Propuestas para adaptar el Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa al uso de tecnologías emergentes y a la explotación intensiva de datos personales en medicina y biología

Itziar de Lecuona
Universidad de Barcelona

1. La utilización de tecnologías emergentes y datos personales en el ámbito de la medicina y la biología[1]

La Unión Europea promueve una sociedad digital guiada por el dato para crear un mercado único digital competitivo que permita el liderazgo en el plano internacional (Comisión Europea, 2014). Buena parte de los procesos de investigación e innovación que tienen lugar en el ámbito de la medicina y la biología utilizan tecnologías emergentes y datos personales, entre los que destacan los datos de salud para mejorar la toma de decisiones. Esta es una decidida apuesta económica y científica que incluye la medicina personalizada, el desarrollo de sistemas sanitarios más eficientes o el envejecimiento activo y saludable,[2] y que permite poner de manifiesto que se trata de una decisión política que genera tensiones entre el interés colectivo e intereses personales entorno a los datos personales. Si bien sería inadecuado no aplicar las tecnologías emergentes y no utilizar datos personales en beneficio de las personas y de la sociedad, no puede afirmarse que los instrumentos internacionales de referencia en bioética, como es el caso del Convenio de Oviedo, recojan las disposiciones necesarias encaminadas a asegurar la protección de los derechos y libertades de sus ciudadanos, en particular la protección de la intimidad y la confidencialidad de los datos personales en contextos altamente digitalizados.

[1] Una versión anterior de este trabajo se ha publicado en la *Revista Internacional de Pensamiento Político*, núm. 15, 2020. Disponible en http://pensamientopolitico.org/presentacion.php.

[2] Programa Marco de Investigación Horizonte 2020. Disponible en https://ec.europa.eu/programmes/horizon2020/en.

Así, la aplicación de la analítica de datos masivos (*big data*), la inteligencia artificial, la biometría o el desarrollo de dispositivos de salud (apps incluidas) y la utilización de datos personales de forma casi rutinaria en los citados ámbitos obligan a revisar transversalmente el Convenio. Se trata de mejorar la toma de decisiones mediante el desarrollo de algoritmos[3] que permitan determinar conductas y predecir patrones de comportamiento. Para ello, se necesitan conjuntos de datos, entre ellos, datos personales, almacenados en buena parte en bases de datos como las que contienen historias clínicas informatizadas bajo criterios de calidad, seguridad y trazabilidad.[4] Así, el objetivo es combinar distintos conjuntos de datos procedentes de distintas bases de datos, entre las que se encuentran otros repositorios dedicados exclusivamente a investigación.[5] Junto con las historias clínicas informatizadas cabe 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, sea de forma voluntaria o involuntaria por parte de su titular.

Ejemplos de uso de tecnologías emergentes y de tratamiento de datos personales en los ámbitos de la medicina y la biología en procesos de creación y transferencia de conocimiento son: el desarrollo de sistemas de predicción y gestión de la pandemia de COVID-19 y las *hackatones,* o retos para desarrollar algoritmos, en las que participan terceros 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 que se lleva a cabo en la actualidad dista mucho de aquella para la que se establecieron pautas tras la Segunda Guerra Mundial,[6] fundamentalmente centrada en el desarrollo de medicamentos y productos sanitarios de uso humano. Hoy, la industria farmacéutica cierra acuerdos con empresas

[3] La Real Academia Española define «algoritmo» como un «Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema».

[4] Por ejemplo, la Historia Clínica compartida en Cataluña (HC3), disponible en https://salutweb.gencat.cat/ca/ambits_actuacio/linies_dactuacio/tecnologies_informacio_i_comunicacio/historia_clinica_compartida/, y el programa de historia clínica informatizada de Cataluña (eCAP), disponible en https://salutweb.gencat.cat/ca/ambits_actuacio/linies_dactuacio/tecnologies_informacio_i_comunicacio/ ecap/.

[5] Por ejemplo, el Sistema de Información para el desarrollo de la Investigación en Atención Primaria de Cataluña (SIDIAP), disponible en https://www.sidiap.org/index.php/es.

[6] Véase Asociación Médica Mundial y National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research.

dedicadas a la genética directa al consumidor[7] para acceder a bases de datos personales, que incluyen información genética y se han creado con fines comerciales para predecir el riesgo a padecer enfermedades de base genética, y que también pueden informar sobre los ancestros.[8] Asimismo, en el ámbito hospitalario se prueban y aplican sistemas de inteligencia artificial para analizar las historias clínicas y aprender de ellas 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 sus contactos como herramientas de apoyo en el marco de la salud pública, con no pocas dudas acerca de su fiabilidad y seguridad.[9] Estos dispositivos digitales de salud forman parte del llamado internet de las cosas y *mHealth*[10] en el ámbito de la salud, en el que distintos dispositivos que también incluyen vestibles o *wearables* permiten la conectividad entre sí y una monitorización constante. Los titulares de los datos personales que alimentan estos sistemas son a su vez destinatarios, en su mayoría, de los resultados de los procesos en los que se utilizan tecnologías emergentes.

No cabe duda de que los datos personales son el petróleo de nuestro tiempo y el interés por acceder a ellos y tratarlos es creciente, también porque permite 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 los datos que aporta sobre sus titulares, pero también por lo que puede predecir, si se destinan suficientes recursos humanos y materiales y se formulan las hipótesis adecuadas. Por ello, en el ámbito de la medicina y la biología es preciso evitar oportunistas que accedan a los datos personales con intereses espurios alejados del bien común o el interés colectivo que habilitaría tratarlos (De Leucona, 2016: 267-296). Es necesario evitar mer-

[7] 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. 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 (2008).

[8] «GlaxoSmithKline strikes $300 million deal with 23andMe for genetics-driven drug research». CNBC, 25/7/2018. Disponible en https://www.cnbc.com/2018/7/24/glaxosmithkline-23andme-team-up-on-genetics-driven-drug-research.html; véase también Tutton, R. y Prainsack, B. (2011).

[9] Manifiesto en favor de la transparencia en desarrollos de software públicos, septiembre 2020. Disponible en https://transparenciagov2020.github.io/.

[10] 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». Global Observatory for eHealth (2011). *mHealth / New horizons for health through mobile technologies*. Disponible en https://www.who.int/goe/publications/goe_mhealth_web.pdf.

cados de datos disfrazados de investigación e innovación en salud que aumenten las desigualdades existentes y la discriminación[11] y que permitan el lucro de terceros mediante la monetización de datos personales (De Lecuona, 2018: 576-578). Estos posibles mercados de datos personales vestidos de buenas intenciones, como puede ocurrir a propósito de la pandemia de COVID-19, deben identificarse 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.

El acceso a datos personales confiere un poder extraordinario a terceros, sea la iniciativa pública o privada, sobre los titulares de los mismos y puede dar lugar a usos no deseados y a discriminaciones, algunas de ellas encubiertas. Por otra parte, el «solucionismo tecnológico» (Morozov, 2015), que entiende la aplicación de la tecnología *per se* como la solución a los problemas y retos de nuestro tiempo, y el ajetreo que provoca la velocidad a la que se desarrolla la tecnología digital (Wajcman, 2017) banalizan el uso de datos 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 que hay que 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 pudiera tener para su titular y para las generaciones futuras. La utilización de información genética es un magnífico ejemplo. Conviene recordar que el sistema de investigación en nuestro contexto se asienta en los principios de solidaridad y altruismo. Así, las personas donan muestras biológicas y datos personales[12] para que el aumento de conocimiento y las intervenciones y tratamientos que se desarrollen reviertan en beneficio de la sociedad y de las generaciones futuras, entendiendo que no siempre obtendrán provecho de manera directa.

Además, 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. Y, así, hemos dejado de ser anónimos para ser reidentificables. Esta situación exigiría que se establecieran medidas técnicas y organizativas para que el uso de las tecnologías con determinados fines en el ámbito de la medicina y

[11] Casado, M. (coord.) (2016); García Manrique, R. (coord.) (2018).
[12] Véase, por ejemplo, la Ley 14/2007, de 3 de julio, de Investigación biomédica.

la biología no permitiera la reidentificación de las personas, es decir, la atribución de personalidad. Esta es una cuestión 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 (de Lecuona, 2018: 576-578).

En la mayoría de 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».[13] De otra forma, se genera una falsa seguridad asentada en una cláusula ya obsoleta como es la anonimización. Hoy la posibilidad de reidentificar a una persona con datos como el sexo, el código postal y la fecha de nacimiento es muy elevada (Sweeney, 2000); Pensemos también en los proyectos de historia clínica compartida o los programas de analítica de datos masivos en investigación y salud que han implementado algunos países basándose en sistemas de consentimiento presunto y por razones de solidaridad (de Lecuona y Villalobos-Quesada, 2018: 291-298). Si ampliamos el espectro más allá de la biomedicina, países como Estonia han convertido su Administración pública en digital.

El análisis de la aplicación de tecnologías emergentes y la utilización de datos personales en el ámbito de la medicina y la biología requiere considerar también el obstáculo que supone para la ciencia y para la toma de decisiones políticas no contar con bases de datos que permitan el acceso, la interoperabilidad y la reutilización de datos, incluidos los datos personales (Comisión Europea, 2016 y 2018). Los datos personales objeto de tratamiento deben ser fiables, de calidad, y almacenarse de formar segura, permitiendo su trazabilidad. Los datos personales, y en particular los datos de salud, no pueden estar al alcance de cualquiera. Por ello, no solo existen obligaciones jurídicas sino también éticas y deontológicas para garantizar la más elevada protección (Martínez Montauti, 2018).

La pandemia de COVID-19 ha puesto de manifiesto que Europa no tiene infraestructuras públicas suficientes que permitan un sistema de gestión de datos sólido y eficaz. Además, tanto los Estados miembros, como la Unión Europea dependen en exceso de las grandes tecnológicas fundamentalmente nor-

[13] Real Academia Española. *Diccionario panhispánico del español jurídico*. Disponible en dpej.rae.es.

teamericanas, centradas en extraer valor de los datos y no en crear valor (Mazzucato, 2014 y 2019). Estas empresas a las que recurre la iniciativa tanto pública como privada para la prestación de servicios tienen, como es lógico, objetivos distintos a la investigación e innovación en medicina y biología, e interés en acceder a los conjuntos de datos, especialmente los de carácter personal. Un interés que difiere del que pueda tener el profesional de la medicina o la biología en el contexto asistencial o investigador. El modelo de negocio de las *bigtech* se basa en el acceso a datos personales para su explotación y monetización. Hoy se cuestionan los perniciosos efectos que ha generado la economía de la atención promovida fundamentalmente por el imperio GAFAM (Google, Apple, Facebook, Amazon y Microsoft por sus siglas en inglés), que ha abierto un pujante mercado de servicios basado en el tratamiento intensivo de datos personales y del que somos dependientes, voluntaria e involuntariamente.[14]

Los softwares, las interfaces de programación de aplicaciones (API), las nubes y los servicios que se usan en el ámbito biomédico son en su mayoría propiedad de las *bigtech*. Así, es alarmante que no existan, por ejemplo, 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.[15] 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 los mismos por parte de sus titulares.[16] Y para ello, desde el plano internacional, es preciso contar con instrumentos jurídicos con vocación universal a fin de establecer los principios, derechos y garantías para la sociedad digital.

Asimismo, el avance del conocimiento en medicina y biología y su aplicación tienen lugar en ambientes de mucha competitividad, con equipos interdisciplinares, de distinta procedencia geográfica y culturalmente diversos, en los que «publicar o morir» y las reglas del mercado se imponen. Un ejemplo es la faceta emprendedora que se exige al académico-investigador para transferir al mercado los resultados de su investigación a fin de que sean valorizados a través de fondos de inversión o de capital-riesgo, entre otras fórmulas.

[14] Patino, B. (2020); Zuboff, S. (2019).

[15] Grupo de trabajo multidisciplinar COVID-19 del Ministerio de Ciencia e Innovación (2020).

[16] En el mes de febrero de 2020, justo antes de la pandemia de COVID-19, la Unión Europea presentó su estrategia de datos y el Libro Blanco sobre Inteligencia Artificial. Véase Comisión Europea (2020a) y (2020b).

Este requisito viene impuesto por las agencias de acreditación del sistema universitario y de investigación de los Estados, provocando muchas veces efectos no deseados en los procesos de creación de conocimiento científico (Casado *et al.,* 2016).

También 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 (Casado y Puigdomènech, 2018). En la aplicación de las tecnologías emergentes y el uso de datos personales, lo cual incluye el desarrollo de dispositivos de salud, predomina la opacidad propia de los negocios digitales (Pasquale, 2015). Situación que debe evitarse para transitar hacia un modelo que permita la gobernanza de los datos y el acceso a la información de forma transparente. El acceso abierto y la ciencia abierta (Leru, 2020) que Europa propugna deben ser uno de los pilares sobre los que se construya la sociedad digital y abren paso al análisis de nuevas fórmulas de gobernanza de datos que se asienten en los principios de transparencia y rendición de cuentas a lo largo de todo el proceso, desde el diseño hasta el acceso a los resultados.[17]

Un factor determinante es que, en el desarrollo y aplicación de las tecnologías, el riesgo cero no existe y que, como sociedad, debemos determinar el umbral de riesgo que estamos dispuestos a asumir. Si bien esta es una cuestión obvia, se torna compleja, puesto que, como es sabido, determinadas aplicaciones de la inteligencia artificial, por poner un ejemplo, generan cajas negras que no permiten su inteligibilidad. Estas plantean retos para la toma de decisiones sobre si aplicar aquella inteligencia o no y sobre 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.[18]

En definitiva, la explotación intensiva de datos personales obliga a repensar la forma en la que se investiga e innova en medicina y biología mediante el recurso a las tecnologías emergentes y el uso de datos personales. Conviene, entre otras cuestiones, revisar el modelo de información y consentimiento informado desarrollado durante la segunda mitad del siglo xx y explorar nuevas fórmulas de gobernanza de los datos personales que prioricen la transparencia y la rendición de cuentas. Los Estados deben promover las condiciones para asegurar que las personas toman decisiones libres e informadas, el control so-

[17] Observatorio de Bioética y Derecho. «Investigación e Innovación Responsable (RRI).» Disponible en http://www.bioeticayderecho.ub.edu/es/rri; de Lecuona, I. *et al.* (2017: 673-681).

[18] Barcelona Declaration for the Proper Development and Usage of Artificial Intelligence in Europe.

bre los datos personales y que los distintos agentes que intervienen en los tratamientos de datos personales hacen un uso adecuado de estos, así como impedir su monetización y prohibir la discriminación algorítmica, para evitar sesgos y no incrementar o generar desigualdades (O'Neil, 2018).

2. Aportaciones del Consejo de Europa sobre el tratamiento de datos personales para su protección ante el uso de tecnologías *big data* e inteligencia artificial

Es habitual caer en el error de que no existen referentes para tratar los retos que plantea toda nueva tecnología desde la perspectiva ética, legal y social. El Consejo de Europa ha efectuado aportaciones relativamente recientes y del todo relevantes a fin de dar respuesta a los dilemas y problemas antes descritos para la protección de datos personales en cuanto al tratamiento automatizado de datos y ante el uso del *big data* y la inteligencia artificial. El resultado es aplicable a otras tecnologías y permite encontrar los referentes en los que fundamentar la propuesta de cambio normativo del Convenio sobre Derechos Humanos y Biomedicina.

En primer lugar, se analiza el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 (Convenio 108) del Consejo de Europa (Consejo de Europa, 1981) y su proceso de modernización en 2018 (Convenio 108+).[19] Seguidamente, se estudian y sistematizan las aportaciones contenidas en las Pautas para la protección de las personas con respecto al tratamiento de datos personales en contextos *big data* (2017)[20] y las Pautas sobre inteligencia artificial y protección de datos (2019),[21] para llegar a conclusiones y propuestas.

[19] Consejo de Europa. Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data. 18/5/2018. Disponible en https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

[20] Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (2017).

[21] Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (2019).

2.1. El Convenio para la protección de las personas con respecto al tratamiento automatizado de carácter personal de 1981 (Convenio 108)

El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del Consejo de Europa, el Convenio 108, hecho en Estrasburgo y abierto a su firma el 28 de enero de 1981, fue el primer instrumento jurídico internacional con carácter vinculante para proteger a las personas de los potenciales abusos del uso de sus datos personales por razón de su tratamiento automatizado. Entró en vigor el 1 de octubre de 1985 con 5 ratificaciones.[22] El Convenio 108 establece garantías para la protección de los derechos y las libertades fundamentales, especialmente el derecho a la intimidad y a la vida privada, considerando que la libre circulación de información es necesaria en un contexto de desarrollo tecnológico en expansión. Sus bases jurídicas son el derecho a la protección de los datos de carácter personal del Tratado de Funcionamiento de la Unión Europea (artículo 16), [23] así como el respeto de la vida privada y familiar y la protección de datos de carácter personal reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea (artículos 7 y 8).[24] El derecho a la vida privada y familiar también está reconocido en el Convenio Europeo sobre Derechos Humanos (artículo 8),[25] que también debe considerarse un referente en la materia. El Convenio 108 incluye una serie de definiciones: «datos de carácter personal», esto es,

[22] Véase la lista de firmas y ratificaciones del Convenio 108. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=xxYaS9V7.

[23] Tratado de Funcionamiento de la Unión Europea. Artículo 16 (antiguo artículo 286 TCE): «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea».

[24] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 8: «Protección de datos de carácter personal: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

[25] Convenio Europeo sobre Derechos Humanos del Consejo de Europa, Roma, 1950.

cualquier información relativa a una persona física identificada o identificable; «fichero automatizado», entendido como cualquier conjunto de informaciones que sea objeto de un «tratamiento automatizado»,[26] y «autoridad controladora del fichero»[27] (artículo 2). El Convenio 108 se aplica a los ficheros y a los tratamientos automatizados de datos de carácter personal tanto en los sectores público como privado (artículo 3), si bien las Partes pueden establecer excepciones para determinadas categorías de ficheros automatizados de datos de carácter personal.

El Convenio 108 establece los principios para la protección de datos (capítulo II), instando a las Partes a tomar las medidas necesarias para que los hagan efectivos. Los principios, referidos a la calidad de los datos, son: que los datos de carácter personal que sean objeto de un tratamiento automatizado se obtengan leal y legítimamente; que se registren para finalidades determinadas y también legítimas y que no se puedan utilizar de una forma que sea incompatible con las finalidades establecidas; que sean exactos y se actualicen, cuando sea necesario. Y, finalmente, que se conserven de tal forma que sea posible identificar a las personas afectadas durante el plazo de tiempo que se considere necesario para llevar a cabo las finalidades que justifican su recogida y que sean adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado (artículo 5). A continuación, el Convenio establece como categorías especiales los datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas y otras convicciones, así como los datos de carácter personal sobre la salud, la vida sexual y las condenas penales. Estos datos no podrán tratarse de forma automatizada salvo que el Derecho interno establezca las necesarias garantías (artículo 6).

El principio de seguridad de los datos también se halla recogido en el capítulo dedicado a establecer los principios básicos para la protección de datos (artículo 7). Así, el Convenio 108 establece que se tomen las medidas de seguridad apropiadas para la protección de datos de carácter personal que estén registrados en ficheros automatizados para evitar la destrucción accidental o no autorizada, así como la pérdida accidental. También se refiere a medidas de

[26] «Por "tratamiento automatizado" se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones Lógicas aritméticas, su modificación, borrado, extracción o difusión.» Artículo 2c del Convenio 108.

[27] «Autoridad "controladora del fichero" significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.» Artículo 2d del Convenio 108.

seguridad para evitar el acceso, la modificación o la difusión no autorizada de datos personales. A continuación, el Convenio 108 introduce una serie de garantías para la persona afectada (artículo 8), que consisten, entre otras, en tener conocimiento del fichero automatizado de datos de carácter personal, así como de la finalidad para la que se crea y de los datos relativos a la autoridad que controla el fichero. Establece también la rectificación de los datos personales contenidos y su eliminación en determinados supuestos, además de la posibilidad de recurso en el caso de que no se haya satisfecho la pretensión del titular de los datos. El Convenio 108 introduce una serie de excepciones y restricciones (artículo 9), así como sanciones y recursos (artículo 10) y la posibilidad de que las Partes puedan conceder a las personas afectadas una protección más amplia que la prevista en el mismo (artículo 11). El Convenio se ocupa de los flujos transfronterizos de datos de carácter personal (capítulo III) y de las cuestiones que atañen al derecho interno de los Estados miembros (artículo 12), e incorpora una serie de preceptos dedicados a establecer las condiciones de ayuda mutua (capítulo IV) para la cooperación entre las Partes. Se establece también la composición y funciones del Comité Consultivo —y su procedimiento— (capítulo V). Se trata de un Comité formado por representantes de cada Parte (artículo 18) con la misión de presentar propuestas para facilitar o mejorar la aplicación del Convenio, proponer enmiendas, formular opiniones al respecto y, a petición de una Parte, expresar su opinión sobre las cuestiones relacionadas con la aplicación del Convenio (artículo 19). El funcionamiento del Comité Consultivo (artículo 20) también está previsto en el Convenio. Finalmente, está contemplada la propuesta de enmiendas (capítulo VI, artículo 21), seguida de las cláusulas finales (capítulo VII), como la entrada en vigor y la posibilidad de que Estados no miembros se adhieran, la cláusula territorial, la reserva, la denuncia y las notificaciones (artículos 22 a 27). Después de tres décadas en vigor, el Convenio 108 necesitaba adaptarse a las necesidades de la sociedad digital para asegurar la protección de los datos de carácter personal.

2.1.1. Proceso de modernización: Convenio 108+

En 2011, durante el 30.º aniversario del Convenio 108, el Secretario General del Consejo de Europa llevó a cabo un proceso de consulta a una diversidad de actores y grupos interesados, con el fin de identificar aquellas áreas que requerían una modernización para enfrentarse a los retos planteados por el desarrollo de las nuevas tecnologías y el tratamiento de datos personales. Entre 2013 y

2016, el Comité intergubernamental creado *ad hoc* para la protección de datos, revisó y examinó las propuestas surgidas, que fueron sucesivamente revisadas por el Comité de Ministros para adoptar, en 2018, el Protocolo que modifica el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.[28] Paralelamente, la Unión Europea redactó y aprobó el Reglamento General de Protección de Datos de 2016, aplicable desde mayo de 2018.[29] La actualización del Convenio 108 tenía que alinearse con esta propuesta para seguir siendo el referente en el plano internacional.

De las revisiones surgió el texto modernizado, el Convenio 108+, que se abrió a la firma el 10 de octubre de 2018 en Estrasburgo,[30] con los objetivos de hacer frente a los retos de las nuevas tecnologías y reforzar la aplicación efectiva del propio Convenio. El resultado fue que debía mantenerse el carácter general y neutro de las disposiciones con respecto a la tecnología; preservarse la coherencia y compatibilidad del Convenio con otros marcos jurídicos; y reafirmar su carácter abierto y con vocación universal.[31] En su Preámbulo, el Convenio 108+ hace constar la necesidad de proteger la autonomía de las personas a través del control de sus datos y de su tratamiento ante el uso intensivo de datos personales a escala global. El Convenio 108+ consolida los principios establecidos originariamente, reforzando algunos de ellos y añadiendo nuevas salvaguardias al derecho a la protección de datos de carácter personal en entornos informatizados y digitales. Una de las aportaciones principales es la introducción de principios que se habían desarrollado en el ámbito de la protección de datos durante el tiempo en el que el Convenio 108 había estado vigente y no habían formado parte del documento original, como los principios de transparencia, proporcionalidad, minimización de datos y privacidad desde el diseño.

En su nueva versión, el objeto del Convenio 108+ está claramente identificado en el capítulo I, que establece que la protección de las personas en cuanto al tratamiento de sus datos personales, independientemente de su nacionalidad o residencia, contribuye al respeto a sus derechos humanos y libertades fundamentales y, en particular, a su derecho a la intimidad (artículo 1). Las definiciones se han actualizado para ceñirse a los conceptos y terminología comúnmente utilizados en el ámbito de la protección de datos (artículo 2). Tras definir dato personal, el Convenio 108+ introduce el «tratamiento de datos», el cual «significa

[28] Consejo de Europa. «Background on Data Protection and Convention 108.»
[29] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
[30] El estado de firmas y ratificaciones se pueden consultar en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures.
[31] Consejo de Europa (2018).

cualquier operación o conjunto de operaciones llevadas a cabo sobre los datos personales, tales como su recopilación, almacenamiento, preservación, alteración, recuperación, divulgación, suministro, eliminación o destrucción, o llevar a cabo operaciones lógicas y/o aritméticas sobre dichos datos» (artículo 2b). Se definen también las categorías de responsable y encargado del tratamiento y de receptor. El Convenio 108+ se aplica al sector público y privado sujeto a la jurisdicción de las Partes, que deben asegurar la protección de los datos personales de sus titulares en estos ámbitos (artículo 3).

En cuanto a los deberes de las Partes (artículo 4) sobre los principios para la protección de datos personales, se reconoce la potestad evaluadora del Comité del Convenio sobre la eficacia de las medidas tomadas por los Estados para hacer efectivas las disposiciones del Convenio 108+. Se consolidan los principios de licitud del tratamiento y de calidad de los datos (artículo 5). El tratamiento de datos debe ser proporcional al objetivo que se persigue, debe ser legítimo y transparente, y debe reflejar, a lo largo de todas las etapas, un balance equitativo entre los intereses, tanto públicos como privados, y los derechos y libertades en juego. Asimismo, los datos personales deben ser adecuados, relevantes y no excesivos en relación con el objetivo para el que se procesan. Se hace referencia aquí al principio de minimización del dato. Además, deben ser exactos y, cuando sea necesario, deben actualizarse. Los datos personales deben preservarse de tal forma que sea posible la identificación de la persona titular de los datos personales durante un tiempo determinado, que no exceda al que sea necesario para alcanzar los objetivos establecidos para el tratamiento. Se introduce el enfoque de gestión de los riesgos que pueden surgir debido al tratamiento y afectar a los intereses, los derechos y libertades fundamentales del titular de los datos, haciendo especial referencia al riesgo de discriminación.

El tratamiento de datos debe efectuarse sobre la base del consentimiento libre, específico, inequívoco e informado de la persona afectada o estar justificado por una base legítima establecida por ley. No es posible que los datos personales sean procesados de tal forma que sean incompatibles con los fines que motivaron su tratamiento. En este punto, el Convenio 108+ se refiere a posibles tratamientos y archivo justificados por el interés público, con fines de investigación científica o histórica o propósitos estadísticos, que serían compatibles siempre que se establecieran las adecuadas salvaguardias (artículo 54.b).

El Convenio 108+ amplía el catálogo de datos personales considerados categorías especiales. Incluye el tratamiento de datos genéticos y biométricos que identifiquen de forma única a la persona, y de datos personales que revelen el origen étnico (artículo 6). Se consolida también el principio de seguridad de

los datos (artículo 7), en el que se establece que las Partes deben asegurar que el responsable y, en su caso, el encargado del tratamiento, toman las medidas de seguridad necesarias para evitar riesgos como aquellos debidos al acceso accidental o no autorizado, la destrucción, la pérdida, la modificación o la revelación de los datos personales. Es necesario, además, notificar sin dilación a las autoridades de supervisión competentes las brechas de seguridad que puedan afectar seriamente a los derechos humanos y libertades fundamentales de las personas.

El Convenio 108+ establece específicamente el principio de transparencia en el tratamiento de datos (artículo 8), referido a la información que el responsable del tratamiento de datos debe poner a disposición de los titulares de los datos: identidad y residencia habitual o establecimiento; la base legal y las razones para el tratamiento de datos; las categorías de datos personales procesados; los destinatarios de los datos personales; las condiciones para el ejercicio de los derechos al respecto y cualquier información adicional para asegurar que los datos personales son procesados de forma justa y transparente. A continuación, el Convenio establece los derechos de los titulares de los datos (artículo 9), ampliando de forma considerable aquellos establecidos originariamente como, por ejemplo, que las personas tienen derecho a no ser objeto de una decisión que pueda afectarles de forma significativa y esté basada únicamente en un tratamiento automatizado de datos sin que se haya tenido en cuenta su opinión (artículo 9.1.a). Ahora bien, este derecho no se aplicaría si la decisión está autorizada por una ley que el responsable del tratamiento debe acatar, la cual también establece las medidas necesarias para garantizar los derechos y libertades de la persona y su interés legítimo (artículo 9.2).

El titular de los datos también tiene derecho a obtener, previa solicitud, a intervalos razonables y sin demoras ni gastos excesivos, confirmación del tratamiento de los datos personales que le conciernen; tiene asimismo derecho a la comunicación en una forma inteligible de los datos tratados, de toda la información disponible sobre su origen, del período de conservación, así como de cualquier otra información que el responsable del tratamiento deba proporcionar para garantizar su transparencia.

Asimismo, el titular de los datos personales tiene derecho a obtener, previa solicitud, información sobre el razonamiento subyacente al tratamiento de datos cuando se le apliquen los resultados de este. También tiene derecho a oponerse en cualquier momento, por motivos relacionados con su situación, al tratamiento de datos personales que le conciernen a menos que el responsable del tratamiento demuestre motivos legítimos para este que sean superiores a sus intereses o derechos o libertades fundamentales.

El Convenio 108+ reconoce además el derecho del titular de los datos a obtener, previa solicitud, sin excesiva demora y de forma gratuita, la rectificación o borrado de los datos personales, si estos están siendo tratados o han sido recogidos contraviniendo las disposiciones establecidas. El titular de los datos puede recurrir en el caso de que los derechos reconocidos hayan sido objeto de violación, tal como establece el artículo 12. También puede solicitar, cualquiera que sea su nacionalidad o residencia, la ayuda de la autoridad supervisora correspondiente para el ejercicio de los derechos reconocidos en este Convenio.

El Convenio 108+ establece obligaciones adicionales (artículo 10) para que las Partes aseguren que el responsable del tratamiento y, en su caso también el encargado, llevan a cabo un análisis con carácter previo del posible impacto de los tratamientos de datos en los derechos y libertades fundamentales de sus titulares. Así, el tratamiento de datos debe diseñarse para minimizar el riesgo de afectación. Se deben implementar las medidas técnicas y organizativas que permitan el respeto del derecho a la protección de datos personales en todas las etapas del tratamiento. Este enfoque proactivo y de gestión de los riesgos que ya introdujo el Reglamento General de Protección de Datos se establece aquí con vocación universal. Asimismo, el Convenio 108+ reconoce en estas obligaciones adicionales los principios de privacidad desde el diseño y por defecto en el tratamiento de datos personales. Seguidamente, introduce una serie de excepciones y restricciones (artículo 11), así como sanciones y recursos (artículo 12), y establece que las previsiones incluidas en el mismo no deben entenderse como limitantes, sino que las Partes pueden garantizar una protección más amplia a los titulares de los datos (artículo 13). El capítulo III dispone los movimientos transfronterizos de datos personales entre miembros o terceros Estados, siempre y cuando se reúnan las garantías suficientes para la protección de los derechos de sus titulares. El Convenio 108+ establece también la potestad de supervisión de las autoridades correspondientes de los Estados parte para que se cumplan las previsiones establecidas (capítulo IV, artículo 15). No solo reconoce su capacidad para intervenir, investigar, detectar y denunciar las violaciones de la protección de los datos, sino también su responsabilidad en las tareas de concienciar, informar y educar a todos los actores involucrados en el tratamiento de datos personales. El Convenio 108+ se ocupa nuevamente de la cooperación y la asistencia mutua entre las Partes (capítulo V). Cabe destacar que el anterior Comité Consultivo se transforma en el Comité del Convenio (capítulo VI), que tiene funciones consultivas, pero también evaluadoras y de seguimiento con respecto al cumplimiento del Convenio 108+. Finalmente, este Convenio incluye disposiciones relativas a las enmiendas (capítulo VII) y una serie de cláusulas finales (capítulo VIII)

relacionadas, entre otras cuestiones, con su entrada en vigor. Se incluye un Apéndice al Protocolo con los elementos para las reglas de procedimiento del Comité del Convenio.

2.2. Pautas para la protección de las personas con respecto al tratamiento de datos personales en contextos «big data»

Las Pautas para la protección de las personas con respecto al tratamiento de datos personales en contextos *big data* fueron elaboradas por el Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y publicadas en enero de 2017. Como ya se ha descrito, el Convenio 108, redactado originalmente en 1981 con la finalidad de proteger a las personas del tratamiento automatizado de datos de carácter personal, estuvo en proceso de revisión y modernización en 2017 y se abrió a la firma en 2018. 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 las Partes pudieran desarrollar las políticas y medidas apropiadas para hacer efectivos los principios y las disposiciones del Convenio 108 en el contexto del *big data*.

El *big data* implica un cambio de paradigma y pone en entredicho los principios de protección de datos.[32] Si bien existen varias definiciones, hace referencia a que es tecnológicamente 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.[33] Esta tecnología serviría para mejorar la toma de decisiones. El *big data* incluye la analítica de datos masivos y puede aportar valor e innovación a la sociedad, así como mejorar la productividad y la actividad del sector público y la participación social. Así, el *big data* 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 las Partes, 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 se deriva del aná-

[32] En este sentido véase Llàcer, M.R. *et al.* (2015).
[33] Las Pautas definen *big data* en el apartado III sobre terminología.

lisis de los datos, a 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 impiden su participación efectiva. Las medidas recogidas en estas Pautas son de carácter general y pueden ampliarse para aplicarlas en campos específicos como, por ejemplo, la salud. Se trata de asegurar la protección de la autonomía de las personas mediante su derecho a controlar la información personal y el tratamiento de sus datos personales. Un derecho que debe analizarse 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 tratamiento 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 del tratamiento a analizar el impacto del tratamiento 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 y, con ello, cumplir las obligaciones establecidas en el Convenio 108. 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. Así, el Convenio sobre Derechos Humanos del Consejo de Europa debe ser el referente, entre otras disposiciones, en el que se recogen los valores éticos que guían la aplicación del *big data*.

Las Pautas recurren a la creación *ad hoc* o al recurso a comités de ética ya establecidos para que identifiquen aquellos valores éticos que deben preservarse, en el caso de que la evaluación del impacto de los tratamientos de datos personales en contextos *big data* detecte un riesgo elevado. Estos comités deben ser independientes y objetivos, y estar formados por personas aptas por su competencia, experiencia y cualificación profesional.

El siguiente principio se refiere al desarrollo de políticas de prevención y a las evaluaciones de los riesgos, las cuales se articulan a través de un enfoque precautorio para tratar la protección de datos personales y son tarea de los responsables de los tratamientos. Estas políticas están en consonancia con los principios de prevenir y minimizar los potenciales impactos del tratamiento de datos en los derechos fundamentales ya establecidos en el Convenio 108. La

evaluación de los riesgos debe realizarse 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 dimensiones legal, social, ética y técnica. También hay que 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 siguientes principios a los que las Pautas hacen referencia son la limitación del propósito y la transparencia. Los usos del tratamiento 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 los riesgos deben ser accesibles públicamente, con las pertinentes salvaguardias que disponga la ley.

El enfoque desde el diseño se despliega en las diferentes etapas del tratamiento de datos masivos con el objetivo de minimizar su uso, evitar sesgos ocultos y eliminar 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. Las Pautas señalan que los controladores y los encargados del 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 establecidos inicialmente y 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 tal 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 la citada reidentificación de las personas afectadas y los costes. El responsable del tratamiento debe demostrar la pertinencia de las medidas adoptadas y asegurar de forma efectiva la no atribución de personalidad a los titulares de los datos. Para prevenir posibles reidentificaciones es necesario aplicar medidas técnicas combinadas con obligaciones legales y con-

tractuales, 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 exponer las consecuencias que pudieran 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 que permitan presumir que ha habido discriminación directa o indirecta basada en el análisis de *big data*, los responsables y encargados del 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.

Las Pautas hacen hincapié en que la iniciativa pública y privada establezca 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 y explotar diferentes datos que provengan de distintos conjuntos de datos, de nuevo por el riesgo de reidentificación. Por último, la educación y alfabetización digital es necesaria para contribuir a que las personas puedan comprender adecuadamente las implicaciones de los usos del *big data*. La alfabetización digital debe considerarse una competencia esencial.

2.3. Pautas sobre Inteligencia Artificial y Protección de Datos

El desarrollo de la inteligencia artificial (IA) trae consigo nuevas oportunidades de creación y aplicación de soluciones para dar respuesta a las necesidades sociales, pero también comporta retos para la intimidad de las personas y la confidencialidad de los datos personales, que deben ser analizados por las instituciones y desde el marco que proporcionan los derechos reconocidos y la innovación responsable. Las Pautas sobre Inteligencia Artificial y Protección de Datos del Consejo de Europa también fueron elaboradas por el Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento de datos de carácter personal y se publicaron en enero de 2019. El

objetivo es proporcionar un conjunto de medidas que sirvan de referencia para ayudar a que gobiernos, desarrolladores, fabricantes y proveedores de servicios de IA se aseguren de que las aplicaciones de IA no socavan la dignidad y los derechos humanos, especialmente el derecho a la protección de datos personales. En el ámbito de la IA son aplicables las cuestiones ya tratadas por el Consejo de Europa en las Pautas antes descritas sobre protección de datos personales en contextos *big data*.

Las aplicaciones de la IA se refieren a sistemas basados en IA, 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 también se ha descrito más arriba. En las orientaciones generales de las Pautas se incide en que, ante las consecuencias que pueden tener las aplicaciones de IA, la protección de la dignidad humana y la salvaguardia de los derechos humanos y las libertades fundamentales deben preservarse ante el desarrollo de esta tecnología. Situación especialmente relevante en el caso de que la IA sirva como herramienta de apoyo para tomar decisiones. Así, este desarrollo debe estar alineado con el Convenio 108+ y fundamentarse en los principios de licitud, equidad, limitación del propósito, proporcionalidad del tratamiento de datos, 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 el campo de la IA, 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 IA deben permitir el control del tratamiento de datos por parte de los interesados.

En las orientaciones para desarrolladores, fabricantes y proveedores de servicios de IA, las Pautas vuelven a incidir en el deber de adoptar un enfoque orientado al respeto por los valores consensuados desde el diseño de los productos y las intervenciones, de manera que sean conformes al Convenio 108+ y los demás referentes e instrumentos jurídicos del 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 tiene que 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 IA deben evaluar la calidad, naturaleza, origen y volumen de los datos personales usados. Es necesario reducir la cantidad de datos tratados durante el proceso

de desarrollo, para eliminar aquellos que sean redundantes o se consideren marginales. Esta acción también se aplicaría a las etapas de entrenamiento de los sistemas y serviría para hacer el seguimiento con objeto de determinar la exactitud del modelo mientras es alimentado con nuevos datos. Para minimizar la cantidad de datos personales usados, se recomienda recurrir a datos sintéticos, esto es, aquellos generados por modelos de datos que se han creado a partir de datos reales.

La evaluación de las posibles consecuencias negativas de la IA en los derechos y libertades fundamentales recae en los citados actores, y se recomienda 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 también deben tenerse en cuenta en el desarrollo y uso de aplicaciones de IA.[34] Como ya se ha hecho antes en el contexto del *big data,* las Pautas sobre IA vuelven a incidir en la posibilidad de crear o consultar a comités de expertos independientes en distintos ámbitos, y animan a trabajar en colaboración con instituciones académicas independientes. Esta colaboración puede ayudar a contribuir a un diseño de IA que incorpore los valores éticos y sociales e identifique posibles sesgos. En cuanto a los citados comités, estos pueden desarrollar 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 de los riesgos 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 IA 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 en el usuario confianza en las aplicaciones de IA y, para ello, tanto los desarrolladores como los fabricantes y los proveedores de servicios deberían preservar la libertad de los destinatarios para decidir sobre el uso de estas aplicaciones, lo que requiere proporcionar alternativas a estas. Los desarrolladores, fabricantes y proveedores de servicios de IA deben adoptar formas de vigilancia algorítmica para promover la rendición de cuen-

[34] Posteriormente y en el ámbito de 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 incluyen una evaluación desde el enfoque de los valores y el respeto por los derechos humanos para el desarrollo de aplicaciones de IA. Disponible, en inglés, en https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

tas de todos los actores implicados a lo largo del ciclo de vida de estas aplicaciones, de tal forma que sea posible cumplir la normativa aplicable en materia de protección de datos y derechos humanos. Para cerrar el apartado dedicado a los desarrolladores, fabricantes y proveedores de servicios de IA, las Pautas incluyen una serie de directrices respecto a los derechos de los titulares de los datos; estos deben ser informados acerca de si interactúan con una aplicación de IA y obtener información sobre el razonamiento subyacente al tratamiento de datos de la IA que se les aplique y las consecuencias de la lógica aplicada. Las Pautas establecen que 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 establecidas en las Pautas sobre Inteligencia Artificial y Protección de Datos establecen que se puede mejorar la confianza en los productos y servicios de IA mediante el respeto del principio de rendición de cuentas, la adopción de procedimientos de evaluación de los riesgos y el desarrollo de códigos de conducta y mecanismos de certificación. Además, en los procesos de contratación pública para desarrolladores, fabricantes y proveedores de servicios de IA, 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 —esto es, vigilancia algorítmica— sobre los potenciales efectos adversos y las consecuencias de las aplicaciones de IA. 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 que supervisan la protección de datos y otros organismos que tengan competencias relacionadas con la IA (protección del consumidor, competencia, etc.). En esta ocasión, las Pautas refieren únicamente que los comités de expertos antes mencionados deben contar con los mecanismos necesarios para asegurar su independencia. Las personas, los grupos y otros interesados deben ser informados y participar activamente en el debate sobre el desarrollo y aplicación de la IA. Las Pautas se refieren de forma específica a que estos pueden contribuir a determinar el lugar que ocupa la IA en la dinámica social y en la toma de decisiones.

Es necesario que los legisladores y responsables políticos inviertan recursos en educación y alfabetización digital para que las personas puedan mejorar su comprensión de los efectos de las aplicaciones de IA. Además, los legisladores y responsables políticos deben fomentar la capacitación y formación de los

desarrolladores de IA para que estos también entiendan las implicaciones que tiene sobre individuos y sociedades. Es necesario apoyar la investigación sobre IA desde el enfoque de los derechos humanos.

3. Propuestas para la actualización del Convenio sobre Derechos Humanos y Biomedicina

Considerando la velocidad a la que se desarrollan las tecnologías emergentes y la utilización intensiva de datos personales, y teniendo en cuenta la tendencia a la mercantilización de la información personal y la posible discriminación algorítmica a la que podrían estar sujetos individuos y sociedades, es necesario revisar de forma transversal el Convenio sobre Derechos Humanos y Biomedicina del Consejo de Europa. Es urgente que este Convenio de 1997, concebido en las postrimerías de la sociedad analógica, se adapte a la sociedad digital «guiada por el dato» para garantizar la protección de las personas en los citados ámbitos. Las implicaciones que puede tener para la dignidad y los derechos y libertades en los ámbitos de la medicina y la biología se han puesto de manifiesto a lo largo de este capítulo, que también ha permitido identificar aquellos principios y requisitos que deberían incorporarse mediante el análisis de las recientes contribuciones del Consejo de Europa, entre los años 2016 y 2019. Se formulan las siguientes propuestas, debido a la naturaleza de los datos que se tratan en el ámbito de la medicina y la biología, como son los datos personales, y entre ellos, los datos de salud.

a) *Primacía del ser humano sobre la aplicación de las tecnologías emergentes.* El artículo 2 del Convenio sobre Derechos Humanos y Biomedicina establece la primacía del ser humano sobre los intereses de la sociedad o de la ciencia. Se propone añadir también «de la tecnología» ante la aplicación de tecnología como la analítica de datos masivos o la inteligencia artificial en el ámbito de la medicina y la biología. Los derechos e intereses en juego ya descritos justificarían la propuesta, especialmente por el carácter invasivo de las tecnologías emergentes.

b) *Derecho al control de los datos personales y de las actividades de tratamiento.* En los capítulos II y V del Convenio se establece el consentimiento libre e informado de la persona afectada en salud e investigación científica. Es en estos ámbitos donde se reconoce la autonomía de la persona para tomar decisiones, que ahora convendría actualizar, indicando que esta también incluye el dere-

cho al control de sus datos personales y de las actividades de tratamiento de estos. Esta cuestión entronca con el derecho a la vida privada y a la información reconocido en el capítulo III. El artículo 10.1 establece que «Toda persona tendrá derecho a que se respete su vida privada cuando se trate de informaciones relativas a su salud» y el artículo 10.2 dispone, por su parte, que «Toda persona tendrá derecho a conocer toda información obtenida respecto a su salud. No obstante, deberá respetarse la voluntad de una persona de no ser informada». Y a continuación, en el apartado 3, el Convenio establece las excepciones que puedan tener lugar de modo excepcional, por ley y en interés del paciente.

Parece necesario incorporar los principios de protección de datos personales y los derechos de las personas al respecto. Tal como se desprende del análisis efectuado, si el Convenio sobre Derechos Humanos y Biomedicina aspira a ser un referente internacional en los ámbitos de la medicina y la biología, no puede quedarse atrás y no incluir los siguientes principios en relación con el tratamiento de los datos: «licitud, lealtad y transparencia» en relación con el interesado; «limitación de la finalidad», que se refiere a que los datos deben ser recogidos con fines determinados, explícitos y legítimos; «minimización», que significa que los datos deben ser adecuados, pertinentes y limitados a aquello que es necesario en relación con las finalidades para las que se tratan; «exactitud», entendiendo que los datos serán exactos y, si fuera necesario, actualizados, y que se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan; «limitación del plazo de conservación» e «integridad y confidencialidad», que se refiere a que los datos sean tratados de forma segura. Por último, los principios de la protección de datos «desde el diseño» y «por defecto» para determinar las medidas técnicas y organizativas necesarias para asegurar el cumplimiento de los principios señalados.

c) *Derecho a no ser objeto de una decisión automatizada.* Se deberían incorporar específicamente los derechos reconocidos en el contexto europeo para la protección de los datos personales. En particular, el derecho a no ser objeto de una decisión automatizada, a que esta siempre esté supervisada por un humano en el ámbito de la medicina y la biología y a que pueda explicarse, esto es, que sea posible conocer el razonamiento que subyace a ella y que la persona afectada pueda rechazar su aplicación y contar con alternativas analógicas que permitan preservar su libertad para decidir entre las opciones existentes. Los derechos en materia de protección de datos incluyen, además del derecho a ser informado, el derecho de acceso, rectificación y oposición, el derecho al borrado o al olvi-

do, y el derecho a la portabilidad de los datos. El derecho a la revocación del consentimiento prestado cobra fuerza en el uso de tecnologías emergentes.

d) *Principio de precaución y evaluación de los riesgos de los tratamientos de datos personales.* El Convenio no contempla, al contrario que otros instrumentos normativos de carácter internacional, el principio de precaución ni tampoco incorpora la gestión de los riesgos, que ahora también se proyectarían sobre los datos personales. Como hemos visto, es necesario llevar a cabo evaluaciones del impacto de los tratamientos de datos en los derechos de las personas, incluyendo las generaciones futuras, para evitar usos no deseados y posibles efectos adversos en personas y grupos. Este enfoque proactivo y de gestión de los riesgos desde una perspectiva precautoria y orientada a la protección de los derechos de las personas implicadas debería incorporarse en el Convenio.

e) *Seudonimización de la información personal.* El Convenio sobre Derechos Humanos y Biomedicina debería incorporar la garantía de seudonimización de los datos personales, incluyendo su definición, para que los Estados introduzcan esta cláusula ante el problema de la posible reidentificación de las personas antes descrito y las consecuencias que comporta no garantizar la seudonimización para los derechos y libertades fundamentales. En la sociedad de la inteligencia artificial y los datos masivos, entre otras tecnologías emergentes, el anonimato no puede garantizarse.

f) *Prohibición de discriminación algorítmica.* De la misma forma que el Convenio de Oviedo establece la no discriminación (artículo 11), en el capítulo dedicado al genoma humano (capítulo IV), debería recoger también la no discriminación algorítmica debido a la aplicación de las tecnologías emergentes, como se ha puesto de manifiesto en las aplicaciones de IA antes descritas. La elaboración del Convenio de Oviedo estuvo marcada por la obsesión de proteger a las personas en una sociedad analógica que temía la discriminación genética, pero nada vaticinaba la discriminación algorítmica. Es el momento de establecer las condiciones para asegurar que, en el ámbito de la medicina y la biología, las decisiones que se tomen con el apoyo de las tecnologías emergentes sean siempre supervisadas por el humano. El objetivo es evitar sesgos de distinta naturaleza y no perpetuar desigualdades o fomentar la creación de nuevas condiciones que supongan una discriminación para las personas afectadas, incluyendo aquellas encubiertas. El Convenio de Oviedo también debería incorporar los principios de transparencia y rendición de cuentas. Los Estados deben establecer las condiciones para evitar la opacidad en los entornos digitales.

g) *Uso de muestras biológicas de origen humano.* En el ámbito de la medicina y la biología, la investigación con muestras biológicas de origen humano es crucial para aumentar el conocimiento generalizable y avanzar en el desarrollo de una medicina personalizada, regenerativa y traslacional. Las muestras se almacenan en repositorios públicos y privados bajo criterios de calidad, seguridad y trazabilidad. Estos son también una valiosa fuente de información que puede combinarse con otras bases datos que contengan información personal para extraer conclusiones y mejorar la toma de decisiones. El Convenio sobre Derechos Humanos y Biomedicina debería tratar esta cuestión en su articulado, dedicando un capítulo al uso de muestras biológicas de origen humano, o elaborar un Protocolo adicional específico. En los trabajos preparatorios del Convenio de Oviedo esta cuestión se dejó en manos de los Estados y no se consideró una prioridad en aquel momento (de Lecuona, 2011).

h) *Prohibición de lucro sobre los datos personales.* La prohibición de lucro sobre el cuerpo humano y sus partes que el Convenio establece en el artículo 21 debería extenderse también a los datos personales en el ámbito de la medicina y la biología, en el que la generación y aplicación de conocimiento depende de datos personales de calidad y con un alto grado de protección. Estos no deberían estar sometidos a las reglas del mercado precisamente porque forman parte de la intimidad de las personas. Los datos personales no deberían ser objeto de lucro y deberían considerarse un bien común que debe protegerse. La tendencia a la mercantilización del cuerpo humano y sus partes se ha puesto de manifiesto en el análisis efectuado y, por ello, es necesario actualizar las disposiciones del Convenio para que, desde la perspectiva internacional, sea posible articular un marco jurídico que permita evitar mercados de datos personales disfrazados de investigación e innovación en el ámbito de la medicina y la biología.

i) *Educación y alfabetización digital.* Si bien el Convenio de Oviedo establece que los Estados promuevan un debate social informado (artículo 28), también debería incluirse una disposición específica sobre el fomento de la educación y alfabetización digital. Estos deberían promover las condiciones necesarias para capacitar a las personas para tomar decisiones libres e informadas en los contextos descritos. En este sentido, las aportaciones del Consejo de Europa sobre inteligencia artificial y protección de datos son determinantes. Los Estados deberían invertir recursos en educación y alfabetización digital para que las personas puedan mejorar su comprensión sobre los efectos de las tecnologías en las personas, así como fomentar la capacitación y formación de los respon-

sables de su desarrollo para que entiendan las implicaciones que tienen sobre individuos, sociedades e incluso democracias.

4. Bibliografía y normativa

Asociación Médica Mundial. Declaración de Helsinki / Principios éticos para las investigaciones médicas en seres humanos. Adoptada por la 18.ª Asamblea Médica Mundial, Helsinki, Finlandia, junio 1964, y enmendada por la 29.ª Asamblea Médica Mundial, Tokio, Japón, octubre 1975; 35.ª Asamblea Médica Mundial, Venecia, Italia, octubre 1983; 41.ª Asamblea Médica Mundial, Hong Kong, septiembre 1989; 48.ª Asamblea General Somerset West, Sudáfrica, octubre 1996; 52.ª 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; 59.ª Asamblea General, Seúl, Corea, octubre 2008; 64.ª Asamblea General, Fortaleza, Brasil, octubre 2013. Disponible en https://www.wma.net/es/policies-post/declaracion-de-helsinki-de-la-amm-principios-eticos-para-las-investigaciones-medicas- en-seres-humanos/.

Barcelona Declaration for the Proper Development and Usage of Artificial Intelligence in Europe. Disponible en https://www.iiia.csic.es/barcelonadeclaration/.

Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01). Disponible en https://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Casado, M. (coord.) (2016). *De la solidaridad al mercado: el cuerpo humano ante el comercio biotecnológico.* México: Editorial Fontamara. Reeditado por Edicions de la Universitat de Barcelona en 2017. Disponible en http://diposit.ub.edu/dspace/bitstream/2445/116007/1/9788447541195.pdf.

Casado, M.; Patrão Neves, M.; de Lecuona, I.; Carvalho, A. y Araújo, J. (2016). *Declaración sobre integridad científica en investigación e innovación responsable.* Barcelona: Publicacions i Edicions de la Universitat de Barcelona. Disponible en http://www.bioeticayderecho.ub.edu/es/declaracion-sobre-integridad-cientifica-en-investigacion-e-innovacion-responsable.

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

Comisión Europea (2014). Communication on data-driven economy, COM(2014) 442 final. Disponible en https://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-442-EN-F1-1.Pdf.

— (2016). Directorate-General for Research & Innovation H2020 Programme: Guidelines on FAIR Data Management in Horizon 2020, 26/07/2016. Disponible en https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf.

— (2018). *Turning FAIR into reality.* Bruselas. Disponible en https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_0.pdf.
— (2020a). 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, COM(2020) 66 final. Bruselas, 19/2/2020. Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX:52020DC0066.
— (2020b). *White Paper on Artificial Intelligence – A European approach to excellence and trust,* COM(2020) 65 final. Bruselas, 19/2/2020. Disponible en https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.
Consejo de Europa (1981). Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, Consejo de Europa, hecho en Estrasburgo el 28 de enero de 1981. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12945.
— (2008). Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes (CETS núm. 203), hecho en Estrasburgo el 27 de noviembre de 2008. Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/203.
— «Background on Data Protection and Convention 108.» Disponible en https://www.coe.int/en/web/data-protection/background-modernisation.
— (2018). Convention 108+ Explanatory Report. Disponible en https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. Disponible en https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0.
— (2019) Guidelines on artificial intelligence and data protection. Disponible en https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8.
De Lecuona, I. (2011). *Los comités de ética como mecanismos de protección en investigación biomédica: Análisis del Régimen Jurídico Español.* Cizur Menor: Civitas.
— (2016). «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.), págs. 267-296.
— (2018). «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, págs. 576-578. DOI: 10.1016/j.gaceta.2018.02.007.
De Lecuona, I.; Casado, M.; Marfany, G.; Baroni, M.J. y Escarrabill, M. (2017). «Gene Editing in Humans: Towards a Global and Inclusive Debate for

Responsible Research.» *The Yale Journal of Biology and Medicine,* 90(4), págs. 673-681.

De Lecuona, I. y Villalobos-Quesada, M. (2018). «European perspectives on big data applied to health: The case of biobanks and human databases.» *Developing World Bioethics,* vol. 18, núm.3, págs. 291-298. DOI: 10.1111/dewb.12208.

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

Grupo de trabajo multidisciplinar COVID-19 del Ministerio de Ciencia e Innovación (2020). *Informe sobre datos e información en la epidemia COVID-19 y propuestas para la evolución digital del sistema de salud*, octubre 2020.

Harari, Y.N. (2019). «Los cerebros hackeados votan.» *El País*, 6 de enero de 2019. Disponible en https://elpais.com/internacional/2019/01/04/actualidad/1546602935_606381.html.

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. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-1999-20638.

Instrumento de Ratificación del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, hecho en Roma el 4 de noviembre de 1950, y enmendado por los Protocolos adicionales números 3 y 5, de 6 de mayo de 1963 y 20 de enero de 1966, respectivamente. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-1979-24010.

LERU (2020). «Towards a Research Integrity Culture at Universities: From Recommendations to Implementation.» enero 2020. Disponible en https://www.leru.org/files/Towards-a-Research-Integrity-Culture-at-Universities-full-paper.pdf.

Ley 14/2007, de 3 de julio, de Investigación biomédica. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2007-12945.

Llàcer, M.R., Casado, M. y Buisán, L. (2015). *Documento sobre bioética y Big Data de salud: explotación y comercialización de los datos de los usuarios de la sanidad pública.* Barcelona: Publicacions i Edicions de la Universitat de Barcelona. Disponible en http://www.bioeticayderecho.ub.edu/es/documento-sobre-bioetica-y-big-data-de-salud-explotacion-y-comercializacion-de-los-datos-de-los.

Martínez Montauti, J. (2018). *La relación médico-paciente*. Barcelona: Publicacions i Edicions de la Universitat de Barcelona.

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

— (2019). «Preventing Digital Feudalism.» *Social Europe*. Disponible en https://www.socialeurope.eu/preventing-digital-feudalism.

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

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,* EEUU, 1979.

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

Pasquale, F. (2015). *The black box society: the secret algorithms that control money and information.* Cambridge, Massachusetts; Londres, Inglaterra: Harvard University Press.

Patino, B. (2020). *La civilización de la memoria de pez*. Madrid: Alianza Editorial.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679.

Sweeney, L. (2000). «Simple Demographics Often Identify People Uniquely.» Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh. Disponible en https://dataprivacylab.org/projects/identifiability/paper1.pdf.

Tratado de Funcionamiento de la Unión Europea. Disponible en https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12016E/TXT.

Tutton, R. y Prainsack, B. (2011). «Enterprising or altruistic selves? Making up research subjects in genetics research.» *Sociology of Health & Illness*, vol. 33, núm. 7, págs. 1081-1095. Disponible en https://doi:10.1111/j.1467-9566.2011.01348.x.

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

Zuboff, S. (2019). *The age of surveillance capitalism*. Nueva York: PublicAffairs.