RIESGOS PARA LA PRIVACIDAD EN LA APLICACIÓN DE LA INTELIGENCIA ARTIFICIAL AL ÁMBITO BIOSANITARIO. IMPLICACIONES ÉTICAS Y LEGALES

Risks for Privacy in the Application of Artificial Intelligence to the Biosanitary Field. Ethical and Legal Implications *

F. Javier Blázquez Ruiz**

Anales de la Cátedra Francisco Suárez
Fecha de recepción: 30/06/2021
Fecha de aceptación: 01/10/2021
ISSN: 0008-7750, núm. 56 (2022), 245-268
http://dx.doi.org/10.30827/ACFS.v56i0.21677

RESUMEN Las posibilidades que ofrece el desarrollo de la inteligencia artificial y el manejo de macrodatos (*big data*) son ingentes. Sus aplicaciones se extienden también al ámbito sanitario en el que resulta difícil separar la práctica médica y el proceso creciente de digitalización. Sin embargo, no todo es luz en este nuevo universo algorítmico. Existe igualmente otro lado apenas perceptible, más opaco, pero impregnado de brumas provenientes de los intereses y expectativas de las grandes empresas multinacionales. De ahí la necesidad de incidir en la protección de los datos personales sanitarios, así como en la salvaguarda de la privacidad del paciente, teniendo presente que la defensa de los derechos fundamentales constituye un instrumento inequívoco de limitación del poder, en este caso, tecnocientífico.

Palabras clave: Inteligencia artificial, algoritmo, macrodatos, salud, bioética, derechos fundamentales, privacidad.

ABSTRACT The possibilities offered by the development of artificial intelligence and the management of macro data (big data) are enormous. Its applications also extended to the healthcare field where it is difficult to separate medical practice and the growing process of digitalization. However, not everything is light in the new algorithmic universe. There is also another barely perceptible side, opaquer, but impregnated with mists from the interests and expectations of large multinational companies. Hence the need to influence measures for the protection of personal health data, as well as the safeguarding of patient privacy, bearing in mind that the defense and protection of fundamental

* Para citar/citation: Blázquez Ruiz, F. J. (2022). Riesgos para la privacidad en la aplicación de la inteligencia artificial al ámbito biosanitario. Implicaciones éticas y legales. *Anales de la Cátedra Francisco Suárez*, 56, pp. 245-268.

** Departamento de Derecho. Facultad de Ciencias Jurídicas. Universidad Pública de Navarra. Campus Arrosadía, s/n. 31006 Pamplona, Navarra (España).
Email: *javier.blazquez@unavarra.es* Número ORCID ID: 0000-0002-4515-8624

rights constitutes at all times an unequivocal instrument of limitation of power, in this case, techno scientific.

Keywords: Artificial intelligence, algorithm, big data, healthcare, bioethics, fundamental rights, privacy.

1. Introducción

La IA se ha convertido en los últimos años en una prioridad estratégica para los países más desarrollados que tratan de convertirse en líderes mundiales respecto a la aplicación de los algoritmos de aprendizaje automático en diversos campos, entre ellos el sanitario. Sin embargo, es fácil constatar que mientras los sistemas de la IA siguen creciendo de manera exponencial, los planteamientos y propuestas reguladores se prodigan en menor medida tanto en el ámbito institucional, por parte de los diversos Estados o de la propia Unión Europea, como en el campo empresarial, especialmente.

En este contexto tecnocientífico omniabarcante de la IA, es preciso promover de forma simultánea una conciencia tecnológica permeable, basada en una teoría crítica de los derechos, que sea dúctil y que permanezca abierta ante los avances continuos aportados por la ciencia y la tecnología (Habermas, 2002). Esa reflexión ha de realizarse simultáneamente al proceso de desarrollo de los sistemas y aplicaciones de la IA. No *a posteriori,* con el fin de evitar incurrir en el problema que I. Kant ya advirtió en sus textos de filosofía de la historia cuando recordaba que los avances técnicos se anticiparon a las orientaciones morales sobre cómo utilizarlos; y evocaba a su vez de forma análoga, que la invención del puñal precedió a la conciencia del imperativo categórico ("no matarás") (Cortina, 2019, p. 379).

Hablamos de una conciencia que posibilite al mismo tiempo un debate interdisciplinar en torno a los principios que han de tenerse presentes para regular su uso (De Asís, 2014, p. 88). Un debate abierto y fecundo que no incurra en la tentación de escindir los aspectos técnicos y científicos, de las implicaciones éticas, legales y sociales que se derivan de la utilización de estas tecnologías emergentes (Lecuona, 2020, p.164).

Por otra parte, sería deseable que estas propuestas que van más allá de cuestiones puramente tecnológicas y métricas no quedasen reducidas después a una estrategia larvada de dilación, o al ejercicio de un "mero maquillaje". Resultaría estéril. Es sabido que algunas macroempresas han decidido crear comités éticos en sus organigramas corporativos, pero no resulta difícil constatar que esas iniciativas han surgido de forma reactiva, no proactiva. Se han constituido después de las críticas que han recibido reiteradamente, debido al uso inapropiado de la IA respecto a la privacidad de los usuarios y a la utilización de algunas aplicaciones sin supervisión.

De ahí la conveniencia de tener presente esa tendencia recurrente hacia una especie de *blanqueo ético,* que conlleve un supuesto interés por la ética. En realidad, se trataría de propuestas impostadas con el fin de evitar el cumplimiento de las normas institucionales. Con esa dinámica conseguirían aplicar una nueva forma de regulación que resultase menos restrictiva que las normas jurídicas. Sin embargo, el debate que propician sobre la ética de la IA, podría ocultar una resistencia reiterada a la regulación legal.

No es de extrañar que, para hacer frente a esa dinámica, hayan surgido propuestas de marcos éticos en el ámbito de la Unión Europea tales como el *Ethical Framework for a Good AI Society: Opportunities, Risks, Principles and Recomendations,* propuesto por el AI4People en diciembre de 2018*,* o las *Ethics Guidelines for Trustworthy AI del High-Level Expert Group on Artificial Intelligence,* elaboradas por la Comisión Europea en abril de 2019. Estos documentos defienden la conveniencia de configurar el marco ético de una IA confiable, alejada de la oscura opacidad, y que sea capaz de rendir cuentas ante los ciudadanos para evitar incurrir en sesgos o generar efectos imprevisibles (Cortina, 2019, p. 387). De hecho, tal y como expondremos más ampliamente, el principio de transparencia aporta un valor adicional de notable trascendencia, como es la posibilidad de seguir la trazabilidad, y fiscalizar el desarrollo y las aplicaciones de la IA (Castellanos, 2020, p. 144).

En este sentido*,* organismos internacionales como el Consejo Económico y Social han dejado constancia expresa en el dictamen de 2018 sobre inteligencia artificial, de que la repercusión que alcanzará la inclusión de la IA generará controversia y problemas de orden práctico, habida cuenta de su previsible trascendencia en el universo laboral (Goñi, 2019, p. 14). Lo mismo podría decirse de campos como el sanitario, cuya singular complejidad e incidencia en ámbitos diversos, entre ellos el económico, lo convierte en candidato idóneo para convertirse en objetivo destacado de la expansión progresiva de la IA y las crecientes posibilidades de computación.

Por todo ello, el objetivo principal del presente artículo no es otro que analizar las implicaciones éticas y jurídicas de la inteligencia artificial en un contexto específico preñado de grandes opciones como es el biosanitario. Para lo cual nos centraremos inicialmente en las ventajas y riesgos que conlleva el desarrollo de la IA en el terreno biomédico. Abordaremos después el impacto que provoca la IA en la esfera de los derechos fundamentales, incidiendo en las medidas de protección de los datos personales sanitarios, así como en la salvaguarda de la privacidad del paciente. Por último, concluiremos con unas reflexiones biojurídicas sobre el entorno sanitario del futuro próximo, teniendo presente que la defensa y protección de los

derechos humanos constituye un instrumento inequívoco de limitación del poder (De Asís, 2014, p. 88).

2. Aplicaciones biomédicas de la IA

2.1. Con el paso del tiempo, es posible que los sistemas de inteligencia artificial lleguen a provocar cambios tan amplios y profundos en la estructura de la sociedad, como en su momento los originaron históricamente la invención de la escritura, la irrupción de la máquina de vapor, o el descubrimiento de la telefonía, entre otros, con la consiguiente transformación cultural y social (Rodríguez, 2016, p. 9). Aunque en este caso, la metamorfosis que se produzca será más rápida y de carácter global, habida cuenta de la relevancia que puede alcanzar la evolución tecnológica y el uso progresivo de los algoritmos en aspectos cruciales de la vida de las personas (Tegmark, 2018, p. 139).

Entre los sectores afectados por el desarrollo de la IA cabe destacar por su trascendencia el sanitario, en el que están teniendo lugar alteraciones profundas en el proceso de diagnóstico, al tiempo que se incorporan instrumentos y prácticas innovadoras a partir del aumento exponencial de datos. Esta nueva dinámica comienza a poner en cuestión aspectos tan relevantes en la práctica médica como puedan ser las modalidades de cuidado tradicionales (Cárcar, 2020, p. 15), o las medidas terapéuticas más idóneas, tal y como sucede por ejemplo en el campo de la oncología, la diabetes, o a la hora de prever las resistencias bacterianas a determinados antibióticos. Todo lo cual permitirá especificar el tratamiento más adecuado para cada paciente, contribuyendo así a una progresiva personalización de la Medicina (Romeo, 2020, p. 10).

No cabe duda de que la transformación digital del universo sanitario alberga un gran potencial. Algunos grupos de investigadores tratan de desarrollar aplicaciones (Apps) que permitirán captar con la cámara del teléfono indicios de un posible cáncer de piel u otras enfermedades cutáneas. En el ámbito asistencial, la IA consigue perfilar los medicamentos o especificar las dosis correspondientes (Calvo, 2019, p. 162), y contribuye a mejorar la salud de los pacientes, así como a innovar en la gestión del centro sanitario. A su vez, la monitorización de pacientes en tiempo real a través de dispositivos electrónicos facilita a los equipos médicos la realización de diagnósticos con más rapidez y de forma más precisa (Fogel, *et al.,* 2018, p. 3).

Por tanto, los instrumentos y recursos que aporta la IA van a erigirse en herramientas eficaces de ayuda inestimable para el profesional de la medicina que le permitan agilizar y simplificar las tareas que realiza habi-

tualmente. De ese modo, no tendrá que dedicarse a las actividades más repetitivas y podrá liberar tiempo para llevar a cabo aquellas funciones en las que cada facultativo sea más apto y pueda aportar más valor.

De ahí la pertinencia de centrarnos a continuación en las aplicaciones biomédicas de la IA que tienen lugar en el campo sanitario, para examinar de cerca el contexto específico en el que se desenvuelven, así como adentrarnos en el marco jurídico en el que los profesionales sanitarios y los nuevos sistemas de IA llevan a cabo su labor. Solo así podremos aprehender y ser conscientes de la singularidad de estas tecnologías emergentes (Lecuona, 2020, p. 139).

Entre otras razones, porque es fácil constatar que los seres humanos no tenemos la capacidad necesaria de cómputo que permite al algoritmo procesar datos y aprender de ellos de forma inmediata. Por medio de estas herramientas innovadoras pueden obtenerse resultados óptimos a veces, pero no resulta fácil describir el proceso seguido con detalle. Y esa opacidad conlleva el riesgo de que después, el profesional de la salud no pueda validar o descartar la propuesta del sistema, porque desconoce el intrincado proceso a través de la cual se ha llegado a alcanzar dicho resultado (Romeo, 2020, p. 19).

No ha de extrañar que este principio de transparencia, *explainability,* se haya convertido en uno de los requisitos que debe requerirse a cualquier empresa u organización vinculada a la IA. El motivo es debido a que en los procesos seguidos por los algoritmos en el *Deep learning* o aprendizaje profundo, no queda clara la inclusión y relación entre los *inputs* y los *outputs*. De ahí que el concurso de esa larvada opacidad sea calificado, después, como "caja negra" (black box) debido a que los algoritmos creados por el aprendizaje profundo se tornan inextricables incluso para el propio programador (Capdeferro, 2020, p. 10). Y es que los algoritmos diseñados inicialmente van generando otros nuevos, cuyo grado de complejidad resulta cada vez mayor, hasta el extremo de que su comprensión deviene inaprehensible. A consecuencia de lo cual el derecho a la reversibilidad se convierte en una especie de quimera (López Baroni, 2021, p. 31).

En realidad, los efectos provocados por esa "caja negra" provocan escenarios en los que, a partir de un momento determinado, los programadores no son capaces de realizar una predeterminación fiable respecto a los resultados que habían previsto. Lo cual equivale a confiar de forma prácticamente ciega en el procesamiento de datos y en su combinación, otorgando un crédito desmesurado al supuesto de que la programación se haya realizado de forma correcta, aunque se torne ininteligible (Boix Palop, 2020, p. 231).

En este contexto de imprevisibilidad, el grado de incertidumbre e inseguridad se acrecienta cada vez más con las implicaciones negativas

subsiguientes desde la vertiente jurídica, asentada tradicionalmente en paradigmas de predeterminación normativa. De ahí que la necesidad de contar con mecanismos de control irrumpa como una de las reivindicaciones más demandadas (Boix Palop, 2020, p. 231). Ya que uno de los mayores retos de la sociedad digital va a ser examinar el uso secundario que pueda realizarse de la información proveniente de los datos personales. Hablamos de usos indirectos no deseados, que puedan provocar un trato discriminatorio (Lecuona, 2020, p. 142).

2.2. Podría decirse que la diferencia fundamental entre la tecnología basada en la IA respecto a la utilizada por las tecnologías tradicionales en el campo de la salud radica en la celeridad y eficiencia a la hora de obtener información, procesarla y ofrecer a continuación un diagnóstico o unas medidas terapéuticas precisas.

Históricamente, los datos médicos podían presentarse a veces de forma fraccionada, descoordinada o incluso, en algunas ocasiones, incompleta. Sin embargo, a través del reconocimiento óptico de caracteres (OCR), el dictado y el escaneo automatizado basado en el procesamiento del lenguaje natural, facilitan que la IA logre unificar bases de datos —también las que contienen datos no estructurados, como las notas clínicas— y los ponga a continuación a disposición de los profesionales de la medicina.

Ahora bien, para reducir el margen de error posible, los algoritmos de aprendizaje automático, basados en IA, capaces de reconocer patrones de comportamiento, necesitarían someterse a evaluaciones y revisiones continuas (Cárcar, 2020, p. 21). Ya que la transformación digital del ámbito sanitario está posibilitando que buena parte de las decisiones relacionadas con los procesos asistenciales se dejen en manos de los algoritmos debido a su amplia capacidad de análisis, interacción y predictibilidad que los caracteriza (Calvo, 2019, p. 155).

No cabe duda de que la utilización de la IA en el campo de la atención sanitaria puede aportar beneficios tanto a los médicos e investigadores biosanitarios como a los propios pacientes, sin olvidar el entramado administrativo de los centros hospitalarios. Así, respecto a la gestión de los recursos sanitarios y su traducción en términos económicos el informe Korster y Seider reveló en 2010 que solo en Estados Unidos el coste derivado de la falta de eficiencia en el ámbito sanitario ascendía a 2,5 trillones de dólares. Ese informe advertía al mismo tiempo que, si se hubiese realizado una adecuada digitalización del sector, ese gasto innecesario habría podido reducirse hasta alcanzar un 35% (Calvo, 2019, p. 156).

Desde hace tiempo, en el ámbito hospitalario se prueban sistemas de inteligencia artificial con el objetivo de analizar las historias clínicas

informatizadas para mejorar los procesos asistenciales. A su vez, está produciéndose un auge en el desarrollo de Apps de salud –aplicaciones basadas en programas diseñados con el fin de realizar funciones específicas– para evaluar síntomas de los enfermos o bien para identificar posibles casos positivos infectados por COVID-19, así como rastrear a sus eventuales contactos. Se trata de herramientas de apoyo a la asistencia sanitaria cotidiana, aunque su aplicación no está exenta de dudas razonables respecto al grado de fiabilidad y seguridad que ofrecen (Lecuona, 2020, p. 142).

Estos dispositivos digitales de salud se integran en el internet de las cosas y en *mHealth,* y están cada vez más presentes en la práctica médica a través de dispositivos como teléfonos móviles, o bien dispositivos de vigilancia de pacientes. También cabe mencionar los asistentes digitales personales (PDA) y otros dispositivos de uso inalámbrico (Arigo, et al., 2019). Todos ellos permiten la conectividad entre sí y una permanente monitorización de los pacientes, pero deben ser probados en entornos en los que participen personas ajenas a la empresa que los haya creado, para que sean validadas antes de su utilización de forma generalizada y puedan obtener la certificación correspondiente (Lecuona, 2020, p. 143).

Sin embargo, aunque la IA vaya a generar un impacto relevante en la práctica médica, a la hora de mejorar, por ejemplo, la interpretación de imágenes diagnósticas como las radiografías, conviene precisar que existe una diferencia ostensible entre la actividad de utilizar sistemas inteligentes eficientes en el proceso de toma de decisiones y, por otra parte, dejar en manos de los algoritmos y procesos informáticos las determinaciones significativas, relacionadas con la vida y el tratamiento de la salud (Cortina, 2019, p. 381). Es evidente que las máquinas no pueden reemplazar al ser humano en una relación asistencial que incluye necesariamente, más allá de datos, gráficos y análisis, tanto la autonomía del paciente, como la competencia profesional y el principio de responsabilidad médica (Romeo, 2020, p. 18).

Eso no obsta para que, en estos nuevos escenarios, sea cada vez más necesaria una formación específica y permanente por parte de los sanitarios en sus respectivas especialidades. De hecho, los galenos tendrán que conocer tanto las posibilidades como las limitaciones de la aplicación de estas técnicas en sus respectivas áreas. Actualmente no abundan profesionales sanitarios que estén capacitados para examinar los pormenores que caracterizan el proceso algorítmico.

Sin embargo, dada la responsabilidad del clínico a la hora de explicar al paciente las decisiones adoptadas con estos sistemas, no solo es pertinente formar a los profesionales sanitarios en esta tecnología innovadora, sino que, además de tener en cuenta el principio de transparencia en la interac-

ción con el paciente, será necesario también incorporar consentimientos informados específicos (Romeo, 2020, p. 19).

Por otra parte, será preciso que los facultativos dispongan de formación y competencias adecuadas en el campo de la IA que les habilite para poder evaluar estas herramientas adaptadas a las diversas especialidades médicas. Formación a la que no deberían permanecer ajenos los miembros de los Comités de ética asistencial y clínica, CEA, así como los integrantes de los Comités de investigación, CEI, habida cuenta de su responsabilidad a la hora de evaluar proyectos.

Los CEA, además de responder a los casos clínicos a partir del proceso de deliberación apoyado en los principios de la bioética, incluyen entre sus funciones la de contribuir activamente a la formación continua del personal sanitario del centro. A su vez, los Comités de ética de la investigación tienen que promover la alfabetización digital de los miembros que lo integran, así como sensibilizar respecto a la necesidad de la protección de datos en la investigación sanitaria. Por otra parte, tanto los CEA como los CEI pueden contribuir a un debate abierto e interdisciplinar que advierta al personal sanitario de los respectivos centros sobre los riesgos de la combinación masiva de datos por medio de algoritmos, y promueva una cultura de respeto a la privacidad (Lecuona, 2018, p. 578).

Y es que, si bien la práctica médica es una actividad profesional basada en el manejo constante de información fluida y compartida, a partir de ahora será preciso diseñar procedimientos técnicos y algoritmos que permitan anonimizar los datos recabados de los pacientes. Y habrá que hacerlo con las garantías suficientes para evitar que el derecho a la privacidad de los usuarios pueda verse vulnerado.

2.3. Conviene advertir que el proceso de anonimización que se venía aplicando ha mostrado sus limitaciones. Este recurso se presentaba antes como la opción más idónea para procesar los datos con el fin de proteger la privacidad de los pacientes. Sin embargo, en los últimos años han tenido lugar casos de reidentificación de bases de datos que habían sido anonimizadas con anterioridad. Y es que, a pesar de que la anonimización implica desvincular la información respecto al titular de esos datos, el proceso de reidentificación de sujetos es —técnicamente— cada vez más sencillo de lograr (Gil, 2011, p. 126).

Se da la circunstancia de que en el universo de los *big data*, debido al cúmulo de información personal almacenada, junto con la capacidad de combinación que ofrecen las innovaciones técnicas, el análisis de esa ingente cantidad de información puede facilitar la identificación de pacientes que antes permanecían anónimos. De hecho, no deberían considerarse

válidos buena parte de los procesos de información y consentimiento informado basados en esta garantía de anonimización. De otro modo, se incurriría en el riesgo de propiciar una falsa seguridad (Lecuona, 2020, p. 144).

Y es que la posibilidad de reconocer sujetos a partir de datos de carácter personal como pueda ser el código postal, la fecha de nacimiento y el sexo respectivo, es muy alta. De ahí la necesidad de establecer medidas técnicas y organizativas con el fin de que el uso de las tecnologías con determinados fines en salud no permita la reidentificación de las personas (Lecuona, 2020, p. 143).

En este sentido, algunos autores defienden que es posible que la protección y la privacidad subsiguiente no sea fácil de alcanzar, con el desarrollo creciente de la IA y el uso masivo de *big data*. Por su parte, la European Union Agency for Network and Information Security se planteaba que la pretensión de aunar privacidad y *big data* al mismo tiempo, tal vez pueda considerarse un oxímoron (ENISA, 2015, p. 18). Es evidente que existen muchos intereses y expectativas en juego, por lo que será preciso reconfigurar el equilibrio necesario entre los riesgos y beneficios que puede conllevar el tratamiento de datos a través de la IA. El riesgo principal radica en que en muchos casos estos usos secundarios no se conocen realmente (Gil, 2011, p. 127).

A los CEI les compete comprobar que quienes intervienen en el procesamiento de datos personales realizan en sus proyectos un uso adecuado de los mismos, que posibilita la protección de las personas que participan en la investigación. También debe velar para evitar sesgos y eventuales discriminaciones generados por los algoritmos que puedan provocar desigualdades sociales (Lecuona, 2020, p. 163).

Respecto a la implicación de los pacientes, el consentimiento informado –principal exponente del principio bioético de autonomía– debería ser específico, *ad hoc,* ya que un consentimiento indiscriminado, sin especificar la finalidad del tratamiento, no debería admitirse. El CI, además de ser comprensible, ha de referirse con claridad al alcance y consecuencias derivadas del tratamiento de datos. De otro modo, el consentimiento se convertiría en una especie de "carta blanca" que conllevaría el descontrol del flujo de los datos personales. Lo cual equivaldría a evidenciar la inoperancia del sistema de protección de la privacidad, supuestamente habilitado a tal efecto (Cotino, 2017, p. 145).

En realidad, el CI, tal y como lo conocemos actualmente, no es suficiente para garantizar el adecuado tratamiento de los datos personales que facilita el paciente. Es necesario exigir que se cumplan los principios de transparencia y rendición de cuentas (Felzmann, et al., 2020, p. 3358), tanto en los procesos de generación como respecto a la transferencia de cono-

cimiento en el ámbito sanitario para evitar el riego de que se produzcan asimetrías (Lecuona, 2020, p. 162).

Y es que, el carácter específico del CI implica también que, si la finalidad para el que los datos han sido recabados inicialmente se modifica, entonces el paciente ha de ser informado y habrá que elaborar un nuevo CI, ya que cuando el complejo proceso de *big data* interviene es necesario que el CI se aplique en un contexto restringido. El motivo principal es debido a que el valor de los macrodatos radica también en la nueva información que se deriva a partir del análisis de los datos iniciales, dado que permite dar nuevos usos a esos datos recabados, con el riesgo subsiguiente para la privacidad del paciente. Y es ahí, justamente en este uso secundario donde reside el potencial inherente a los *big data* (Gil, 2011, p. 61).

Por otra parte, sería conveniente –adicionalmente– redactar documentos oficiales susceptibles de trasladar la normativa legal al campo determinado de trabajo por medio de protocolos de actuación, guías prácticas o materiales diversos. Estos materiales creados *ad hoc* permitirían a los sanitarios actuar con plenas garantías jurídicas tanto respecto al desempeño de su ejercicio profesional, como en todo lo concerniente a la protección de los derechos de los pacientes (Romeo, 2020, p. 21).

A su vez, la coordinación entre los diversos agentes que intervienen en el proceso de obtención de datos deviene igualmente clave, ya que el impacto que puede provocar un algoritmo en la asistencia sanitaria guarda estrecha relación con el grado de interacción entre quienes participan en todo el proceso, tanto en la vertiente de producción y procesamiento de datos, como en el diseño previo de ese algoritmo y en la determinación de patrones (Cárcar, 2020, p. 19).

No cabe duda de que la incorporación de los sistemas de la IA a las guías clínicas tras el consenso de las sociedades científicas y el apoyo de las Administraciones públicas, puede contribuir a mejorar la calidad de la asistencia sanitaria, aunque habrá que tener presente su carácter orientativo, pero no necesariamente vinculante. Ya que la autonomía del médico a la hora de tomar decisiones debe quedar garantizada en todo momento y, por tanto, ha de ser respetada igualmente cuando estime que el proceso de aplicación de la IA no es pertinente para la salud del paciente (Sánchez Caro, 2021, p. 11).

3. Impacto de la IA en el ejercicio de los derechos fundamentales. Protección de los datos personales sanitarios y salvaguarda de la privacidad de los pacientes

3.1. La medicina del futuro, la denominada Medicina P4 (preventiva, participativa, personalizada y predictiva), va a seguir desarrollándose a

través de la aplicación de la IA, el aprendizaje automático y el *big data*. Lo cual va a posibilitar que el sistema de salud llegue a ser cada vez más eficiente a la vez que personalizado (Alonso, 2021, p. 19), pero será necesario consensuar a su vez un marco axiológico preciso. Un marco regulador que oriente y guíe el proceso de digitalización, teniendo en cuenta, no solo el procesamiento de datos y sus respectivas aplicaciones biomédicas, sino también las legítimas expectativas de los pacientes eventualmente afectados.

Hablamos de un desarrollo de la IA y de una implementación de la Bioética de las Cosas (Bioethics of Things) en el proceso de clarificar, justificar y orientar el desarrollo de los entornos hospitalarios y asistenciales. Proceso que, además de estar basado en la hiperconectividad, datificación y algoritmización (Calvo, 2019, p. 162) no excluya otros principios inexcusables como son la responsabilidad, trasparencia, y predictibilidad, así como una tendencia a no provocar la aparición eventual de "víctimas inocentes" (Bostrom y Yudkowsky, 2014, p. 318).

Si analizamos las implicaciones de la IA desde las coordenadas de los derechos fundamentales, uno de los debates actuales sobre la relación entre sistemas democráticos e inteligencia artificial gira en torno a cómo han de abordar los Gobiernos y el derecho internacional esa nueva realidad tecnológica a la hora de establecer límites, con el fin de afrontar las consecuencias que comporta el desarrollo y aplicación de esta tecnología innovadora.

Conviene recordar que el propio A. Einstein precisaba con lucidez hace varias décadas que la investigación científica es necesaria, pero no suficiente, porque "la inteligencia tiene un ojo agudo para los métodos e instrumentos, pero es ciega para los fines y valores" (Einstein, 2007). Del mismo modo, H. Kelsen defendía esa misma línea de argumentación en su célebre artículo "Science and Politics" cuando indicaba que la ciencia puede determinar los medios, pero no precisar los fines (Kelsen, 1951).

De ahí la conveniencia de analizar las implicaciones éticas, legales y sociales (ELSI) de la IA simultáneamente, tal y como sucedió hace tres décadas mientras se desarrollaba el Proyecto Genoma Humano, habida cuenta de su trascendencia en la medicina predictiva. Hablamos del derecho a la privacidad, protección de datos, seguridad personal, igualdad de acceso, inclusión, o no discriminación, entre otros, que encontramos positivados en la mayor parte de las constituciones de los Estados democráticos.

En este sentido, la Comisión Europea presentó el 19 de febrero de 2020 un *Libro blanco* en torno al desarrollo de una inteligencia artificial fiable, que establece las bases jurídicas para su inminente regulación en el ámbito de la Unión. Su objetivo principal es movilizar recursos y promover los incentivos apropiados que permitan acelerar la implantación de la IA en diversos estamentos, incluidas las pequeñas y medianas empresas, así como

las diversas Administraciones Públicas. Para lo cual considera imprescindible la colaboración eficaz entre los Estados miembros y la comunidad investigadora. Adopta, a su vez, un enfoque basado en la inversión económica, así como en la regulación jurídica con el objetivo de promover la implantación progresiva de la IA, pero sin obviar los riesgos que se derivan del uso de esta tecnología innovadora (Barrio, 2021, p. 272).

Este *Libro blanco* de la UE propone que las aplicaciones de la inteligencia artificial en campos de riesgo elevado, como la salud, administración de justicia o actividades policiales, deben ser en todo momento transparentes, susceptibles de comprobar su trazabilidad y han de garantizar al mismo tiempo la realización de una verificación no técnica sino humana.

En particular, las autoridades públicas deben poder comprobar y certificar los datos que han sido utilizados por los algoritmos, tal y como sucede hoy en día en el sector de los automóviles. Además, el documento insiste en la necesidad de poder contar con datos no sesgados para que los sistemas que dispongan de un nivel elevado de riesgos sean desarrollados de tal forma que su funcionamiento garantice "el respeto de los derechos fundamentales, en particular la no discriminación" (COMISIÓN EUROPEA, 2020).

Con antelación, el Parlamento Europeo ya había advertido igualmente sobre la posibilidad de encontrarnos con "algoritmos sesgados, correlaciones falsas, errores" así como ante el riesgo de subestimar los efectos de sus aplicaciones, lo cual podía abocar a la utilización de "datos con fines discriminatorios o fraudulentos y la marginación del papel de los seres humanos en esos procesos" (Parlamento Europeo, 2017), porque el *big data* y los algoritmos pueden reflejar prejuicios y reproducir patrones de exclusión como correlato de las decisiones que han sido tomadas a la hora de seleccionar la información correspondiente.

Es fácil constatar que millones de personas en todo el mundo permanecen actualmente en la periferia de *big data*. Su información no es recopilada ni analizada porque no participan en aquellas actividades para las que el *big data* está diseñado. De ahí que tanto sus preferencias como necesidades cotidianas corran el riesgo de continuar al margen o ser ignoradas cuando los gobiernos y las empresas privadas utilizan datos masivos y los correspondientes análisis para configurar las políticas públicas y decidir respecto a los intereses del mercado (Cotino, 2017, p. 13).

En este sentido, es bien sabido que la aplicación de los sistemas algorítmicos viene planteando continuamente cuestiones polémicas relacionadas con la parcialidad y la discriminación en las decisiones que adoptan. Ante lo cual, diversas investigaciones han intentado modificar y mejorar los estándares de dichos sistemas (Brundage y Avin, 2018, pp. 85-86). Sin

embargo, el proceso seguido no siempre ha tenido presentes las cuestiones jurídicas o los procedimientos públicos en el proceso de toma de decisiones. Como resultado de esa actuación, los dispositivos métricos habilitados no se ajustan en todo momento a los ordenamientos jurídicos vigentes.

Es evidente que las garantías constitucionales que hacen posible una protección efectiva de la privacidad no son eficaces si no cuentan con procedimientos habilitados de rendición de cuentas que puedan aplicarse a quienes abusan con el manejo de datos y procesan información personal obtenida de forma ilícita (Moreno, 2017, p. 17). No podemos obviar que los investigadores, además de procesar, también interpretan los datos al seleccionarlos, y es frecuente que en ese procesamiento se produzca una especie de "depuración" de carácter subjetivo. De ahí que existan lagunas permanentes entre el proceso de investigación técnica y el ámbito del Derecho público, así como entre las respectivas leyes y las características técnicas propias de estos sistemas (Barrio, 2020, p. 3).

Si hacemos referencia explícita al derecho a la privacidad, la disponibilidad de gran cantidad de datos para ser procesados y analizados por las herramientas de IA, puede constituir, inicialmente, una ventaja manifiesta en el campo de la atención sanitaria. El *big data* hace uso de herramientas que permiten establecer predicciones y encontrar patrones que facilitan la adopción de medidas preventivas para evitar la irrupción de riesgos en el cuidado de la salud (Martínez, 2017, p. 157).

Pero, desde otra perspectiva, conviene advertir que esas herramientas permiten establecer a su vez correlaciones entre los datos manejados, posibilitando, como indicábamos en el apartado anterior, la obtención de información adicional de carácter personal que no siempre ha sido aportada por el individuo. De ahí la necesidad de informar previamente al paciente sobre la posibilidad de descubrir datos inesperados relativos a su salud, que inicialmente no formaban parte del proceso de investigación; con el fin de que pueda tomar una decisión antes de comenzar los correspondientes análisis. Ya que la aportación de los sistemas digitalizados no puede alterar los fundamentos de la relación de confianza habitual que ha de darse entre médico y paciente.

Se trata de una cuestión de gran relevancia vinculada a las implicaciones que se derivan del auge de los sistemas de la IA: la eventual vulneración del derecho de los ciudadanos a su privacidad. En este sentido, las Naciones Unidas, a través del Comité Internacional de Bioética, elaboró durante 2017 un amplio informe sobre *big data* y salud, en el que ponía de manifiesto la contribución del manejo ingente de datos para la salud. En dicho informe, advertía sobre la necesidad de evitar que sus aplicaciones pudieran afectar al ejercicio de los derechos fundamentales consagrados en diversos documen-

tos internacionales, en particular en la Declaración Universal sobre Bioética y Derechos Humanos (Cárcar, 2020, p. 15).

Los pacientes deben contar con la seguridad de que se cumplen determinadas garantías jurídicas en el procesamiento y análisis de datos personales. De ahí el interés en adoptar medidas específicas de carácter restrictivo, para evitar que esos datos puedan caer en manos de terceros con los riesgos subsiguientes, tanto de violación de la intimidad personal, como a la hora de evitar el lucro eventual derivado de su manejo ilegítimo.

3.2. Otro aspecto fundamental de gran relevancia en el ámbito de los derechos fundamentales, aplicado al campo sanitario, es el ejercicio del derecho de autonomía, que remite directamente a la capacidad de los pacientes para poder decidir sobre el uso de sus propios datos personales. Actualmente la autorización de los pacientes es requerida para poder disponer de sus datos privados, tanto en el terreno de la investigación clínica como en la práctica asistencial hospitalaria. El motivo es debido a que dichos pacientes pueden oponerse a compartir tales datos o que estos puedan ser objeto de procesamiento por parte de sistemas inteligentes.

Esta posibilidad de negación está contemplada en la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. El articulado de esta ley especifica que los pacientes tienen el deber de aportar los datos que sean precisos para llevar a cabo el diagnóstico médico, pero no están obligados a desvelar otra información de carácter personal, con el fin de que sean incluidos en una base de datos o que sean susceptibles de utilizarse en el proceso de aprendizaje de los algoritmos de IA (Romeo, 2020, p. 13). En este sentido, el apartado segundo del artículo 5 de la Ley 14/2007, de 3 de julio, de Investigación biomédica, especifica que "la cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el consentimiento expreso y escrito del interesado".

Por otra parte, estrechamente relacionado con el respeto a la autonomía y la aplicación de la IA al ámbito biosanitario, se encuentra igualmente el principio de explicabilidad o de trazabilidad, en virtud del cual, las personas implicadas tienen derecho a controlar el uso de sus datos respectivos, así como a conocer los algoritmos que intervienen en su procesamiento. Ya que los seres humanos, independientemente de su actividad, pueden contar con preferencias personales que interfieran en el proceso de toma de decisiones, pero los sistemas autómatas no son ajenos a ellos y sus aplicaciones son menos perceptibles que en el caso de los humanos (Cortina, 2020, p. 390).

Los pacientes tienen derecho a ser informados de todos estos supuestos que se encuentran relacionados estrechamente con su tratamiento digital, en especial cuando se empleen herramientas de IA (Romeo, 2020, p.13).

Conviene precisar que los poderes públicos y las respectivas Administraciones –tanto en el ámbito sanitario como en otros campos ya sean de carácter administrativo, policial o judicial– no siempre pueden acceder al itinerario seguido por los algoritmos, incluso en aquellos casos en los que ellos mismos hacen uso del *big data* y la IA en sus funciones públicas. Han pasado así de crear y controlar los instrumentos de acción y de cambio social, a ser deudores de los servicios que les ofrece el sector privado, con la correspondiente dependencia (Cotino, 2017, p. 142).

Por todo lo expuesto, constatamos que la transformación digital del ámbito sanitario está convirtiéndose en un factor que puede alterar y tornarse disruptivo respecto a los principios tradicionales de la bioética –beneficencia, no maleficencia, autonomía y justicia– en la práctica clínica (Calvo, 2019, p. 162). Sin olvidar que la protección de datos está configurada como un derecho fundamental, recogido en el artículo 16 del Tratado de Funcionamiento de la Unión Europea, así como en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (Gil, 2011, pp. 18 y ss.).

4. Implicaciones éticas, legales y sociales

Algunos expertos están planteando diversas propuestas para que el principio de privacidad sea contemplado también desde otra perspectiva con objeto de que su cumplimiento pueda resultar más efectivo, siendo susceptible de insertarse en el código de funcionamiento del dispositivo técnico. Se trataría de velar por la salvaguarda de la privacidad desde el momento en el que comienza a diseñarse el correspondiente dispositivo técnico. No después. Así, la privacidad dejaría de ser considerada solo desde la vertiente jurídica, para ser asumida también desde la óptica empresarial. De esta manera los diseñadores de los algoritmos podrían implicarse más activamente en todo el proceso productivo haciendo posible el desarrollo de herramientas que contribuyan y aseguren un mayor grado de protección (Gil, 2011, p. 135).

A partir de ese enfoque y desde distintas instancias se postula la posibilidad de desarrollar un modelo más dúctil basado en la co-regulación en el que tanto las responsabilidades como los derechos pudieran ser compartidos. Ese sistema podría ir acompañado de medidas de ciberseguridad acre-

ditadas en cada momento (Gil, 2011, p. 139). De ese modo, la convergencia de ambos planos, jurídico, por una parte, y técnico-empresarial, por otra, podría ser más efectiva y permitiría a su vez eludir el riesgo de incurrir en un paralelismo disfuncional. Pero se trata de un planteamiento que no se ha traducido todavía en compromisos firmes. El motivo subyacente no es otro que los cuantiosos intereses económicos vinculados al desarrollo de la IA. Intereses que adquieren tal magnitud que ningún agente de la escena internacional desea limitarse y renunciar a ellos.

En el extremo opuesto, nos encontraríamos ante la actitud de algunas megacorporaciones internacionales que actúan de forma unilateral y tratan de fomentar debates supuestamente éticos en foros diversos, a veces impostados. Todo ello envuelto en un planteamiento de innovación tecnológica aderezada de supuesta responsabilidad. Intentan incurrir así, estratégicamente, en una dinámica aviesa como es la de generar debates infructuosos y posponer la "no regulación" con el objetivo de ganar tiempo, sembrar dudas en torno a los principios que han de regir y evitar el cumplimiento inexcusable de las normas institucionales. De ese modo, los macrodatos y algoritmos tratarían de erigirse progresivamente en una especie de binomio de control larvado que la tecnociencia va imponiendo sobre la sociedad (Gutiérrez, 2020, p. 107).

No cabe duda de que ese planteamiento con fines manifiestamente dilatorios resulta inviable a medio y largo plazo, en la medida en que la supuesta autonomía de estos sistemas inteligentes no puede servir de excusa para una eventual dilución de responsabilidades. Por el contrario, será imprescindible introducir los mecanismos adecuados para que en última instancia tanto las responsabilidades como obligaciones respecto al funcionamiento de estos sistemas inteligentes sean bien definidas de forma inequívoca (Marín, 2019, p. 18). El impacto de la transformación digital apoyada en el desarrollo y aplicación de la IA no puede ser ajeno a la protección de los derechos fundamentales que fomentan y sustentan el entramado jurídico de los estados constitucionales (Martínez, 2017, p. 154).

De hecho, la repercusión de la inteligencia artificial en el ámbito de los derechos humanos constituye probablemente, como advertíamos supra, uno de los factores más relevantes que dejarán huella en el periodo en que vivimos, tal y como advertía en mayo de 2019 el Consejo de Europa a través del *Unboxing artificial intelligence: 10 steps to protect human rights*-Commissioner´s Recommendation on Artificial Intelligence and Human Rights (Castellanos, 2020, p. 139).

Tal vez, el desequilibrio existente actualmente entre el desarrollo tecnocientífico de la IA y el *big data,* por una parte, y las limitaciones reguladoras en el ámbito jurídico, por otra, se deben en gran medida a que

nos movemos en escenarios provenientes del siglo pasado, que requieren actualización y adaptación a la nueva sociedad digital en la que estamos inmersos (Moreno, 2017, p. 17).

Ante lo cual, conviene recordar una vez más que ni la actividad científica ni el desarrollo de la tecnología en sus diversas etapas avanzan y se desarrollan solas. Ambas necesitan contar en su entorno con brújulas que sirvan de guía y con principios que regulen su curso de acción y anticipen los eventuales efectos negativos que pueden conllevar (Romeo, 2020, p. 15).

En este sentido, la Declaración adoptada en Toronto por diversos organismos internacionales pro-derechos humanos, tales como Human Rights Wachts y Amnistía Internacional, entre otros, en mayo de 2018, destacaba por una parte las potencialidades que ofrecen las nuevas tecnologías e incidía en su capacidad de transformación de la vida cotidiana; hacía alusión también al desarrollo de nuevos medicamentos y subrayaba la eficacia que podría alcanzar en el tratamiento de diversas enfermedades. Sin embargo, advertía, al mismo tiempo que un uso inadecuado de la IA puede discriminar a grupos pertenecientes a minorías sociales ampliando la desigualdad entre poblaciones vulnerables.

En ese caso, la brecha digital subsiguiente acentuaría las diferencias existentes en el terreno de la salud entre las personas con recursos suficientes para disponer de tecnología más avanzada —con los servicios más valiosos del mercado— y, por otra parte, las personas con menor o ningún poder adquisitivo. Con lo cual, el desigual acceso a los bienes tecnológicos iría socavando la cohesión social (Cortina, 2019, p. 391).

Esa desigualdad, que puede afectar en determinadas ocasiones a cuestiones relativas a la igualdad de género[1], podría producirse igualmente entre la población residente en zonas urbanas y la que habita en zonas rurales, teniendo en cuenta que la calidad y extensión de los servicios de conectividad pueden ser tan distintos que les aboquen a disponer de una tecnología inferior del mercado. De ahí la relevancia de adoptar medidas específicas para que el proceso de transformación digital del ámbito sanitario se realice con suficientes garantías, con el objetivo de que sus beneficios puedan llegar a todos los afectados posibles. Y en especial a los pacientes que sean más vulnerables con el fin de evitar que puedan provocarse mayores "cotas de desigualdad tras exclusión social" (Calvo, 2019, p. 158).

No podemos olvidar que uno de los problemas más lacerante en este milenio es la manifiesta desigualdad que arrastran históricamente los paí-

1. Nuevo informe de la UNESCO sobre Inteligencia Artificial e Igualdad de Género, 31/08/2020.

ses emergentes (Nussbaum, 2010, p. 54). Desigualdad que corre el riesgo de verse incrementada en los próximos decenios a partir de la progresiva brecha digital que puede producirse debido a un déficit de tecnología cuya adquisición no siempre es fácil lograr[2].

A este respecto, las palabras de L. Ferrajoli siguen siendo elocuentes cuando advertía que el grado de legitimidad de un ordenamiento jurídico, propio de una democracia constitucional, puede identificarse con el grado de efectividad de las garantías de los derechos constitucionales. Pudiendo evidenciar ese ordenamiento al mismo tiempo su correspondiente ilegitimidad por medio de las eventuales violaciones de dichas garantías o incluso a través de las lagunas existentes. Lagunas que es preciso colmar necesariamente y que no admiten dilación (Ferrajoli, 2016, p. 25).

Se trata de tener presentes en el proceso de elaboración de las normas, relacionadas con los sistemas de IA y *big data,* la inclusión de principios inexcusables que venimos enunciando, tales como: transparencia, prevención del riesgo, equidad, autonomía, etc., así como la superación de la distinción entre la posibilidad de aplicar un Derecho "duro" de carácter vinculante y un derecho considerado "blando" no vinculante (*hard y soft law*) a la hora de regular su aplicación a los diversos sectores concernidos (García San José, 2021, p. 276).

En este sentido, al igual que sucedió en similares retos de calado tecnocientífico, motivados por el auge de proyectos de gran relevancia como la investigación embrionaria humana o derivados del desarrollo de la nanotecnología y los nanomateriales (Casado, 2010, p. 282), el concurso del derecho internacional ha sido capaz de habilitar instrumentos válidos para afrontar y canalizar los riesgos que conlleva el desarrollo las nuevas tecnologías emergentes.

---

2. El Profesor Philip Alston, siendo relator para la pobreza de las Naciones Unidas, presentó un informe en 2019 sobre pobreza extrema y derechos humanos ante la Asamblea General, alertando sobre el uso que se realizaba de la IA para vigilar y hostigar a las personas más pobres. Denunciaba que las megaempresas tecnológicas siguen un proceso de desregularización eludiendo el cumplimiento de las leyes mientras se instalan en lo que denomina "zonas francas de derechos humanos". En el parágrafo 73 de su último informe advertía "Se objetará razonablemente que este informe es desequilibrado, o unilateral, porque se centra en los riesgos más que en las muchas ventajas que potencialmente se derivan del estado de bienestar digital. La justificación es sencilla. Hay un gran número de animadoras (cheerleaders) que ensalzan los beneficios, pero muy pocos aconsejan una reflexión sobria sobre sus desventajas" (García San José, 2020, p. 259).

5. Conclusiones

Por todo lo expuesto, no cabe duda de que la aplicación de la IA en el campo de la salud puede generar notables beneficios tanto a los médicos e investigadores biosanitarios como a los propios pacientes, sin olvidar el apoyo tecnológico y administrativo en los centros hospitalarios. Su aportación puede ser muy valiosa para diagnosticar y formular propuestas terapéuticas, siempre que no vulnere la protección de los datos personales o contribuya a ampliar la brecha de las desigualdades; habida cuenta que tanto la aplicación de algoritmos como el procesamiento del *big data* pueden generar o reproducir prejuicios, así como eventuales patrones de exclusión. El impacto de la transformación digital no puede ser ajeno a la protección de los derechos fundamentales que sustentan el entramado jurídico de los estados constitucionales.

Por ello, es necesario examinar, simultáneamente, las implicaciones del uso de las tecnologías emergentes siguiendo muy de cerca las cuestiones técnicas que llevan aparejadas desde el inicio de su diseño. Solo de ese modo, conociendo su complejidad, aprehendiéndola, será posible promover y aplicar normas jurídicas que permitan que derechos como la privacidad o la toma de decisiones libre e informada se vean protegidos en un ámbito sanitario cada vez más digitalizado. Y es que, así como a lo largo de la historia la dinámica de la ciencia no ha sido nunca éticamente neutral, tampoco los desarrollos tecnológicos se caracterizan actualmente por su imparcialidad o por resultar inocuos.

Las aplicaciones de la inteligencia artificial en campos de riesgo elevado, como son la salud, la administración de justicia o la seguridad ciudadana, entre otros, deben ser transparentes, susceptibles de comprobar su trazabilidad, y han de garantizar al mismo tiempo la realización de una verificación no técnica, sino humana. De hecho, la transparencia está convirtiéndose en un principio fundamental sobre el que ha de girar, inexorablemente, el análisis y la reflexión jurídica de la programación algorítmica. Sin embargo, es fácil constatar cómo determinadas aplicaciones de la IA albergan "cajas negras" que no facilitan su inteligibilidad. Esa opacidad latente u "oscuridad por diseño" inherente al procesamiento de *big data*, implica que después, el profesional de la salud no pueda validar o descartar la propuesta del sistema, porque desconoce la lógica interna y el intrincado proceso seguido para alcanzar dicho resultado.

De ahí que uno de los retos mayores para el ámbito sanitario es examinar el uso secundario que pueda realizarse de la información proveniente de los datos personales. Hablamos de usos indirectos no deliberados, que puedan provocar un trato discriminatorio, a veces encubierto. De hecho,

es fácil constatar que ya no es posible garantizar el anonimato. Tampoco deberían considerarse válidos buena parte de los procesos de información y consentimiento informado basados en esta garantía de anonimización. De otro modo se incurriría en el riesgo de propiciar una falsa seguridad, porque la posibilidad de reidentificar sujetos a partir de datos de carácter personal es muy alta debido a que el proceso de anonimización que se venía aplicando respecto a la información sanitaria ha mostrado sus limitaciones; ha quedado desfasado.

Asistimos, de este modo, a lo que podría denominarse la "paradoja de la transparencia", en virtud de la cual el procesamiento de datos masivos y su respectiva combinación, hacen posible el acceso de forma invasiva a gran cantidad de información privada, pero por otra parte la obscuridad e ininteligibilidad que presiden esos tratamientos de datos permite a sus creadores mantener en secreto el diseño del algoritmo, así como los pasos dados en su aplicación. A consecuencia de ello, el derecho a la reversibilidad se convierte prácticamente en una especie de entelequia. Sin embargo, conviene recordar que las garantías constitucionales que hacen posible la protección efectiva de la privacidad no son eficaces realmente si no cuentan con procedimientos habilitados de rendición de cuentas que puedan aplicarse a quienes abusan con el manejo de datos personales obtenidos de forma ilícita.

En cuanto a la implicación de los pacientes con el objetivo de preservar la privacidad, el consentimiento informado debería ser específico, *ad hoc,* ya que un consentimiento indiscriminado, sin precisar la finalidad del tratamiento, no debería ser admitido. El CI, además de ser comprensible, ha de referirse con claridad al alcance y consecuencias derivadas del tratamiento de datos. De otro modo, el consentimiento otorgado se convertiría en una especie de "carta blanca" que comportaría el descontrol del flujo de los datos personales. Lo cual equivaldría a evidenciar la inoperancia del sistema de protección, supuestamente habilitado a tal efecto.

Y es que los pacientes deben contar con la seguridad de que se cumplen determinadas garantías jurídicas en el procesamiento de datos personales. De ahí la necesidad imperiosa de adoptar medidas específicas de carácter restrictivo para evitar que esos datos puedan caer en manos de terceros con los riesgos subsiguientes, tanto de violación de intimidad personal, como a la hora de evitar el lucro eventual derivado de su manejo ilegítimo.

Por último, sería deseable igualmente que los usuarios de los servicios sanitarios se familiarizasen, por su parte, con las medidas concernientes a la privacidad de sus datos. De ese modo sería más fácil promover y exigir la adopción de buenas prácticas con el fin de reducir el riesgo de padecer abusos e incidencias diversas que puedan afectar, eventualmente, a los pacientes de forma negativa.

Referencias bibliográficas

Alonso Betanzos, A. (2021). Prólogo en Sánchez Caro, J. – Abellán-García Sánchez, F.*, Inteligencia artificial en el campo de la salud. Un nuevo paradigma: aspectos clínicos,* éticos y legales (pp. 14-20), Madrid: Fundación Merck Salud, Colección Bioética y Derecho Sanitario.

Andrés, B. (2021). El reinicio tecnológico de la inteligencia artificial en el servicio público de salud, *IUS ET SCIENTIA, Revista electrónica de Derecho y Ciencia,* Vol. 7, n. 1, 327-356.

Barrio Andrés, M. (2020). Retos y desafíos del estado algorítmico de Derecho. *Análisis del Real Instituto Elcano (ARI),* ARI 82 - 9/6/2020.

Arigo, D., Jake-Schoffman, D., Wolin, K., Beckjord, E., Heckler, E., Pagoto, Sh. L. (2019). The history and future of digital health in the field of behavioral medicine. *Journal Behavioral Medicine,* 42, 67-83. doi:10.1007/s10865-018-9966-z.

Boix Palop, A. (2020). Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones. *Revista de Derecho Público, Teoría y Método*, Vol. 1, 223-270.

Bostrom, N. y Yudkowsky, E. (2014). The ethics of artificial intelligence, en Frankish. K., Ramsey, W. M., Ed. *The Cambridge Handbook of Artificial Intelligence* (pp. 316-334). Cambridge University Press doi:10.1017/CB09781139046855.020.

Brenot, S. (2019). Les enjeux de l´intelligence artificielle dans le milieu du droit, *Rédaction du Village de la Justice,* Vendredi, 10 mai.

Brundage, M., Avin, S, Clark (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. February, https://www.researchgate.net/publication/323302750, 85-86.

Calvo, P. (2019). Bioética de las Cosas: sobre la algoritmización de la deliberación moral en la práctica clínica, *Filosofía Unisinos. Unisinos Journal of Philosophy* 20 (2), may/aug, p 162, Unisinos – doi: 10.4013/fsu.2019.202.05.

Capdeferro Villagrasa, O. (2020). La inteligencia artificial del sector público: desarrollo y regulación de la actuación administrativa e inteligente en la cuarta revolución industrial. *Revista de los Estudios de derecho y Ciencia Política,* IDP, n.30, marzo, 1-10.

Cárcar Benito, J. E. (2020). La asistencia sanitaria dentro del ámbito de la inteligencia artificial (IA): el problema de los derechos de los pacientes. *Papeles el tiempo de los derechos*, n.1, 1-23.

Casado, M. J. (coord.) (2010). *Bioética y Nanotecnología.* Pamplona: Civitas, Reuters.

Castellanos Claramunt, J. (2020). Democracia, Administración pública e inteligencia artificial desde una perspectiva política y jurídica. *Revista catalana de dret públic*, 60, 137-147. https://doi.org/10.2436/rcdp.i60.2020.3344.

Coeckelbergh, M. (2020). Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability. *Science and Engineering Ethics,* Vol. 26, 4, 2051-2068.

Colmenarejo, R. (2018). Ética aplicada a la gestión de datos masivos. *Anales de la Cátedra de Francisco Suárez,* 52, 113-129.

COMISIÓN EUROPEA (2020). Bruselas, 19.2.2020 65 final. *LIBRO BLANCO* sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.

COMISION EUROPEA (2018). Bruselas, 25.4.2018 COM 237 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Inteligencia artificial para Europa {SWD (2018) 137 final}.

Consejo de Europa (2019). Commissioner´s Recommendation on Artificial Intelligence and Human Rights, *Unboxing artificial intelligence: 10 steps to protect human rights*, Mayo.

Cortina, A. (2019). Ética de la inteligencia artificial. *Anales de la Real Academia de Ciencias Morales y Políticas,* Nª 96, 2019, 379-393.

Cotino, L. (2017). Big data e inteligencia artificial. Una aproximación a su tratamiento desde los derechos fundamentales. *Dilemata*, n. 24, 131-150.

De Asís, R. (2014). *Una mirada a la robótica desde los derechos Humanos***,** Instituto de Derechos Humanos "Bartolomé de las Casas", Madrid: Universidad Carlos III de Madrid-Dykinson.

Einstein, A. (2007). *The human side/ Sobre el humanismo*, Barcelona: Ed. Paidós.

ENISA (2015). European Union Agency for Network and Information Security, "Privacy by design in Big Data: An overview of privacy enhancing technologies in the era of Big Data analytics".

European Group on Ethics in Science and New Technologies (2018). Artificial Intelligence, Robotics and "Autonomous" Systems. *European Commission*, Brussels.

Felzmann, H., Fosch-Villaronga, E., Lutz, Ch., Tamo-Larrieux, A. (2020). Towards Transparency by Design for Artificial Intelligence. *Science and Engineering Ethics,* VL, 6, 3333-3361.

Ferrajoli, L. (2016). *Derechos y garantías: la ley del más débil.* Madrid: Ed. Trotta.

Fogel, A. L. y C. Kvedar, J. (2018). Artificial intelligence powers digital medicine. *NPJ Digital Medicine,* Marz, 4, 1-5. doi:10.1038/s41746-017-0012-2.

Frankish, K., Ramsey, W. M. (ed.) (2014). *The Cambridge Handbook of Artificial Intelligence,* Cambridge University Press, doi:10.1017/CB09781139046855.020.

García San José, D. (2021). Implicaciones jurídicas y bioéticas de la inteligencia artificial (IA). Especial consideración al marco normativo internacional. *Cuadernos de Derecho Transnacional,* marzo, Vol. 13, n. 1, 255-276.

Gil, E. (2011). *Big data, privacidad y protección de datos*, Madrid: Agencia Española de Protección de Datos, BOE.

Goñi, J. L. (2019). "Defendiendo los derechos fundamentales frente a la inteligencia artificial*". Lección inaugural del Curso Académico 2019-2020,* Universidad Pública de Navarra.

Grupo de Expertos de Alto Nivel de la UE (2019). Directrices éticas para una inteligencia fiable. (Ethics Guidelines for Trustworty AI) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60423.

Gutiérrez Rubí, A. (2020). Tecnopolítica y los algoritmos. En Sabariego, J, et al. *Algoritarismos* (pp. 102-112). Sao Paulo: Tirant lo blanch.

Habermas, J. (2002). *El futuro de la naturaleza humana. ¿Hacia una eugenesia liberal?* Barcelona: Paidós.

Kelsen, H. (1992). Science and Politics. *American Political Science Review,* September, 1951, *Qué es justicia*, Barcelona: Ariel.

Lecuona, I., de (2020). Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el *big data* en salud en un contexto de pandemia. *Revista Internacional de Pensamiento político,* Vol. 15, 139-166.

Lecuona., I., de (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 pp. 576-578. DOI: 10.1016/j.gaceta.2018.02.007.

Lerman, J. (2013). Big Data and Its Exclusions. *Stanford Law Review Online,* 66 Stanford Law Review Online 55, SSRN.

López Baroni, M. J. (2021). Los derechos fundamentales de las Inteligencias Artificiales frente a los seres humanos, en Soriano Díaz, R.- Marín-Conejo, S., Eds. *El reto de los derechos humanos: cuestiones actuales controvertidas* (pp. 27-43). Madrid: Dykinson, Colección "Teoría y Práctica de los Derechos Humanos".

Llano, F. (2018). *Homo excelsior. Los límites ético-jurídicos del transhumanismo.* Valencia: Tirant lo Blanch.

Marín García, S. (2019). Ética e inteligencia artificial. *Cuadernos de la Cátedra CaixaBank de Responsabilidad Social Corporativa,* n. 42, Septiembre, 1-29.

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

Moreno Muñoz, M. (2017). Privacidad y procesado algorítmico de datos personales mediante aplicaciones y bots. *Dilemata*, n. 24, 1-23.

Nussbaum. M. C. (2010). *Sin fines de lucro. Por qué la democracia necesita de las humanidades,* Buenos Aires: Katz.

Parlamento Europeo (2017). Resolución de 14 de marzo de 2017 sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI)).

Pasquale, F. **(**2015). *The black box society: the secret algoritms that control money and information,* Boston: Harvard University Press.

Pavón, N. A. (2018). De los algoritmos a la salud. La inteligencia artificial en la atención sanitaria, *Revista de Occidente,* N. 446-447, 63-75.

Pérez G. (2016). Peligros del uso de los *big data* en la investigación en salud pública y en epidemiología. *Gaceta Sanitaria*, Núm. 30, 66-68.

Rodríguez, R. y Martínez. F. (2016). *Desmontando el mito de Internet. Restricción de contenidos y censura digital en la red.* Barcelona: Icaria.

Romeo Casabona, C. (dir.) (2020). Inteligencia artificial en salud: retos éticos y legales. *Informes anticipando,* Fundación Instituto Roche, noviembre.

Sánchez Caro, J. y Abellán-García Sánchez, F. (2021). *Inteligencia artificial en el campo de la salud. Un nuevo paradigma: aspectos clínicos, éticos y legales,* Madrid: Fundación Merck Salud, Colección Bioética y Derecho Sanitario.

Schesky, H. (1963). *Eisamkeit und Freiheit,* Hamburgo: Verlag.

Surden, H. (2017). Values Embedded in Legal Artificial Intelligence. University of Colorado Law *Legal Studios Research Paper*, n. 17, 13 Marzo, http://dx.doi.org/10.2139/ssrn.2932333.

Sweeney, L. (2000). *Simple demographics often identify people uniquely.* Pittsburgh: Carnegie Mellon University, Data Privacy Working Paper, 3.

Tegmart, M. (2018). *Vita 3.0. Essere umani nell´era dell´inteligenza artificiale.* Milán: Raffaello Cortina Editore.

UNESCO (2020) Nuevo informe sobre Inteligencia Artificial e Igualdad de Género, 31/08/2020. https://unesdoc.unesco.org/ark:/48223/pf0000374174