

**LA DISRUPCIÓN TECNOLÓGICA EN EL ÁMBITO SANITARIO
EUROPEO: IMPLICACIONES DE LA TELEMEDICINA PÚBLICA
EN LA PROTECCIÓN DE DATOS DE LOS PACIENTES¹**

**TECHNOLOGICAL DISRUPTION IN EUROPEAN
HEALTHCARE: IMPLICATIONS OF PUBLIC TELEMEDICINE
FOR THE PROTECTION OF PATIENTS' DATA**

JUAN FRANCISCO RODRÍGUEZ AYUSO

Profesor Ayudante Doctor (acreditado a Profesor Contratado Doctor) de Derecho Administrativo
Coordinador Académico del Grado en Ciencias Jurídicas de las Administraciones Públicas
Universidad Nacional de Educación a Distancia (UNED)
jfrodriguez@der.uned.es

¹ Este trabajo ha sido realizado en el marco del Proyecto de Investigación “Nuevos retos en materia de protección de datos y de derechos digitales y efectos ante la crisis global propiciada por el COVID-19: análisis multidisciplinar” (DERPRODAT), de la Universidad Internacional de La Rioja, donde intervengo como Investigador Principal. También es fruto de la labor realizada en el seno del Grupo de Investigación “Derecho Público y Nuevas Tecnologías” (PUBLITECH), de la Universidad Internacional de La Rioja, donde intervengo como Director.

Sumario: I. Introducción.—II. El impacto de los avances tecnológicos en el ámbito sanitario: la telemedicina. 1. Concepto y principales manifestaciones. 2. Las plataformas digitales como actores esenciales en la intermediación de servicios de medicina a distancia. 3. Marco jurídico aplicable.—III. La telemedicina y la protección de datos personales. 1. El refuerzo en la protección de categorías especiales de datos personales: el caso de los datos de salud. 2. El consentimiento como base de legitimación esencial en el tratamiento de datos sanitarios y especialidades del principio de limitación de la finalidad para un tratamiento seguro de la información.—IV. Conclusiones.—V. Referencias bibliográficas.

Resumen: El presente trabajo de investigación indaga en torno a la noción y naturaleza jurídica de la telemedicina como servicio de intermediación en línea que, merced a la configuración de aplicaciones móviles implementadas por plataformas digitales, posibilita la prestación telemática del derecho de los pacientes a ser atendidos sanitariamente. Fruto de este análisis, se propone una aproximación al marco normativo aplicable, sobre la base de la necesaria distinción entre el servicio médico prestado y el medio virtual a través del cual se presta, fundamental para indagar en el entramado legal y la ferviente multiplicación de reglas orientadas a disciplinar figuras, como esta, surgidas al amparo de las TIC. Finalmente, se aborda una cuestión no menos relevante: la implicación que este tratamiento masivo de información altamente sensible tiene en el derecho fundamental de los interesados a la protección de sus datos, siendo preciso atender a aspectos tan importantes como la propia noción de datos de salud, la regla que prohíbe su tratamiento, la relevancia que presenta el consentimiento del paciente como elemento habilitador del mismo, los fines perseguidos por las apps de eHealth o las medidas a adoptar para garantizar una seguridad acorde al elevado riesgo que conllevan este tipo de operaciones.

Palabras clave: telemedicina; servicio de intermediación en línea; plataforma digital; datos personales de salud; eHealth

Abstract: This research work investigates the notion and legal nature of telemedicine as an online intermediation service which, thanks to the configuration of mobile applications implemented by digital platforms, makes possible the telematic provision of patients' right to health care. As a result of this analysis, an approach to the applicable regulatory framework is proposed, based on the necessary distinction between the medical service provided and the virtual medium through which it is provided, which is fundamental to investigate the legal framework and the fervent multiplication of rules aimed at disciplining figures, such as this one, that have arisen under the protection of ICTs. Finally, a no less relevant issue is addressed: the implication that this massive processing of highly sensitive information has on the fundamental right of the interested parties to the protection of their data, and it is necessary to address such important aspects as the

very notion of health data, the rule that prohibits its processing, the relevance of patient consent as an enabling element, the purposes pursued by eHealth apps or the measures to be adopted to guarantee security in accordance with the high risk involved in this type of operation.

Keywords: telemedicine; online brokering service; digital platform; personal health data; eHealth; eHealth

I. Introducción

La firme consolidación de lo que, no sin amplias confusiones y fuertes imprecisiones terminológicas, ha dado a conocerse como “sociedad de la información”² supone un dinamismo sin precedentes. En efecto, los avances tecnológicos, de todo tipo y entidad, han determinado una evolución constante, tanto más, vertiginosa, que ha tenido su plasmación en todos los órdenes principales del desenvolvimiento relacional de los individuos.

Sobre la base de esta afirmación, nada puede extrañar al constatar la dimensión que, en el ámbito médico, ha propiciado esta virtualización, posibilitando formas, hasta ahora inimaginables, de obtención masiva de datos y de procesamiento lógico y tratamiento inteligente de los mismos³. Estamos, pues, en presencia de la eSalud (o, en inglés, *eHealth*), que, como sostiene la doctrina, alude «[...] al conjunto de recursos y cuidados de salud que se llevan a cabo por medios electrónicos, esto es, mediante la aplicación de las TICs (Tecnologías de la Información y Comunicación) como herramienta en el entorno sanitario, tanto en materia de prevención, diagnóstico, tratamiento o seguimiento, como también en la gestión de la salud»⁴, procurando incrementar, de forma cuantitativa

² Definida, en los orígenes de su nacimiento, como aquella sociedad «[...] que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material» [Yoneji Masuda, *The information society as post-industrial society* (New Brunswick: Transaction Publishers, 1980), 14], pronto se advierte la relevancia que, para el tratamiento y difusión de la información, tendrá el avance, impulso y consolidación paralelos de las Nuevas Tecnologías de la Información y de la Comunicación, elemento inmaterial fundamental que, amén de dar nombre a este nuevo modelo de sociedad, determina y condiciona su funcionamiento.

³ María Falcón Romero y Aurelio Luna Ruiz-Cabello. «Las aplicaciones móviles en el ámbito sanitario. Consideraciones éticas y legales», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 15; Miguel Martínez Muñoz. «Los sujetos especialmente vulnerables ante los nuevos derechos digitales en el ámbito del consumo», en *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, ed. por Juan Francisco Rodríguez Ayuso (Cizur Menor: Aranzadi, 2022), 549-573.

⁴ María Nélida Tur Fernández. «E-salud, derecho a la información y consentimiento informado», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 33. En la misma línea, Organización Mundial de la Salud, *Perfiles de países de Atlas eSalud: basados en los resultados de la segunda encuesta mundial sobre salud electrónica* (Ginebra: WHO Library Cataloguing-in-Publication Data, 2010).

y cualitativa, los niveles de atención prestacional merced a las bondades que brinda el entorno virtual⁵.

Más concretamente, y dentro de ella⁶, hemos de poner en el foco en el marco de la asistencia médica, tradicionalmente configurada como una relación presencial y de confianza entre el paciente y el especialista (que basaba su diagnóstico en el empleo de métodos tradicionales de recogida de información, como la auscultación, la anamnesis o la exploración) y que, en este nuevo contexto, se abre a grandes retos y desafíos (motivados, en parte, por las extraordinarias oportunidades que brindan técnicas como la Inteligencia Artificial y el empleo de algoritmos inteligentes en la atención, detección y predicción de enfermedades), pero también a importantes riesgos y amenazas, económicos, sociales, éticos o jurídicos, que un uso inadecuado de tan poderosos instrumentos puede traer consigo.

Las cuestiones a abordar, como se puede observar, son amplias y vienen condicionadas por una multiplicidad de factores (verbigracia, heterogeneidad cultural, desigual nivel formativo, especificaciones técnicas de las aplicaciones implementadas, exposición de la información). Empero, de todas ellas, resultan especialmente significativas, huelga decirlo, aquellas que suponen una mayor incidencia en los derechos fundamentales de los afectados, como el relativo a su privacidad, motivo por el que, a lo largo de las próximas líneas, trataremos de delinear, razonadamente, los contornos esenciales que nos permitan arrojar conclusiones certeras en torno a la plausibilidad de estas medidas en el campo de la telemedicina pública, a la vista de las competencias que tiene el Estado, las Comunidades Autónomas y los Entes locales en materia de sanidad.

II. El impacto de los avances tecnológicos en el ámbito sanitario: la Telemedicina

1. Concepto y principales manifestaciones

La telemedicina puede ser definida, siguiendo las palabras de la Organización Mundial de la Salud (en adelante, OMS), como «[...] la prestación de servicios de atención de la salud, donde la distancia es un factor crítico, por todos los profesionales de la salud que utilizan tecnologías de la información y de la comunicación para el

⁵ Gabriel Eisenbach, «What is health?», *The journal of medical Internet research*, n.º 3 (2001): 1-20. A su vez, cuando la eHealth se sirve de la tecnología móvil, personificada en teléfonos inteligentes o *smartphones*, podemos hablar de *mHealth* o salud móvil [Marcial García Rojo, «mHealth (Salud móvil)», *I+S: Revista de la Sociedad Española de Informática y Salud*, n.º 110 (2015): 6-7].

⁶ La asistencia médica directa y virtual forma parte de la eSalud, que también comprende las técnicas de digitalización de registros médicos y de información sanitaria, haciéndolos interoperables; la telesalud, como término más amplio; la labor pedagógica que, sobre esta materia, se puede impartir a la ciudadanía, o el e-commerce, cuando aglutina productos y/o servicios relacionados con el cuidado y mantenimiento de la salud [Organización Mundial de la Salud, *eSalud: analizarán la aplicación de las tecnologías de la información y comunicación en la atención de la salud* (Ginebra: WHO Library Cataloguing-in-Publication Data, 2012)].

intercambio de información válida para el diagnóstico, tratamiento y prevención de enfermedades y lesiones, la investigación y la evaluación, todo en aras de avanzar en la salud de los individuos y sus comunidades»⁷; estamos, en otras palabras, ante un conjunto integral de comunicaciones que, integradas virtualmente, posibilitan atender remotamente a todo aquel que así lo necesite⁸. Vemos, por tanto, que la telemedicina alude específicamente a la atención sanitaria de forma virtual y remota, frente al concepto, más aglutinador, de la eSalud⁹.

Bajo el término de telemedicina podemos incluir servicios de seguimiento sanitario del paciente, donde se subsume la petición, sincrónica o diacrónica, de diagnósticos o consejos médicos, sea cual fuere el medio de comunicación empleado para poder llevarlos a cabo. También la teleasistencia, que, como su propio nombre indica, permite al profesional sanitario desarrollar funciones de soporte y valorar a distancia al paciente desde su propio hogar y bajo su propia responsabilidad, o la telemonitorización o televigilancia, cuando el cuidado de los interesados se produce a través de dispositivos electrónicos que recaban datos que se transfieren ulteriormente a un equipo remoto que la hace inteligible, minorando los períodos de estancia en los centros sanitarios. Por último, nada impide agrupar, dentro de esta noción, la asistencia coordinada y a distancia que puedan llegar a realizar los sanitarios cuando las circunstancias así lo requieran¹⁰.

Tal y como se anticipaba, a modo de introito, al inicio del presente estudio, la potencialidad transformadora que la evolución digital trae consigo conforma un mundo líquido¹¹, en permanente cambio y plagado de bondades, pero también de amenazas. Las técnicas de Inteligencia Artificial son una clara muestra de ello.

Concebida como aquella vertiente de la informática centrada en el estudio y desarrollo de sistemas susceptibles de llevar a cabo actividades propias de la inteligencia

⁷ World Health Organization, *Telemedicine: opportunities and developments in Member States* (Ginebra: WHO Library Cataloguing-in-Publication Data, 2010), 8.

⁸ Francesca Ferretti y María Paola Nico. «Telemedicina y responsabilidad civil», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 155-184.

⁹ Javier Sánchez Caro. «Telemedicina», en *Enciclopedia de Bioderecho y Bioética*, ed. por Carlos María Romeo Casabona (Granada: Comares, 2011); Javier Sánchez Caro y Fernando Abellán-García Sánchez. *Telemedicina y protección de datos sanitarios: aspectos legales y éticos* (Granada: Comares, 2002); Pilar Nicolás Jiménez. «Medicina personalizada de precisión y diagnóstico genético», en *Manual de Bioderecho (adaptado a la docencia en ciencias, ciencias de la salud y ciencias sociales y jurídicas)*, ed. por Carlos María Romeo Casabona, Pilar Nicolás Jiménez y Sergio Romeo Malanda (Madrid: Dykinson, 2022), 309-331.

¹⁰ Sandra Ferrer Gelabert. «E-salud: la tecnología al servicio de la salud», en *E-Salud, autonomía y datos clínicos. Un nuevo paradigma*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2021), 18.

¹¹ Zygmunt Bauman, *Tiempos líquidos. Vivir en una época de incertidumbre* (México D.F.: Tusquets Editores, 2007), 17.

humana, en particular, la capacidad de comportarse autónomamente¹², la Inteligencia Artificial ha promovido el progreso de la Medicina en los últimos años. Véase, por ejemplo, la creación de robots que actúan de manera autónoma o dirigida o la creación de dispositivos que facilitan y mejoran el diagnóstico o asisten en la movilidad, susceptibles, todos ellos, de concluir, técnica y mecánicamente, análisis cada vez más completos y complejos y en un menor período de tiempo.

Ahora bien, una valoración realista de estas herramientas de aprendizaje inteligente (donde se integrarían otras técnicas, como el *machine learning* o el *Internet of Things*, ambos sustentados en el empleo sistemático y a gran escala -*Big Data*- de datos, personales y no personales, capaces de extraer secuencias que nos permiten arrojar conclusiones lógicas, masivas e inmediatas en la toma de decisiones) exige, a la vez, tomar en consideración una serie de riesgos o amenazas que ponen de manifiesto, entre otras cuestiones, la necesidad de reforzar el nivel formativo y las habilidades técnicas que habrán de adquirir los especialistas sanitarios que, en mayor o menor medida, deberán ponerlas en valor. Asimismo, en el centro del sistema habrá que situar al paciente, deliberadamente empoderado, a fin de evitar su exclusión en todas aquellas decisiones que, de forma mediata o inmediata, conciernan a su estado, físico y/o mental¹³.

Todo ello pasa, necesariamente, por la necesidad de procedimentar reglas y protocolos que, amparados en una adecuada estructura clínica y jurídica, posibiliten esta práctica sanitaria virtual, sin que, por ello, sufran menoscabo aspectos como la intimidad, la confidencialidad, el secreto de las comunicaciones o, como no, el derecho fundamental de los interesados a la protección, adecuada y suficiente, de sus datos de carácter personal¹⁴.

2. *Las plataformas digitales como actores esenciales en la intermediación de servicios de medicina a distancia*

Como hemos podido observar hasta ahora, la prestación de servicios sanitarios de forma digital y no presencial se encuadra dentro de la categoría, ciertamente más amplia y aglutinadora, de “servicios de la sociedad de la información” (también denominados, a veces induciendo al error, “servicios digitales”, “servicios en línea” o “servicios prestados a través de Internet”). Integran este espacio todos aquellos servicios que, de forma

¹² Al respecto, José Vida Fernández. «Los retos de la regulación de la Inteligencia Artificial: algunas aportaciones desde la perspectiva europea», en *Sociedad digital y Derecho*, ed. por Tomás de la Quadra Salcedo y José Luis Piñar Mañas (Madrid: Ministerio de Industria, Comercio y Turismo, 2018), 2063-207.

¹³ Ana Isabel Herrán Ortiz. «Inteligencia Artificial, salud y Derechos Humanos: ¿hacia un gobierno de los algoritmos?», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 298-299. En la misma línea, Julián Valero Torrijos. «Los derechos en la era digital», en *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, ed. por Juan Francisco Rodríguez Ayuso (Cizur Menor: Aranzadi, 2022), 25-45.

¹⁴ Beatriz Pascual de la Pisa, María José García Lozano y Juan González Lama, «Aspectos legales de la telemedicina», *FMC: Formación Médica Continuada en Atención Primaria*, n.º 10 (2021): 546-547.

acumulada, cumplan cuatro características básicas: en primer lugar, que se presten, de forma habitual (por lo que admite excepciones), a cambio de una contraprestación (las aplicaciones que permiten la práctica de la telemedicina son, a menudo, onerosas); en segundo lugar, que lo hagan a distancia, es decir, que tanto el prestador (médico, en este caso) como el destinatario (paciente) no se hallen sincrónicamente presentes en un mismo espacio físico; en tercer lugar, electrónicamente (por lo que no basta con esta falta de presencialidad, sino que se requiere que el mecanismo empleado se articule a través de equipos electrónicos que traten y almacenen la información, excluyendo, entre otros, los que posibilitan la práctica de la telemedicina vía telefónica), y, en cuarto lugar, mediando la solicitud previa del interesado (de suerte que no cabe que el diagnóstico y el consecuente tratamiento y/o seguimiento obvien la voluntad primera del paciente de vehicular su atención sirviéndose de este medio)¹⁵.

A su vez, las personas, físicas o jurídicas, encargadas de prestar estos servicios son los denominados, también de forma amplia, “prestadores de servicios de la sociedad de la información”. No obstante, dentro de ellos, es preciso circunscribirse a la labor concreta de quienes ponen en contacto a ambos lados¹⁶ de la relación (paciente y sanitario), es decir, debemos prestar atención a las plataformas digitales o, lo que es lo mismo, a los proveedores de servicios de intermediación en línea, definidos por el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo de 20 de junio de 2019 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea (artículo 2, letra 2)¹⁷, como aquellos que «[...] permiten a los usuarios profesionales¹⁸ ofrecer bienes o servicios a los consumidores¹⁹, con el objetivo de facilitar el inicio de transacciones directas entre dichos usuarios profesionales y consumidores, con independencia de dónde aquellas concluyan en última instancia y se prestan a los usuarios profesionales sobre la base de relaciones contractuales entre el proveedor de los servicios y los usuarios profesionales que ofrecen los bienes o servicios a los consumidores».

¹⁵ Juan Francisco Rodríguez Ayuso, *Privacidad y Coronavirus: aspectos esenciales* (Madrid: Dykinson, 2020), 37-39. En la misma línea, Juan Francisco Rodríguez Ayuso, «La firma electrónica como medio reforzado de verificación del consentimiento de los menores de edad en materia de protección de datos personales por parte de las Administraciones Públicas», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 53 (2020): 53-54.

¹⁶ Cabe, incluso, que esta relación bilateral se convierta en multilateral si en ella intervienen, además, terceros que aportan servicios auxiliares o complementarios (por ejemplo, publicidad, suministro de equipos médicos, servicios de pago, etc.).

¹⁷ Diario Oficial de la Unión Europea (en lo sucesivo, DOUE) L 186/57, de 11 de julio de 2019.

¹⁸ Se refiere a cualquier persona, ya sea física o jurídica, que participa en el desarrollo de una actividad de carácter comercial o profesional a través de servicios de intermediación en línea [artículo 2.1) Reglamento (UE) 2019/1150].

¹⁹ Que, contraponiéndolos a los anteriores, intervienen al margen de su actividad comercial, negocio, oficio o profesión.

Es el caso, en esencia, de las aplicaciones móviles (teléfonos inteligentes, tabletas y otros dispositivos de naturaleza similar) de salud (también conocidas como “salud móvil” o “M-health”), que, combinando el empleo de los avances tecnológicos con las comunicaciones electrónicas en el sector sanitario, permiten una mejora en el proceso asistencial de los interesados. Más allá de las incidencias que presentan en la captación masiva de categorías especiales de datos personales (de las que nos haremos eco más adelante), lo cierto es que su difusión ha experimentado un impulso exponencial en los últimos años, favoreciendo su empleo en el sector sanitario, tanto público como privado, en aras de conseguir una mejora en la calidad de vida de los pacientes²⁰.

3. Marco jurídico aplicable

A la hora de establecer una aproximación al marco legal de estos servicios de telemedicina, y dado el crecimiento exponencial y desordenado de las normas que, directa o indirectamente, les afectan, conviene hacer dos precisiones iniciales que permitirán configurar más adecuadamente el escenario normativo que disciplina esta vertiente de la eSalud:

De un lado, es preciso realizar una separación entre el servicio prestado (medicina) y el canal empleado para proporcionarlo (el electrónico, merced al empleo de instrumentos o herramientas tecnológicas). Únicamente de esta manera seremos capaces de especificar el compendio de reglas que resulta aplicable.

De otra parte, hemos de partir de una constatación, reforzada a medida que se consolida el impulso de las TIC: la técnica legislativa aplicada variará, de forma que, en unos casos, la normativa se organizará estratificadamente, estructurándola de la más general a la más especial y aplicándola de forma acumulada; en otros, empero, la norma aplicable desplazará a todas las demás.

Partiendo de esta premisa, seguidamente, podemos realizar un intento de sistematización, en nada sencillo ni excluyente, pero sí deliberadamente sistemático e integrador, del régimen jurídico básico:

Así, partiendo de la, *supra* indicada, separación entre el continente y el contenido y atendiendo al primero de ellos, deberíamos hacer mención:

1) A la legislación horizontal que, de forma general, establece criterios mínimos para todos los servicios de la sociedad de la información:

²⁰ Recurrente es, también, el debate en torno a la posible consideración de las apps de salud como productos sanitarios. Se trata de un tema complejo y abierto a debate que no alcanza a tener una respuesta unánime, aunque parte de la doctrina se inclina por afirmar la necesidad de efectuar una más amplia evaluación de estas aplicaciones en orden a concretar si han de estar sujetas, o no, a la normativa relativa a productos sanitarios; en esta línea, De Lorenzo Aparici, O. (2022). ¿Pueden todas las aplicaciones de salud considerarse productos sanitarios? Responsabilidad y aplicaciones de salud. En C. Gil Membrado (drtora.). *Bioderecho y retos: m-health, genética, IA, robótica y criogenización* (87-109). Madrid: Dykinson; Lina Keutzer y Ulrika Simonsson, «Medical device apps: an introduction to regulatory affairs for developers», *JMIR Mhealth Uhealth*, n.º 8 (2020): 6.

Si atendemos a la normativa europea, podemos afirmar que la normación de dichos servicios fue impulsada a finales de los noventa, mediante un texto que, justificado por la (temprana) época en la que vio la luz, quedo circunscrito a conseguir una supervisión de las medidas previstas por los países comunitarios en relación con los servicios digitales. Aludimos a la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas²¹, más tarde suprimida por la, todavía vigente, Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información²².

Ahora bien, el verdadero punto de inflexión tuvo lugar inmediatamente después, con la aprobación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico, también conocida como DCE), aún en vigor²³. La pretensión de este texto, abiertamente ambicioso, era consolidar un auténtico marco legal para los servicios de la sociedad de la información, disciplinando aspectos básicos, como el régimen de establecimiento y de responsabilidad o el deber de información de quienes los prestan.

2) Se encuentra la regulación, igualmente transversal, si bien especial, que avanza en esta conformación del régimen legal, esta vez atendiendo, bien a concretos servicios de intermediación en línea, bien a puntuales y determinados aspectos relacionados con ellos:

Por lo que respecta al marco concreto de aquellos servicios, también de la sociedad de la información, que no tienen una finalidad en sí misma, sino que posibilitan que otros puedan ser prestados (servicios de intermediación en sentido estricto²⁴), hemos de añadir la regulación contenida en el Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (en adelante, Reglamento de Servicios Digitales o, también, DSA, acrónimo que alude a su denominación en inglés *Digital Services Act*)²⁵, que provoca un desplazamiento del régimen de responsabilidad previsto para estos prestadores en los artículos 12 a 15 DCE, que quedarían subsumidos en los preceptos 3, 4, 5 y 7 DSA.

²¹ Diario Oficial de las Comunidades Europeas (en lo sucesivo, DOCE) L 204/37, de 21 de julio del año 1998.

²² DOUE L 241/1, de 17 de septiembre de 2015.

²³ DOCE L 178/1, de 17 de julio de 2000. La transposición en nuestro ordenamiento jurídico interno se produjo con la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (Boletín Oficial del Estado -en adelante, BOE- número 166, de 12 de julio de 2007).

²⁴ Nos referimos a aquellos servicios de mera transmisión, de memoria tampón o de alojamiento de datos, entre otros, siguiendo la terminología empleada por la DCE.

²⁵ DOUE L 277/1, de 27 de octubre de 2022.

Por contraposición, para aquellos otros servicios que sí tienen esta pretensión finalista, habremos de estar a lo que se dicta en el, antes citado, Reglamento 2019/1150. Aplicable a todos los Estados miembros, trata de coadyuvar al robustecimiento del mercado interior comunitario a través de la configuración de directrices orientadas a propugnar una actuación transparente y equitativa.

Finalmente, atendiendo a aspectos concretos de estos servicios prestados por plataformas digitales en línea, tendríamos que adicionar:

a) la Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo de 20 de mayo de 2019 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales²⁶;

b) el Reglamento (UE) N° 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE²⁷, que aglutina el régimen de los conocidos como “servicios de confianza”, también relevantes a la hora de prestar determinados servicios médicos, como la receta electrónica, y en los que confluyen cumulativamente los aspectos esenciales, ya vistos, para merecer la consideración de servicios digitales, o

c) el Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (en lo sucesivo, Reglamento de Mercados Digitales o, como es comúnmente conocido, DMA, acrónimo que hace referencia a su denominación en inglés *Digital Markets Act*)²⁸. Este texto introduce una regulación hasta ahora inexistente y focalizada tan solo en aquellos grandes superintermediarios o influyentes plataformas digitales de intermediación, también conocidas como “gatekeepers” (“guardianes de acceso”), dada la capacidad que tienen para influir significativamente en el mercado, sirviendo como elemento de entrada imprescindible a la hora de posibilitar la interacción de todos los actores intervinientes en este espacio, merced a la fuerte consolidación, presente o incipiente, que ostentan (apartado primero del artículo 3 DMA). En concreto, la DMA define (o más bien, describe los elementos que han de concurrir para adquirir la condición de tal) al guardián de acceso como aquella «empresa prestadora de servicios básicos de plataforma, designada de conformidad con el artículo 3» [artículo 2.1)], introduce un doble requisito para proceder

²⁶ DOUE L 136/1, de 22 de mayo de 2019.

²⁷ DOUE L 257/73, de 28 de agosto de 2014.

²⁸ Diario Oficial de la Unión Europea (en adelante, DOUE) L 265/1, de 12 de octubre de 2022. El texto refuerza la necesidad de regular a las plataformas digitales mediante instrumentos supranacionales, al apuntar, entre otras cuestiones, un aspecto relevante, pues, «[...] aunque los guardianes de acceso tienden a adoptar modelos de negocio y estructuras algorítmicas mundiales o al menos paneuropeos, también pueden adoptar, y en algunos casos así lo han hecho, diferentes condiciones y prácticas comerciales en distintos Estados miembros, lo que puede crear disparidades entre las condiciones de competencia de los usuarios de los servicios básicos de plataforma prestados por guardianes de acceso, en detrimento de la integración del mercado interior».

al nombramiento de los guardianes de acceso, a saber: a) prestar servicios básicos de plataforma, es decir, servicios de intermediación de la sociedad de la información; b) ser designado de conformidad con el artículo 3.

Se antoja, pues, necesario analizar minuciosamente el contenido de este último precepto. De acuerdo con su apartado primero, tres serán los aspectos que, cumulativamente, deberá reunir un prestador digital que presta servicios básicos de plataforma para ser designado como guardián de acceso:

Uno, ha de tener una gran influencia en el mercado.

Dos, ha de prestar un servicio básico de plataforma que constituye una importante puerta de acceso²⁹, una barrera de entrada, de los usuarios profesionales a los usuarios finales intermediados (derivada de los efectos de red, de las economías de escala o de la cautividad de los usuarios³⁰).

Tres, ha de gozar, o presumiblemente gozará en un futuro cercano, de una posición afianzada y duradera, en lo que concierne a sus operaciones.

Para poder concretar estos requisitos (sustentados, a simple vista, en conceptos jurídicos indeterminados), el Reglamento establece una primera vía, amparada en criterios puramente cuantitativos, que presume (presunción *iuris tantum*) el cumplimiento de estos requisitos si [artículo 3.2, letras a) a c), DMA]:

En relación con el primero de ellos, la plataforma digital consigue un volumen de negocios anual en la Unión Europea de, como mínimo, 7.500.000.000 de euros en cada uno de los tres últimos ejercicios, o cuando su capitalización bursátil media o su valor justo de mercado equivalente ascienda como mínimo a esta cantidad en el último ejercicio, y preste el mismo servicio básico de plataforma en, al menos, tres Estados miembros de la Unión Europea.

En relación con el segundo, la plataforma digital proporciona un servicio básico de plataforma que, en el último ejercicio, ha tenido, como mínimo, 45.000.00 mensuales de usuarios finales activos establecidos o situados en territorio comunitario y, al menos, 10.000 usuarios profesionales activos anuales establecidos en la Unión Europea, identificados y calculados de conformidad con la metodología y los indicadores establecidos en el anexo de la DMA, a fin de proporcionar seguridad jurídica a las plataformas (metodología e indicadores que, por lo demás, podrán ser actualizados por medio de actos delegados adoptados por la Comisión, en los términos previstos en el artículo 49 DMA y de conformidad con el artículo 3.7 DMA)³¹.

²⁹ Como acertadamente precisan ZURIMENDI ISLA, Aitor y FERNÁNDEZ GARCÍA DE LA YEDRA, Ainhoa, *Revista General de Derecho de los sectores regulados: RSR*, núm. 6, 2020, p. 10, «[l]a relación de la plataforma tanto con cada nuevo oferente como con cada nuevo demandante surge de un contrato, que suele denominarse de acceso, por el que cada usuario se de alta en la plataforma, y que incluye el programa prestacional que define la actividad de la plataforma».

³⁰ MONTERO PASCUAL, Juan José, *Nuevas Tecnologías 2022*, p. 363.

³¹ Considerandos 20 y 97 DMA.

El *Digital Markets Act*, junto con el DSA, integran el denominado *The Digital Services Act package*. Ambos adoptan la forma de reglamento, lo que coadyuva, fuera de toda duda, a generar una mayor seguridad jurídica y una más amplia armonización normativa (en detrimento, por tanto, de la fragmentación derivada de múltiples y dispares regulaciones en los distintos Estados miembros) en el mercado interior digital (artículo 1.5 DMA); ahora bien, esta vocación, claramente tendente a la unicidad, se acompaña, justo a continuación, de una previsión que deja abierta la posibilidad a que los países comunitarios puedan «[...] imponer a las empresas, incluidas las empresas prestadoras de servicios básicos de plataforma, obligaciones relativas a cuestiones que quedan fuera del ámbito de aplicación del presente Reglamento, siempre que estas obligaciones sean compatibles con el Derecho de la Unión y no deriven de la consideración de las empresas afectadas como guardianes de acceso en el sentido del presente Reglamento».

Como se puede observar, la DMA parte de un concepto básico en torno al cual articula la posterior delimitación del régimen de obligaciones de quienes, en determinadas condiciones y bajo ciertas salvaguardas, los prestan. Es el de “servicio básico de plataforma” [artículo 2.2) del Reglamento de Mercados Digitales], que, lejos de arrojar una definición de esta categoría general, se limita a delimitarla, incluyendo, a modo de elenco *numerus apertus*, una serie de servicios (gran parte de los cuales se refieren a plataformas que brindan servicios digitales, mientras que otras se centran en controlar e influir en el acceso a dichos servicios -como sucede, por ejemplo, con los sistemas operativos o los asistentes virtuales-) que, entonces sí, define y que, por su relevancia, pasamos a enumerar:

En primer lugar, se encuentran los servicios de intermediación en línea [artículo 2.2.a) DMA], definidos [artículo 2.5) DMA], por remisión, en el artículo 2.2 del Reglamento P2B como aquellos servicios que satisfacen, cumulativamente, tres requisitos: son servicios de la sociedad de la información, cualidad de la naturaleza jurídica de estos servicios extensible a todos los demás servicios básicos de plataforma; permiten a los usuarios profesionales ofrecer bienes o servicios a los consumidores (usuarios finales) con el objetivo de facilitar el inicio de transacciones directas entre ambos, con independencia de dónde aquellas concluyan en última instancia, y se prestan a los usuarios profesionales sobre la base de relaciones contractuales entre el proveedor de los servicios (la plataforma digital) y los usuarios profesionales que ofrecen los bienes o servicios a los usuarios finales.

En segundo lugar, los motores de búsqueda en línea [artículo 2.2.b) DMA], donde, de nuevo, se emplea la técnica de la remisión para definirlos. En concreto, tenemos que acudir, de nuevo, al Reglamento (UE) 2019/1150, cuyo artículo 2.5 aclara que un motor de búsqueda será aquel servicio «[...] que permite a los usuarios introducir consultas para hacer búsquedas de, en principio, todos los sitios web, o de sitios web en un idioma concreto, mediante una consulta sobre un tema cualquiera en forma de palabra clave, consulta oral, frase u otro tipo de entrada, y que en respuesta muestra resultados en

cualquier formato en los que puede encontrarse información relacionada con el contenido solicitado» [artículo 2.6) DMA].

En tercer lugar, los servicios de redes sociales en línea [artículo 2.2.c) DMA]. Aquí sí, la norma aporta una definición del servicio como aquel que posibilita «[...] que los usuarios finales se conecten y se comuniquen entre sí, compartan contenidos y descubran contenidos y a otros usuarios a través de múltiples dispositivos y, en particular, mediante chats, publicaciones, vídeos y recomendaciones» [artículo 2.7) DMA].

En cuarto lugar, los servicios de plataforma de intercambio de vídeos línea [artículo 2.2.d) DMA], donde, de nuevo, acudimos a un texto normativo alternativo para encontrar su definición [artículo 2.8) DMA]. Este texto es la Directiva 2010/13/UE del Parlamento Europeo y del Consejo de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual)³², que define este tipo de servicio como aquel «[...] servicio, tal como lo definen los artículos 56 y 57 del Tratado de Funcionamiento de la Unión Europea, cuya finalidad principal propia o de una de sus partes dissociables o cuya funcionalidad esencial consiste en ofrecer al público en general programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretener o educar, a través de redes de comunicaciones electrónicas tal como se definen en el artículo 2, letra a), de la Directiva 2002/21/CE, y cuya organización determina el prestador de la plataforma de intercambio de vídeos, entre otros medios con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación» [(artículo 1.1.a bis)].

En quinto lugar, los servicios de comunicaciones interpersonales independientes de la numeración [artículo 2.2.e) DMA]. Una vez más, la definición se vincula a otra norma [artículo 2.9 DMA], que no es otra que la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018 por la que se establece el Código Europeo de las Comunicaciones Electrónicas (en lo sucesivo, CECE)³³, cuyo artículo 2.7) lo concibe como aquel servicio cuya característica básica y fundamental reside en que «[...] no conecta a través de recursos de numeración pública asignados, es decir, de un número o números de los planes de numeración nacional o internacional, o no permite la comunicación con un número o números de los planes de numeración nacional o internacional».

En sexto lugar, los sistemas operativos [artículo 2.2.f) DMA], que el artículo 2.10) DMA concibe como el «software de sistema que controla las funciones básicas del hardware o del software y permite que se ejecuten en él aplicaciones informáticas».

En séptimo lugar, los navegadores web [artículo 2.2.g) DMA], fácilmente identificables por ser aquellas aplicaciones informáticas que permiten «[...] a los usuarios

³² DOUE L 95/1, de 15 de abril de 2010.

³³ DOUE L 321/36, de 17 de diciembre de 2018.

finales acceder a contenidos web alojados en servidores que están conectados a redes como internet e interactuar con dichos contenidos, incluidos los navegadores web independientes y los navegadores web integrados en software o similares» [artículo 2.11) DMA].

En octavo lugar, los asistentes virtuales [artículo 2.2.h) DMA], que, también conocidos como “mayordomos digitales”, no son sino «un software que puede procesar peticiones, tareas o preguntas, también las formuladas mediante sonidos, imágenes, texto, gestos o movimientos y que, basándose en dichas peticiones, tareas o preguntas, proporciona acceso a otros servicios o controla dispositivos físicos conectados» [artículo 2.12) DMA].

En noveno lugar, los servicios de computación en la nube [artículo 2.2.i) DMA], que agrupa cualquier servicio de la sociedad de la información que haga posible «[...] el acceso a un conjunto modulable y elástico de recursos informáticos que se pueden compartir» [artículos 2.13) DMA y 4.19) de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión³⁴].

En décimo y último lugar, los servicios de publicidad en línea, incluidas las redes de publicidad, las plataformas de intercambio de publicidad y cualquier otro servicio de intermediación publicitaria, prestados por una empresa que preste cualquiera de los servicios básicos de plataforma antes enumerados [artículo 2.2.j) DMA]. Es este el único servicio básico de plataforma que no cuenta con definición, ni directa ni indirecta, en el texto del Reglamento de Mercados Digitales.

d) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos o RGPD)³⁵, en todo lo concerniente, como tendremos oportunidad de analizar, con los datos personales (datos de salud, en su mayoría) implicados en el tratamiento médico a proporcionar al paciente por el sanitario.

3) Centrándonos en el servicio en sí de prestación médica en que consiste la telemedicina, debemos aludir a la regulación vertical que, en su caso, puede llegar a desplazar a las ya descritas. Acudimos, a falta de normativa específica (ni siquiera 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 clínica³⁶, hace

³⁴ DOUE L 194/1, de 19 de julio de 2016.

³⁵ DOUE L 119/1, de 04 de mayo de 2016. Adaptándolo y completándolo surge, en nuestro país, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD -BOE número 294, de 06 de diciembre de 2018-).

³⁶ BOE número 274, de 15 de noviembre de 2002.

alusión a la telemedicina), a aquella regulación aplicable a la actuación sanitaria presencial y tradicional, plasmada en:

De un lado, la Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias³⁷, que propugna la plena autonomía, científica y técnica, con la que cuentan los profesionales sanitarios en el ejercicio de su actividad, sin más límites que los previstos en el ordenamiento jurídico y los propios de los principios deontológicos (artículo 4.7).

De otro, la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud³⁸, que, en su artículo 21.2, adiciona lo siguiente: «[...] Las nuevas técnicas, tecnologías o procedimientos serán sometidas a evaluación, con carácter preceptivo y previo a su utilización en el Sistema Nacional de Salud, por la Red Española de Agencias de Evaluación de Tecnologías Sanitarias y Prestaciones del Sistema Nacional de Salud»; sin embargo, los requisitos de esta evaluación, previstos en el apartado siguiente, no han sido acreditados a día de hoy, motivo por el que, actualmente, carecemos de información cierta de cuáles de ellas (incluida la telemedicina) podrán llegar a ser utilizadas por dicho Sistema.³⁹

A la vista de ello, procede acudir a la jurisprudencia, que reitera la necesidad de apoyarse en el código deontológico para completar el marco jurídico aplicable a la telemedicina. Buen exponente de ello son las Sentencias del Tribunal Supremo 1267/2006, de 05 de diciembre, y del Tribunal Constitucional 219/1989, de 21 de diciembre, que sostienen la conveniencia de acudir, por una parte, al conjunto normativo que contiene los deberes de carácter profesional de los especialistas médicos y, por otra, a las reglas morales previstas en los códigos de conducta, pues, aun cuando estas carecen de fuerza coactiva, sirven en la configuración de los principios rectores (especialmente los relacionados con el nivel de diligencia de los profesionales sanitarios) que inciden en la práctica médica y definen el contenido de las obligaciones a cumplir en la praxis asistencial.

Destaca, al respecto, la aprobación, a finales de diciembre del año 2022, por parte de la Asamblea General del Consejo General de Colegios Oficiales de Médicos de España (CGCOM), de un nuevo Código de Deontología Médica, que incorpora, en lo que aquí interesa, novedosos capítulos en los que se regulan aspectos deontológicos relevantes, como los relativos a la telemedicina, los médicos y las redes sociales, la seguridad del paciente, las grandes bases de datos sanitarias y la Inteligencia Artificial aplicada a la Medicina. Más concretamente, introduce un capítulo XXIII, titulado “Telemedicina y

³⁷ BOE número 280, de 22 de noviembre de 2003.

³⁸ BOE número 128, de 29 de mayo de 2003.

³⁹ Cristina Gil Membrado. «Una asignatura pendiente: la regulación de la prestación sanitaria a través de telemedicina (TDM)», en *El nuevo marco legal del teletrabajo en España: Presente y futuro, una aproximación multidisciplinar*, ed. por Juan Francisco Rodríguez Ayuso y Elena Atienza Macías (Madrid: Wolters Kluwer, 2021), 193-215. Elena Atienza Macías. «Legal challenges for robots and autonomous artificial intelligence systems in the healthcare context with special reference to Covid-19 health crisis», *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, n.º 1 (2021): 119-134.

Tecnologías de la Información y la Comunicación (TIC)”, que comprende los artículos 80 a 84, que, por su relevancia, pasamos a transcribir:

«Artículo 80

1. El uso de los medios telemáticos u otros sistemas de comunicación no presenciales destinados a la ayuda en la toma de decisiones dentro del ámbito profesional es conforme a la Deontología Médica, siempre que sea inequívoca la identificación de quienes intervienen, se asegure la confidencialidad y se usen vías de comunicación que garanticen la máxima seguridad disponible.

2. Se debe registrar en la historia clínica el medio de telemedicina por el que se ha realizado la consulta, así como el tratamiento médico pautado y recomendaciones dadas.

Artículo 81

1. En el uso de la telemedicina y todas las modalidades de atención no presencial rigen los preceptos deontológicos de este Código acerca de la relación médico-paciente, la defensa de los derechos y la seguridad del paciente, así como el respeto y autonomía de los profesionales sanitarios.

2. Cuando un médico hace uso de los sistemas de comunicación, debe ser responsable de sus actos y de los daños directos e indirectos que de su actuación se puedan derivar.

3. Cuando el médico utilice la telemedicina, sus intervenciones deben estar presididas por base científica, profesionalidad, veracidad y prudencia, y siempre serán conformes al contenido de este Código.

4. En los sistemas de comunicación social el médico debe cuidar su actitud y su imagen, así como emplear un lenguaje adecuado en forma y contenido.

5. La contribución a divulgar informaciones falsas y no contrastadas que van contra la evidencia científica es contraria a la Deontología Médica.

Artículo 82

1. El médico que utiliza la telemedicina y todas las modalidades de atención no presencial con fines asistenciales o docentes debe extremar las medidas destinadas a proteger la seguridad y la confidencialidad del paciente, poniendo especial atención en la configuración de la privacidad de dichos medios.

2. La investigación y otras actividades relacionadas con las bases de datos de salud y la Inteligencia Artificial deben ser en beneficio de la sociedad y de los objetivos de salud pública.

3. En la Inteligencia Artificial es fundamental que el médico se comprometa en la protección de la confidencialidad, control y propiedad de los datos del paciente y en desarrollar modelos que incluyan el consentimiento y la gestión de los datos.

Artículo 83

1. Las publicaciones o la difusión del conocimiento a cargo de un médico en las redes sociales e internet deben realizarse con el rigor y la seriedad establecidos en este Código, y siempre con la debida identificación del autor.

2. El médico no debe difundir información que cree falsas expectativas, alarma social o que genere confusión o dudas respecto al cuidado, el mantenimiento o la prevención de la salud.

Artículo 84

1. La publicidad médica, el marketing sanitario y el proceso de creación de una marca en la red deben cumplir las normas establecidas en este Código con respecto a la publicidad.

2. El médico que difunde contenidos profesionales en medios telemáticos o de análoga naturaleza debe mencionar explícitamente los patrocinios recibidos y los posibles conflictos de intereses».

Junto al anterior, se encuentra el importante Capítulo XXIV, sobre “Inteligencia Artificial (IA) y bases de datos sanitarios”, que establece la necesidad de que el médico exija un control ético y finalista de la investigación con Inteligencia Artificial basado en la transparencia, la reversibilidad y la trazabilidad de los procesos en los que intervenga, para garantizar la seguridad del paciente, además de que los datos de salud extraídos de grandes bases de datos sanitarias o los sistemas robóticos puedan servir de ayuda en la toma de decisiones clínicas y sanitarias, siempre que no sustituyan a la obligación que el médico tiene de utilizar los métodos necesarios para la buena práctica profesional. De igual modo, obliga al médico a no colaborar en la manipulación intencionada de datos o de resultados obtenidos de grandes bases de datos sanitarias.

III. La Telemedicina y la protección de datos personales

1. *El refuerzo en la protección de categorías especiales de datos personales: el caso de los datos de salud*

Los datos de salud forman parte de la categoría, más amplia, de datos personales, definidos por el RGPD como «toda información sobre una persona física identificada o identificable» (artículo 4.1). En consecuencia, cualquier información que, directa o mediatamente, sea susceptible de identificar al interesado en cuanto titular de la misma será susceptible de ser considerada como dato personal⁴⁰.

A su vez, los datos personales se estructuran en torno a una triple clasificación, atendiendo a la incidencia que su difusión a terceros pueda llegar a tener en la intimidad o privacidad del afectado⁴¹. Hablamos, así, en orden creciente exposición, de datos personales básicos, datos relativos a condenas o infracciones penales y datos especialmente protegidos o categorías especiales de datos personales.

⁴⁰ Juan Francisco Rodríguez Ayuso, «Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos», *Revista de Derecho político*, n.º 110 (2021): 302.

⁴¹ Así lo puso de manifiesto, entre otras, la paradigmática Sentencia del Tribunal Constitucional 70/2009, de 23 de marzo.

Sólo estos últimos aparecen circunscritos, a modo de listado *numerus clausus*, que los restringe a aquellos «[...] que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida u orientación sexual de una persona física» (artículo 9.1 RGPD). Ello conlleva que esta categoría, por ser más sensible, esté investida de determinadas reglas especiales que la refuerzan y dotan de una mayor protección⁴², reglas, todas ellas, presididas por la general prevista en el mencionado apartado, que preceptúa la prohibición de proceder al tratamiento de este tipo de datos, salvo que este tratamiento se produzca en alguna de las circunstancias excepcionales previstas en su apartado segundo⁴³.

Entre los datos personales especialmente protegidos se encuentran, precisamente, como hemos podido ver, los relativos a la salud del interesado, es decir, los concernientes «[...] 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» (artículo 4.15 RGPD⁴⁴). También, como categorías específicas en ellos subsumida, los datos genéticos y biométricos, definidos en las letras 13 y 14 del mismo precepto del Reglamento, respectivamente.

2. *El consentimiento como base de legitimación esencial en el tratamiento de datos sanitarios y especialidades del principio de limitación de la finalidad para un tratamiento seguro de la información*

Como hemos podido ver, el consentimiento constituye una de las bases de legitimación por antonomasia en el tratamiento de datos personales, amén de ser la única de todas ellas que, cuando es explícito (por contraposición al expresado mediante una clara acción afirmativa), sirve para anular la regla general que impide el tratamiento de

⁴² Manuel Medina Guerrero. «Categorías especiales de datos», en *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*, ed. por Artemi Rallo Lombarte (Valencia: Tirant lo Blanch, 2019), 257-258; Juan Francisco Rodríguez Ayuso, «Criterios para el acceso oficial de ciudadanos especialmente vulnerables a servicios prestados por las Administraciones Públicas», *Revista jurídica de Castilla y León*, n.º 53 (2021): 151.

⁴³ En cambio, las demás categorías de datos personales podrán tratarse sin necesidad de que concurra situación excepcional alguna. En cualquier caso, todo tratamiento deberá respetar el principio de licitud, que exige estar amparado en alguna de las bases jurídicas previstas en el artículo 6 RGPD [consentimiento del interesado, ejecución de un contrato en el que el titular de los datos personales sea parte, cumplimiento de una obligación legal aplicable al responsable del tratamiento (en cuanto persona, física o jurídica, que determina los fines y medios del tratamiento -artículo 4.7 RGPD-), necesidad de proteger los intereses vitales del afectado, cumplimiento de una misión realizada en interés público o en la satisfacción de intereses legítimos del responsable del tratamiento].

⁴⁴ En la misma línea, y para una acepción más completa y detallada de esta noción, el considerando 35 RGPD.

categorías especiales de datos personales, como son los de salud⁴⁵. Y es que, el consentimiento, tras la promulgación del Reglamento general de protección de datos, experimenta una redacción novedosa, que lo convierte en «toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen» (artículo 4.11), anulando la posibilidad, prevista en el régimen anterior⁴⁶, de consentimientos tácitos o implícitos y exigiendo, entre otras cuestiones, una previa información (sobre la base de los artículos 12 a 14 RGPD, reforzada con los artículos 7 y 8 RGPD y 7 LOPDGDD) sobre los fines específicos (expresados en un lenguaje claro, sencillo, cognoscible y comprensible) perseguidos con el pretendido tratamiento⁴⁷.

Aplicado al caso que nos ocupa, será necesario, pues, que las aplicaciones móviles sanitarias, en cuanto plataformas digitales a través de las cuales se prestan servicios de telemedicina, recaben adecuadamente la voluntad del interesado de ser sometido a determinadas acciones (como el diagnóstico inicial, el asesoramiento médico o el seguimiento de su evolución). En otras palabras, deben poder probar que el consentimiento se produjo y que este tuvo lugar explícitamente después de que el paciente fuese informado de todas las circunstancias que rodean al tratamiento, circunstancias de entre las que destaca, por su relevancia en el ámbito de la medicina a distancia, la finalidad perseguida por el responsable del tratamiento, especialmente cuando este tiene naturaleza pública y, por ende, está investido de la obligación de procurar el interés general de todos los ciudadanos.

Al respecto, tales finalidades deberán ser, igualmente, explícitas, amén de determinadas y legítimas, no pudiendo ser tratados los datos de salud del afectado, a la postre, de manera incompatible con aquellos fines sobre los que recayó, en este caso, su consentimiento. Se exceptúan, de esta incompatibilidad, los tratamientos posteriores que se realicen con fines de archivo en interés público, investigación científica e histórica o estadísticos, al amparo de lo dispuesto por el artículo 89.1 RGPD.

⁴⁵ Bien es cierto que esta aseveración ha de verse acompañada por la rigidez del artículo 9.1 LOPDGDD, que excluye la posibilidad de superar la prohibición del artículo 9.1 RGPD cuando los datos especiales tratados sean algunos de los en él citados, no incluyéndose, entre ellos, a los datos personales relativos a la salud del interesado.

⁴⁶ Este régimen jurídico venía representado por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE número 298, de 14 de diciembre de 1999) y por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (BOE número 17, de 19 de enero de 2008), que emanan de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE L 281/31, de 23 de noviembre de 1995).

⁴⁷ Al respecto, Juan Francisco Rodríguez Ayuso, «Instrumentos cualificados para el registro identificativo en el entorno de la e-Administración Pública», *Revista española de Derecho administrativo*, n.º 210 (2021): 162.

En las apps de salud, estos fines se centrarán en garantizar el bienestar del paciente, analizando su situación física y/o psíquica para ofrecerle un diagnóstico, realizarle pruebas sanitarias o someterle a un seguimiento sobre la base de una autorización que se haya producido con carácter previo. No obstante, para poder implementar estas operaciones de forma adecuada, será preciso exponer las funcionalidades de estas herramientas de manera separada (si, por ejemplo, se persigue el diagnóstico de una patología y, además, el posterior seguimiento del tratamiento recetado por el médico, es preciso hacer constar por separado qué datos de salud serán tratados para uno y otro fin y qué legitimación requiere cada uno de ellos), a fin de que el usuario tenga el mayor control posible sobre los datos que permiten satisfacerlas, lo que requiere conocer qué información está en posesión de terceros y con qué objetivo. Lo anterior impone a los poderes públicos la prohibición de convertir los datos así captados en información disponible sin revestirlos de garantías suficientes, previniendo los riesgos que puedan suscitarse derivados de un acceso o divulgación no autorizadas a dicha información por parte de terceros.

En el seno de la telemedicina, será necesario, por tanto, redactar una política de privacidad que, contenida en la aplicación 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 aquellos que gestionan las complementariedades recogidas en la plataforma como servicios auxiliares) 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 personal y sensible que le concierne.

Lo anterior no será posible si, además de las correspondientes garantías jurídicas, el tratamiento no se ve acompañado de medidas técnicas que proporcionen una seguridad adecuada de los datos en su triple dimensión: confidencialidad⁴⁸, disponibilidad⁴⁹ e integridad⁵⁰. Partiendo de esta premisa [recogida en el artículo 5.1.f) RGPD], el artículo 32 RGPD establece la necesidad de realizar un análisis de riesgos que permita concretar qué medidas, técnicas y organizativas (cifrado, seudonimización, nombramiento de un delegado de protección de datos, copias de seguridad, etc.)⁵¹, requiere aplicar el servicio

⁴⁸ La confidencialidad es aquella dimensión de la seguridad que evita que los datos personales sean revelados a terceros no autorizados.

⁴⁹ La disponibilidad, por su parte, engloba todas aquellas medidas que impiden la pérdida de los datos a tratar por el responsable del tratamiento.

⁵⁰ La integridad, por último, procura que el contenido de la información concerniente al afectado (al paciente, en este caso) no se vea alterado o modificado sin su autorización ni consentimiento.

⁵¹ Manuel Carpio Cámara. «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad», en *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, ed. por José Luis Piñar Mañas (Madrid: Reus, 2016), 335-350.

digital de telemedicina para prever un nivel de seguridad acorde al tratamiento de los datos de salud que posibilitará atender a las necesidades del afectado⁵².

Cuando, como en este caso, los datos personales implicados son especialmente sensibles, el riesgo previsible del tratamiento será elevado, motivo por el que, además de realizar el correspondiente análisis de riesgos, será necesario proveer una evaluación del impacto previsto con las operaciones de tratamiento (artículo 35 RGPD). Más específicamente, este procedimiento habrá de seguirse cuando, como sucede en el seno de la *eHealth*, se produzcan evaluaciones sistemáticas y exhaustivas de aspectos personales de los interesados, sobre la base de un tratamiento automatizado, que permitan la adopción de decisiones que generen consecuencias jurídicas para ellos o que les afecten significativamente de modo similar; también, como previsiblemente sucederá con la recogida masiva de datos a través de aplicaciones móviles, para tratamientos a gran escala de datos de salud. En consecuencia, antes de proceder a estos tratamientos, el responsable del tratamiento (aplicación sanitaria que reúne a los profesionales médicos encargados de prestar los servicios digitales asistenciales en que se traduce la telemedicina) deberá efectuar una consulta previa a la autoridad de control (Agencia Española de Protección de Datos, en nuestro caso) para que, mediando la información requerida por el artículo 36.3 RGPD, esta se pronuncie en torno a la idoneidad (o falta de ella) de las medidas propuestas para mitigar los posibles efectos negativos o perjudiciales previstos con el tratamiento.

IV. Conclusiones

A lo largo de estas líneas, se ha puesto de manifiesto cómo la telemedicina comparte una doble dimensión: la de ser un servicio de la sociedad de la información que, cuando es articulado (como suele suceder) a través de aplicaciones móviles, lo convierte, además, en un servicio de intermediación en línea, prestado por plataformas virtuales que ejercen de canalizadoras para poner en contacto a los profesionales sanitarios disponibles, de un lado, con los pacientes necesitados de atención en forma de diagnóstico, seguimiento y prevención, de otro.

La evolución de las Nuevas Tecnologías brinda, a través de avances como la Inteligencia Artificial (y, con ella, el empleo masivo de información *-Big Data-*, utilizada de forma lógica para extraer conclusiones relevantes mediante la utilización de algoritmos inteligentes), la posibilidad de extender los cuidados de la salud a distancia, de modo que

⁵² Con la normativa anterior, esta delimitación de las medidas de seguridad aplicables era automática y estaba ligada, no tanto al riesgo que comporta el tratamiento, cuanto al dato personales sobre el que este se efectuaba. En consecuencia, bastaba con acudir al elenco de medidas de seguridad aplicables, predefinido en el Real Decreto 1720/2007, en función de si estábamos ante (clasificación ya extinta) datos personales de nivel bajo, medio o alto. Ahora, en cambio, el enfoque cambia de manera sustancial, toda vez que lo verdaderamente importante no es el dato personal en sí (que, no obstante, condiciona el resultado final del análisis), sino el contexto en el que se desarrolla dicho tratamiento, es decir, el riesgo.

cada vez un mayor número de personas (muchas de las cuales presentan dificultades ostensibles de movilidad o de ubicación geográfica) pueden beneficiarse de un derecho constitucionalmente protegido por el artículo 43 CE⁵³.

Lo anterior conlleva una consecuencia relevante, plasmada en la necesidad de configurar un complejo marco jurídico en el que confluya, a la vez, una legislación que atiende al elemento nuclear, es decir, a la naturaleza sanitaria de los servicios prestados, con otra que, por su parte, pone el foco en el medio (virtual) a través del cual estos se canalizan. Es preciso, por tanto, tratar de estructurar este régimen mediante la ordenación, no siempre sencilla, de toda la normativa horizontal y vertical que, de forma general o específica, resulta aplicable a la telemedicina.

Por último, también será fundamental abordar los efectos que trae consigo el tratamiento de datos personales especialmente sensibles, como son los datos de salud, por parte de los responsables del tratamiento que prestan estos servicios digitales sanitarios. Al respecto, hemos podido constatar la relevancia que presenta el consentimiento como mecanismo para manifestar la voluntad del interesado, consentimiento que habrá de venir precedido de toda una suerte de garantías que aseguren el cumplimiento de todos y cada uno de los principios relativos al tratamiento (artículo 5 RGPD), especialmente el de transparencia (con una clara separación de los fines perseguidos y de la base jurídica aplicable a cada uno de ellos) y el de seguridad (en su triple dimensión: integridad, disponibilidad y confidencialidad).

V. Referencias bibliográficas

Ana Isabel Herrán Ortiz. «Inteligencia Artificial, salud y Derechos Humanos: ¿hacia un gobierno de los algoritmos?», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 297-335.

Beatriz Pascual de la Pisa, María José García Lozano y Juan González Lama, «Aspectos legales de la telemedicina», *FMC: Formación Médica Continuada en Atención Primaria*, n.º 10 (2021): 544-550.

Cristina Gil Membrado. «Una asignatura pendiente: la regulación de la prestación sanitaria a través de telemedicina (TDM)», en *El nuevo marco legal del teletrabajo en España: Presente y futuro, una aproximación multidisciplinar*, ed. por Juan Francisco Rodríguez Ayuso y Elena Atienza Macías (Madrid: Wolters Kluwer, 2021), 193-215.

Elena Atienza Macías. «Legal challenges for robots and autonomous artificial intelligence systems in the healthcare context with special reference to Covid-19 health crisis», *IUS ET SCIENTIA: Revista electrónica de Derecho y Ciencia*, n.º 1 (2021): 119-134.

⁵³ BOE número 311, de 29 de diciembre de 1978.

Francesca Ferretti y María Paola Nico. «Telemedicina y responsabilidad civil», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 155-184.

Gabriel Eisenbach, «What is health?», *The journal of medical Internet research*, n.º 3 (2001): 1-20.

Javier Sánchez Caro. «Telemedicina», en *Enciclopedia de Bioderecho y Bioética*, ed. por Carlos María Romeo Casabona (Granada: Comares, 2011).

Javier Sánchez Caro y Fernando Abellán-García Sánchez. *Telemedicina y protección de datos sanitarios: aspectos legales y éticos* (Granada: Comares, 2002).

José Vida Fernández. «Los retos de la regulación de la Inteligencia Artificial: algunas aportaciones desde la perspectiva europea», en *Sociedad digital y Derecho*, ed. por Tomás de la Quadra Salcedo y José Luis Piñar Mañas (Madrid: Ministerio de Industria, Comercio y Turismo, 2018), 203-224.

Juan Francisco Rodríguez Ayuso, *Privacidad y Coronavirus: aspectos esenciales* (Madrid: Dykinson, 2020).

Juan Francisco Rodríguez Ayuso, «La firma electrónica como medio reforzado de verificación del consentimiento de los menores de edad en materia de protección de datos personales por parte de las Administraciones Públicas», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, n.º 53 (2020): 1-27.

Juan Francisco Rodríguez Ayuso, «Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos», *Revista de Derecho político*, n.º 110 (2021): 299-318.

Juan Francisco Rodríguez Ayuso, «Criterios para el acceso oficial de ciudadanos especialmente vulnerables a servicios prestados por las Administraciones Públicas», *Revista jurídica de Castilla y León*, n.º 53 (2021): 147-175.

Juan Francisco Rodríguez Ayuso, «Instrumentos cualificados para el registro identificativo en el entorno de la e-Administración Pública», *Revista española de Derecho administrativo*, n.º 210 (2021): 159-182.

Julián Valero Torrijos. «Los derechos en la era digital», en *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, ed. por Juan Francisco Rodríguez Ayuso (Cizur Menor: Aranzadi, 2022), 25-45.

Lina Keutzer y Ulrika Simonsson, «Medical device apps: an introduction to regulatory affairs for developers», *JMIR Mhealth Uhealth*, n.º 8 (2020): 6-21.

Manuel Carpio Cámara. «Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad», en *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, ed. por José Luis Piñar Mañas (Madrid: Reus, 2016), 335-350.

Manuel Medina Guerrero. «Categorías especiales de datos», en *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*, ed. por Artemi Rallo Lombarte (Valencia: Tirant lo Blanch, 2019), 251-274.

Marcial García Rojo, «mHealth (Salud móvil)», *I+S: Revista de la Sociedad Española de Informática y Salud*, n.º 110 (2015): 6-7.

María Falcón Romero y Aurelio Luna Ruiz-Cabello. «Las aplicaciones móviles en el ámbito sanitario. Consideraciones éticas y legales», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 15-32.

María Nélide Tur Fernández. «E-salud, derecho a la información y consentimiento informado», en *Bioderecho y retos: m-health, genética, IA, robótica y criogenización*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2022), 33-55.

Miguel Martínez Muñoz. «Los sujetos especialmente vulnerables ante los nuevos derechos digitales en el ámbito del consumo», en *Nuevos retos en materia de derechos digitales en un contexto de pandemia: perspectiva multidisciplinar*, ed. por Juan Francisco Rodríguez Ayuso (Cizur Menor: Aranzadi, 2022), 549-573.

Organización Mundial de la Salud, *Perfiles de países de Atlas eSalud: basados en los resultados de la segunda encuesta mundial sobre salud electrónica* (Ginebra: WHO Library Cataloguing-in-Publication Data, 2010).

Organización Mundial de la Salud, *eSalud: analizarán la aplicación de las tecnologías de la información y comunicación en la atención de la salud* (Ginebra: WHO Library Cataloguing-in-Publication Data, 2012).

Pilar Nicolás Jiménez. «Medicina personalizada de precisión y diagnóstico genético», en *Manual de Bioderecho (adaptado a la docencia en ciencias, ciencias de la salud y ciencias sociales y jurídicas)*, ed. por Carlos María Romeo Casabona, Pilar Nicolás Jiménez y Sergio Romeo Malanda (Madrid: Dykinson, 2022), 309-331.

Sandra Ferrer Gelabert. «E-salud: la tecnología al servicio de la salud», en *E-Salud, autonomía y datos clínicos. Un nuevo paradigma*, ed. por Cristina Gil Membrado (Madrid: Dykinson, 2021), 18-41.

World Health Organization, *Telemedicine: opportunities and developments in Member States* (Ginebra: WHO Library Cataloguing-in-Publication Data, 2010).

Yoneji Masuda, *The information society as post-industrial society* (New Brunswick: Transaction Publishers, 1980).

Zygmunt Bauman, *Tiempos líquidos. Vivir en una época de incertidumbre* (México D.F.: Tusquets Editores, 2007).