FACULTAD DE DERECHO

PROTECCIÓN DE DATOS E INTIMIDAD PERSONAL EN MATERIA DE *E-HEALTH*

Autor: Inés Colmenar Cascón

Curso: 5ºE-3 Analytics

Área: Derecho Constitucional

Tutor: Federico de Montalvo Jääskeläinen

Madrid

Abril de 2022

RESUMEN

La *e-Health* se constituye como el desarrollo de las TIC en el ámbito sanitario, abarcando desde la perspectiva puramente técnica hasta su aspecto más social. Como tal, esta tecnología entra en contacto, desde su incorporación, con datos de carácter especialmente sensibles, como lo son aquellos de tipo médico o sanitario. Por lo tanto, el ordenamiento jurídico prevé una serie de medidas preventivas y reactivas, a fin de garantizar su protección a través de la salvaguarda del derecho fundamental a la intimidad personal. La gestión de la pandemia ocasionada por la COVID-19 ha puesto de manifiesto algunos conflictos jurídico-morales en relación con la *e-Health*, por lo que este análisis pretende realizar una exposición del *status quo*, a fin de invitar al debate acerca de los principios que deberán informar las siguientes actuaciones de los poderes públicos.

Palabras clave: *e-Health*, derecho a la intimidad, protección de datos, TIC, RGPD, pandemia COVID-19.

ABSTRACT

E-Health is conceived as the development of ICT within the sanitary scope including, not only a purely technical perspective, but also the most social aspect thereof. As such, this technology gains contact, from the moment it is incorporated, with especially sensitive data, as is the case of medical or sanitary information. Therefore, the legal system provides for a series of preventive and reactive measures to guarantee its protection by safeguarding the fundamental right to personal privacy. The management of COVID-19 pandemic has raised some legal and even moral conflicts in relation to e-Health. This analysis aims to present the status quo in order to then promote a debate on the principles that should inform the subsequent actions of public authorities with relation to e-Health.

Keywords: *e-Health, right to privacy, data protection, ICT, GDPR, COVID-19 pandemic*.

Listado de abreviaturas

TIC Tecnologías de la Información y la Comunicación

JMIR Journal of Medical Internet Research

OMS Organización Mundial de la Salud

OPS Organización Panamericana de la Salud

CE Constitución Española de 1978

CUDH Carta Universal de Derechos Humanos

TCFA Tribunal Constitucional Federal de Alemania

CDF Carta de Derechos Fundamentales de la Unión Europea

UE Unión Europea

TEDH Tribunal Europeo de Derechos Humanos

RGPD Reglamento General de Protección de Datos

PE Parlamento Europeo

AEPD Agencia Española de Protección de Datos

LOPD Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales

LAP Ley de Autonomía del Paciente

TS Tribunal Supremo

Índice.

Capítulo 1. INTRODUCCIÓN.

El acelerado desarrollo de la tecnología en las últimas décadas y todo lo que ello conlleva está conduciendo a una evolución sin precedentes, concretada en una transformación en la manera en la que las personas trabajan y se relacionan. Si bien son los cambios en estos ámbitos los que más consideración y comentarios reciben, por su obviedad y cotidianeidad, el avance de la tecnología está afectando en muchos más aspectos de nuestra vida, incluso más importantes que los mencionados, como es la salud. Desde hace ya unos años, el término *e-Health* se encuentra extendido como el desarrollo tecnológico en el marco sanitario, si bien no acaparaba la misma atención que otros avances, por su aparente menor relevancia práctica. Sin embargo, tras haber presenciado la gestión de la pandemia ocasionada por la COVID-19, esta tecnología ha dejado de ser una nimiedad para la mayoría de los ciudadanos, puesto que ha constituido, en gran parte, el soporte de las medidas sanitarias preventivas y de contención de la propagación de contagios.

En cualquier caso, toda novedad, especialmente en el caso de los avances tecnológicos, supone un elemento disruptivo en el orden preexistente. Este análisis se centrará, por tanto, en la adaptación de la *e-Health* en el marco del ordenamiento jurídico español y comunitario, específicamente en lo que a la salvaguarda de los derechos fundamentales a la intimidad y protección de datos respecta. Los derechos de la personalidad, como se analizará con posterioridad, se encuentran íntimamente vinculados a la dignidad humana y es por ello por lo que su protección debe garantizarse en todo caso. Asimismo, como consecuencia de sus características propias, sufren un mayor riesgo de vulneración como consecuencia del desarrollo tecnológico e informático. Al fin y al cabo, la información recabada y tratada por medios electrónicos corre un mayor riesgo de escapar a los límites adecuadamente marcados como necesarios.

La *e-Health*, concretamente, aspira a alcanzar una comunidad de usuarios en un entorno digital, donde los datos se encuentren perfectamente almacenados y delimitados, en concordancia con los respectivos ordenamientos jurídicos. Para ello, resulta tremendamente importante definir los límites que deberán, en todo caso, observarse; así como los espacios en los que el desarrollo se encuentra menos coartado, para así poder consolidar los avances de manera segura y coherente con el sistema. Es por esto por lo que el presente análisis se

encuentra perfectamente justificado: para poder construir un entorno de desarrollo sostenible en el ámbito sanitario, es necesario que se avive el debate racional, teleológico y jurídico acerca de los límites de la tecnología en el mismo, específicamente aquellos relacionados con los datos personales, por su vital importancia para el libre desarrollo de la personalidad.

El objetivo del análisis es, por lo tanto, la identificación de puntos sensibles en lo que a la protección de datos e intimidad personal en relación con la introducción de la *e-Health* respecta. De esta manera, se pretende localizar aquellos aspectos que requieren una especial atención por parte del legislador y del desarrollador, así como de las instituciones que hacen uso de esta tecnología, a fin de obtener un punto de partida para el debate acerca de la adecuación del ordenamiento jurídico a las circunstancias actuales del sector sanitario.

Para la consecución de dicho objetivo, la metodología a seguir se fundamenta en la permanente adaptación del ordenamiento jurídico a las necesidades de las personas que conforman la sociedad regida por el mismo. Así, no se pretende criticar el desarrollo por su incompatibilidad con las bases sentadas por el orden preexistente en materia de derechos de la personalidad, sino que se enfoca el análisis en la delimitación de extremos para el examen y armonización de lo restante.

En este sentido, la estructura del estudio se encuentra claramente delimitada en tres partes diferenciadas. Comienza con el análisis del concepto de *e-Health* y algunos de los cambios que con ella vienen implícitos, para continuar con la profundización en el derecho a la intimidad personal y a la protección de datos. Finalmente, el estudio culmina con la convergencia de ambos, a partir de una discusión informada acerca de la situación jurídica actual en materia de protección de datos en *e-Health* en el marco español y comunitario. Se introduce, además una reflexión acerca del pasaporte de inmunidad COVID a modo de conclusión del estudio.

Capítulo 2. DEFINICIÓN DE *E-HEALTH* EN EL MARCO DE LAS TIC EN SANIDAD.

El concepto de *e-Health* no puede sino definirse de manera dinámica, puesto que, en lugar de adquirir una definición determinada e inamovible, a medida que evoluciona la tecnología en el sector sanitario, el espectro de su significado se va ampliando. Teniendo esto en cuenta, resulta procedente realizar un recorrido de las definiciones que ha ido adquiriendo la *e-Health* a lo largo de los últimos años, desde el momento en el que empezó a hacerse uso del término en el marco de salud y sanidad.

2.1 *E-HEALTH* A PRINCIPIOS DEL SIGLO XXI: CARACTERIZACIÓN DEL CONCEPTO A TRAVÉS DE LAS 10 "E'S".

Hasta 1999, el término *e-Health* era totalmente desconocido para el público general. El auge de este amplio concepto tuvo lugar a principios del siglo XXI, cuando los continuos avances fruto de la investigación y desarrollo en el sector de las TIC[1] dificultaban enormemente la tarea de alcanzar una definición contrastada y homogénea, puesto que pocos expertos tenían una clara percepción de lo que realmente implicaba su incorporación para el sector sanitario. Teniendo esto en cuenta, en aquel primer momento predominaba la tendencia de definir el concepto de *e-Health* como un compendio de avances tecnológicos en materia sanitaria, así como la manera de razonar y actuar de la propia sociedad en relación con estos. Analizándolo ahora de manera retrospectiva, se puede concluir que, a principios de siglo, el término *e-Health* comprendía también una expectativa y predisposición a la interconectividad y globalidad en asuntos relacionados con la salud.

El investigador G. Eysenbach aportó en este contexto una definición integral del concepto, tratando la *e-Health* como un "campo emergente en la intersección de la informática médica, salud pública y las iniciativas privadas, en referencia a los servicios de salud y la información entregada o mejorada a través de Internet y las tecnologías relacionadas". Asimismo, ofreció también una definición más amplia, afirmando que el término comprendía "no sólo un

[1] Tecnologías de la Información y la Comunicación. *Vid.* Listado de abreviaturas.

desarrollo técnico, sino también un estado de ánimo, una manera de pensar, una actitud y un compromiso para las redes y el pensamiento global, para mejorar la atención de la salud a nivel local, regional y mundial mediante el uso de tecnología de información y comunicación" (Eysenbach, 2001).

En este sentido, resulta relevante traer a colación las denominadas "10 e's en *e-Health*"[2], concepto acuñado también por Eysenbach[3] a través del JMIR[4] en el año 2001 y que aún hoy sirve para acotar lo que comprende la *e-Health*. Estas diez características pretenden aportar un marco teórico para la definición del concepto y comprensión de sus implicaciones. A fin de destacar las más relevantes para el objeto de este análisis, la eficiencia (*efficiency*) es una de las constantes en materia de *e-Health*, puesto que su misión incluye, intrínsecamente, el acortamiento de procesos administrativos y técnicos y aumento en la rapidez en los trámites, minimizando así los costes. Sin embargo, esta eficiencia en los procesos carecería de su verdadero sentido sin la mejora en la calidad de servicio (*enhancing quaility of care*), ya que la interconectividad sanitaria que se pretende alcanzar tiene como objetivo facilitar la experiencia de los pacientes y profesionales del sector, permitiendo así ofrecer un servicio de mejor calidad a un mayor espectro de individuos.

Asimismo, resulta importante destacar el empoderamiento (*empowerment*) que se pretende otorgar a los pacientes a través de esta tecnología. El JMIR afirma que la *e-Health* refuerza la educación en salud de los individuos, así como el autoconocimiento y control de sí mismos, incrementando su poder de decisión y posibilidades de actuación ante cualquier condición o circunstancia médica. A lo largo del presente análisis, se discutirá la veracidad de esta afirmación, contrastando la teoría con la práctica observada a lo largo de los últimos veinte años.

Por último, puesto que este estudio pretende enfocarse en los derechos constitucionales en relación con la *e-Health*, resulta de especial relevancia la ética (*ethics*) de la misma, a la que el propio JMIR se refiere de manera abstracta e indefinida, pero indudablemente necesaria,

---

[2] Las 10 "e's" de *e-Health*, más allá del obvio *electronic*: *efficiency*, *enhancing quality of care*, *evidence based*, *empowerment*, *encouragement*, *education*, *enabling information exchange and communication*, *extending the scope*, *ethics*, *equity*.
[3] Eysenbach, G. (2001). *What is e-health?* Journal of medical Internet research, 3(2), e20.
[4] Journal of Medical Internet Research. *Vid.* Listado de abreviaturas.

en el contexto de la tecnología sanitaria[5]. Ya a principios de siglo se preveían las amenazas y retos que el uso de la tecnología avanzada en el ámbito de la salud ha resultado presentando en la actualidad, por lo que la ética no podía, en ningún caso, separarse de su definición.

2.2 *E-HEALTH* Y CONCEPTOS RELACIONADOS: ACOTANDO EL SIGNIFICADO.

A lo largo de los últimos años, la discusión acerca de la *e-Health* ha venido acompañada de otros términos como son la *m-Health*[6], la telemedicina o la Salud 2.0. Como consecuencia de la relevancia que las TIC han adquirido en el marco sanitario, resulta imprescindible alcanzar una definición distintiva de la *e-Health* en relación con estos conceptos, a fin de evitar su confusión.

A estos efectos, conviene analizar la manera en la que la OMS[7] y la OPS[8] definen la *e-Health* en el marco de sus medidas políticas y estratégicas: "La *e-Health* consiste en el apoyo que la utilización costo-eficaz y segura de las tecnologías de la información y las comunicaciones ofrece a la salud y a los ámbitos relacionados con ella, con inclusión de los servicios de atención de salud, la vigilancia y la documentación sanitaria, así como la educación, los conocimientos y las investigaciones en materia de salud" (Fernández Silano, 2013). En el caso de la OMS, concretamente, esta definición se remonta al año 2005, durante la 58ª Asamblea Mundial de la Salud, en la que se impulsó una estrategia global para la *e-Health*.

Como se puede apreciar, esta definición se enfoca principalmente en la eficacia intrínseca a la *e-Health*, mencionada también anteriormente en el enfoque de Eysenbach[9]. En cualquier caso, a diferencia de lo aportado por este último, ambas organizaciones prescinden del componente más social de estas tecnologías, al no referirse en ningún caso a la interconectividad o construcción de una comunidad de salud que se pretende alcanzar por medio de ellas. Independientemente de ello, adoptando ambas organizaciones una definición técnicamente amplia, se pueden apreciar en ellas algunos principios que se pretenden

[5] *Ibíd*, nota 3.
[6] *Mobile health*, salud móvil.
[7] Organización Mundial de la Salud. *Vid*. Listado de abreviaturas.
[8] Organización Panamericana de la Salud. *Vid.* Listado de abreviaturas.
[9] *Íbid*, nota 3.

vincular al concepto de *e-Health* y que nos permiten discernir este de otros términos que, en lo que a el presente análisis respecta, se incluyen en el mismo.

En este sentido, optando por una definición amplia, la *e-Health* engloba los conceptos de telemedicina y telesalud, entendiendo el primero de manera más global, como el uso de las TIC para el ejercicio de la profesión a distancia; y el segundo de manera más acotada, ya que se focaliza en sistemas de prevención de enfermedades. Asimismo, la *m-Health* está también incluida en el espectro de la *e-Health* y se refiere al acceso a servicios sanitarios por medio de los pacientes a través de dispositivos móviles, como puede ser un *smartphone*. Por último, cabe destacar el concepto de *e-Learning* como principio imprescindible para que la *e-Health* logre el empoderamiento del paciente, como preveía ya Eysenbach[10]. Consiste, de manera concisa, en el uso de las TIC para el conocimiento y monitorización de la salud personal.

Cabe hacer alusión a una sección de la comunidad de investigación de las TIC en el sector sanitario que se refiere a la mencionada *m-Health*, así como a la *t-Health*[11], como una evolución de la *e-Health*, en lugar de plantearse como componentes de esta. En cualquier caso, si bien es cierto que la mayoría de las aplicaciones prácticas de la *e-Health* conciernen el uso de un dispositivo móvil, para los efectos de este análisis resulta más apropiado considerar la *m-Health* como uno de los conceptos englobados en la *e-Health*, en lugar de contemplarlo como una versión evolucionada de la misma. En lo que a la *t-Health* respecta, se define como "todo servicio sanitario que se ofrece a través de la televisión interactiva" (de Abajo, 2011). La idea que trasciende a esta tecnología consiste, en la práctica, en la capacidad de los ciudadanos de concertar una cita médica mediante el uso de las mismas herramientas con las que ven diferentes programas en televisión digital. De nuevo, esta tecnología se considerará, para el propósito del presente análisis, incluida en el significado de *e-Health*.

Conviene analizar, en este punto de la investigación, un concepto llamado Medicina 2.0[12], que surge del entorno de la Web 2.0, término acuñado por primera vez a mediados de 2004

[10] *Íbid*, nota 3.
[11] *Television health*, salud televisiva.
[12] En función de las preferencias técnicas del entorno, este concepto recibe el nombre de Medicina 2.0 o Salud 2.0, sin perjuicio de que su significado se mantenga idéntico.

por Tim O'Reilly[13] y definido por el mismo como la red "social" médica, en tanto que su principal activo reside en su continua actualización y mejora a medida que aumenta el número de usuarios, de manera que se crean "efectos de red a través de una arquitectura de participación, yendo más allá de la metáfora de la página de la Web 1.0 para ofrecer experiencias integrales al usuario" (O'Reilly, 2005).

Optando por una definición simple, la Medicina 2.0 consiste en la adopción de la tecnología de la Web 2.0 por parte de la medicina, aportando así una serie de herramientas sociales disponibles tanto para profesionales de la salud como para pacientes. El pilar principal de estas herramientas reside en la interconectividad de las personas que aspiran a formar parte de una misma comunidad, a fin de publicar y encontrar información del ámbito sanitario que les resulte de interés (Fernández Cacho, 2016).

En definitiva, la Medicina 2.0 encajaría dentro del espectro de la *e-Health* según la definición aportada por Eysenbach[14], materializando la séptima "e" de su previamente mencionada lista de características atribuidas a ella: permitir el intercambio de información y la comunicación (*enabling information exchange and communication*). En cualquier caso, la inclusión de la Medicina 2.0 como parte de la *e-Health* no carece de controversia. Por ejemplo, el foco en las redes sociales no encuentra un lugar tan obvio en la visión aportada por la OMS, ya que esta se centra puramente en su aspecto más técnico.

Tratándose la *e-Health* de un concepto no solo técnico, sino también social y esencialmente dinámico, resulta lógico que no pueda aportarse una única definición para el mismo. Tras el análisis de sus diferentes atributos y principios, resulta pertinente alcanzar una definición que sirva como punto de partida para el posterior estudio de la protección de datos en salvaguarda del derecho fundamental a la intimidad personal. Por lo tanto, utilizando las diez "e's" de Eysenbach[15] como base, acotada por la visión más concisa de la OMS, para el propósito del presente análisis se define la *e-Health* como el conjunto de herramientas basadas en la aplicación de las TIC en el ámbito de la medicina y salud, caracterizadas por

[13] Tim O'Reilly acuñó el término Web 2.0 en el entorno de O'Reilly Media, una editorial cuyas publicaciones guardan estrecha relación con la informática. En años posteriores, O'Reilly tuvo gran importancia en lo que a la popularización del concepto respecta (Fernández Silano, 2013).
[14] *Íbid*, nota 3.
[15] *Íbid*, nota 2.

la eficiencia de su uso y su vocación de empoderamiento de la comunidad de profesionales y pacientes.

2.3 La popularización de la *e-Health* a través de la gestión de la pandemia ocasionada por la COVID-19.

La gestión de la pandemia ocasionada por la COVID-19 se ha caracterizado por el intensivo uso de los medios tecnológicos y el análisis de datos masivos. En este sentido, ha supuesto también una oportunidad para la experimentación de múltiples herramientas de *e-Health*, aprobadas con mayor rapidez debido a la urgencia y magnitud de la situación. En líneas generales, el principal dilema jurídico atribuido a este tipo de gestión se concreta en la ponderación del interés colectivo de la salud global frente al derecho subjetivo a la intimidad.

Sin perjuicio de las implicaciones jurídicas que en materia de protección de datos puedan tener, en este punto se pretende aportar una visión genérica del tipo de herramientas utilizadas en la gestión de la pandemia, puesto que esta ha supuesto un punto de inflexión en lo que al avance e incorporación de la *e-Health* respecta. En este sentido, las grandes novedades tecnológicas se pueden concretar en tres: geolocalización de individuos, aplicaciones de rastreo de contagios y pasaportes digitales de inmunidad.

En lo que a la geolocalización de individuos respecta, se trata de la medida menos invasiva y desconocida, puesto que, con anterioridad a la pandemia, ya estaba generalizado el registro de la ubicación de usuarios por parte de determinadas aplicaciones móviles. Asimismo, desde hace años, a través de una mera búsqueda en internet, el sitio web correspondiente goza de la capacidad de registrar y utilizar de manera anonimizada este tipo de datos[16]. En cualquier caso, es cierto que la pandemia ha puesto de manifiesto la utilidad colectiva de la geolocalización electrónica, así como los riesgos que acarrea a nivel individual. En definitiva, no se trata de algo técnicamente novedoso, si bien su relevancia ha aumentado de

[16] Los sitios web registran y almacenan gran cantidad de información acerca de la localización e intereses de aquellos usuarios de los que reciben visitas, generalmente con fines comerciales. En cualquier caso, el tratamiento de estos datos deberá realizarse de manera anonimizada, en concordancia por lo prescrito por el ordenamiento jurídico. *Vid*. Capítulo 6.2.2. *Cookies* y registro de búsquedas en internet.

manera exponencial como consecuencia de la nueva situación derivada de la amenaza de la COVID-19.

La geolocalización puede ser registrada tanto por los operadores de telecomunicaciones como por distintas redes sociales. En cualquier caso, esta información se proporciona exclusivamente de manera anonimizada, a excepción de que se exija lo contrario por demanda de las Fuerzas y Cuerpos de Seguridad, previa orden judicial (Agencia Española de Protección de Datos, 2020). Esto permite la construcción de una detallada base de datos para el control y análisis de los movimientos de la población bajo los regímenes de confinamiento, lo cual, implementado de manera adecuada y proporcional, revierte en una gran utilidad para el interés colectivo de la salud.

En esta misma línea, las aplicaciones desarrolladas para el rastreo de contagios suponen un paso adicional a la geolocalización de usuarios. A través de ellas, se recoge la ubicación de los individuos contagiados que, voluntariamente, decidan notificarlo. Realmente, se trata de una combinación de dos prácticas: la notificación obligatoria a las autoridades de un contagio por COVID-19 y la geolocalización de usuarios proporcionada por medio de los teleoperadores o redes sociales. A través de esta combinación, el riesgo para la protección de datos personales se ve incrementado, ya que el crucial anonimato pierde ciertas garantías. Sin embargo, la contribución a la salud pública de la base de datos resultante de esta práctica es verdaderamente notable, ya que permite la integración de dos importantes piezas en la gestión de la pandemia: la ubicación de la población y el número de contagios.

Posiblemente, la mayor novedad resultante de la pandemia en términos de *e-Health* se concreta en los llamados pasaportes de inmunidad. Por su compleja configuración a nivel jurídico, ya que se manejan conceptos altamente sensibles en cuanto a intimidad y discriminación, han sido objeto de múltiples discusiones a nivel supranacional. De hecho, no se ha alcanzado un consenso total en cuanto a la legitimidad de su uso, debido a conflictos morales plasmados en el ordenamiento jurídico sobre los que se reflexionará al final de este análisis[17]. En cualquier caso, su utilidad para el interés común resulta evidente, puesto que se configura como un documento certificado que permite comprobar la supuesta protección

[17] *Vid.* Capítulo 7. Pasaporte COVID: reflexión y conclusiones.

de un individuo frente a la COVID-19, bien por medio de una pauta completa de vacunación, bien a través de la obtención de anticuerpos gracias a una recuperación reciente o bien por medio de una prueba de resultado negativo.

Si bien, actualmente, se cuestiona la utilidad de estos pasaportes por la comprobada ineficacia de las vacunas frente al contagio, es importante tener en cuenta que estas se administraron con la convicción de que tendrían el efecto deseado. El estudio empírico ha demostrado, con posterioridad a su implantación *quasi* obligatoria en numerosos estados, que el beneficio de la vacunación es más individual que colectivo, puesto que, si bien protege al individuo de los efectos adversos del virus, no parece proteger a los demás de ser contagiados por él[18]. En el futuro próximo, deberá definirse la utilidad de estos pasaportes, que se encontrará estrechamente relacionada con el avance de la pandemia y el desarrollo de otras potenciales situaciones equiparables a esta.

[18] Si bien tiene poca relevancia para los efectos de este estudio, resulta importante incidir en que la utilidad colectiva de la vacunación contra la COVID-19 radica en la liberación del sistema sanitario que, durante los meses de marzo, abril y mayo de 2020 sufrió un elevado colapso. Esta liberación revierte en la población en su conjunto, ya que permite conservar la garantía del derecho a la salud, entendido como el acceso al sistema sanitario.

Capítulo 3. LA NUEVA RELACIÓN ENTRE PACIENTE Y DOCTOR, IMPULSADA POR LA *E-HEALTH*.

El desarrollo de las TIC tiene como uno de sus principales objetivos, en cualquier ámbito en el que tenga aplicación, alcanzar una manera más eficiente de obtener los resultados pretendidos. A continuación, se analizarán los potenciales conflictos jurídicos y morales que la *e-Health* puede conllevar en lo referente a la relación entre médico y paciente, por lo que es importante iniciar el estudio incidiendo en este punto en los muchos beneficios que esta tecnología ofrece. Realmente, se están produciendo avances transformacionales que, en muchos aspectos, tienen la capacidad de conducir a una asistencia médica de mayor calidad, así como a una mejor educación personal en salud. Precisamente en estos avances radica el interés práctico por el desarrollo de esta disciplina, a pesar de los conflictos jurídicos y morales que pueda plantear.

3.1 EL PAPEL DE LA TECNOLOGÍA COMO SUSTITUTORIA DEL MÉDICO Y POSIBLES CONFLICTOS MORALES.

La introducción de las TIC en materia de salud ha reavivado el debate acerca de la relación médico-paciente, que ya en las últimas décadas del siglo pasado albergaba distintas opiniones. Con anterioridad a la proliferación de la *e-Health*, se hablaba de una reconfiguración comunicacional entre dos modelos de relación. El primero de ellos, basado en una relación de carácter paternalista en la que el paciente adopta una posición pasiva y acepta sin mayor reserva las indicaciones del médico. El segundo, más moderno y disruptivo, con foco en el espíritu crítico y autonomía del paciente, que es consciente de su capacidad de decisión en lo que a su integridad física respecta, y por tanto dialoga con el médico y contrasta la información obtenida de distintas fuentes (Petracci, 2020).

En este contexto, la incorporación de la *e-Health* desde principios del siglo XXI, así como su aceleradísimo desarrollo en la última década, ha puesto de manifiesto una tercera vertiente en lo que a la relación médico-paciente respecta, que encuentra su punto de partida en la autonomía del paciente, impulsada por la libertad y disponibilidad de información.

Asimismo, se aborda la agilización de procesos sanitarios a través de la tecnología. Con esta reinterpretación del papel del paciente y actuación del médico, surgen también riesgos en dos principales frentes. En primer lugar, en relación con la fiabilidad de la información obtenida por el paciente por medios alternativos al propio médico; y en segundo, con respecto a la seguridad de los datos personales registrados en medios telemáticos, lo que se analizará en detalle a lo largo de este análisis (Petracci, 2020).

Actualmente, es muy frecuente oír hablar de la "sociedad del dato", lo que hace referencia precisamente a la mencionada libertad y accesibilidad de información. Sin perjuicio de ello, o precisamente como consecuencia de esta desmesurada disponibilidad, podría hablarse también de la "sociedad de la desinformación". Naturalmente, la cantidad no equivale a calidad y, si bien la información correcta puede obtenerse a través de internet, es necesario tener para ello un espíritu crítico, alcanzado a través de un profundo conocimiento previo de la materia. Esta aproximación resulta especialmente relevante en el campo de la salud, por su amplitud y sensibilidad. El paciente "proactivo", definido anteriormente, se desarrolla en el ámbito de la *e-Health* de manera peligrosamente autónoma, asumiendo el riesgo de la desinformación. Precisamente por ello, teniendo en cuenta la rapidísima -y prácticamente obligatoria, como consecuencia de la pandemia ocasionada por la COVID-19- transición a la vía telemática de muchos procesos médicos que anteriormente eran de naturaleza exclusivamente presencial, es importante asegurar la protección de la salud a través de las TIC, de la misma manera que se asegura con las intervenciones personales del médico.

El derecho a la salud, entendido en el ordenamiento jurídico español como una garantía especialmente protegida y, por naturaleza, competencia de los poderes públicos, comprende una serie de deberes atribuidos a estos, en salvaguarda de su contenido esencial como derecho subjetivo[19]. En desarrollo de esta garantía, la Ley 14/1986[20], establece los criterios sustantivos que rigen la actuación de los poderes públicos, comprendiendo aspectos organizativos y estructurales. Para los efectos de este análisis, resulta de especial interés el

[19] "2. Compete a los poderes públicos organizar y tutelar la salud pública a través de medidas preventivas y de las prestaciones y servicios necesarios. La ley establecerá los derechos y deberes de todos al respecto" (Artículo 43 CE).
[20] Ley 14/1986, de 25 de abril, General de Sanidad.

Capítulo I de la referida Ley, que enuncia los principios generales que deberán informar la actuación pública en el ámbito sanitario.

En este sentido, el artículo 6 de esta Ley 14/1986 guarda especial concordancia con el papel del paciente "proactivo" explicado anteriormente, estableciendo una clara tendencia por parte de las Administraciones Públicas con respecto a sus actuaciones en materia de sanidad. Concretamente, deberán "promover el interés individual, familiar y social por la salud mediante la adecuada educación sanitaria de la población". Este precepto, que sirve de guía orientativa para la actividad pública en garantía del derecho a la salud, adquiere un significado diferenciado en el contexto de la tecnología *e-Health*, como consecuencia de las posibilidades que esta ofrece al paciente proactivo. Precisamente por esta razón, es importante entender estas directrices en el contexto íntegro de la Ley 14/1986, pudiendo así inferirse que la promoción del individuo interesado e informado en su propia salud no pretende tener un alcance tan individual como colectivo. El legislador trata de asegurar una adecuada educación en salud de la población general, acorde con el estado de bienestar propio de las últimas décadas. Se trata, por tanto, de la promoción de una conciencia general en lo que a salud respecta, no así de un pretendido traspaso del conocimiento y experiencia propios de los profesionales a la población general. Este matiz tiene una especial relevancia por el efecto multiplicador de las actuaciones de la Administración Pública; el impacto de estas varía enormemente con un leve cambio en su orientación.

3.2 POSICIONAMIENTO DE LA *E-HEALTH* EN EL CENTRO DEL DEBATE MÉDICO COMO CONSECUENCIA DE LA GESTIÓN DE LA PANDEMIA OCASIONADA POR LA COVID-19.

La relevancia de la relación entre médico y paciente y las posibles modalidades en las que esta puede presentarse responden a un debate surgido en la segunda mitad del siglo XX, si bien es cierto que la gestión de la pandemia de la COVID-19 ha traído al presente el fervor de ciertos aspectos de la discusión que parecía haberse amainado. Sin perjuicio de que las aplicaciones móviles de salud hayan tenido su auge en los últimos diez años, con el desarrollo de la nanotecnología y la conexión de datos 3-, 4- y 5G, es importante incidir en

que el trasfondo de la discusión que avivan estas tecnologías comenzó a finales del siglo pasado[21].

En este sentido, resulta importante definir los vértices más relevantes de la influencia de las TIC en la relación entre médico y paciente. Por un lado, desde el punto de vista del desarrollo, permiten al personal médico lograr un mayor alcance y seguimiento de aquellos pacientes a los que, por razones de tiempo o geografía, no podrían ofrecer estas prestaciones de otra manera. No solo esto, sino que también se propicia una mayor interconectividad entre profesionales de la salud, permitiendo el intercambio de conocimiento y opiniones y fomentando una discusión informada dirigida a un más rápido avance en la investigación médica (Petracci, 2020).

Por otro lado, desde el punto de vista más conservador, resulta preciso tener en cuenta que la humanidad se halla en la "era de la desinformación", en la que, al existir tanta información a disposición de (casi) todo el mundo, la carencia de pensamiento crítico resulta en un profundo desconocimiento, fruto de una falsa seguridad generada por un entendimiento erróneo de la información obtenida de la red. Esta desinformación se genera también en los pacientes que, al encontrarse en un "nuevo" entorno de salud en línea, y acostumbrados a hallar todas las respuestas en la red, recurren al peligroso autodiagnóstico, dudando e incluso prescindiendo de la opinión médica.

[21] "(…) desde la década de los años ochenta, la RMP (relación médico paciente) asiste a los cambios originados por las tecnologías de la información y la comunicación (TIC) en la interface comunicación y salud, por ejemplo, las prácticas de *eHealth* en la vigilancia sanitaria, las tecnologías móviles destinadas a transmitir mensajes sobre cambios en los comportamientos para prevenir enfermedades y mejorar la calidad de vida, el desarrollo de *big data*, genómica e inteligencia artificial" (Petracci, M., & Cuberli, M. (2020)).

Capítulo 4. DERECHO A LA INTIMIDAD PERSONAL

Tras el análisis conceptual de lo que supone la *e-Health* en el entorno sanitario, resulta procedente realizar una profundización teórico-práctica del derecho a la intimidad personal, a fin de examinar, posteriormente, su protección con respecto a los avances tecnológicos en salud.

4.1 CONFIGURACIÓN Y CONTENIDO ESENCIAL DEL DERECHO A LA INTIMIDAD PERSONAL.

El derecho a la intimidad personal encuentra su fundamento en la libertad inherente a cada individuo, configurándose generalmente como uno de los derechos de la personalidad[22], cuya vocación es permitir su libre desarrollo. El contenido esencial de este derecho, así como la razón por la que resulta imprescindible en los ordenamientos jurídicos, reside en la capacidad de autodeterminación de cada individuo, alcanzada mediante la posibilidad de ejercer el control acerca de lo que se conoce sobre uno mismo.

Con base en su importancia, la intimidad personal se reconoce como derecho fundamental y se protege como tal desde mediados del siglo XX, incluyéndose en la CUDH[23] de 1948, en su artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". En cualquier caso, las últimas décadas se caracterizan por el aceleradísimo desarrollo de las TIC, conllevando grandes implicaciones para la concepción de la privacidad.

[22] Los derechos de la personalidad buscan garantizar la libertad de cada individuo respecto a sus atributos más personales y propios, diferenciándose entre ellos, en gran medida, en función del ámbito de características que pretenden proteger (de Montalvo Jääskeläinen, 2016). Tratándose de derechos de la personalidad, se encuentran íntimamente ligados a la dignidad humana, tal y como se extrae del artículo 10 de la CE, resultando incluso más importantes los mecanismos previstos por el ordenamiento jurídico para su protección (Villanueva-Turnes, 2016).

[23] Carta Universal de Derechos Humanos. *Vid.* Listado de abreviaturas.

Específicamente, el factor más condicionante de la nueva percepción de la intimidad personal es el tratamiento masivo de datos, que supone una amenaza a la seguridad que estos deben preservar en salvaguarda del mencionado derecho fundamental. Como respuesta a esta situación, se ha desarrollado un concepto adicional, denominado el derecho a la intimidad informática o autodeterminación informativa. Este derecho fue acuñado por el TCFA[24] en 1983, por el cual cada individuo goza de derecho a decidir libremente la información personal que comparte, así como a imponer el momento en el que llevar a cabo la comunicación y los límites que para ello considere. Sin perjuicio de la protección que se pretende otorgar frente a la recopilación de datos personales, es importante incidir en el verdadero problema que existe en el contexto de los datos masivos, ya que la controversia no se encuentra tanto en su mero almacenamiento, como en el uso que de los mismos se hace (Cuadrada, 2007).

Desenvolviéndonos, en el momento actual, en un claro entorno VUCA[25], los avances tecnológicos tienden a sobrepasar la velocidad de adaptación de los ordenamientos jurídicos, por lo que resulta de enorme importancia atender a la evolución del *status quo* de la tecnología en los ámbitos que más impacto tienen en los derechos fundamentales. En este sentido y sin necesidad de una explicación exhaustiva por el momento, cabe realizar una breve alusión a la relevancia que para las empresas han cobrado los datos masivos y lo necesarios que resultan para alcanzar una verdadera competitividad de mercado. Esta situación ha derivado en el negocio de compraventa de datos, resultando en que, hoy en día, la recopilación de datos supone una importante fuente de ingresos para muchas empresas que gozan de un fuerte componente tecnológico, materializada mediante la venta de estos a otras entidades que los utilizan para la determinación de su estrategia, como puede ser la especialización de sus campañas de marketing.

En lo que a este análisis respecta, resulta importante conocer la motivación que existe, en cada caso, para la recopilación de datos personales, a fin de entender la necesidad de proveer a los individuos con una protección frente a la misma, como se analizará posteriormente en el marco jurídico de la protección de datos.

[24] Tribunal Constitucional Federal de Alemania, *Vid.* Listado de abreviaturas.
[25] Entorno VUCA, definido por sus siglas como volátil (*volatile*), incierto (*uncertain*), cambiante, (*changing*) y ambiguo (*ambiguous*).

4.2 Derecho a la vida privada en el marco de la Unión Europea.

El derecho a la intimidad personal está recogido en el artículo 7 de la CDF[26] de la UE[27], como el derecho al respeto de la vida privada y familiar: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones". A nivel supranacional, el derecho a la vida privada es equiparable al derecho a la intimidad personal recogido en el ordenamiento jurídico español, puesto que el contenido de ambos resulta equivalente.

Es importante resaltar que la interpretación de las disposiciones internacionales con respecto a los derechos fundamentales depende, en gran medida, del posicionamiento de los respectivos órganos del poder judicial (Maqueo Ramírez, 2017). En este sentido, el TJUE, entre otros organismos, incide en la clara delimitación del derecho a la vida privada frente a la protección de datos, caracterizando aquel con carácter negativo o defensivo y este con carácter positivo o activo (Martín, 2021). Sin perjuicio de lo anterior, la protección de datos y el derecho a la vida privada -o intimidad- guardan una estrechísima relación, ya que el objeto del primero incluye al segundo. Por lo tanto, procede profundizar en el derecho a la intimidad personal en el ordenamiento jurídico español, para así poder concretar posteriormente el marco normativo de la protección de datos, precisando específicamente su contenido y analizando el impacto de las tecnologías de *e-Health* sobre el mismo.

4.3 Derecho a la intimidad personal en el ordenamiento jurídico español. Énfasis en el derecho a la libertad informática.

4.3.1 Delimitación del derecho a la intimidad personal en el marco del artículo 18.1 de la Constitución Española.

El derecho a la intimidad personal está recogido en el ordenamiento jurídico español en el artículo 18.1 de la CE[28], de manera que "Se garantiza el derecho al honor, a la intimidad

[26] Carta de Derechos Fundamentales. *Vid.* Listado de abreviaturas.
[27] Unión Europea. *Vid.* Listado de abreviaturas
[28] Constitución Española. *Vid.* Listado de Abreviaturas.

personal y familiar y a la propia imagen". Del tenor literal del texto se extrae una referencia a tres derechos distintos y diferenciados, a pesar de encontrarse enunciados en el mismo artículo constitucional. La asociación lógica que de esta agrupación surge resulta natural, puesto que los tres derechos, formando parte de los llamados derechos de la personalidad, se fundamentan en la capacidad del individuo de decidir cuánto y de qué manera expone ante el mundo su vida personal. Por su ubicación en el texto constitucional, en la Sección 1ª del Capítulo Segundo, estos derechos tienen la consideración de fundamentales, gozando, por tanto, del mayor grado de protección ofrecido por el ordenamiento jurídico español.

En cualquier caso, a fin de delimitar el contenido esencial del derecho a la intimidad personal en el ordenamiento jurídico español, resulta necesario hacer una breve alusión al derecho al honor y a la propia imagen, con el objetivo de que la diferenciación entre estos y aquel quede claramente expuesta. En este sentido, el significado del derecho a la propia imagen adquiere un amplio espectro, en tanto que protege de cualquier intromisión a los atributos personales, y no necesariamente íntimos, de un individuo, sin necesidad de que dicha intromisión se presente de manera negativa o dañina para su propia imagen. A grandes rasgos, en esta definición se encuentran las principales diferencias entre el derecho a la imagen y el derecho al honor y a la intimidad personal. Por un lado, el derecho al honor protege aquellas intromisiones que sí resultan denigrantes o dañinas, dentro de la objetividad de las normas vigentes en el momento de la intromisión. Por otro lado, el derecho a la intimidad personal -y familiar, aunque este resulta más prescindible para el presente análisis- protege aquellos asuntos que, siendo personales, encajan también en la definición de íntimos[29] (de Montalvo Jääskeläinen, 2016).

En definitiva, se puede considerar aclarado el significado del derecho a la intimidad personal en el ordenamiento jurídico español como la capacidad del individuo de mantener en su propia esfera aquellos atributos personales que gozan de la cualidad de íntimos, considerándose, por tanto, ilegítima cualquier intrusión en dicha esfera que no resulte necesaria a través de una ponderación de intereses personales y colectivos.

[29] La definición de "íntimo", según la Real Academia Española, tiene varias acepciones, dos de las cuales encajan mejor en el contexto del presente análisis: "Lo más interior o interno"; "Perteneciente o relativo a la intimidad, o que se hace en la intimidad".

4.3.2 La libertad informática en el ordenamiento jurídico español.

Como consecuencia del creciente desarrollo tecnológico y la necesidad resultante de los individuos de hacer uso de la TIC, ha adquirido una mayor importancia la libertad informática, recogida en el artículo 18.4 de la CE: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Como se extrae del tenor literal del texto constitucional, la libertad informática guarda una estrecha relación con el derecho a la intimidad, si bien se constituye como un derecho autónomo que tiene como objeto de protección todos los datos personales de los individuos, independientemente de que encajen o no en la definición de "íntimos" (de Montalvo Jääskeläinen, 2016).

La libertad informática se prevé en el texto constitucional con la intención de prevenir la intrusión en la esfera personal de los individuos a través de medios telemáticos, que ya en 1978 se concebían como una posible vía de ataque a los derechos fundamentales, por su inmaterialidad y anonimato. La idea que trasciende este derecho es similar al fundamento de los derechos al honor, intimidad personal e imagen propia, tratándose de la garantía de control y disposición de cada individuo sobre sus datos personales, así como sobre su uso y destino, a fin de impedir el tráfico de estos que pudiera resultar lesivo para su dignidad (STC 290 y 292/2000, de 30 de noviembre[30]).

[30] BOE núm. 4, de 4 de enero de 2001, páginas 70 a 93 y 104 a 118. Recursos de inconstitucionalidad promovidos contra diversos artículos de la LO 5/1992 y de la LO 15/1999, por vulneración del derecho fundamental a la protección de datos personales.

Capítulo 5. PROTECCIÓN DE DATOS.

Habiendo analizado en el capítulo anterior la necesidad de salvaguardar la intimidad personal en relación con la recopilación de datos, resulta necesario realizar un ahondamiento en la materia de su protección, especialmente en la regulación vigente en el contexto de la UE y España. Con ello, se pretende aportar un marco jurídico que, junto con el fundamento previamente analizado de la protección de la intimidad personal y su relación con los datos masivos, permita analizar finalmente el papel que desempeña la *e-Health* y su concordancia con el marco jurídico en lo que a protección de derechos fundamentales respecta.

5.1 DEFINICIÓN TEÓRICO-PRÁCTICA DE LA PROTECCIÓN DE DATOS EN EL MARCO DE LA UNIÓN EUROPEA.

5.1.1 Directiva 95/46/CE de protección de datos personales.

La protección de datos comenzó a regularse de manera exhaustiva en la UE con la Directiva 95/46/CE[31]. Resulta importante realizar una breve alusión a las características jurídicas de las directivas como normas vinculantes de la UE, ya que difieren de los reglamentos en lo que a la manera de vincular a los estados miembros destinatarios respecta. Mientras que los reglamentos gozan de aplicabilidad directa en los distintos ordenamientos jurídicos, las directivas solamente serán aplicables en cada estado cuando estos elaboren, individualmente, normas de transposición de su contenido.

En este sentido, las directivas constituyen el instrumento jurídico predilecto de la UE para la mera armonización de legislaciones en los estados miembros, puesto que vinculan a estos exclusivamente para el fin que se pretende alcanzar, pudiendo cada uno decidir los pormenores de las medidas en sus normas de transposición. De esta manera, resulta menos radical para los ordenamientos jurídicos respectivos de cada estado miembro destinatario y, por ello, más apropiado si la materia no requiere una regulación específicamente homogénea.

[31] 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.

Es decir, si el objetivo de lo estipulado por la normativa europea en cuestión es principalmente teleológico, su formalización a través de una directiva probablemente sea lo más acertado. Teniendo esto en cuenta, al elaborarse la Directiva 95/46/CE, se pretendían alcanzar principios coercitivos comunes en los diferentes estados miembros en lo que a protección de datos personales respecta, sin perjuicio de que cada uno pudiera delimitar de una u otra manera la forma de lograrlos y las sanciones previstas para su incumplimiento.

Tal y como se establece en las disposiciones generales de la Directiva 95/46/CE, su objeto principal consiste en la garantía de la protección del derecho a la intimidad de las personas físicas, en lo que al tratamiento total o parcialmente automatizado de los datos personales respecta[32]. Con este fin, su Capítulo II establece una serie de condiciones generales para la licitud del tratamiento de datos personales en el ámbito de los estados miembros de la UE. En este sentido, resulta relevante incidir, entre otros, en los principios de información, acceso y consentimiento del interesado en lo relativo al tratamiento de sus propios datos personales. Como se ha aclarado anteriormente, el derecho a la intimidad personal protege la totalidad de información íntima relativa a una persona, por lo que la Directiva 95/46/CE se refiere en su ámbito de aplicación a los datos de carácter personal.

En materia de protección de datos, cobra especial importancia el principio de información, que se resume en la comunicación al interesado de los datos que de su persona han sido recabados, así como del tratamiento que se les va a dar y del fin perseguido con ello por el responsable, cuya identidad también debe ser conocida[33]. Siguiendo en esta línea de transparencia, la Directiva 95/46/CE establece que el interesado gozará también de acceso libre a los datos que sobre él hayan sido recopilados y podrá, en su caso, rectificarlos o suprimirlos en caso de no adecuarse a las garantías estipuladas, incluida la veracidad. Esto último enlaza con el requisito del consentimiento del interesado para el tratamiento de sus datos, a excepción de determinadas obligaciones legales o interés público[34].

---

[32] "Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero" (Artículo 1 Directiva 95/46/CE).
[33] Artículos 10 y 11 Directiva 95/46/ CE.
[34] "Los estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca o (…) c) es necesario para el cumplimiento de una obligación jurídica (…)" (Artículo 7 Directiva 95/46/CE).

Sin embargo, resulta llamativa una última excepción al consentimiento inequívoco del interesado, recogida en el apartado f) del artículo 7 de la Directiva 95/46/CE, por la cual se podrá prescindir del consentimiento en tanto y cuanto el tratamiento de datos sea "necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento (…), siempre que no prevalezca el interés o derechos y libertades fundamentales del interesado que requieran protección". Puede observase que, a través de esta excepción, se realiza una ponderación de intereses en el caso concreto, tomando por un lado al interesado y su intimidad personal y, por otro, al responsable y su interés legítimo en el tratamiento de los datos recopilados. Teniendo en cuenta el carácter de derecho fundamental que emana de la intimidad personal, puede intuirse un riesgo en la ponderación concreta de este frente al interés del responsable. Precisamente en este y otros matices residía la necesidad de adaptar la regulación europea en materia de protección de datos al frenético ritmo del siglo XXI, como se expondrá a continuación[35].

5.1.2 Reglamento 2016/679 de protección de datos personales.

La Directiva 95/46/CE se mantuvo vigente en el marco de la UE hasta el año 2016, cuando se publicó el RGPD[36], derogando la anterior Directiva y otras regulaciones europeas referidas a esta materia. El objetivo de este nuevo RGPD consiste, principalmente, en la adaptación de la regulación vigente desde hacía ya dos décadas al rapidísimo desarrollo de las TIC y el impacto que ello lleva implícito en la protección de los datos personales. Teniendo en cuenta el enorme cambio resultante de dos décadas de innovación y desarrollo tecnológico, el RGPD pretende realizar una reforma sustancial en el sistema de protección de datos, para así adaptarlos la nueva "sociedad del dato" (Ortega Giménez, 2018).

[35] El RGPD realiza, en su artículo 7.f, una importante aclaración en relación con esta ponderación de intereses, añadiendo que "lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones", excluyendo así una potencial vía de desprotección del ciudadano frente al estado.

[36] 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 por el que se deroga la Directiva 95/46/CE. Reglamento General de Protección de Datos. *Vid.* Listado de abreviaturas.

Los cambios introducidos por el RGPD en el marco jurídico europeo de protección de datos se concentran en dos secciones claramente delimitadas. En primer lugar, se pretende ampliar significativamente el nivel de protección de los datos personales, adaptándose así al incremento en el riesgo de que estos se vean amenazados, motivado por el desarrollo de las TIC. La UE, así como otros organismos internacionales, detectó la necesidad de salvaguardar la privacidad de los ciudadanos frente a las nuevas tecnologías, a fin de respetar los derechos de la personalidad; en especial el derecho fundamental a la intimidad personal, no solo por el sustento del ordenamiento jurídico que ampara a todos los individuos que por él se rigen, sino también por la íntima relación que dichos derechos tienen con la dignidad y salud.

En segundo lugar, el RGPD se elaboró con vocación de realizar una verdadera homogenización de la normativa relativa a la protección de datos personales en el conjunto de la UE, logrando así una regulación única en los distintos estados miembros. Como se mencionaba anteriormente, los reglamentos son, junto con las directivas, normas vinculantes de carácter supranacional. Sin embargo, mientras que estas requieren una norma de transposición por parte del estado miembro en cuestión para resultar aplicable en el mismo, aquellos gozan de aplicabilidad directa. En este sentido, teniendo en cuenta la vocación homogeneizadora del RGPD, resulta lógico que el PE[37] optara, en esta ocasión, por utilizar este instrumento jurídico para la sustancial reforma que a través de este se realiza del régimen de protección de datos.

5.1.2.1 Novedades introducidas por el Reglamento 2016/679: intensificación del nivel de protección de datos personales en la UE.

El fundamento que justifica la elaboración del RGPD en derogación de la preexistente normativa europea en materia de protección de datos personales se resume en la necesidad de intensificar esta protección, a fin de permitir su adaptación a las nuevas amenazas que la sociedad del dato presenta frente a la privacidad. Por lo tanto, la UE profundiza a través del RGPD en una serie de derechos de cada individuo en relación con sus datos personales.

[37] Parlamento Europeo. *Vid.* Listado de abreviaturas.

Por un lado, se refuerza el derecho a la información del individuo sobre sus propios datos y el tratamiento que de los mismos se hace[38]. Como se comentaba anteriormente, la Directiva 95/46/CE ya regulaba esta garantía, si bien el RGPD incrementa la protección del interesado al añadir la identificación obligatoria del delegado de protección de datos[39], además de la del responsable. Esta garantía guarda una estrecha relación con el refuerzo del consentimiento explícito para el uso de datos personales, especialmente en relación con el caso mencionado anteriormente, al analizar la Directiva 95/46/CE, por el cual se exceptuaba el consentimiento del interesado en favor del interés del responsable, siempre y cuando esto no supusiera una vulneración de la intimidad personal del primero. El RGDP introduce el derecho del interesado a solicitar información acerca de estos intereses legítimos, que justifican prescindir de su consentimiento. Resulta relevante mencionar que, en lo que a las transferencias internacionales de datos respecta, se garantiza al interesado el acceso a la información acerca del destinatario, así como de la potencial transferencia de los datos recopilados a un tercer país u organización internacional. Con el fin de blindar a los individuos de posibles vulneraciones de su intimidad personal, se introduce a través del RGPD una serie de condiciones para que el consentimiento sea lícito y goce de todas las garantías[40].

Asimismo, se incide en el derecho del interesado a acceder a sus datos personales recopilados y tratados, a fin de tener conocimiento sobre ellos y poder, en su caso, rectificarlos o suprimirlos[41]. Es decir, no se trata solo de la transparencia en lo que a tratamiento de datos personales respecta, sino que se enfatiza en el control del interesado sobre ellos, con el fin de garantizar el mayor grado de respeto a la intimidad personal en el marco de las TIC. Este último punto tiene una especial trascendencia, ya que uno de los principios que pretende reforzar el RGPD es precisamente el derecho al olvido en materia de datos personales[42], que se define por la AEPD[43] como el "derecho a impedir la difusión

[38] Artículo 13 Reglamento 2016/679.
[39] La figura del delegado de protección de datos se introduce en la sección 4 del capítulo IV del Reglamento 2016/679. Este será designado por el responsable y el encargado del tratamiento, en el caso de que este último sea en un organismo público y aquel realice operaciones que requieran una observación sistemática de interesados a gran escala. Sin perjuicio de lo anterior, un propio grupo empresarial podrá nombrar un delegado de protección de datos público (Artículo 37 Reglamento 2016/679).
[40] Artículo 7 Reglamento 2016/679.
[41] Artículo 15 Reglamento 2016/679.
[42] Artículo 17 Reglamento 2016/679.
[43] Agencia Española de Protección de Datos. *Vid.* Listado de abreviaturas.

de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa" (Ortega Giménez, 2018).

El derecho al olvido es un concepto que ya existía anteriormente, por lo que el RGPD simplemente incide en la necesidad de respetarlo en el ámbito del tratamiento de datos personales de manera automatizada, a fin de desechar la noción generalizada de que aquellos datos que ya se encuentran en la red no pueden eliminarse. Asimismo, se realiza un importante inciso para definir los motores de búsqueda como herramientas de tratamiento de datos personales, por lo que su archivo, en este contexto, deberá atender a los mismos requerimientos previstos para las entidades que almacenan y gestionan estos datos. Lógicamente, el derecho al olvido no es ilimitado, y encuentra su barrera en la transmisión de información personal realizada "en pro de la libertad de información, cumplimiento de una obligación legal, necesaria para el interés público, información histórica o estadística, y para acciones de defensa" (Ortega Giménez, 2018).

Por otro lado, es importante incidir en el carácter coercitivo del RGPD y las disposiciones que en él se recogen, lo que se ve materializado en el sistema sancionador dispuesto, a través del cual se intensifican las consecuencias del incumplimiento en materia de protección de datos personales. De esta manera, se introduce un esquema de sanciones con un doble límite superior, cuantificado en multas de hasta 20 millones de euros (o el 4% del volumen de negocios anual, si fuera superior)[44] en caso de vulneración de derechos personales, y de hasta 10 millones de euros (o el 2% del volumen de negocios anual, si fuera superior)[45] para el incumplimiento de las obligaciones dispuestas por la normativa europea. Asimismo, la sanción se verá moderada hasta lograr su adecuación a la infracción correspondiente en función de su gravedad, intencionalidad o negligencia y grado de responsabilidad del infractor.

Por último, en salvaguarda de la seguridad jurídica en lo que a protección de datos se refiere, a pesar del continuo desarrollo de las TIC, el RGPD introduce la implementación de códigos de conducta y certificaciones como medida de transparencia empresarial en lo que al uso de la información personal de los usuarios se refiere. Los códigos de conducta podrán ser

[44] Artículo 83, apartado 5 Reglamento 2016/679.
[45] Artículo 83, apartado 4 Reglamento 2016/679.

promovidos tanto a nivel estatal como a nivel privado, otorgándose así la capacidad a las instituciones empresariales de elaborar una propia serie de reglas y principios que, guardando plena concordancia con el RGDP y demás normativa europea y estatal, rija su comportamiento y plantee una serie de expectativas para los interesados. Por otro lado, los estados miembros y demás autoridades europeas competentes promoverán una serie de modelos de certificación que sirvan como constatación de cumplimiento con la regulación pertinente en materia de protección de datos.

5.1.2.2 Novedades introducidas por el Reglamento 2016/679: homogenización del régimen jurídico de protección de datos personales en los estados miembros de la Unión Europea.

Como se adelantaba anteriormente, las características del instrumento jurídico que constituye un reglamento de la UE se pueden resumir en que se trata de una norma vinculante y directamente aplicable. Teniendo esto en cuenta, el PE pretendió, mediante su elaboración, alcanzar una normativa homogénea en el conjunto de la UE para el tratamiento de datos personales total o parcialmente automatizados, logrando así un mercado único digital (Ortega Giménez, 2018).

Una importante novedad introducida por el RGPD que avala la homogeneización de la normativa es el concepto de ventanilla única, ideado para las empresas operativas en más de un estado miembro, y consistente en la concentración de la responsabilidad del cumplimiento coercitivo de la normativa de protección de datos personales en la autoridad supervisora del estado miembro donde se encuentre el establecimiento principal del negocio. Esta previsión no es sino una materialización de la homogenización normativa en la UE en materia de protección de datos personales.

Por otro lado, el RGPD establece como una de sus novedades una serie de principios que necesariamente deberán ser tomados en consideración de manera coercitiva por parte de los estados miembros, resultando asimismo en una homogenización de los valores que inspiran la normativa en protección de datos. En primer lugar, los datos adquiridos de manera total o parcialmente automatizada deberán ser tratados con lealtad, exactitud y transparencia, en referencia a unos fines determinados y legítimos, a los que el individuo deberá acceder de manera explícita o inequívoca. Además del consentimiento, la seguridad de los datos

gestionados es fundamento esencial de la reforma, por lo que las sanciones ante el incumplimiento de cualquiera de las previsiones normativas en materia de protección de datos se ven reforzadas por el RGPD.

5.1.2.3 Régimen de cooperación internacional en relación con las transferencias internacionales de datos.

Además de la previamente mencionada "sociedad del dato", se puede hablar de la "era de la globalización" para definir el momento actual en el que se encuentra la humanidad. La persistente revolución de las TIC y la inmediatez y sobreinformación que esta implica hace necesaria una regulación acerca de la manera de transferir los datos personales recopilados para fines determinados y consentidos. En este sentido, la Directiva 95/46/CE ya regulaba este aspecto de los datos personales, por medio de un régimen de principios y excepciones a los mismos. El RGPD propone un cambio de paradigma al que dedica la totalidad de su Capítulo IV, introduciendo un método diferente, sostenido en un principio de prohibición general de transferencias internacionales en ausencia de los principios de adecuación, del ejercicio de las garantías adecuadamente previstas y del régimen dispuesto por las normas corporativas vinculantes[46]. Este principio de prohibición se ve atenuado por una serie de excepciones a los requisitos mencionados, fundamentadas en la cooperación internacional.

La principal ventaja observada a través de este régimen reside en la exhaustividad con la que se regula la transferencia internacional de datos, de manera que todos los estados miembros gozan de una regulación homogénea a este respecto, lo que supone un alto nivel de protección y seguridad jurídica para los interesados.

[46] La prohibición general a la transferencia de datos personales se recoge, enunciada como autorización condicionada al cumplimiento de una serie de requerimientos, en el artículo 44 RGDP: "Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado."

5.2 LEGISLACIÓN VIGENTE PARA LA PROTECCIÓN DE DATOS EN EL ORDENAMIENTO JURÍDICO ESPAÑOL.

La materia de protección de datos personales se encuentra regulada en el ordenamiento jurídico español a través del marco otorgado por el RGPD y la LOPD[47]. Esta última tiene como objeto la adaptación del ordenamiento jurídico español al RGDP, ejerciendo así de manera conjunta la protección de los datos personales recogidos en el artículo 18.4 de la CE. A diferencia de la regulación europea, la LOPD enfatiza de manera específica en su Título X la garantía de los derechos digitales, lo que resulta de especial interés para el objeto del presente análisis acerca de la protección de datos en materia de *e-Health*. Por lo tanto, teniendo en cuenta el desarrollo realizado de la normativa europea en lo que a la protección genérica de datos personales respecta, se examinarán algunas notas de la normativa interna con respecto a la protección de datos en el entorno específico de las TIC, con el fin de concretar el marco normativo en el que se inserta la *e-Health*.

En primer lugar, la LOPD incide en la aplicabilidad en Internet de todos los derechos y libertades recogidos en el ordenamiento jurídico español, asignando así a los proveedores de servicios digitales el deber de garantizarlos[48]. Asimismo, se recoge el derecho de acceso universal a Internet, realizando un especial énfasis en aquellos colectivos para los que la transición a la era digital presenta más dificultades. Estos dos puntos serán de vital importancia a la hora de analizar la concordancia de la *e-Health* con la protección de datos; tratándose de un derecho fundamental, resulta necesario que se garantice en todos los niveles, no solo para aquellos colectivos que gocen de mayor capacidad de adaptación.

5.3 PROTECCIÓN DE DATOS EN EL SECTOR SANITARIO ESPAÑOL.

Tras haber analizado el marco jurídico de protección de datos vigente en el ordenamiento jurídico español, resulta pertinente comenzar a enfocar el análisis en torno al objeto de investigación; la protección de datos e intimidad personal en materia de *e-Health*. Como se

[47] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Vid.* Listado de abreviaturas.
[48] Artículo 79 LOPD.

mencionaba anteriormente, el derecho a la protección de datos tiene por objeto la salvaguarda de la intimidad personal. En el caso del sector sanitario, al tratarse de datos principalmente sanitarios y por tanto sensibles, el enfoque principal del análisis se encontrará en los riesgos que de la implementación de esta tecnología pudieran surgir, así como las medidas o buenas prácticas instauradas para la protección de esta información. Esta aproximación a la gestión de datos en el sector sanitario español, en combinación con la inicial delimitación del concepto de *e-Health* y el detallado estudio acerca de la protección de datos e intimidad personal permitirá concluir el impacto, riesgos y medidas de las TIC en lo que a la protección de la información sanitaria personal respecta.

Naturalmente, todo lo enunciado anteriormente en relación con el RGPD y la LOPD goza de aplicación en el ámbito sanitario, puesto que los datos médicos de los pacientes se ubican en el ámbito de aplicación de ambas normas jurídicas. Sin embargo, puesto que se trata de información notablemente sensible, resulta necesario asegurar una protección integral de los mismos, por lo que se incide en algún aspecto adicional a los contemplados para el tratamiento de datos generales. En este sentido, el principal punto de protección adicional se concentra en la llamada confidencialidad del paciente, regulada por la LAP[49], cuyo ámbito de aplicación no se limita a los datos del paciente, sino también a los de los propios profesionales y centros médicos[50]. Goza de especial importancia el artículo 7 de la LAP, en el que se define el derecho a la intimidad del paciente en ámbito sanitario, de manera reforzada frente a lo previsto en el marco normativo general. Específicamente, los datos sanitarios de cada individuo adquieren carácter confidencial, por lo que se requerirá una autorización amparada por la mencionada LAP para el acceso a ellos. No solo esto, sino que, a efectos de protección de datos, los centros sanitarios serán responsables de adoptar las medidas necesarias para asegurar el cumplimiento de lo anterior.

Adicionalmente, en esta misma LAP se encuentra regulado el segundo principal factor de refuerzo en lo que a protección de datos en el sector sanitario respecta; la conservación y

[49] Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica. Ley de Autonomía del Paciente. *Vid.* Listado de abreviaturas.
[50] Artículo 1 LAP.

acceso de la historia clínica[51]. Este documento, cuya principal función consiste en garantizar una adecuada asistencia al paciente, será archivado en el centro correspondiente, que será responsable de su seguridad y conservación, a través de un mecanismo de custodia activa[52]. La regulación de la UE en relación con la protección de datos enuncia el derecho de acceso del interesado a sus propios datos, lo cual se adapta al sector sanitario, donde dichos datos son naturalmente más sensibles y se encuentran formal y obligatoriamente recogidos en la historia clínica. Teniendo esto en cuenta, se respetará el derecho del interesado a acceder a sus datos de manera personal o través de un representante, si bien, en este último caso, se prestará especial atención para garantizar la voluntad de acceso del interesado[53].

Por último, resulta procedente hacer mención al Código de Deontología Médica, en el que se recogen los principios y estándares de actuación por parte de los médicos que ejercen su actividad en el estado español. Concretamente, es especialmente relevante para los efectos del presente análisis lo dispuesto en el Capítulo V, relativo al secreto profesional del médico. En este, se configura en el secreto médico como uno de los pilares que sostienen la relación entre médico y paciente, basada en la confianza. Comprende, por tanto, toda la información obtenida por parte del médico de manera directa, a través del propio paciente, o indirecta por medio de sus propias observaciones y conclusiones. En este sentido, la separación de información clínica y administrativa relativa a cada paciente resulta primordial, puesto que la primera deberá gozar de un mayor nivel de protección y compromiso, teniendo en cuenta su carácter especialmente sensible. Como consecuencia de los hechos vividos en los últimos dos años a raíz de la pandemia ocasionada por la COVID-19, resulta especialmente llamativo lo dispuesto en el apartado 6 del artículo 27 del Código, por el cual "el médico podrá cooperar en estudios epidemiológicos (…) con la condición expresa de que la información en ellos utilizada no permita identificar ni directa ni indirectamente, a ningún paciente". Teniendo en cuenta el aceleradísimo desarrollo de las TIC, en este caso en materia de *e-*

[51] "La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente" (Artículo 14.1 LAP).
[52] "El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad (…)" (Artículo 19 LAP).
[53] Artículo 18 LAP.

Health, será importante analizar el cumplimiento de este principio con respecto a la gestión de datos masivos adquiridos de manera electrónica.

Capítulo 6. PROTECCIÓN DE DATOS E INTIMIDAD PERSONAL EN MATERIA DE *E-HEALTH*.

La protección otorgada por el ordenamiento jurídico a la intimidad personal de cada individuo goza de un ámbito de aplicación global, en tanto que la base de su contenido resulta aplicable a todas las materias en las que los datos personales tengan relevancia. Sin perjuicio de ello, como se ha analizado anteriormente, el sector de salud y sanidad precisa de una especial protección a este respecto, puesto que los datos generados en él son, por naturaleza, especialmente sensibles.

Además, con la proliferación de las TIC en el sector sanitario, la protección de datos médicos y de salud adquiere mayor complejidad. Como se ha mencionado anteriormente, la libertad informática se configura como el derecho a decidir sobre la información de carácter personal, independientemente de que sea o no íntima. En este sentido, se puede inferir una especial protección a los datos gestionados por las TIC, en gran parte debido al desconocimiento acerca de su alcance. Su vertiginosa velocidad de evolución impide la inmediata adaptación del ordenamiento jurídico a los nuevos riesgos y amenazas que de ellas pudieran resultar.

La sensibilidad de los datos médicos o de salud de cada individuo, en combinación con el riesgo que presentan las TIC en lo que a la seguridad de los datos respecta, justifica la necesidad de analizar la protección de estos datos en el contexto de la *e-Health*, comenzando por la identificación de las principales diferencias que esta presenta con respecto a la gestión tradicional de datos.

6.1 DIFERENCIAS CON RESPECTO A LA GESTIÓN TRADICIONAL DE DATOS SANITARIOS.

El desarrollo de los datos masivos y las herramientas para su tratamiento y análisis han traído a la realidad una nueva manera de almacenar y gestionar la información, caracterizada por una incrementada eficiencia y mayor claridad en el orden. Asimismo, se presentan múltiples maneras de utilizar la información aportada por estos datos, al poner unos en relación con otros para la extracción de conclusiones. Si bien esto está ocurriendo en multitud de

disciplinas, todas ellas con sus respectivos riesgos, en el sector sanitario se espera un especial cuidado, traducido en una mayor seguridad para los individuos.

Como se definía en puntos anteriores, el término *e-Health* comprende una amplia selección de aplicaciones de las TIC en el ámbito sanitario. Sin embargo, no todas plantean el mismo nivel de riesgo en relación con la protección de datos personales. Por ejemplo, los sistemas de *software* orientados al almacenamiento y tratamiento interno de los datos de los pacientes de un determinado hospital se ubican dentro del paraguas de la *e-Health*, si bien suponen un riesgo menor que los datos registrados en la nube por parte de aplicaciones de medicina online. Por lo tanto, resulta importante analizar las distintas opciones que se presentan en lo que a recopilación y almacenamiento de datos personales médicos respecta.

Analizando, por su comparabilidad con el pasado, la gestión de datos recopilados en centros clínicos, se observa una serie de importantes diferencias atribuidas a la implementación de las TIC. En este sentido, las fichas médicas que anteriormente se almacenaban en un soporte físico, se ubican en la actualidad en grandes bases de datos internas, que en ocasiones se encuentran vinculadas a otro tipo de información en la nube. Es decir, no se trata de ficheros locales, a los que exclusivamente se podrá acceder a través de un ordenador y compartir por medio de un disco duro. Por el contrario, estos datos se ubican en redes virtuales a las que tiene acceso un número determinado de usuarios, normalmente por medio de una serie de verificaciones de identidad. Generalmente, estas redes se traducen en la llamada intranet; comprendida como carpetas compartidas de acceso restringido.

En cualquier caso, si bien la teoría determina que el acceso a esta información debería ser de carácter puramente interno por parte de los profesionales de cada centro, la realidad es que el traspaso de información de una institución a otra es muy frecuente. Como se observaba anteriormente, el paciente deberá estar informado del uso que de sus datos personales recopilados se haga, sin perjuicio de puedan existir ciertas excepciones al amparo del interés general. El problema que de la transmisión -aún autorizada- de datos médicos surge se concreta en el descontrol de la información manipulada por las TIC, especialmente en el caso de que se comparta por internet. Asimismo, si bien la transmisión debe ser, de una u otra manera, autorizada por el paciente, la realidad es que determinadas empresas, como es el caso de las aseguradoras, pueden acceder de manera parcial al historial médico de los

pacientes, si bien este acceso debería de estar restringido a lo estrictamente necesario (Kress, 2017).

En esta línea, procede hacer una nueva alusión a la LAP, que establece como principio general la limitación del acceso al historial médico de un paciente exclusivamente al personal sanitario directamente involucrado en su tratamiento. Sin perjuicio de lo anterior, se presentan tres principales excepciones a esta regla. Esto es, el acceso a los datos médicos de un individuo será lícito en caso de que exista una orden judicial para ello, o bien por razones epidemiológicas, en los casos en los que el interés general supere al derecho subjetivo del paciente. Por último, también será posible el acceso por parte de personal sanitario con el objetivo de evaluar la calidad de la asistencia médica.

En definitiva, si bien los datos recopilados por los propios profesionales suponen un mayor riesgo con la influencia de las TIC, no presentan tantos problemas en la teoría jurídica, puesto que su protección se encuentra claramente amparada por el ordenamiento jurídico. En cualquier caso, será necesario alcanzar un mayor grado de claridad y homogeneidad en cuanto a su transmisión en los casos autorizados por el paciente, así como incluir una mayor visibilidad en cuanto a las posibles implicaciones de esa transmisión, por tratarse de información especialmente sensible.

6.2 MARCO TEÓRICO: POTENCIALES CONFLICTOS CON LA INCLUSIÓN DE LA *E-HEALTH*.

Como ya se adelantaba anteriormente, el desarrollo de la *e-Health* no implica únicamente conflictos de carácter puramente jurídico, sino que, por la naturaleza de la información que a través de ella se gestiona, existe un importante componente moral a la hora de analizar las distintas prácticas derivadas de ella. Habiendo comentado ya el peligro del autodiagnóstico, por el cual el paciente proactivo alcanza un extremo peligroso para su propia salud y amenazante para el orden colectivo, se pondrá el foco en este punto en la protección de datos recopilados por aplicaciones de salud, así como la recopilación de información de los usuarios de determinadas páginas web a través de las famosas *cookies*.

6.2.1 La protección de datos recopilados por aplicaciones móviles.

Uno de los mayores retos a los que se enfrenta el ordenamiento jurídico en relación con la protección de datos médicos reside en la proliferación de aplicaciones móviles, concretamente en el uso que de ellas se hace. Por su comodidad y aparente fiabilidad, así como la sensación de control que transmiten al usuario, su empleo se ha generalizado en los últimos años, fomentado por el desarrollo de relojes y pulseras inteligentes. Conceptualmente, el dilema de las aplicaciones móviles de salud radica en la siguiente reflexión: si los profesionales de la salud deben atender a las exigencias legales, así como al juramento del código deontológico tras la superación de una larga carrera para el registro y tratamiento de datos médicos personales, ¿qué justifica que una aplicación móvil pueda almacenar y tratar estos mismos datos? ¿Qué garantías ofrece en lo que a su seguridad y veracidad respecta?

En primer lugar, resulta relevante acudir de nuevo al concepto del consentimiento para el almacenamiento y tratamiento de datos médicos. Como ya se ha reiterado a lo largo del análisis, la recopilación de datos personales, especialmente aquellos de carácter notablemente sensible, como son los relativos a la salud, está supeditada al consentimiento expreso e informado del paciente, sin perjuicio de unas pocas excepciones ya mencionadas. Sin embargo, en el contexto de las aplicaciones móviles, existe un cierto vacío en cuanto a la legalidad del consentimiento del usuario. Esto es, al instalar una aplicación móvil e iniciar una cuenta en ella, normalmente se aceptan unas condiciones generales de protección de datos, plasmadas en un extenso documento que prácticamente ningún usuario lee antes de pulsar la casilla de "aceptar". En el caso de las aplicaciones de salud, por tanto, ¿cómo se justifica la recopilación y tratamiento de datos sensibles sin un verdadero consentimiento informado?

Verdaderamente, resulta complicado definir los límites en cuanto al uso de los datos recopilados por estas aplicaciones, ya que el tenor literal de las disposiciones legales se ve cumplido, puesto que se informa del propósito trascendente a la recopilación de estos datos. En este sentido, además de los mencionados RGPD y LOPD, es de aplicación para el tratamiento de datos personales por medio de aplicaciones móviles la LSSI[54]. En cualquier

[54] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

caso, el ordenamiento jurídico prevé una serie de garantías para datos de carácter más o menos personal, típicamente recopilados por aplicaciones móviles para usos primordialmente comerciales. Distinto asunto es el tratamiento de datos médicos, por su naturaleza especialmente sensible. El ordenamiento jurídico prevé para ellos un tratamiento distinto, que resulta difícilmente transferible a este tipo de aplicaciones, por encontrarse en un área gris de validez moral, si bien los preceptos legales existentes parecen cumplirse de manera más o menos clara. En cualquier caso, será necesaria una regulación explícita de protección de datos en materia de *e-Health* para la concreción de estos asuntos, teniendo en cuenta el aspecto moral y deontológico del tratamiento de información médica. Especialmente relevante será en el futuro próximo, después del auge que estas tecnologías han registrado durante los años de presencia de la pandemia ocasionada por la COVID-19.

En segundo lugar, muchas de estas aplicaciones proporcionan al usuario información acerca de su estado de salud a través de los datos introducidos por él o recogidos por medio de distintos sistemas tecnológicos. En este sentido, se puede observar claramente un importante riesgo en relación con la veracidad de esta información, puesto que un desvío en ella podría suponer tanto una falsa alarma o una ingenua tranquilidad. De nuevo, surge un dilema parecido al observado anteriormente: si un médico, para poder diagnosticar a un paciente -aún en el caso de condiciones de escasa relevancia- y sugerir posibles vías para la mejora de su condición, requiere de una larguísima carrera, así como experiencia en la práctica, ¿por qué una aplicación puede realizar esta tarea de la misma manera? ¿Qué garantía de veracidad puede ofrecer? ¿De qué manera están configurados los algoritmos que rigen su funcionamiento para asegurar plena fiabilidad en la información emitida por ella?

La razón por la que resulta tan relevante asegurar la veracidad de la información emitida por estas aplicaciones radica en el mismo fundamento que configura el efecto placebo. Este consiste en "una sustancia que, careciendo por sí misma de acción terapéutica, produce algún efecto favorable en el enfermo, si este la recibe convencido de que esa sustancia posee realmente tal acción"[55]. En este sentido, la emisión de ciertos datos por parte de una aplicación, sean positivos o negativos, generarán en el usuario una creencia de que eso se corresponde con la realidad. En el caso de que la información sea de carácter negativo, el

[55] "Placebo" (Diccionario de la Real Academia Española).

usuario podría llegar incluso a enfermar, siendo tan potente el efecto psicológico sobre el cuerpo humano. Por el otro lado, en caso de tratarse de un dato falsamente positivo, el usuario podría prescindir de adoptar una actuación necesaria para su condición. La educación médica es difícilmente sustituible, y las carencias que las aplicaciones de salud presentan residen principalmente en el irremplazable espíritu crítico del médico, conformado después de años de educación para la consecución de ese preciso fin.

6.2.2 *Cookies* y registro de búsquedas en internet.

Como se definía anteriormente, la *e-Health* incluye en su significado el acceso a páginas web con información sobre salud, especialmente en el caso de redes sociales o foros. En este sentido, adquiere relevancia la política de protección de datos en internet, de aplicación genérica para cualquier tipo de búsqueda. Sin embargo, al tratarse de información de carácter especialmente sensible, esta regulación podría resultar insuficiente ante las exigencias del sector sanitario. La protección de datos en lo relativo a las búsquedas en internet se construye alrededor del concepto de *cookies*, entendido como archivos recopilados y almacenados con datos del usuario, como pueden ser el nombre, la dirección IP o el historial de navegación.

En el ámbito comunitario, la UE elaboró la llamada Directiva *ePrivacy*[56] en 2002, modificándola siete años después para adaptarla al vertiginoso desarrollo de internet en la primera década de este siglo. En el ordenamiento jurídico español, esta directiva se vio transpuesta por la LSSI. En cualquier caso, con la incorporación del RGPD, esta directiva se encuentra pendiente de revisión, en la cual será necesario realizar un detallado escrutinio de los riesgos que plantea el desarrollo de la Web 2.0 para la protección de los usuarios, a fin de garantizar unos adecuados límites. Actualmente, el contenido de la Directiva se resume en unas pautas para la obtención del consentimiento del usuario a la utilización de *cookies* por parte del sitio web. En cualquier caso, como se comentaba anteriormente en el caso de las aplicaciones móviles, resulta ciertamente conflictivo que dicha autorización pueda

[56] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

concretarse en la aceptación de condiciones a través de un mero *click*, ya que esto no garantiza, como consecuencia del formato, que el usuario quede debidamente informado.

Si bien toda esta problemática resulta de aplicación para todo tipo de datos personales recogidos en internet, se complica especialmente en el caso de los datos relacionados con la información médica o de salud. En este sentido, al acceder a páginas con este tipo de contenido, la recopilación de datos personales adquiere ciertos riesgos adicionales, puesto que se puede realizar una asociación directa de datos identificativos de una persona a un cierto interés hacia un asunto determinado relativo a la salud. En definitiva, independientemente de la revisión de la Directiva *ePrivacy*, con alcance general, la evolución de *e-Health* requiere de una protección adicional por parte del ordenamiento jurídico, que por el momento no se ve íntegramente garantizada. Sin perjuicio de lo anterior, en defensa de las garantías ofrecidas a este respecto por parte de la Administración Pública, la AEPD se erige como autoridad competente en protección de datos, y responsable del uso indebido de la información recopilada.

6.3 HERRAMIENTAS JURÍDICAS PARA LA PROTECCIÓN DE DATOS E INTIMIDAD PERSONAL EN MATERIA DE *E-HEALTH*.

En vista de los comentados conflictos jurídicos y morales que del tratamiento tecnológico e informático de los datos de salud pueden surgir, resulta conveniente hacer alusión a dos importantes herramientas dispuestas por los ordenamientos jurídicos para su salvaguarda y protección: la protección de datos en intercambios transfronterizos y el derecho de oposición al tratamiento de datos y elaboración de perfiles.

En este sentido, en relación con las mencionadas diferencias en el tratamiento de datos sanitarios como consecuencia del desarrollo de la *e-Health* en centros médicos, cabe mencionar la regulación de la UE sobre la protección de los derechos de los pacientes en materia de asistencia sanitaria transfronteriza. En el contexto de la cooperación comunitaria

en materia del derecho a la salud, se elaboró la Directiva 2011/24/UE[57], a fin de garantizar la movilidad de los pacientes entre países miembros, así como su asistencia y tratamiento reembolsables en cualquiera de ellos. Como se mencionaba anteriormente, la recopilación y almacenamiento de datos sanitarios se realiza, en la actualidad, de manera electrónica, por lo que su transmisión entre centros adquiere, necesariamente, carácter tecnológico.

Habida cuenta de la competencia nacional de la aplicación de las TIC en materia sanitaria[58], la Directiva 2011/24/UE se enfoca en la creación de una "red voluntaria que conecte a las autoridades nacionales encargadas de la sanidad electrónica que designen los Estados miembros", con el principal objetivo de "conseguir unos beneficios económicos y sociales sostenibles merced a sistemas y servicios europeos de sanidad electrónica"[59]. Para ello, resulta imprescindible el desarrollo de una serie de directrices en lo relativo a la inclusión de datos personales y sanitarios de los pacientes en sus respectivas historias clínicas, que podrán ser transmitidas de manera transfronteriza (Andreu, Alarcón Sevilla, Salcedo, & Soro, 2014). Es precisamente en este punto donde adquieren importancia los mecanismos de protección de datos introducidos por la normativa comunitaria; primero por la Directiva 95/46/CE y más adelante por el mencionado RGPD.

A fin de alcanzar el objetivo introducido por la Directiva 2011/24/UE, la Comisión elaboró la Recomendación 2019/243, definiendo un formato de transmisión seguro e interoperable de historiales clínicos en el ámbito comunitario[60]. En este sentido, se establece la garantía de acceso y transmisión transfronteriza de los datos médicos de los ciudadanos en los términos que cada uno determine, gozando así de plena protección aquella información que se quiera compartir. En este sentido, la Recomendación 2019/243 posiciona al ciudadano como eje principal, alrededor del cual se construyen en materia de *e-Health* los principios enunciados en el RGPD. Especial relevancia tendrán, entre otros, los principios de transparencia de la información y acceso, en este caso, transfronterizo, a los datos personales. Por otro lado, son de especial importancia, por su relevancia práctica para la efectiva

[57] Directiva 2011/24/UE, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza.
[58] Considerando 56, Directiva 2011/24/UE, de 9 de marzo de 2011.
[59] Artículo 14, Directiva 2011/24/UE, de 9 de marzo de 2011.
[60] Recomendación (UE) 2019/243 de la Comisión de 6 de febrero de 2019 sobre un formato de intercambio de historiales médicos electrónicos de ámbito europeo.

protección del historial clínico, los principios de identificación y autenticación, concretadas a través de las identificaciones electrónicas nacionales, reconocidas mutuamente en el ámbito comunitario, según lo previsto por el Reglamento 910/2014[61].

Poniendo ahora el foco del análisis sobre el derecho de oposición y de decisiones individuales automatizadas, resulta importante incidir de nuevo en el consentimiento individual e inequívoco como base para la recopilación y tratamiento de datos personales, a excepción de los ya mencionados escenarios. En salvaguarda de este principio, el RGPD recoge en la Sección 4 de su Capítulo III el derecho de cualquier individuo a oponerse al tratamiento de sus datos personales aún en los excepcionales casos en los que no se requiere su consentimiento, a menos que existan "motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado"[62]. En cualquier caso, en el supuesto de que dichos fines se refieran a la mercadotecnia directa, prevalecerá el derecho de oposición.

Con fundamento similar al derecho de oposición, el RGPD recoge también el derecho a no ser objeto de una decisión basada en el tratamiento automatizado que produzca efectos jurídicos sobre uno mismo[63]. Se hace, con esto, especial alusión a la creación de perfiles, como la caracterización de un individuo a partir del tratamiento automatizado de sus datos personales[64]. Si bien es cierto que la normativa comunitaria enuncia una prohibición genérica –sin perjuicio de la existencia de excepciones- a este tipo de tratamiento de datos, existe una protección superior en el caso de datos de carácter sensible, como es el supuesto de aquellos relativos a la salud[65]. Por lo tanto, en materia de *e-Health*, es especialmente importante garantizar que los individuos no se verán afectados, especialmente a nivel jurídico, por su

[61] Reglamento (UE) 910/2014, 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 el que se deroga la Directiva 1999/93/CE.
[62] Artículo 21.1 Reglamento 2016/679.
[63] "Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar" (Artículo 22.1 Reglamento 2016/679).
[64] "4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física" (Artículo 4 Reglamento 2016/679).
[65] Artículo 9.1 Reglamento 2016/679.

perfilación a través de la gestión automatizada de datos. Si bien el principal peligro que se presenta se concreta en la discriminación de individuos con base en información de carácter personal y protegida por el ordenamiento jurídico, la mera caracterización del interesado realizada a través de estos medios supone una vulneración de su intimidad personal.

Capítulo 7. PASAPORTE COVID: REFLEXIÓN Y CONCLUSIONES.

Como se adelantaba anteriormente, al analizar el concepto de *e-Health* en el ámbito de la gestión de la pandemia ocasionada por la COVID-19, el pasaporte de inmunidad ha constituido un punto verdaderamente conflictivo y de difícil consenso a nivel supra e intra nacional[66]. El debate se ha enfocado en torno a dos principales frentes, concretados en la limitación del derecho fundamental a la libre movilidad entre países miembros de la UE y la vulneración del derecho a la intimidad personal. Para los efectos del presente estudio, la reflexión se centrará en el segundo frente, si bien ambos se encuentran, en la práctica, estrechamente relacionados.

En el contexto comunitario, la UE aprobó a mediados de 2021 el Reglamento 2021/953 relativo a los certificados COVID[67], en el que se establecen las pautas para la emisión y verificación de los pasaportes de inmunidad por parte de los distintos estados miembros, así como las directrices generales en cuanto a las limitaciones de movilidad que su carencia podría conllevar. En cualquier caso, la concreción de estas pautas se ha realizado a nivel nacional, e incluso regional. En todo caso, las medidas impuestas deben someterse al principio de proporcionalidad, puesto que son limitativas de derechos.

Como suele ser el caso en la protección de datos en materia de *e-Health*, el debate principal acerca de la legalidad del certificado COVID gira en torno a la ponderación del interés general frente al derecho subjetivo a la intimidad personal de cada individuo. En este sentido, el principio de proporcionalidad sirve de criterio esencial para resolver este conflicto de derechos. Concretamente, el dilema que se presenta con los pasaportes de inmunidad –así como con otro tipo de medidas impuestas para la gestión de la pandemia- pone en balanza

[66] En el caso del estado español, por ejemplo, la exigencia del pasaporte de inmunidad para la realización de determinadas actividades ha variado enormemente en función de la comunidad autónoma correspondiente. Mientras que en la Comunidad de Madrid se ha prescindido absolutamente de este tipo de documentación, Galicia y Cataluña lo han exigido para el acceso a locales de ocio, a su vez de manera más o menos estricta en función de la zona.

[67] Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo de 14 de junio de 2021 relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19.

el derecho a la salud, en su vertiente colectiva, frente al derecho a la intimidad personal, en su vertiente individual. Este detalle tiene una gran relevancia, puesto que los derechos fundamentales adquieren un peso superior cuando se trata de la protección de su vertiente colectiva. Naturalmente, no se trata en ningún caso de una superioridad absoluta por la que sea innecesaria la observancia del principio de proporcionalidad. Al contrario, se trata precisamente de un criterio adicional que se deberá tener en cuenta en la ponderación de intereses, informada por el principio de proporcionalidad.

Como se ha analizado en distintos momentos a lo largo de este estudio, la información médica o de salud personal goza de un especial nivel de protección, explicado por su carácter sensible. Por lo tanto, la constitucionalidad de la exhibición obligatoria de un certificado que contiene información médica para la realización de determinadas actividades resulta dudosa. Si bien la obligatoriedad de presentar prueba de vacunación para viajar a otros países puede resultar proporcional en salvaguarda de la salud pública[68] – sin perjuicio del problema que surge en el ámbito comunitario al verse vulnerada la libertad de movimiento -, el verdadero dilema radica en la limitación del acceso a determinados lugares a quienes no presenten este certificado.

Poniendo el foco en el ordenamiento jurídico español, la concreción de esta exigencia ha variado en función de las decisiones tomadas por cada comunidad autónoma. En el caso de Galicia, por ejemplo, la obligación impuesta a los lugares de ocio de exigir a los clientes el certificado COVID para permitir su acceso fue objeto de debate jurisprudencial, que se cerró con la STS 1112/2021[69], en la que avala estas prácticas bajo la justificación que se expondrá a continuación. Tras haberse descartado inicialmente las medidas impuestas por la Comunidad Autónoma de Galicia[70], el TS[71] atendió al recurso de casación interpuesto por la

[68] La vacunación obligatoria para acceder a determinados países no constituye una práctica novedosa; hace ya años que esto es habitual. El fin de estas medidas es evitar la contracción de enfermedades graves propias de un ecosistema diferente al del lugar de origen del individuo, para así evitar que se propaguen de manera descontrolada.

[69] Sentencia 1112/2021, de 14 de septiembre, en vista del recurso de casación sobre la ratificación o autorización adoptadas por las autoridades sanitarias que puedan limitar derechos fundamentales; en especial, acerca del pasaporte COVID

[70] El Tribunal Superior de Justicia de Galicia se pronunció en contra de las medidas impuestas por la Xunta con respecto al pasaporte COVID en el Auto de 20 de agosto de 2021, sobre ratificación de las medidas aprobadas por Orden, de 13 de agosto de 2021, del Consejero de Sanidad de la Xunta.

[71] Tribunal Supremo. *Vid.* Listado de abreviaturas.

Xunta de Galicia, ratificando así la Orden de la Consejería de Sanidad de 13 de agosto de 2021 en relación con la exhibición del pasaporte COVID en los locales de ocio.

La ratificación realizada por parte del TS se fundamentó en el test de proporcionalidad mencionado anteriormente, calificando así la medida como idónea y necesaria, al no existir otra menos restrictiva para la consecución del resultado perseguido, y estrictamente proporcional (Garrido, 2021). Como resulta lógico, este último punto es el más conflictivo, puesto que la proporcionalidad de esta exigencia es difícilmente constatable en el contexto de la pandemia desde finales de 2021 hasta la actualidad. Por ello, adquiere sentido realizar una reflexión acerca de la proporcionalidad de la medida en lo que a protección de datos e intimidad personal se refiere.

En primer lugar, es importante clarificar que la protección de datos se encuentra garantizada por esta medida, puesto que la exigencia se concreta en la exhibición del pasaporte COVID, impidiéndose el registro de datos personales. El centro de la cuestión radica en la intimidad personal, que se ve vulnerada por la mera obligación de revelar datos personales de carácter sensible para el acceso a un local. El TS justifica en la STS 1112/2021 la proporcionalidad de esta medida por tratarse de "una pieza básica y esencial para impedir la propagación de la infección por el SARS-CoV-2 y, por tanto, de la preservación de la vida y la salud de todos". Sin embargo, si bien este razonamiento podría haber tenido validez al principio de la pandemia, cuando verdaderamente suponía una amenaza contra la salud colectiva, tanto por los propios síntomas y efectos de la COVID-19, como por el colapso sanitario que ocasionaba, resulta dudoso que en septiembre de 2021 pudiera justificarse la vulneración de la intimidad personal en salvaguarda de la salud colectiva.

En cualquier caso, la importancia de esta cuestión no radica tanto en el propio certificado COVID, sino más bien en su función como justificante de la vulneración de la intimidad personal. Aún en el contexto actual de relajación de medidas de prevención –si bien, llamativamente, en Galicia aún es obligatorio el certificado COVID para el acceso al ocio nocturno-, e incluso potencial disipación de la pandemia para dar paso a una epidemia, la vulneración de derechos que se ha observado a lo largo de su gestión mantiene su importancia. La razón principal para ello es que, en caso de inobservancia de las consecuencias pertinentes, podría servir de precedente para futuras vulneraciones de derechos fundamentales. En este sentido, el derecho a la intimidad personal se encuentra en

una especial situación de riesgo, puesto que el contexto actual de proliferación de las TIC, especialmente en lo que a la Web 2.0 se refiere, dificulta el respeto y protección de los datos personales. En el contexto de la *e-Health*, el pasaporte COVID supone un claro punto de inflexión en lo que a intimidad personal con respecto a información médica respecta, por lo que es importante evitar que el debate y los mecanismos jurídicos de defensa activados a lo largo de los últimos años caigan en el olvido al llegar la pandemia a su fin.

Como se exponía en la introducción del estudio, el principal objetivo perseguido por este se concreta en el análisis de las previsiones del ordenamiento jurídico en lo que a la protección de datos e intimidad personal en materia de *e-Health* respecta. La más importante razón para ello radica en la necesaria valoración de la adecuación de las previsiones jurídicas a la realidad fáctica de las TIC en materia sanitaria, en especial en lo relativo a la garantía de derechos fundamentales de la personalidad. En este sentido, el pasaporte COVID no es sino una clara demonstración de los conflictos morales y jurídicos que de los avances tecnológicos pueden surgir cuando entran en contacto con datos de carácter especialmente sensible, como es el caso de los historiales médicos personales.

BIBLIOGRAFÍA

I. LEGISLACIÓN

Constitución Española de 1978.

Ley 14/1986, de 25 de abril, General de Sanidad (BOE 29 de abril de 1986).

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 respeta al tratamiento de datos personales y a la libre circulación de estos datos (BOE 23 de noviembre de 1995).

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 (BOE 4 de mayo de 2016).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (BOE 6 de diciembre de 2018).

Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica (BOE 15 de noviembre de 2002).

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (BOE 12 de julio de 2002).

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (BOE 31 de julio de 2002).

Reglamento (UE) No 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/CE (DOUE 28 de agosto de 2014).

Reglamento (UE) 2021/953 del Parlamento Europeo y del Consejo de 14 de junio de 2021 relativo a un marco para la expedición, verificación y aceptación de certificados COVID-19 interoperables de vacunación, de prueba diagnóstica y de recuperación (certificado COVID digital de la UE) a fin de facilitar la libre circulación durante la pandemia de COVID-19 (BOE 15 de junio de 2021).

II. JURISPRUDENCIA

Sentencia del Tribunal Constitucional 290/2000, de 30 de noviembre de 2000. Recursos de inconstitucionalidad acumulados 201/93, 219/93, 226/93 y 236/93.

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000.

Sentencia del Tribunal Supremo 1112/2021. Recurso de casación contencioso-administrativo.

III. OBRAS DOCTRINALES

Agencia Española de Protección de Datos. (2020). *El uso de las tecnologías en la lucha contra el COVID19. Un análisis de costes y beneficios.*

Andreu, B., Alarcón Sevilla, V., Salcedo, J., & Soro, B. (2014). Sanidad electrónica e intercambio de información sanitaria en Europa a la luz de la nueva regulación sobre protección de datos personales. *DS: Derecho y Salud*, págs. 276-286.

Cuadrada, E. B. (2007). *La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad.*

de Abajo, B. S.-C. (2011). M-health y T-health. La evolución natural del E-health. *RevistaeSalud.com, 7(25),11*. Obtenido de RevistaeSalud.com, 7(25), 11: https://dialnet.uniroja.es/descarga/articulo/3407842.pdf

de Montalvo Jääskeläinen, F. (2016). Tema 16: Los derechos y las libertades públicas (II). En *Lecciones de Derecho Constitucional* (pág. 387).

Eysenbach, G. (2001). *What is e-health?* Journal of medical Internet research, 3(2), e20.

Fernández Cacho, L. M. (2016). *Enfermería y Salud 2.0. Recursos TICs en el ámbito sanitario. Index de Enfermería, 25(1-2), 51-55.*

Fernández Silano, M. (2013). La Salud 2.0 y la atención de la salud en la era digital. *Revista Médica de Risaralda, 20 (1).*

Garrido, C. D. (2021). ¿Pasaporte para el ocio? Comentario a la Sentencia del Tribunal Supremo 1112/2021, de 14 de septiembre, que avala la solicitud del "pasaporte covid" en bares y restaurantes de Galicia. *Revista CESCO de Derecho de Consumo*.

Kress, A. (2017). *La Unión Europea como modelo de protección de datos en eHealth, su influencia y barreras a la convergencia.*

Maqueo Ramírez, M. S. (2017). Protección de datos personales, privacidad y vida privada: La inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia)* , 30(1), 77-96.

Martín, J. M. (2021). *La protección de datos personales en el ámbito de la salud: transparencia y acceso a la información pública sanitaria.*

O'Reilly, T. (2005). *Web 2.0: compact definition.*

Ortega Giménez, A. &. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. *Revista de la Facultad de Derecho, (44)*, 31-73.

Petracci, M. &. (2020). e-Health y pandemia Covid-19: nuevos tiempos para las relaciones entre médicos y pacientes. *Chasqui: Revista Latinoamericana de Comunicación, (145), 281-300*.

Salud, O. M. (2005). 58ª Asamblea Mundial de la Salud. Resoluciones y Decisiones., (págs. 114-116). Ginebra.

Villanueva-Turnes, A. (2016). El derecho al honor, a la intimidad y a la propia imagen, y su choque con el derecho a la libertad de expresión y de información en el ordenamiento jurídico español. *Díkaion Revista de Fundamentación Jurídica, 25(2)*, 190-215.