Cuadernos de Bioética. 2024; 35(114): 143-155
DOI: 10.30444/CB.170

IMPLICACIONES ÉTICAS Y LEGALES DE LAS APLICACIONES DIGITALES DE SALUD MENTAL

ETHICAL AND LEGAL IMPLICATIONS OF DIGITAL MENTAL HEALTH APPLICATIONS

JAVIER GÓMEZ LANZ *(ORCID: 0000-0002-6627-2717)*
FEDERICO DE MONTALVO JÄÄSKELÄINEN *(ORCID: 0000-0002-9272-7359)*
VANESA MORENTE PARRA *(ORCID: 0000-0003-0168-6510)*
LUCÍA HALTY BARRUTIETA *(ORCID: 0000-0003-1258-5950)*
Universidad Pontificia Comillas
C/ Alberto Aguilera, 23, 28015, Madrid, 915422800
jglanz@comillas.edu; fmontalvo@comillas.edu; vmorente@comillas.edu; lhalty@comillas.edu

RESUMEN:

Palabras clave:
salud mental digital, *apps,* protección de datos personales de salud

Recibido: 18/01/2024
Aceptado: 27/04/2024

La digitalización de la salud mental abre la puerta a cambios significativos en la práctica clínica, pues el tratamiento de datos masivos derivados del uso de *apps* y *wearables* puede contribuir a mejorar la investigación médica, la atención a los pacientes y la eficiencia del sistema. Este proceso, sin embargo, comporta riesgos éticos y jurídicos relevantes. En el ámbito ético, la tutela de la privacidad y la confidencialidad de los datos sensibles, así como la transformación de la relación médico-paciente a través de la interacción tecnológica aparecen como preocupaciones principales. En la esfera regulatoria, la caracterización de esta tecnología como producto sanitario, la garantía de una protección eficaz de los datos de salud mental y la atención a los riesgos penales que aparecen en este contexto constituyen retos ineludibles. Este artículo presenta de forma panorámica este escenario con el fin de catalizar el debate ético y jurídico que reclama la salud mental digital.

ABSTRACT:

Keywords:
digital mental health, apps, wearables, personal health data protection

The digitization of mental health enables significant shifts in clinical practice by harnessing vast amounts of data derived from the use of apps and wearables to enhance medical research, patient care, and health system efficiency. However, this process brings forth pertinent ethical and legal risks. Ethically, concerns primarily revolve around safeguarding the privacy and confidentiality of sensitive data, alongside the transformation of the doctor-patient relationship through technological interaction. Within the regulatory realm, issues encompass the classification of these tools as medical products, ensuring normative assurance of effective protection of mental health data, and addressing potential legal risks within this domain. This article aims to provide an overarching view of this landscape, serving as a catalyst for the technological, ethical, and legal discourse necessitated by digital mental health.

1. Oportunidades derivadas de la digitalización de la salud mental

La práctica clínica genera diariamente una ingente cantidad de información relevante para conocer la incidencia, prevalencia y evolución de las enfermedades. El desarrollo de la historia clínica electrónica en cada sistema de salud, como repositorio de toda la información asistencial con un identificador único por paciente que enlaza las diferentes bases de datos, ha permitido no sólo un acceso eficiente a esta información, ya resulte estructurada o no estructurada[1], sino su posterior utilización en el marco de la investigación y de la atención clínica. El éxito de este proceso de digitalización ha abierto la puerta a nuevas herramientas de prevención, diagnóstico, tratamiento y seguimiento de enfermedades que operan en escenarios no sanitarios en los que la generación de datos de salud es asombrosa. La relevancia de la *eHealth* o eSalud, articulada a través de *apps*[2] y *wearables* (sensores de movimiento, fisiológicos o bioquímicos[3]) constituye ya un hecho asentado tanto en el contexto institucional[4] como en el académico[5]. La considerable cantidad de datos recopilados, la ubicuidad y continuidad del proceso de comunicación en el ecosistema móvil y la interconectividad y accesibilidad simultánea por una variedad de motores de análisis sin apenas fricción ofrecen una estructura que facilita el análisis conjunto de grandes volúmenes de datos relevantes para la salud. Ello puede resultar crucial para la investigación biomédica[6], para la atención[7] y, en última instancia, para aumentar la eficiencia del sistema.

El efecto de la digitalización en la prevención de la enfermedad resulta, además, multiplicado como consecuencia de la interconexión entre distintas clases de datos que no integran sólo los tradicionalmente definidos como "datos de salud". Ello puede propiciar una caracterización más amplia de estos últimos[8] y, además, como recuerda el Comité Internacional de Bioética de la UNESCO en su informe sobre *Big Data* y Salud de 2017, desarrollar una visión holística de la salud en la que la frontera entre el sector de la atención sanitaria y otros sectores se difumine progresivamente. Esta es ya, en buena medida, la definición de salud que ofrece la OMS como "estado de completo bienestar físico, mental y social" y no sólo como ausencia de enfermedad. El *Big Data* ofrece la oportunidad de articular esta visión al no limitar la explotación de datos a los estrictamente asistenciales, permitiendo incorporar datos sobre estilos y hábitos de vida e, incluso, el entorno. Además, estos macrodatos facultan el incipiente desarrollo de la inteligencia artificial en la salud, que contribuirá a resolver la incertidumbre que rodea todos los aspectos de la práctica sanitaria: desde la incertidumbre diagnóstica (cómo clasificar las condiciones del paciente) y la pato-fisiológica (por qué y cómo se desarrolla la patología) a la terapéutica (qué tratamiento es apropiado) y pronóstica (si habrá recuperación con o sin tratamiento específico)[9].

1 Alcalde, G. y Alfonso, I. "Utilización de tecnología Big Data en investigación clínica". *Rev Der Gen H*. 2019; nº. extra, 59.

2 Más de un millón de las *apps* disponibles en las plataformas Google Play y Apple App Store están relacionadas con la salud, el estado físico, la alimentación y el bienestar general.

3 Alós, F. y Puig-Ribera, A. "Uso de wearables y aplicaciones móviles (mHealth) para cambiar los estilos de vida desde la práctica clínica en Atención Primaria: una revisión narrativa". *Atención Primaria Práctica*. 2021; 3(1), 1-5.

4 *Cfr.* el informe del Comité Nacional de Bioética de Italia sobre los aspectos bioéticos de las aplicaciones móviles de salud de 28 de mayo de 2015 y el informe *Los ciudadanos ante la e-Sanidad. Opiniones y expectativas de los ciudadanos sobre el uso y aplicación de las TIC en el ámbito sanitario*, elaborado por el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información en abril de 2016.

5 Alcalde, G. y Alfonso, I., *op. cit.*, 61.

6 *Cfr.* el informe *Big Data and health. Data sovereignity as the shaping informational freedom*, 2018, 9, del Consejo Nacional de Ética de Alemania, el Cons. 157 del Reglamento 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 el Cons. 18 de la Recomendación (UE) 2019/243 de la Comisión, de 6 de febrero de 2019, sobre un formato de historiales médicos electrónicos del ámbito europeo.

7 *Vid*. el informe *Redesigning Health in Europe for 2020*, de la *eHealth Task Force* de la Unión Europea.

8 Como señala Romeo, C.M. "Revisión de las categorías jurídicas de la normativa europea ante la tecnología del *big data* aplicada a la salud". *Rev Der Gen H.* 2019; nº. extra, 94, cabe asimilar a los datos de salud otros datos en tanto estos últimos o una parte de ellos se hallen vinculados de forma permanente o temporal con los datos de salud y sean utilizados con propósitos o en contextos relacionados directamente con la salud.

9 Cabitza, F., Ciucci, D. y Rasoini, R. "A Giant with Feet of Clay: On the Validity of the Data that Feed Machine Learning in Medicine", en *Organizing for the Digital World*: *IT for Individuals,*

Estos beneficios se ponen de manifiesto de manera especialmente intensa si se concentra la mirada en el ámbito de la salud mental digital, que, tras la exacerbación de la vulnerabilidad del sistema a resultas de la pandemia de COVID-19, constituye una de las vanguardias de la salud pública[10]. Los biomarcadores digitales generados por *wearables* prometen una revolución en la detección y el manejo remoto de la salud mental, ofreciendo una visión más precisa y en tiempo real del estado del paciente. Este avance acredita el poder de la tecnología para renovar la atención médica, permitiendo intervenciones más tempranas y personalizadas y permitiendo diseñar ensayos clínicos más eficientes y centrados en el paciente. La oportunidad es de tal calibre que obliga a renunciar a un enfoque apriorístico que conciba negativamente cualquier tratamiento de datos de salud[11].

2. Los riesgos éticos de la digitalización de la salud mental

Sin embargo, la digitalización de la salud mental comporta también importantes riesgos. Como indica el Comité Internacional de Bioética en el citado informe sobre *Big Data* y Salud de 2017, la visión holística de la salud aúna aspectos positivos y desafíos complejos.

Un primer ámbito de preocupación concierne a la protección de los derechos del usuario, en particular en cuanto atañe a la tutela de la privacidad y la confidencialidad de los datos sensibles que las *apps* recopilan y analizan. A este respecto, el informe, ya referido, del Comité Nacional de Bioética de Italia de 2015 sobre los aspectos bioéticos de las *apps* móviles de salud destaca el riesgo de generación de perfiles de ciudadanos (en atención a rasgos de salud, conducta y hábitos de vida) mediante la conexión, interoperabilidad y explotación de sus datos[12]. En este contexto, es preciso, por una parte, patrocinar un consentimiento informado que emerja de una comprensión clara por el usuario de la forma en que se van a utilizar sus datos y de los posibles riesgos asociados y, por otra, fomentar su autonomía a través del propio diseño de las *apps*.

Una segunda dimensión del debate ético relativo a las *apps* y *wearables* de salud mental digital atiende a la posibilidad de que su empleo altere las características que deben presidir la relación entre el profesional sanitario y el paciente. Varios riesgos pueden contribuir a ello. En primer lugar, el recurso a tecnologías algorítmicas, pese a su utilidad desde un análisis de coste y beneficio, puede descuidar aspectos no mecánicos de la atención[13]. La interacción máquina-individuo que caracteriza a las *apps* diluye el elemento moral que, junto con el científico, integra el proceso de diagnóstico y tratamiento: el médico es un agente moral, un experto "confiable" capaz de realizar una evaluación subjetiva y comprender al paciente como persona social[14]. La relación a través de *apps*, en cambio, afecta a ingredientes vitales de la actuación médica como la salvaguarda de la autonomía y el bienestar moral del paciente o la afirmación de su complicidad en la intervención[15]. El paradigma tecnológico puede, además, alentar una medicina defensiva que prescriba pruebas adicionales cuyo valor principal no sea clínico, sino funcional para el entrenamiento de sistemas de IA[16]. Y a todo ello se suma que el conjunto de datos recabados por *apps* y *wearables* puede paradójicamente diluir la información sobre el contexto del paciente, prescindiendo de aspectos difíci-

Communities and Societies, Cabitza, F., Batini, C. y Magni M. (eds.), Springer, Cham, 2019, 122.

10 Según el informe *Digital Health Trends,* elaborado en 2021 por el IQVIA Institute for Human Data Science, dentro de las *apps* dirigidas a la gestión de condiciones específicas de salud, el porcentaje mayor (22%) correspondía en ese momento a *apps* de control y seguimiento de salud mental y trastornos del comportamiento.

11 Martínez, R. "Big data, investigación en salud y protección de datos personales ¿Un falso debate?". *Revista Valenciana d'Estudis Autonòmics*. 2017; 62, 236.

12 No es inusual que la información sobre los usarios recogida por los proveedores de motores de búsqueda en el marco de la *eHealth* se procese `con vistas al desarrollo de estrategias de marketing personalizadas basadas en el historial de búsqueda del usuario y su participación en grupos en línea.

13 Mittelstadt, B. *The impact of artificial intelligence on the doctor-patient relationship.* Consejo de Europa. 2021; 43.

14 Emanuel, E.J. y Emanuel, L.L.. "Four models of the physician-patient relationship". *JAMA: The Journal of the American Medical Association*. 1992; 267, 2221-2226.

15 Pellegrino, E.D. y Thomasma, D.C. *The Virtues in Medical Practice*. Oxford U. Press, Nueva York, 1993.

16 En su informe de 2015, el Comité italiano subraya la falta de información transparente a los usuarios de las *apps* en relación no sólo con el control, almacenamiento y combinación de sus datos, sino con su empleo para fines de investigación o de otra clase (como el entrenamiento de sistemas de inteligencia artificial).

les de recabar. La descontextualización del paciente, especialmente alarmante en el ámbito de la salud mental, puede determinar una pérdida de oportunidades para desarrollar una comprensión íntegra de su salud y bienestar[17]. A fin de conjurar este riesgo, al menos en parte, es razonable reclamar que la decisión adoptada por una *app* de salud mental resulte supervisada por un ser humano en los términos que apunta la AEPD en su *Guía sobre la adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial*, esto es, una "supervisión (…) realizada por una persona competente y autorizada para modificar la decisión" que constituya "una acción significativa y no simbólica"[18]. La necesidad de una previsión de esta naturaleza aparece recogida, aun sin valor normativo, en el apartado XXIII de la Carta de Derechos Digitales aprobada por el Gobierno de España en 2021[19]. En estos casos, de hecho, los estudios demuestran que el empleo de *apps* resulta beneficioso para el tratamiento de determinadas condiciones de salud mental cuando aquellas complementan la terapia tradicional dirigida por un profesional[20].

Así mismo, es preciso mencionar el peligro asociado al protagonismo que en la *eHealth* han adquirido empresas tecnológicas ajenas al tradicional contexto sanitario, que recolectan datos para un seguimiento ubicuo del ciudadano y desarrollan el *software* para modular la toma de decisiones a partir del análisis de aquellos[21]. La asunción de obligaciones propias de la relación médico-paciente por parte de estos actores tecnológicos es, sin duda, motivo de preocupación; dar primacía única a la autonomía del paciente, si supone que el médico quede reducido a mero proveedor de servicios tecnológicos, impedirá que imperen en la relación las virtudes médicas y normas deontológicas de la práctica médica[22].

Como guía para gestionar la creciente heterogeneidad de operadores de *eHealth*, el Comité italiano propone en su informe de 2015 distinguir entre las *apps* que pertenecen a dispositivos médicos y las que no, dada la divergencia de controles de seguridad y eficacia a las que ambas se someten. Muchos dispositivos no médicos no están operados por organismos científicos y su empleo se supedita al rango de aprobación expresado por los consumidores y no a la validación científica. La duda sobre la seguridad y eficacia de las *apps* asociadas a estos dispositivos es relevante, ya que puede propiciar que el usuario adopte decisiones, conductas o hábitos que no sean beneficiosos para su salud mental o que, incluso, resulten perjudiciales.

En buena medida, la relajación del escrutinio al que se somete a las nuevas *apps* vinculadas a la salud que no constituyen tecnologías sanitarias en sentido clásico se funda en la convicción de que, aun si no garantizan un beneficio para la salud del usuario, en modo alguno son capaces de causar daño. Esta pregonada inocuidad provee de una narrativa propicia a su implantación; no obstante, ninguna intervención de salud está libre de riesgos y menos cuando, como en este caso, va dirigida a un gran número de personas mayoritariamente sanas[23]. En particular, estas *apps* pueden producir un efecto "nocebo", un efecto inespecífico perjudicial de anticipación psicológica negativa en forma de ansiedad, miedo o repulsión al tratamiento, de disminución de su eficacia terapéutica o de interferencia en el curso de la enfermedad[24]. El informe de 2015 del Comité italiano advierte a este respecto de la aptitud de las *apps* para

17 Mittelstadt, B., *op. cit.*, 52.

18 En el ámbito sanitario, quien puede realizar dicha acción significativa es el profesional sanitario, como se deduce de los artículos 3 de la Ley 41/2002 y 4 de la Ley 44/2003.

19 Que señala que "el empleo de sistemas digitales de asistencia al diagnóstico y en particular de procesos basados en inteligencia artificial no limitará el derecho al libre criterio clínico del personal sanitario". El Comité de Bioética español, en su *Informe* sobre el borrador de Carta, propugnaba garantías adicionales: que el uso de las tecnologías digitales fuera complementario y no sustitutivo del trato humano y la atención directa del sanitario con el paciente.

20 Hayoung, B., Hyemin, S., Han-Gil, J., Jun Soo, K., Hyungsook, K., y Ji-Won, H. "App-Based Interventions for Moderate to Severe Depression. A Systematic Review and Meta-Analysis". *JAMA Network Open*. 2023; 6(11), 1-14.

21 Prainsack, B. "The political economy of digital data". *Policy Studies*, 2020; 41(5), 439-446.

22 Mittelstadt, B., *op. cit.,* 42-43.

23 Royo-Bordonada, M. y Román-Maestre, B. "Towards public health ethics". *Public Health Reviews*, 2015; 36(3), 1-15.

24 Häuser, W., Hansen, E. y Enck, P. "Nocebo phenomena in medicine: their relevance in everyday clinical practice". *Dtsch Arztebl Int*, 2012; 109(26), 459-465. El término "nocebo", acuñado en 1961 por Kennedy [Data-Franco, J. y Berck, M. "The nocebo effect: A clinicians guide" *Australian & New Zealand Journal of Psychiatry*, 2012; 7(6), 617-623], suele ejemplificarse con el experimento de Schweiger y Parducci en 1981 [Schweiger, A. y Parducci, A. "Nocebo: the psychologic induction of pain". *The Pavlovian journal of biological science*, 1981; 16(3), 140-143], en el que más de dos tercios de una muestra no seleccionada de 34 estudiantes

generar adicción y dependencia personal y, en suma, patologías genuinas de conciencia de la salud, exacerbando el miedo a la enfermedad, la atención continua a detalles insignificantes y la medicalización.

Todo ello conduce a una concepción "cuantificada" del ser humano[25] en la que el individuo, enfocado en exceso en su salud, asume la creencia de que cada ciudadano es responsable de su propia salud y enfermedad, lo que puede determinar, en el largo plazo, la estigmatización y discriminación de quienes no comparten esa focalización. En el peor de los escenarios, esta dependencia individual puede derivar en una dependencia política que convierta la utilización de esta tecnología en obligatoria, limitando la autonomía individual y legitimando una intrusión cada vez más intensa en la esfera personal, así como económica, si el precio de esta tecnología, al principio insignificante, se ajusta al alza conforme crezca la demanda[26]. Este riesgo convierte en perentorio garantizar el acceso en condiciones de equidad a la atención digital, de forma que la aplicación de la tecnología a la salud mental no perpetúe disparidades ya existentes ni se convierta en un lujo. Es crucial, a este respecto, que los servicios digitales se diseñen y articulen de forma que sean accesibles y asequibles con independencia del poder económico, la edad, la capacidad tecnológica o la ubicación geográfica.

Conviene, además, recordar que, como apunta el Comité de Bioética español en el *Informe sobre el borrador de Carta de Derechos Digitales*, la vigente arquitectura del entorno digital no es neutral ni inexorable, sino fruto de un diseño que persigue como objetivos concretos la obtención de datos y la predicción a partir de ellos de la conducta del usuario. Este modelo de entorno digital ha permeado el ámbito sanitario, donde se advierte, además, el tránsito de la predicción del comportamiento a la incidencia en el mismo: el tratamiento masivo de datos permite el conocimiento profundo de las preferencias del usuario y facilita identificar los sutiles empujones (*nudges*) que pueden conducir su conducta en la dirección deseada, generando un instrumento de ingeniería social tan eficaz como insidioso. El ecosistema de salud mental digital constituye un ejemplo paradigmático de esta falta de neutralidad y de la pluralidad de intereses que en él se manifiestan. Como señala el informe, es preciso promover un debate público sobre el ajuste de ese entorno digital a las exigencias de la salud no sólo en el nivel político, sino en el ético-cívico y en el jurídico. Precisamente a este último nos referiremos a continuación.

3. El reto regulatorio de la salud mental digital

La generalización de las *apps* de salud mental digital plantea también un importante desafío regulatorio dada la constante y veloz evolución de la innovación tecnológica que, a menudo, supera la capacidad de adaptación del marco legal. La ordenación jurídica debe equilibrar el fomento de la innovación con la tutela del consumidor, garantizando que los dispositivos no solo sean efectivos, sino seguros y accesibles, monitoreando su efectividad en tiempo real a fin de identificar y abordar problemas derivados de su integración en la práctica. La aprobación de terapias digitales por las agencias, la creación de estructuras legales que permitan el reembolso y la generación de datos de alta calidad y la fijación de políticas y directrices claras y coherentes son objetivos fundamentales para una implementación exitosa de la salud mental digital.

3.1. La regulación europea y nacional de apps *y wearables como productos sanitarios*

En primer lugar, cabe plantear si el control y seguridad demandado a las *apps* y *wearables* de salud mental puede alcanzarse mediante su sometimiento al marco regulatorio propio de los productos sanitarios, lo que exige determinar si aquellos pueden o no caracterizarse como tales.

En su sentencia de 7 de diciembre de 2017 (*Syndicat national de l'industrie des technologies médicales (Snitem) y Philips France contra Premier ministre y Minis-*

informaron de dolores de cabeza leves tras ser advertidos de que una inexistente corriente eléctrica iba a pasar por sus cabezas .

25 Lupton, D. *The quantified self*. Polity Press, Cambridge, 2016.

26 *Cfr.* el informe de 2017, *The Quantified Human. Ethical aspects on self-monitoring by wearables and health apps,* del Comité Sueco de Ética Médica (Smer).

tre des Affaires sociales et de la Santé), el Tribunal de Justicia de la Unión Europea declaró que se desprende del art. 1.2.a) de la Directiva 93/42 que un programa informático constituye o no un producto sanitario en atención a la finalidad perseguida y la acción producida. A tal efecto, es producto sanitario el destinado por el fabricante a su uso en seres humanos con fines de diagnóstico, prevención, control, tratamiento o alivio de una enfermedad, lesión o deficiencia. Como precisa el consid. 6 de la Directiva 2007/47, cuyo art. 2 modifica la redacción del citado precepto, un programa informático es un producto sanitario si está específicamente destinado por el fabricante a una o varias de las finalidades médicas establecidas en la citada definición, de forma que el mero empleo de un programa informático de uso general en el marco de la asistencia sanitaria no convierte a aquel en producto sanitario. Para ello es necesario, además, que su finalidad, definida por el fabricante, sea específicamente médica (sentencia de 22 de noviembre de 2012, Brain Products, C-219/11, EU:C:2012:742, apartados 16 y 17).

Esta focalización en la finalidad del producto es también perceptible en la definición dada por el art. 2 del vigente Reglamento 2017/745 del Parlamento Europeo y del Consejo, de 5/04/2017, sobre productos sanitarios, que define como tal "todo instrumento, dispositivo, equipo, programa informático, implante, reactivo, material u otro artículo destinado por el fabricante a ser utilizado en personas, por separado o en combinación, con alguno de los siguientes fines médicos específicos:

- diagnóstico, prevención, seguimiento, predicción, pronóstico, tratamiento o alivio de una enfermedad,
- diagnóstico, seguimiento, tratamiento, alivio o compensación de una lesión o de una discapacidad,
- investigación, sustitución o modificación de la anatomía o de un proceso o estado fisiológico o patológico,
- obtención de información mediante el examen in vitro de muestras procedentes del cuerpo humano, incluyendo donaciones de órganos, sangre y tejidos,

y que no ejerce su acción principal prevista en el interior o en la superficie del cuerpo humano por mecanismos farmacológicos, inmunológicos ni metabólicos, pero a cuya función puedan contribuir tales mecanismos"[27].

A fin de resolver la incertidumbre sobre los programas informáticos que cabe considerar como productos sanitarios, la Comisión Europea ha publicado varios documentos aclaratorios, como la *Guidance on Qualification and Classification of Software in Regulation* (EU) 2017/745 — *MDR and Regulation (EU) 2017/746 — IVDR* o la segunda versión (diciembre 2022) del *Manual sobre productos frontera y clasificación de productos sanitarios bajo MDR e IVDR*. Si bien estos documentos no tienen valor normativo, pueden resultar muy útiles precisamente en casos en los que la calificación de la *app* como producto sanitario resulta más discutible.

De cualquier forma, parece que, en aplicación del principio de precaución, cabe defender que cuando una *app* o *wearable* incide sobre algún aspecto de salud o recopila datos de salud debe atribuirse, en caso de duda, la condición de producto sanitario. En el ámbito europeo, ello implica la obtención del marcado CE tras demostrar su conformidad ante un Organismo Notificado, lo que exige evaluación clínica y seguimiento clínico postcomercialización. Este modelo ha sido objeto de cuestionamiento tanto por Comités de Bioética[28] como por la doctrina, que debate si estas tecnologías debieran someterse a procesos adicionales de certificación con criterios específicos de validación clínica. Así, Lazcoz sostiene que este modelo europeo resulta insuficiente para hacer frente a los desafíos que plantea la IA en el ámbito de la salud, enfatizando (i) el problema relativo a la protección de datos, dada la ausencia de coordinación y comunicación entre los participantes en las fases de desarrollo (fabricante) e implementación (responsable del tratamiento), y (ii) la ausencia de obligaciones jurídicas con impacto suficiente para complementar las carencias

27 A ello se añade que, de conformidad con el art. 1.2 del Reglamento, las disposiciones establecidas para los productos sanitarios son también aplicables a ciertos grupos de productos (que pueden ser programas informáticos, *apps o wearables*) que, pese a no perseguir fines médicos, aparezcan incluidos en el anexo XVI del Reglamento.

28 *Cfr.* el *Informe 2/2023* del Comité de Bioética de Castilla-La Mancha *sobre la relación clínico-digital*, 31.

de la normativa de protección de datos y garantizar la supervisión humana desde el diseño y desarrollo de los sistemas de IA[29].

Estas mismas conclusiones son predicables del reciente Real Decreto 192/2023, de 21 de marzo, en la medida en que esta norma replica para nuestro ordenamiento lo dispuesto en el citado Reglamento (UE) 2017/745 (al que el Real Decreto remite) y asume igualmente una noción de producto sanitario dependiente de la finalidad identificada por el fabricante. De este modo, la definición de producto sanitario establecida en nuestro ordenamiento permite también teóricamente abarcar algunas aplicaciones digitales de salud mental[30].

Una medida que podría disipar la desconfianza hacia estas *apps* —y propiciar, de este modo, su utilización por profesionales y usuarios— sería su regulación específica tal como se ha hecho en Alemania, donde las DiGA (*digital therapeutics*) cuentan, a partir de la aprobación en 2019 de la Ley de Suministro Digital, con un sistema acelerado de evaluación y reembolso para las *apps* de salud digital. A través de este sistema, las aplicaciones pueden acceder a un sello (*Digitale Gesundheitsanwendungen*) que puede obtenerse en el plazo de tres meses, de manera provisional, debiendo durante los doce meses siguientes reunir las evidencias suficientes para acreditar su eficacia e incorporarse al directorio de DiGA[31]. Esta aprobación permite al médico prescribir la *app* en el marco del seguro público de salud alemán o de su seguro médico privado.

3.2. Un problema regulatorio específico: la protección de datos personales de salud mental

Si bien, como se ha indicado, las *apps* de salud mental tienen una función importante en una sociedad cada vez más demandante de asistencia sanitaria psicológica y psiquiátrica —con el consecuente colapso que tal demanda causa en el servicio público de salud mental—, su uso comporta riesgos éticos y jurídicos. Quizá el más acuciante sea el uso y abuso de los datos de salud mental. De conformidad con lo que el RGPD 2016/679 dispone en el considerando 35 de su exposición de motivos, los datos generados por *apps* de salud mental son datos "relativos a la salud", ya que dentro de estos "se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia (…); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; (…) y cualquier información relativa a (…) enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica *in vitro*".

Ya en su articulado —art. 4.15— el RGPD define los datos de salud como "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud". Estos datos, junto con los referentes al origen étnico, racial, religioso, políticos, filosóficos, relativos a la vida sexual, genéticos y biométricos, constituyen, según el art. 9 del RGPD, "categorías especiales de datos personales". En cuanto tales, el citado artículo prohíbe su tratamiento como regla general, a menos que, como criterio habilitante, concurra el consentimiento informado y explícito del afectado. Este consentimiento informado, por tanto, aparece en el RGPD como el acto reglado que proporciona "licitud de origen" al tratamiento de datos personales de naturaleza sensible[32], siendo el responsable

29 Lazcoz, G. [Publicación en línea] "Sistemas de inteligencia artificial en la asistencia sanitaria: cómo garantizar la supervisión humana desde la normativa de protección de datos". 1-67. 2022. https://www.aepd.es/documento/premio-emilio-aced-2022-guillermo-lazcoz.pdf. [Consulta: 10/01/2024]

30 Navas, S. "Aspectos jurídicos de las aplicaciones móviles de salud (apps sanitarias y wearables)". *Diario La Ley,* 2020 (LA LEY 5811/2020).

31 En este directorio aparecen actualmente medio centenar de aplicaciones inscritas, varias de ellas vinculadas a la enfermedad o bienestar mental (https://diga.bfarm.de/de/verzeichnis).

32 Si bien el art. 9 RGPD enumera cuatro fuentes de legitimación adicionales: la ley; el interés general; la ejecución de un contrato y el interés legítimo del responsable del tratamiento de los datos o de un tercero.

de éste el que debe confirmar su "licitud de ejercicio" observando de modo escrupuloso la ley durante el tratamiento.

Para que este consentimiento sea lícito y, por tanto, posibilite el tratamiento de los datos de salud mental, ha de constituir una manifestación de la voluntad libre, específica, informada e inequívoca por la que el interesado acepta por escrito el tratamiento (arts. 4 y 7 RGPD). Por su parte, para que el tratamiento sea lícito ha de ejercerse teniendo en cuenta tres principios. El primero es el de transparencia (art. 12 RGPD) desarrollado por el GT29 en sus "Directrices sobre transparencia", donde se concibe como obligación global que se proyecta a tres ámbitos fundamentales: 1) al suministro de información al interesado, que en todo caso ha de ser concisa, clara, inteligible y de fácil acceso; 2) al método de comunicación del responsable del tratamiento con el interesado en relación con sus derechos; y 3) al modo en que el responsable del tratamiento facilita que el interesado ejerza sus derechos de acceso, rectificación, limitación, oposición y supresión. El segundo principio es el de seguridad o protección desde el diseño y tiene que aplicarse en concurrencia con el tercer principio que es el de seguridad por defecto. Ambos exigen al responsable del tratamiento determinar desde el comienzo los medios y las medidas técnicas y organizativas apropiadas para aplicar efectivamente los principios de protección de datos, tales como la pseudoanonimización, la minimización de datos e, incluso, el sistema de notificación y evaluación del impacto ante una eventual violación de la seguridad (arts. 25 y 33-35 RGPD). Estos principios de seguridad encarnan la demanda de responsabilidad activa —o proactiva, en términos de la propia AEPD— que ha de mostrar el responsable del tratamiento, sobre todo en relación con la evaluación del posible impacto que el tratamiento pueda tener en los derechos de los afectados[33]. El art. 32 RGPD establece la necesidad de realizar un análisis de riesgos que permita concretar qué medidas (cifrado, pseudoanonimización, nombramiento de delegado de protección de datos, copias de seguridad, etc.) requiere aplicar el servicio digital de salud para prever un nivel de seguridad acorde al tratamiento de una categoría especial de datos, como los de salud mental[34].

En el caso de las *apps,* un análisis de riesgos exhaustivo debe analizar necesariamente la naturaleza de las diferentes fuentes de datos personales de las que se surte el algoritmo. Así, en algunos casos, a la fuente primaria, constituida por los datos de salud *stricto sensu* cedidos directa y activamente por el usuario, puede unirse una fuente subsidiaria que provee de datos de diversa naturaleza que son cedidos de forma "pasiva" aunque consentida. Estos datos secundarios -geolocalización, usos del dispositivo móvil e incluso algún dato biométrico como las modulaciones de la voz- pueden, debidamente combinados, ayudar a los facultativos a realizar un mejor diagnóstico. Sin embargo, en atención al principio de minimización —art. 5.1 RGPD— los datos recabados para cualquier tratamiento tienen siempre que ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Si bien más datos suponen mayor riesgo, este podría asumirse siempre que en el tratamiento se cumplan las exigencias de la *Guía de Privacidad desde el diseño* de la AEPD de octubre de 2019. La primera es la información detallada al usuario sobre los tipos de datos de los que se va a valer el algoritmo para elaborar su diagnóstico. La segunda es la "poda" o eliminación parcial de los datos personales que ya no son necesarios, lo que supone determinar de antemano el periodo de conservación de algunos datos personales. Y, en tercer lugar, la eliminación definitiva de los datos una vez hayan dejado de ser relevantes, garantizando que no es posible su recuperación ni siquiera de las copias de seguridad realizadas.

El deber de informar al usuario también es exigido por las *Directrices específicas para apps* de la AEPD como una de las medidas de responsabilidad activa dirigidas al responsable del tratamiento. Este ha de informar al

33 De Lecuona, I. "El valor y el precio de los datos personales de salud en la sociedad digital", en *El cuerpo diseminado. Estatuto, uso y disposición*, García, R. (Coord.), Aranzadi, Pamplona, 2018, 171-189.

34 Rodríguez, J.F. "La disrupción tecnológica en el ámbito sanitario europeo: implicaciones de la telemedicina pública en la protección de datos de los pacientes", *Cuadernos Europeos de Deusto*, 2023; 69, 51.

usuario sobre la política de privacidad de la *app* tanto en la aplicación como en la *app store*, evitando además contradicción entre ambas. El acceso a la información debe ser sencillo y la información debe ser completa, clara y concisa para evitar la "fatiga informativa", lo que se consigue con el suministro de "información por capas"[35]. En esta información debe constar, en todo caso, el tipo de tratamiento que se va a dar a los datos personales —pseudoanonimización o codificación alfanumérica de los datos— qué datos son básicos y, por tanto, son obligatorios, y qué datos son opcionales. El consentimiento informado prestado en la *app* tiene que ser granular, es decir, la gestión de los permisos de acceso a la información personal debe hacerse de forma selectiva e independiente para cada tratamiento y finalidad a la que esté destinada dicha información.

Por otro lado, como ya se advirtió, es indispensable distinguir entre las *apps* de salud móvil que pertenecen a dispositivos médicos y las que no, pues las implicaciones son diferentes. En el primer caso estaríamos en realidad ante un uso de lo que se ha dado en llamar "teleasistencia" o "telemedicina", a través de la que el usuario, tras haber respondido un cuestionario previo, puede ser derivado a un terapeuta que le proporcionará un diagnóstico personalizado. En este supuesto será preciso redactar una política de privacidad que, contenida en la *app* descargada, proporcione, con carácter previo al consentimiento del interesado, una explicación minuciosa de los datos personales a tratar, la/s finalidad/es perseguidas, la posible cesión a terceros (donde cabe incluir a todos los que gestionan los servicios auxiliares recogidos en la plataforma) o, entre otros, los derechos que amparan al paciente, para garantizar, en definitiva, un tratamiento lícito, transparente, seguro, coherente, temporal y responsable de la información obtenida[36].

En el caso de aplicaciones no médicas, en realidad nos hallamos ante el uso de *chatbots* que simulan una asistencia personalizada al entablar una conversación con el usuario, a través de la que proporcionan consejos o pautas de vida saludable, sin ulterior derivación a un facultativo. No obstante, ya se ha advertido que, en atención al Anexo XVI del Reglamento 2017/745, un programa informático sin finalidad médica —es decir, cuyo uso no constituya parte integrante de un tratamiento médico *stricto sensu*— puede considerarse incluido en el listado de productos sanitarios. De ahí que, como recoge también el RD 192/2023, su diseño y comercialización deban cumplir una serie de requerimientos legales, incluso aunque cuenten con medidas de autorregulación. El desarrollador del *software*, por tanto, deberá poder garantizar la satisfacción de la evaluación clínica, así como la adopción de las medidas legales exigidas a fin de proteger debidamente los datos almacenados en la *app*, sobre todo ante un eventual hackeo. De ahí la importancia del puntual cumplimiento del principio de seguridad desde el diseño establecido en el RGPD, incluso si la información sanitaria no va a transferirse fuera de la propia *app*.

Es posible, por otra parte, que los datos de salud mental derivados del uso de una *app* no se pongan en conocimiento de ningún facultativo vinculado con la *app*, pero sí se den a conocer al empleador del usuario si dicha *app* ha sido promovida o facilitada en el entorno laboral al amparo de un plan de salud o bienestar laboral. En este caso, la Ley 3/2018, de Protección de datos personales y derechos digitales, señala en su art. 87.3 que "los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente". Prosigue el artículo afirmando que "el acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados. Los trabajadores deberán ser informados de los criterios de utilización a los que se

35 Este tipo de información consiste en presentar una información básica en primer lugar, de forma resumida o concisa y, después, remitir a la información adicional, en un segundo nivel, donde se presentará detalladamente el resto de la información exigida (*Guía para el cumplimiento del deber de informar de la AEPD*).

36 Rodríguez, J. F., *op. cit.,* 49.

refiere este apartado". En el mismo sentido, el art. 20 bis del Estatuto de los Trabajadores reconoce el derecho de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión, afirmando que "tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

Por último, requiere también regulación específica por su potencial riesgo para el usuario de *apps* de salud mental la práctica de lo que se ha dado en llamar *profiling* y que se produce en el marco de la eventual relación comercial entre desarrolladores de *apps* de salud mental y *data brokers*, empresas que se dedican a comprar datos y venderlos a terceros. A este esquema suelen responder los servicios en línea gratuitos, cuyo modelo de negocio consiste en elaborar perfiles de usuarios con la finalidad de dirigirles publicidad personalizada[37]. Si este modelo de negocio se extiende a datos de salud mental, el riesgo aumenta significativamente. En el mercado de la información, los datos sanitarios son el "nuevo oro", pues "adquieren valor por la información que aportan *per se* y por aquella que se puede desentrañar; lo cual nos enfrenta con situaciones en las que lejos de ser utilizados para el bien común, se instrumentalizan para obtener el máximo rendimiento económico, persiguiendo intereses con fines de lucro vestidos de innovación e investigación"[38]. Los arts. 22.1 y 22.4 RGPD reconocen el derecho a no ser objeto de decisiones automatizadas, incluido el perfilado, si este tiene o puede tener consecuencias jurídicas para el sujeto afectado, sobre todo si el perfil se crea a partir de datos sensibles. Solo si concurre consentimiento del afectado o un interés público esencial podrá realizarse un perfilado con datos personales de salud. No obstante, esta limitación no parece muy garantista si se atiende al automatismo con el que la mayoría de usuarios de servicios en línea y *apps* prestan consentimiento para el tratamiento de sus datos personales. Tampoco una prohibición general de elaborar perfiles sensibles —por ejemplo, sanitarios— supondría una garantía efectiva para la privacidad, pues, como se ha advertido, a través de la aplicación de técnicas de *big data* pueden inferirse datos sensibles y, por consiguiente, perfiles sensibles, de datos que *a priori* no lo son.

3.3. Riesgos jurídico-penales asociados a las apps *de salud mental*

En los apartados anteriores se han explorado algunos aspectos de las *apps* de salud mental sobre los que se proyecta el ordenamiento jurídico. Esa proyección no ha sido, como se ha podido ver, el resultado de una regulación diferenciada de este fenómeno, sino la consecuencia de la extensión al mismo de normas preexistentes de carácter genérico. Esta última posibilidad, como se indicará a continuación, concurre también en la esfera del Derecho penal.

Así sucede, desde un primer momento, con el propio diseño de estas herramientas, ya que, toda vez que ciertos elementos de las *apps* pueden constituir obras originales amparadas por la legislación de propiedad intelectual e industrial —como el propio *software*[39] o los contenidos creativos, tales como logotipos, iconos, fuentes o imágenes de marca, integrados en la interfaz gráfica de usuario[40]—, la infracción de derechos otorgados por aquella puede adquirir relevancia penal. Y aun cuando el algoritmo subyacente a la herramienta queda, en principio, extramuros de esta normativa, ello no entraña que carezca por completo de protección. A tal efecto, si goza de valor empresarial real o potencial y es además secreto (no es "generalmente conocido por personas pertenecientes a los círculos en que normalmente se utilice el tipo de información o conocimiento en cuestión, ni fácilmente accesibles para ellas"), reúne los requisitos para acceder a la tutela de la Ley 1/2019 de

37 Hernández, J. A. "Expectativas de privacidad, tutela de la intimidad y protección de datos", en *Sociedad digital y Derecho*, De la Cuadra, T. y Piñar, J., L. (Dir.), B.O.E. y RED.ES, Madrid, 2018, 279-300.

38 De Lecuona, I., *op. cit.,* 173.

39 Aparicio, J.P. "Derecho de autor y más allá: algoritmos, código de los programas de ordenador y apps". *Pe. i. revista de propiedad intelectual*, 2022; 71, 13-98.

40 Gubby, H., Klaus., J. & Van Nootwijk, K. "Intellectual Property and the Protection of Apps in the European Union". *European Journal of Law and Technology*, 2020; 11(3), 1-17.

Secretos Empresariales[41]. De este modo, tanto los delitos relativos a la propiedad intelectual e industrial tipificados en los arts. 270 y ss. CP como los de descubrimiento de secreto de empresa de los arts 278 y ss. CP pueden ser aplicables ante la vulneración de estos derechos entre competidores en el mercado de la salud mental digital.

También pueden adquirir relevancia penal, por otro lado, comportamientos relativos a las condiciones de prestación del servicio de salud mental digital. Así, en tanto que tal servicio pueda considerarse como actividad sanitaria psicológica o psiquiátrica (promoción, prevención, diagnóstico, tratamiento o rehabilitación, dirigidas a fomentar, restaurar o mejorar la salud mental), quienes lo brindan a través de la *app* deben satisfacer los requisitos legales exigidos para el ejercicio de la profesión. Si no es el caso, la realización de actos propios de la profesión sin el correspondiente título académico expedido o reconocido en España podría ser constitutiva de un delito de intrusismo del art. 403 CP, sin que el hecho de que tal actividad esté mediada por una aplicación digital obstaculice tal calificación. Otra dimensión de la prestación del servicio en la que pueden manifestarse riesgos penales es la relativa a la tutela de la privacidad. A este respecto, como se expuso en el apartado anterior, en cuanto recopilan información personal relativa a la salud y detalles del tratamiento dispensado, las *apps* de salud deben cumplir con las normas de protección de datos, lo que determina que, con carácter general, su tratamiento se supedite al consentimiento explícito del usuario del servicio[42]. Naturalmente, esta conclusión es predicable de las *apps* de salud mental; por ello, la captación no autorizada de datos reservados por parte de estas *apps* puede alcanzar relevancia penal en virtud de lo dispuesto en los arts. 197 y ss. CP, afirmación que cabe extender al acceso no autorizado a tales datos, así como a su difusión, revelación, cesión y modificación o utilización en perjuicio de tercero.

En un último orden de cosas, cabe explorar en qué medida el funcionamiento inadecuado de una *app* de salud mental puede causar daños de distinto tipo a sus usuarios que, de ser atribuibles a una conducta dolosa o negligente, puedan generar responsabilidad legal. En particular, no es descartable que, a resultas de errores diagnósticos, prescripción de tratamientos inadecuados, incumplimiento de deberes de seguimiento adecuado o de otros estándares profesionales, o, en general, de supuestos de atención deficiente, puedan llegar a producirse perjuicios a la salud mental del usuario. Ciertamente, tanto la existencia como la atribución de esa responsabilidad legal presenta dificultades específicas al prestarse el servicio de salud mental de forma telemática. Entre ellas pueden destacarse: (i) problemas de imputación objetiva de resultados lesivos, sobre todo cuando la producción del daño se deriva de forma cumulativa tanto de las indicaciones suministradas por la *app* como de la conducta del propio paciente; (ii) dificultades de individualización de la responsabilidad entre programador y comercializador (sobre todo, ante *apps* que actúan de forma autónoma o no supervisada) y, en su caso, de operadores de la aplicación en el caso de que ésta actúe de forma parcialmente supervisada; y (iii) la complejidad de determinación del contenido exacto de lo que constituye buena y mala praxis en el seno de una actividad regulada aún de forma fragmentaria. De producirse daños de este cariz, no es impensable que a la responsabilidad civil se pueda sumar una responsabilidad penal si los resultados imputables al funcionamiento perjudicial de la *app* son de muerte (arts. 138, 142 y 143 CP) o efectivo menoscabo de la salud mental (arts. 147 CP y 152 CP). Y, como siempre que se contemplan eventos lesivos que pueden dar lugar a responsabilidad civil, surge una complejidad adicional: la posibilidad de mitigar el riesgo mediante la cobertura del seguro.

Sin embargo, aunque se trata de figuras delictivas incorporadas expresamente para atajar la difusión de contenidos nocivos para la salud a través de tecnologías de la información, es difícil que resulten aplicables a estas herramientas digitales los delitos tipificados en los arts. 143 bis, 156 ter y 361 bis CP. Y ello, aunque pudiera

41 Aparicio, J.P., *op. cit,,* 13-98, quien entiende que también puede ser tutelable a través del Derecho de autor.

42 Hidalgo, A. "IntimidAPP: Los problemas del tratamiento de datos biosanitarios en wearables y apps para móviles". *Revista de Derecho y Genoma Humano*, 2019; nº extra, 449-483, y Soto, Y. "Datos masivos con privacidad y no contra privacidad". *Revista de Bioética y Derecho*, 2017: 40, 101-114.

acreditarse que el uso de una *app* de salud mental ha conducido al usuario al suicidio, a la producción de autolesiones o a prácticas alimentarias peligrosas, ya que los preceptos citados exigen taxativamente que el contenido de la aplicación digital esté "específicamente destinado a promover, fomentar o incitar" tales resultados, lo que complica de modo significativo la verificación de esta hipótesis.

Por el contrario, como se ha expuesto antes, la definición de producto sanitario que aparece en el Real Decreto 192/2023 y el Reglamento (UE) 2017/745 puede comprender algunas *apps* de salud mental, lo que obliga a plantearse la operatividad de los delitos contra la salud pública (no ya sólo la personal) de los arts. 359 y ss. CP. Tal es el caso, en particular, de los incriminados en los arts. 361 y 362 CP, dado que estos identifican como posible objeto material no sólo una sustancia o medicamento, sino justamente productos sanitarios. Así las cosas, la producción y comercialización de *apps* de salud mental sin conformidad de la documentación con la normativa o con incumplimiento de exigencias técnicas legales podría dar lugar a la comisión de un delito del art. 361 CP en el caso de que se generara riesgo para la vida o la salud. Si se produce este resultado de peligro, también adquirirían relevancia penal actuaciones próximas al fraude de consumidores (explotar el producto presentando engañosamente datos relevantes sobre origen, cumplimiento de requisitos, historial, etc.) tipificadas en los arts. 362 y ss. CP[43].

Los efectos nocivos de las *apps* de salud mental para el patrimonio de los usuarios pueden generar respuestas adicionales. Así, en tanto que aquellas implican la prestación de un servicio profesional que puede estar remunerado (cuando la aplicación es de pago), si tal servicio no se ajusta a los estándares de calidad anunciados, puede surgir, cuando menos, responsabilidad civil contractual[44]. Si, además, se satisface el elemento típico del engaño bastante, la conducta podría ser constitutiva de delito —leve, en principio— de estafa (art. 248 CP) o publicitario (art. 282 CP).

La viabilidad de calificar estos comportamientos como infracciones penales no garantiza su persecución efectiva, pues, dado que el servicio de salud mental digital puede ser accesible en distintas jurisdicciones, cada una con su marco regulatorio, los problemas legales indicados pueden presentarse de forma desigual en cada territorio. Esta circunstancia genera también problemas de competencia jurisdiccional, toda vez que el hecho se puede cometer en un punto geográfico diferente tanto del lugar donde se halla el medio comisivo como de aquel donde se manifiesta su resultado. Como norma general, en España se aplica la teoría de la ubicuidad, es decir, el delito se entiende cometido tanto donde se realiza la acción como donde se producen sus efectos (esto es, en toda jurisdicción en la que se haya verificado algún elemento típico).

43 Andrés, A.C. "Los delitos farmacológicos", en *Medicamentos, productos sanitarios y protección del consumidor*, Juberías, A. (Coord.), 2017, Reus, Madrid, 179-196.

44 Molina, A. & Juberías, A. "Producto sanitario defectuoso", en *Medicamentos, productos sanitarios y protección del consumidor*, Juberías, A. (Coord.), 2017, Reus, Madrid, 155-177.

Contribución de los autores y agradecimientos

Los cuatro coautores son corresponsables en la misma medida de la conceptualización, metodología, redacción original, revisión y edición del texto. Su elaboración ha tenido lugar en el seno de la Cátedra de Innovación y Salud Mental Digital de la Universidad Pontificia Comillas, cuyo apoyo agradecemos.

Referencias

Alcalde, G. y Alfonso, I. (2019). Utilización de tecnología Big Data en investigación clínica. *Rev Der Gen H*., nº. extra, 55-83.

Alós, F. y Puig-Ribera, A. (2021). Uso de wearables y aplicaciones móviles (mHealth) para cambiar los estilos de vida desde la práctica clínica en Atención Primaria: una revisión narrativa. *Atención Primaria Práctica*., 3(1), 1-5

Andrés, A.C. (2017). Los delitos farmacológicos. Juberías, A. (Coord.) *Medicamentos, productos sanitarios y protección del consumidor*, Reus, Madrid, 179-196.

Aparicio, J.P. (2022). Derecho de autor y más allá: algoritmos, código de los programas de ordenador y apps. *Pe. i. revista de propiedad intelectual* (71), 13-98.

Cabitza, F., Ciucci, D. y Rasoini, R. (2019) A Giant with Feet of Clay: On the Validity of the Data that Feed Machine Learning in Medicine,, en *Organizing for the Digital World: IT for Individuals, Communities and Societies*, Cabitza, F. *et al*. (eds.), Springer, Cham, 121-136.

Data-Franco, J. y Berck, M. (2012) The nocebo effect: A clinicians guide. *Australian & New Zealand Journal of Psychiatry*, 7(6), 617-623.

De Lecuona, I (2018). El valor y el precio de los datos personales de salud en la sociedad digital, en García, R. (Coord.) *El cuerpo diseminado. Estatuto, uso y disposición*, Aranzadi, Pamplona, 171-189.

Emanuel, E.J. y Emanuel, L.L. (1992) Four models of the physician-patient relationship. *JAMA: The Journal of the American Medical Association*, 267, 2221–2226.

Gubby, H., Klaus., J. & Van Nootwijk, K. (2020). Intellectual Property and the Protection of Apps in the European Union. *European Journal of Law and Technology*, 11(3), 1-17.

Häuser, W., Hansen, E. y Enck, P. (2012) Nocebo phenomena in medicine: their relevance in everyday clinical practice. *Dtsch Arztebl Int*, 109(26), 459-465.

Hayoung, B., Hyemin, S., Han-Gil, J., Jun Soo, K., Hyungsook, K., y Ji-Won, H. (2023) App-Based Interventions for Moderate to Severe Depression. A Systematic Review and Meta-Analysis. *JAMA Network Open*, 6(11), 1-14.

Hernández, J. A. (2018), Expectativas de privacidad, tutela de la intimidad y protección de datos, en De la Cuadra, T. y Piñar, J.L. (Dir.), *Sociedad digital y Derecho*, B.O.E. y RED.ES, Madrid, 279-300.

Hidalgo, A. (2019). IntimidAPP: Los problemas del tratamiento de datos biosanitarios en wearables y apps para móviles. *Rev Der Gen H.,* nº ext., 449-483.

Lazcoz, G. (2022) [P. en línea] *Sistemas de inteligencia artificial en la asistencia sanitaria: cómo garantizar la supervisión humana desde la normativa de protección de datos*, 1-67. https://www.aepd.es/documento/premio-emilio-aced-2022-guillermo-lazcoz.pdf [Consulta: 10/01/2024]

Lupton, D. (2016). *The quantified self*. Polity Press, Cambridge.

Martínez, R. (2017). Big data, investigación en salud y protección de datos personales ¿Un falso debate? *Revista Valenciana d'Estudis Autonòmics,* 62, 235-280.

Mittelstadt, B. (2021). *The impact of artificial intelligence on the doctor-patient relationship,* Consejo de Europa.

Molina, A. & Juberías, A. (2017). Producto sanitario defectuoso, en Juberías, A. (Coord.) *Medicamentos, productos sanitarios y protección del consumidor*, Reus, Madrid, 155-177.

Navas, S. (2020). Aspectos jurídicos de las aplicaciones móviles de salud (apps sanitarias y wearables). *Diario La Ley* (LA LEY 5811/2020).

Pellegrino, E.D. y Thomasma, D.C. (1993) *The Virtues in Medical Practice*. Oxford U. Press, Nueva York.

Prainsack, B. (2020). The political economy of digital data. *Policy Studies*, 41(5), 439-446.

Rodríguez, J.F. (2023). La disrupción tecnológica en el ámbito sanitario europeo: implicaciones de la telemedicina pública en la protección de datos de los pacientes, *Cuadernos Europeos de Deusto*, 69, 28-55.

Romeo, C.M. (2019). Revisión de las categorías jurídicas de la normativa europea ante la tecnología del big data aplicada a la salud. *Rev Der Gen H.*, nº. extra, 85-127.

Royo-Bordonada, M. y Román-Maestre, B. (2015) Towards public health ethics. *Public Health Reviews*, 36(3), 1-15.

Schweiger, A. y Parducci, A. (1981) Nocebo: the psychologic induction of pain. *The Pavlovian journal of biological science*, 16(3), 140-143.

Soto, Y. (2017). Datos masivos con privacidad y no contra privacidad. *Revista de Bioética y Derecho*, 40, 101-114.