de carácter personal,

desde el diseño de la intervención que se propone y durante su desarrollo.

Por su parte, el titular de los datos personales tiene derecho a ser informado, derecho de acceso, derecho de rectificación, derecho al borrado/olvido, el derecho a restringir el procesamiento de los datos, el derecho a portabilidad de los datos y el derecho a no ser objeto de una decisión automatizada, que incluye la controvertida elaboración de perfiles, decisiones que deben incorporar la intervención/corrección humana. Se amplía así el catálogo de derechos reconocidos para la protección de la intimidad y la confidencialidad a la estela de los conocidos como derechos de acceso, rectificación, cancelación y oposición, en los que se asienta la autodeterminación informativa, reconocida por tribunales en el siglo XX.

También, deben llevarse a cabo, en función de la tipología de datos a tratar, las correspondientes metodologías para la evaluación del impacto de los tratamientos de datos propuestos en las personas afectadas. Es el caso de las categorías especiales de datos como los datos salud o el uso de nuevas tecnologías[69]. Esta evaluación va a permitir un análisis de los riesgos sobre los datos personales y su mitigación. La evaluación se debe llevar a cabo antes del inicio del tratamiento de datos personales. Este es un proceso vivo, que deberá revisarse periódicamente y permitirá efectuar un seguimiento del ciclo de vida de los datos, desde el inicio, pero también durante su desarrollo y en su finalización.

Los intereses de la ciencia - también de la tecnología- y de la sociedad no deben prevalecer sobre los del individuo. Por ello, conviene revisar la situación de los comités de ética de la investigación, para que estas piezas clave de la investigación e innovación en salud se adapten lo antes posible al paradigma digital, para llevar a cabo su función de protección de las personas en investigación y también en la innovación aparejada. Estos también van a tener que efectuar una relectura de los valores como la intimidad y la libertad. Los comités de ética de la investigación deben evaluar y comprobar que se establecen las condiciones necesarias para que las personas toman decisiones libres e informadas, y que estas tienen el control sobre sus datos personales. También deben comprobar que los distintos agentes que intervienen en los tratamientos de datos personales hacen un uso adecuado de estos y que evitan su acumulación y monetización desde las buenas intenciones y en nombre de la salud pública a propósito de la pandemia por Covid-19. También es su cometido analizar la existencia de posibles sesgos e identificar posibles discriminaciones por razón de los algoritmos para que no se perpetúen sesgos y se aumenten o generen nuevas desigualdades. Los sistemas de inteligencia artificial también debe ser objeto de análisis, considerando que las cajas negras de la inteligencia artificial plantean problemas sobre su inteligibilidad y que se debe exigir la intervención humana como última responsable de la tecnología. La inteligencia artificial tiene que ser una herramienta de apoyo.

En cuanto a la gestión del ciclo de vida de los datos se deben aplicar los principios conocidos como FAIR, por sus siglas en inglés. Así los datos deben estar disponibles y ser accesibles, interoperables y re-

69. Agencia Española de Protección de Datos, *Listado de tipos de tratamientos de datos que requieren evaluación del impacto relativa a la protección de datos*. Última consulta 30 de octubre de 2020, disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

utilizables. Al principio de calidad de los datos se suma la interoperabilidad para un uso adecuado de éstos que permita así su legibilidad e interpretación de forma estandarizada. Europa apuesta por un modelo de ciencia abierta que promueve poner a disposición los datos generados en investigación y que rompe también los tradicionales esquemas de generación de conocimiento propios del modelo analógico. Para reforzar esta tendencia es necesario que tanto la iniciativa pública como privada desarrolle políticas de acceso abierto a los datos con las debidas cautelas.

Se recomienda abandonar el concepto de anonimización para no generar falsas expectativas ni seguridades que dañan la confianza depositada por la sociedad en los procesos de creación y transferencia de conocimiento. En la era de la reidentificación es preciso establecer la seudonimización por defecto, y exigir que los responsables de los tratamientos demuestren desde el diseño de los proyectos en los que se usen tecnologías emergentes que no es posible la atribución de personalidad a los conjuntos de datos que se utilizan para el desarrollo de algoritmos.

La educación y alfabetización digital es necesaria desde la escuela, y también para los distintos operadores con capacidad para tomar decisiones. Es necesario evitar asimetrías entre los titulares y quienes tienen acceso a los datos personales. No es posible prescindir de estos conocimientos, de la formación sobre digitalización, porque de otra forma seremos más esclavos que libres y se tomarán decisiones por nosotros creyendo que somos nosotros los que las estamos tomando, aumentando desigualdades, pero de forma encubierta. En este sentido, y desde el ámbito de la salud, los comités de ética de la investigación deben promover la alfabetización digital tanto de sus miembros como de los investigadores cuyos proyectos evalúan.

En tiempos de pandemia no se pueden relajar los estándares de protección de los derechos de las personas, puede haber restricciones justificadas por el interés colectivo y la salud pública. Restricciones que deben estar justificadas, deben ser proporcionales a los fines que se persiguen y respetuosas con los derechos de los implicados. La pandemia por COVID-19 es la tormenta perfecta para crear mercados de datos personales disfrazados de investigación e innovación en salud a los que por razones de solidaridad o miedo es difícil renunciar. El proceso de digitalización en el que estamos inmersos necesita un análisis interdisciplinar y sólido que no separe los hechos y las cuestiones técnicas y científicas, de las implicaciones éticas, legales y sociales de la utilización de tecnologías emergentes. De otra forma, y desde las buenas intenciones se puede activar un confinamiento digital sin fecha de caducidad.

Bibliografía

Casado, M. (Coord.), *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico*, Editorial Fontamara, México, 2016. Reeditado por Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2018.

Casado, M., Patrão Neves, M., De Lecuona, I., Carvalho, A., Araújo, J., *Declaración sobre integridad científica en investigación e innovación responsable*, Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2016.

Casado, M., Puigdomènech,htto (Coords.) *Documento sobre los aspectos éticos del diálogo entre ciencia y sociedad*, Edicions

i Publicacions de la Universitat de Barcelona, Barcelona, 2018.

Casanovas, P. et al, *AI Approaches to the Complexity of Legal Systems. Complex Systems, the Semantic Web, Ontologies, Argumentation, and Dialogue*, volume 6237, Springer, 2010

Comisión Europea, *Communication on data-driven economy, COM(2014)442 final*

Comisión Europea, *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data,* Bruselas, 19 de febrero de 2020 COM(2020) 66 final

Comisión Europea, *Communication to the commission. European Commission digital strategy. A digitally transformed, user-focused and data-driven Commission*, Brussels, 21.11.2018 C(2018) 7118 final

Comisión Europea, Directorate-General for Research & Innovation H2020 Programme, *Guidelines on FAIR Data Management in Horizon 2020,* de 26 de julio de 2016

Comisión Europea, *Turning Fair into reality*, Bruselas, 2018

Comisión Europea, *White Paper on Artificial Intelligence - A European approach to excellence and trust* Bruselas, 19 de febrero de 2020, COM(2020) 65 final

Consejo de Europa*, Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes,* CETS No.203, Estrasburgo 11 de noviembre de 2008.

Consejo de Europa, *Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina)*, Oviedo, 4 de abril de 1997.

Consejo de Europa, *Convention for the protection of individuals with regard to the processing of personal data*, Estrasburgo, 1981

Consejo de Europa, *Guidelines on Artificial Intelligence and Data Protection,* Estrasburgo, 2019

Consejo de Europa, *Guidelines on Big Data adopted by the Consultative Committee of the Council of Europe´s data protection convention*

De Lecuona, I., "Evaluación de los aspectos metodológicos, éticos, legales y sociales de proyectos de investigación en salud con datos masivos (Big Data)", *Gaceta Sanitaria*, 2018, Vol. 32. Núm. 6, pp. 576-578. DOI: 10.1016/j.gaceta.2018.02.007

De Lecuona, I. (Coord.), *Pautas para evaluar proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales*, octubre 2020, Barcelona.

García Manrique, R. (Coord.), *El cuerpo diseminado. Estatuto, uso y disposición de los biomateriales humanos*, Editorial Aranzadi, Cizur Menor, 2018.

Grupo de Expertos de Alto Nivel Sobre Inteligencia Artificial, *Pautas para una Inteligencia Artificial confiable*, Bruselas, abril 2019

Llácer, M.R., Casado, M., Buisán, L., *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública,* Edicions i Publicacions de la Universitat de Barcelona, Barcelona, 2015.

López Baroni, M.J., *El origen de la bioética como problema*, Editorial de la Universitat de Barcelona, Barcelona, 2016

López Baroni, M.J., "Las narrativas de la inteligencia artificial." *Revista de Bioética y Derecho*, 2019, pp. 5-28.

Martínez Montauti, J. *La relación médico-paciente*. Edicions i publicacions de

la Universitat de Barcelona, Barcelona, 2018.

Mazzucato, M., *El estado emprendedor*. RBA Libros, Barcelona, 2014.

Morozov, E., *La locura del solucionismo tecnológico*. Katz-Clave intelectual, Madrid, 2015.

O'Neil, C., *Armas de destrucción matemática*. Capitán Swing Libros, Madrid, 2018.

Organización Mundial de la Salud, *Global Observatory for eHealth series*, vol.3, Suiza, 2011.

Pasquale, F., *The black box society: the secret algorithms that control money and information Cambridge*, Massachusetts; London, England: Harvard University Press, Boston, 2015.

Patino, B., *La civilización de la memoria de pez*. Alianza Editorial, Madrid, 2020 y ZUBOFF, S., *The age of surveillance capitalism.*, Public Affairs, Nueva York, 2019.

Pérez, G., "Peligros del uso de los big data en la investigación en salud pública y en epidemiología", *Gaceta Sanitaria*, vol. 30, núm. 1, pp. 66-68, DOI: 10.1016/j.gaceta.2015.09.007

Reglamento 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). R. (UE) 2016/679 (27 abril 2016)

Rodotà, S., *La vida y las reglas; Entre el derecho y el no derecho*, Editorial Trotta, Madrid, 2010

Sandel, M., *Lo que el dinero no puede comprar*, Editorial Debate, España, 2013

Sweeney, L., "Simple Demographics Often Identify People Uniquely". Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000.

Tutton, R., Prainsack, B. "Enterprising or altruistic selves? Making up research subjects in genetics research", *Sociology of Health & Illness,* 2011, Vol. 33, núm. 7, pp. 1081-1095. doi:10.1111/j.1467-9566.2011.01348.x

Véliz, C., *Privacy is Power*, Bantam Press, 2020.

Wajcman, J., *Esclavos del tiempo: Vidas aceleradas en la era del capitalismo digital*, Paidós, Barcelona, 2017.