TESIS DOCTORAL

2023

EL DERECHO A LA PORTABILIDAD DE DATOS PERSONALES Y SU IMPACTO EN LA GARANTÍA DEL DERECHO A LA SALUD.

ANÁLISIS COMPARATIVO Y UNA PROPUESTA PARA SU REGULACIÓN EN MÉXICO.

ANA GUADALUPE OLVERA ARELLANO

PROGRAMA DE DOCTORADO EN DERECHO Y CIENCIAS SOCIALES

DIRECTOR, DR. LUIS MIGUEL GONZÁLEZ DE LA GARZA, PROFESOR TITULAR DE LA UNIVERSIDAD, UNED.
CODIRECTORA, DRA. CARMEN MUÑOZ DELGADO, PROFESORA AYUDANTE DOCTORA, UNED.

Para Melissa.

Esperanza no es lo mismo que optimismo.
No es la convicción de que algo saldrá bien,
sino la certeza de que algo tiene sentido,
independientemente de cómo resulte.
Václav Havel

Contenido

Lista de símbolos, abreviaturas y siglas

AEPD	Agencia Española de Protección de Datos
ARCO	Acceso, rectificación, cancelación y oposición
CE	Constitución Española de 1978
CEPD	Comité Europeo de Protección de Datos
CNDH	Comisión Nacional de los Derechos Humanos
CURP	Clave Única de Registro de Población
DGIS	Dirección General de Información en Salud
EIPD	Evaluación de Impacto de Protección de Datos
ENDUTIH	Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares
ENISA	Agencia de la Unión Europea para la Ciberseguridad
GRUPO DE TRABAJO DEL ARTÍCULO 29	Grupo de trabajo del artículo 19
IFAI	Instituto Federal de Acceso a la Información
INAI	Instituto Nacional de Transparencia, Acceso a la Transparencia y Protección de Datos
INEGI	Instituto Nacional de Estadística y Geografía
IFT	Instituto Federal de Telecomunicaciones
OMS	Organización Mundial de la Salud
SCJN	Suprema Corte de Justicia de la Nación
SIRES	Sistemas de Información de Registro Electrónico en Salud
TEDH	Tribunal Europeo de Derechos Humanos
UE	Unión Europea

Lista de tablas e ilustraciones

Resumen

Con la publicación en el Diario Oficial de la Unión Europea del Reglamento General de Protección de Datos Personales (2016) y en el Diario Oficial de la Federación de la República Mexicana de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, se garantizó el derecho de portabilidad de los datos personales, que ya encontraba antecedentes en el campo de las telecomunicaciones y que puede ser exigido en múltiples ámbitos como el de la salud, materia de esta investigación.

En ese sentido, esta investigación pretende analizar si el ejercicio de este derecho, tal y como se encuentra previsto en las normas mencionadas que se encuentran vigentes, resulta beneficioso para los usuarios de los sistemas de salud o si, por el contrario, les representa una carga.

A través del estudio comparado de las legislaciones citadas, además de las correspondientes en derecho sanitario, encontramos que los elementos subjetivos y objetivos de este derecho afectan a la totalidad del ciclo de vida del dato personal, así como las limitaciones existentes para el ejercicio y garantía del derecho a la portabilidad en el ámbito de la salud, muchas de las cuáles tienen que ver, principalmente, con la capacidad que tienen los responsables de tratamiento, de adoptar los avances tecnológicos que les permitan llevar a cabo comunicaciones de datos personales.

Finalmente, y siguiendo la corriente del pragmatismo jurídico de Atienza, formulamos una propuesta para que este derecho pueda ser aprovechado como instrumento, a su vez, de garantía del derecho de protección a la salud.

Palabras clave: derecho de portabilidad; derecho a la salud; expediente clínico; derecho de protección de datos personales.

Abstract

With the publication in the Official Journal of the European Union of the General Data Protection Regulation (2016) and in the Official Journal of the Federation of the Mexican Republic of the General Law for the Protection of Personal Data Held by Obligated Subjects, on January 26, 2017, the right to data portability was guaranteed and already found precedents in the field of telecommunications, and which can be required in multiple fields such as health, the subject of this investigation.

This research aims to analyze whether the exercise of this right, as provided for in the aforementioned regulations, is beneficial for users of health systems or if, on the contrary, it represents a burden.

Through the comparative study of the said legislations, in addition to the corresponding ones in health law, we found that the subjective and objective elements of this right affect the entire life cycle of personal data, as well as the existing limitations for the exercise and guarantee of the right to portability in the field of health; many of which are related with the ability of the responsible for treatment to adopt technological advances that allow them to carry out personal data communications.

Finally, and following the current of Atienza's legal pragmatism, we formulate a proposal in order to make possible this right can be used as an instrument, in turn, to guarantee the right to health protection.

Keywords: portability right; right to health; medical records; right to protection of personal data.

Introducción

La Organización Mundial de la Salud (OMS) desde 1946, conceptualiza a la salud como “un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades" (2007), con lo que resulta claro que se privilegia el estado de bienestar integral del ser humano en las tres esferas en las que se desenvuelve para considerarle saludable.

El derecho a la salud se ha visto positivizado en los ordenamientos constitucionales del siglo XX como resultado de los avances tecnológicos y de la ciencia médica, que han modificado la longevidad del ser humano y por lo tanto, conceptos como el de la muerte. Valadez (2020, p. 13) estima que las consecuencias de los avances no solo influirán a la protección de la salud, sino que impactarán a las materias laboral, educativa, asistencial, habitacional y económica, lo que instará a que se innove en materia jurídica dada la dimensión y velocidad con la que los cambios se presentan cotidianamente.

Coincide Brena (2020, p. 15) al apreciar que la salud es consecuencia “de la interacción de diversas variables ambientales, socioeconómicas, psicológicas y biológicas que inciden en el individuo y en la sociedad”, por lo que su análisis y protección debe ser multidisciplinario ya que no se trata de un derecho que, siendo fundamental, se considere autónomo. Así, resulta de utilidad que su estudio se lleve a cabo desde enfoques como los que ofrecen derechos tales como a tener una vida con calidad, a la dignidad, a la autonomía, a la integridad física y mental, a la intimidad o a la información.

Esto es lo que Ferrajoli (2013, p. 395) expone como los dos sentidos del derecho a la protección a la salud, que define como molecular. El primero es el derecho negativo de inmunidad, es decir, se prohíbe lesionar y por tanto se da una abstención de dañar la salud. El otro, positivo, que “dada su universalidad, sólo podrá ser garantizado a todos si sus garantías positivas se encomiendan a la

esfera pública",[1] es decir, como obligaciones aspiracionales o derechos programáticos. Así, la efectividad del derecho a la salud no puede, ni debe, "limitarse a prever diagnósticos y tratamientos preventivos de carácter público y gratuito" ya que encuentra múltiples expresiones para su garantía, por ejemplo, a ser tratado adecuadamente, al acceso a servicios de salud convenientes, a ser informado acerca del pronóstico diagnóstico y tratamiento, a participar en las decisiones terapéuticas, a expresar el consentimiento informado, a ser resarcido por eventuales daños e incluso, a morir con dignidad (Ferrajoli. 2013, p. 293). En la misma línea argumentativa, Pérez Luño (2012, p. 84) indica que el derecho a la salud, como uno social, requiere de evitar que se le impongan obstáculos para alcanzar su punto de desarrollo, en tanto a la prevención, tratamiento y erradicación de enfermedades infecciosas y contagiosas y también a las investigaciones médicas tendentes a prolongar la vida y su calidad.

Por lo que hace a los órdenes jurídicos nacionales, en México, el artículo 4 de la Constitución Política de los Estados Unidos Mexicanos de 5 de febrero de 1917, además de garantizar el derecho de cualquier persona que se encuentre en el país y no cuente con seguridad social, a recibir de forma gratuita la prestación de servicios públicos de salud, medicamentos y cualquier insumo necesario al momento de requerir la atención, sin importar su condición social; ordena al legislador definir las bases y modalidades para el acceso a los servicios de salud a través de la legislación secundaria, así como la concurrencia entre la Federación y las entidades federativas en materia de salubridad general lo que se desarrolla en la Ley General de Salud, de 7 de febrero de 1984.

En el ámbito de lo local, rigen de manera concurrente[2] las Leyes de Salud promulgadas en cada entidad federativa. En conjunto, establecen como finalidades del derecho a la protección de la salud el bienestar físico y mental del hombre para contribuir al ejercicio pleno de sus capacidades; la prolongación y

[1] Así, el autor refiere que en el primer caso se trata de un derecho absoluto, pero en el segundo de uno relativo pues identifica dos garantías impuestas a los particulares, que son las de asistencia y cuidado a cargo de los padres y la otra, a cargo de los empleadores en los centros de trabajo.

[2] La concurrencia, de acuerdo con el artículo 124 de la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917, consiste en que las facultades que no se concedan por esta a los funcionarios federales se entienden reservadas a las entidades federativas o a la Ciudad de México, en el ámbito de la competencia de cada uno.

el mejoramiento de calidad de la vida humana; la protección y el acrecentamiento de los valores que coadyuven a las condiciones de salud y que contribuyan al desarrollo social; la extensión de actitudes solidarias y responsables de la población para la preservación conservación, mejoramiento y restauración de la salud; el disfrute de los servicios que satisfagan las necesidades de la población y el desarrollo de la enseñanza y la investigación científica y tecnológica para la salud.

En el marco jurídico español, el derecho a la salud se encuentra previsto desde la Constitución de 1978 en su artículo 43 en los términos siguientes:

> 1. Se reconoce el derecho a la protección de la salud.
> 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.
> 3. Los poderes públicos fomentarán la educación sanitaria, la educación física y el deporte. Asimismo, facilitarán la adecuada utilización del ocio. (sic)

En la misma disposición normativa podemos encontrar positivizado la obligación de los poderes públicos de garantizar un sistema de servicios de salud a los ciudadanos durante la tercera edad (artículo 50), así como la salud y defensa de los consumidores (artículo 51). A diferencia del marco jurídico mexicano, el español prevé como titulares de este derecho y el de atención sanitaria a cualquier español y los ciudadanos extranjeros, siempre que tengan establecida su residencia en ese país y son únicamente ellos quienes tienen la legitimación para ejercerlos en la vía administrativa como la jurisdiccional. Para los no residentes y los españoles que se encuentren fuera del territorio nacional, el derecho se garantiza en arreglo de las condiciones que establezcan las leyes y convenios internacionales.

A mayor abundamiento del Comité de Derecho Económicos, Sociales y Culturales de la ONU (2000) a través de la Observación General 14[3], estima que el derecho a la salud no se entiende como el derecho a estar sano, sino como el derecho al disfrute de toda una variedad de beneficios, bienes, servicios y condiciones necesarios para alcanzar el más alto nivel posible de disfrute de este derecho.

Continuando con la Observación General 14 (ONU, 2000, párrafo 37) señala la obligación de cumplir, a través de la importancia de la promoción de medidas positivas por parte del Estado, que incluirán, entre otras, "fomentar la realización de investigaciones y el suministro de información" y la de "apoyar a las personas a adoptar, con conocimiento de causa, decisiones por lo que respecta a su salud", lo que consideramos podrá lograrse además con la mejora de la relación prestador-usuario, ambos del sistema de salud, si se vuelven eficientes los mecanismos de acceso al expediente clínico, cuestiones que se abordarán a lo largo de este trabajo.

Además de las señaladas, entre las obligaciones del Estado que resultan prioritarias, se señalan en el párrafo 44, la de impartir educación y proporcionar acceso a la información relativa a los principales problemas de salud en la comunidad, con inclusión de los métodos para prevenir y combatir esas enfermedades y la de proporcionar capacitación adecuada al personal del sector salud, incluida la educación en materia de salud y derechos humanos. Por medio de su desarrollo se privilegia la creación de conciencia del personal de salud y también del paciente, de que poseen derechos que pueden ejercer y sus obligaciones para cumplir de manera mutua y en un ámbito de respeto a su contraparte y a las disposiciones legales que rigen su comportamiento. Resulta natural que una de las violaciones que establece el Comité es la de la ocultación

[3] Al respecto, el Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito mexicano, se ha pronunciado acerca de la forma idónea de cumplirla en el contexto nacional mediante la siguiente tesis aislada "DERECHO A LA SALUD. FORMA DE CUMPLIR CON LA OBSERVACIÓN GENERAL NÚMERO 14 DEL COMITÉ DE LOS DERECHOS SOCIALES Y CULTURALES DE LA ORGANIZACIÓN DE LAS NACIONES UNIDAS, PARA GARANTIZAR SU DISFRUTE". Datos de localización: publicación en el Semanario Judicial de la Federación y su Gaceta, Décima Época, libro XXV, tesis aislada I. 4o. A, 86 A, Tribunal Colegiado de Circuito, t. 3, octubre de 2013, p. 1759.

deliberada de la información que reviste importancia fundamental para la protección de la salud o para el tratamiento (párrafo 50).

Para cumplir con las finalidades descritas que han dado contexto a este preámbulo, es que se requiere el tratamiento exhaustivo de datos personales de los denominados sensibles, que se encuentran plasmados en las historias clínicas, que si bien es cierto podrían ser anonimizados, en algunos casos se requiere de contar con la identificación plena del sujeto en cuestión, lo que Pérez Luño (2012, p. 84) señala como el punto máximo de tensión entre este derecho y el de la intimidad, del que Troncoso (2016, p. 49) afirma que "[…] es un presupuesto para una mínima calidad de vida, para la dignidad y para la libertad personal".

Así, y como refirió el Instituto Federal de Acceso a la Información (2014, p. 2), "la protección de datos personales es un derecho humano, reconocido en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917 que otorga el poder a toda persona física para que sus datos personales sean tratados de manera lícita y leal, a fin de garantizar su privacidad y derecho a la autodeterminación informativa, es decir, a decidir quién puede tratar sus datos personales y para qué fines". Además de los derechos de acceso, rectificación, cancelación y oposición (ARCO), recientemente en varios países -y en el marco de derecho comparado- ha sido reconocido el derecho a la portabilidad de los datos personales, que como ya se verá, se ejerce de manera parecida a los otros e incluso, algunos autores comentan que se trata de una especie dentro del género del derecho de acceso. De esta forma, la recolección de datos que hace posible el acto médico resulta esencial para establecer el contexto de cuáles son los límites, positivos y negativos, de ejercer el derecho de portabilidad de los datos contenidos en el expediente clínico.

Puccinelli (2018, p. 162), aunque no ofrece una definición del derecho, sí refiere de manera muy específica lo que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, apenas puntualiza, que "la portabilidad, bien entendida, requiere que sean compatibles, no sólo los formatos de tratamiento, sino también de hardware y software. De

hecho, la ejecutabilidad de un mismo programa de computador en diferentes plataformas es condición para un desafío mayor: el de la interoperabilidad de los sistemas, que al entenderse —en sus perspectivas técnica, organizativa y semántica— la habilidad de dos o más sistemas o componentes para intercambiar información y utilizarla intercambiada, se convierte es un concepto clave, tanto en el ámbito privado como en el público, con miras al gobierno electrónico, abierto y al desarrollo de los sistemas inteligentes. Imagínese entonces el alcance que el ejercicio pleno de este derecho, con todos los límites que señala el autor, garantiza al usuario de los servicios de salud de cualquier país."

Es importante mencionar que, a diferencia de lo que sucede en los Estados miembros de la Unión Europea (UE), la República Mexicana no cuenta con legislación tan especializada en materia de salud que haga referencia al problema de estudio descrito, por lo que algunas cuestiones que ya están resueltas en el primer ámbito territorial mencionado, tales como la existencia de una historia clínica electrónica única, los mecanismos para su acceso, conservación, eliminación o bien, lo que respecta a los datos personales de los fallecidos, que en México cuentan con pobre o nula regulación, y tratándose de datos personales sensibles, en su mayoría, resulta evidente la urgencia del abordaje legislativo o cuando menos, uno doctrinal. Además de lo anterior, en México la legislación en materia de datos personales únicamente garantiza el derecho a la portabilidad en la aplicable a entes públicos, lo que supone otro obstáculo para los usuarios de los servicios de salud que quisieran beneficiarse de esta novedad legislativa.

Con el paso del tiempo, la portabilidad como característica, alcanzará relevancia gracias al rápido avance de la tecnología, por lo que entenderla para su utilización dentro del marco de la normativa que lo rige es tarea obligada para los profesionales y usuarios de los sistemas de salud, al ofrecer celeridad y certeza para ambas partes en esa etapa de la transmisión y tratamiento de los datos. Por lo ya descrito, el presente trabajo encuentra viabilidad y encuadre desde los Objetivos de Desarrollo Sostenible, adoptados por la Organización de las Naciones Unidas en 2015, particularmente desde el número tres,

denominado “Salud y bienestar”. A nivel Estado, el mexicano en su Plan Nacional de Desarrollo 2019-2014, publicado en el Diario Oficial de la Federación el 12 de julio de 2019, y que en su eje 2. Política Social, contiene al sub-eje “Salud para toda la población”.

Este último, se desarrolla en el Programa Sectorial Derivado del Plan Nacional de Desarrollo 2019-2024, que en su Objetivo prioritario 3, llamado “Incrementar la capacidad humana y de infraestructura en las instituciones que conforman el Sistema Nacional de Salud, especialmente, en las regiones con alta y muy alta marginación para corresponder a las prioridades de salud bajo un enfoque diferenciado, intercultural y con perspectiva de derechos”, contiene a la “Estrategia prioritaria 3.4 modernizar el sistema de información y comunicación con el propósito de garantizar información confiable y oportuna que facilite las decisiones en política pública, anticipe las necesidades de la población y favorezca la pertinencia cultural en los servicios brindados en el Sistema Nacional de Salud” y como acciones puntuales relacionadas las que a continuación se enumeran:

- 3.4.1 Promover un Centro de Inteligencia en Salud, a partir de la reorganización de áreas para unificar los mecanismos relacionados con registro, conservación y almacenamiento de la información y evitar la fragmentación de la información en los diferentes niveles de atención en el sector.
- 3.4.2 Conformar un Padrón único de Salud, que permita identificar la confición de derechohabiencia de la población y su nivel de accesibilidad a los servicios de protección a la salud bajo el enfoque de redes integradas.
- 3.4.3 Fortalecer los mecanismos para la identificación y registro de datos personales, que consideren las disposiciones de la legislación vigente, que se evite la duplicidad de registros y favorezca el acceso y manejo de la información.
- 3.4.4 Articular los sistemas de información y comunicación existentes en el sector para procurar su unificación, conservación y

aprovechamiento, especialmente para la conformación de plataformas y bases de datos confiables.

- 3.4.5 Implementar progresivamente tecnologías de información y comunicación tendientes a garantizar el funcionamiento de los sistemas de información, digitalización de expedientes e interoperabilidad interinstitucional, entre los diferentes niveles de atención en las instituciones que conforman el Sistema Nacional de Salud.

A su vez, el Reino de España cuenta con la Estrategia España 2050. Fundamento y propuestas para una Estrategia Nacional de Largo Plazo, elaborado por el Ministerio de la Presidencia en 2021; la Estrategia de Salud Digital del Sistema Nacional de Salud, elaborado por la Secretaría General de Salud Digital, Información e Innovación para el Sistema Nacional de Salud de 2 de diciembre de 2021, documento en el que se prevén líneas para implementar la Estrategia de Salud Digital y como objetivos, los que se especifican:

- 5.2.1 Personas y Salud.
- 5.2.2 Procesos de Valor
- 5.2.3 Información interoperable y de calidad
- 5.2.4 Innovación y atención sanitaria de Salud Pública

Por lo ya expuesto, la hipótesis propuesta es que el derecho de portabilidad de los datos contenidos en el expediente clínico, puede ser determinante en el ejercicio del derecho a la salud del titular de los datos, por lo que resulta adecuado, en mayor beneficio del paciente, permitir el acceso a la totalidad del expediente clínico, incluyendo la información derivada, inferida, creada o generada por el médico tratante, mediante un sistema de expediente clínico electrónico único, que permita facilitar el ejercicio del derecho materia de estudio. Consideramos que el ejercicio del derecho de portabilidad de los datos contenidos en el expediente clínico puede ser determinante en el ejercicio del derecho a la salud del titular de los datos. De esta suerte y, al estudiarlo de manera integral, se establecerá su utilidad y beneficios en materia sanitaria. Al reconocer las limitantes de su ejercicio, podrá hacerse una propuesta para su

mejor utilización en este ámbito particular, específicamente en la República Mexicana.

Para cumplir con el objetivo de esta investigación y comprobar la hipótesis, desarrollamos una metodología de análisis de derecho comparado, así como una investigación documental retrospectiva y cualitativa, en tanto se trata de un análisis de documentos ya existentes. Además de profundizar en la calidad de la muestra seleccionada y no en la cantidad, será exploratoria y descriptiva en un inicio y llegará a ser explicativa en cuanto se refiere a la descripción de procesos y la elaboración de la propuesta final del caso mexicano, para la que nos apegamos al pragmatismo jurídico de Atienza (2017, pp. 75-77) entendido como "la vinculación del derecho con ciertas necesidades prácticas de los hombres", con una "visión instrumental y finalista" pues considera a la ciencia jurídica como "un instrumento para resolver (o prevenir, o tratar) conflictos, un medio para la obtención de fines sociales" resultando entonces, útiles los enunciados propuestos, ya que "la teoría del derecho que se suele elaborar en los países latinos (tanto la dogmática como la teoría general), adolece precisamente de ese defecto: la falta de pragmatismo, de incapacidad para incidir en las prácticas jurídicas".

Su marco temporal irá desde 2016 a julio de 2023 y los datos serán recabados mediante la revisión de la literatura existente, así como el estudio de jurisprudencia y legislación, principalmente mexicanas y españolas, pero también se ha incluido a otros países como Australia y algunos miembros de la Unión Europea, por considerar de interés para esta investigación la experiencia casuística y legislativa que ofrecen.

Para dar respuesta a las interrogantes que motivan a la investigación, ésta se dividirá en cinco partes. Así, en la primera se brindará el marco conceptual y legal de la portabilidad como categoría dogmática, explicando primero el contexto de digitalización y cobertura de la conexión a internet que tienen tanto México como España, con la finalidad de entender el contexto en el que debe ejercerse tal como se encuentra regulado el derecho a la portabilidad, pero también, para considerar todas las circunstancias que influirán en el diseño de

nuestra propuesta; exponiendo también el caso del modelo estadounidense donde ya se llevan a cabo prácticas de portabilidad de datos personales. Así mismo, exponemos los antecedentes normativos de este derecho recién positivizado, es decir, a los de acceso rectificación, cancelación y oposición en el caso del orden jurídico mexicano; y a los de acceso, rectificación, supresión, limitación del tratamiento y de no ser objeto de decisiones automatizadas, en el caso del orden jurídico español y comunitario.

La segunda parte aborda el estudio doctrinal y legal del derecho de la portabilidad de datos personales y se establecerá si este derecho es uno nuevo o bien, se trata de una especie del derecho de acceso a la información personal. También se explicará qué es un formato estructurado y comúnmente utilizado, qué es la interoperabilidad, las obligaciones que tiene el responsable del tratamiento para su garantía y cuáles son las causas de improcedencia de su ejercicio y los medios de impugnación ante la falta de respuesta o la respuesta no satisfactoria ante una solicitud del ejercicio de la portabilidad. Igualmente se expone a la información inferida y su clarificación, con la finalidad de reconocer los límites de ejercicio del derecho de portabilidad, así como las medidas de seguridad que en los órdenes jurídicos mexicano, español y comunitario deberán garantizar para llevar a cabo cualquier tipo de comunicación de datos personales, en su jurisdicción territorial o con otros países.

En la tercera parte se analizará la forma en la que se ejerce el derecho de portabilidad de datos personales en el contexto sanitario, en el que se enmarca esta investigación. en las diversas legislaciones estudiadas, particularmente en el marco de los Sistemas Nacionales de Salud mexicano y español, en comparación al Espacio Europeo de Datos Sanitarios y la Historia Clínica Electrónico (ePA) de Alemania, como ejemplos de buenas prácticas.

La cuarta parte desarrollará el análisis y discusión de lo expuesto con anterioridad y en la quinta parte, se ofrecerán las conclusiones alcanzadas en la investigación. Se definirá si es que en el Estado Mexicano existen las condiciones para ejercer el derecho de portabilidad mediante un sistema de

expediente clínico electrónico único, haciendo la propuesta de solución conducente.

Primera parte. La portabilidad como categoría dogmática.

1.1 Contexto geográfico. La digitalización y cobertura de conexión de internet.

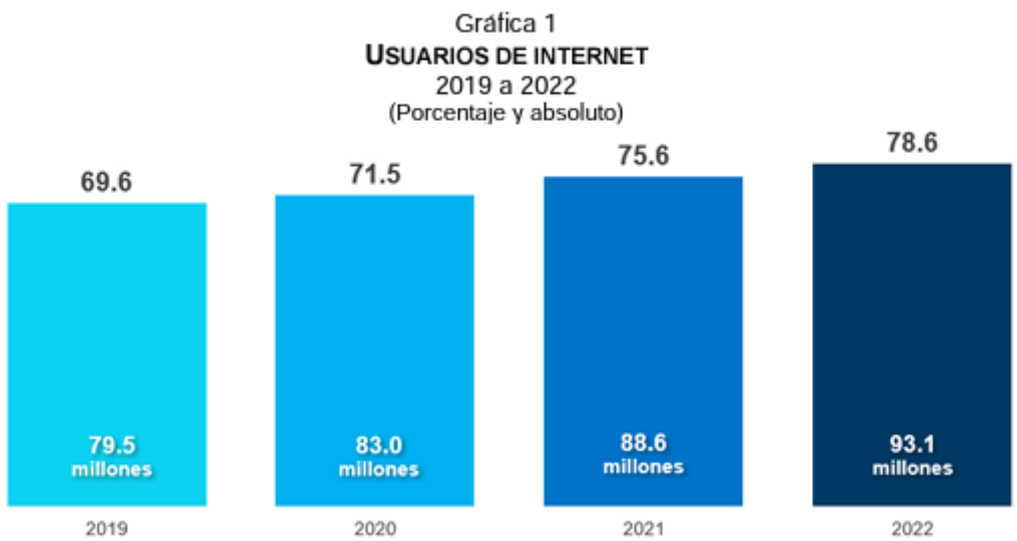
Para conocer el contexto en que se ejerce el derecho de portabilidad de datos personales, así como para determinar el alcance y viabilidad de la propuesta que realizaremos, nos resulta indispensable conocer en primer lugar el porcentaje de digitalización y de acceso que se tiene a la tecnología que permite tanto el acceso y tratamiento de los datos personales, como el ejercicio y garantía del derecho en cuestión.

1.1.1 México

Según la última Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (en adelante, ENDUTIH) (INEGI, IFT 2022), en México, durante 2022:

93.1 millones de mexicanos a partir de los seis años son usuarios de internet, lo que equivale a un 78.6% de la población. (ENDUTIH, 2022, p. 1)

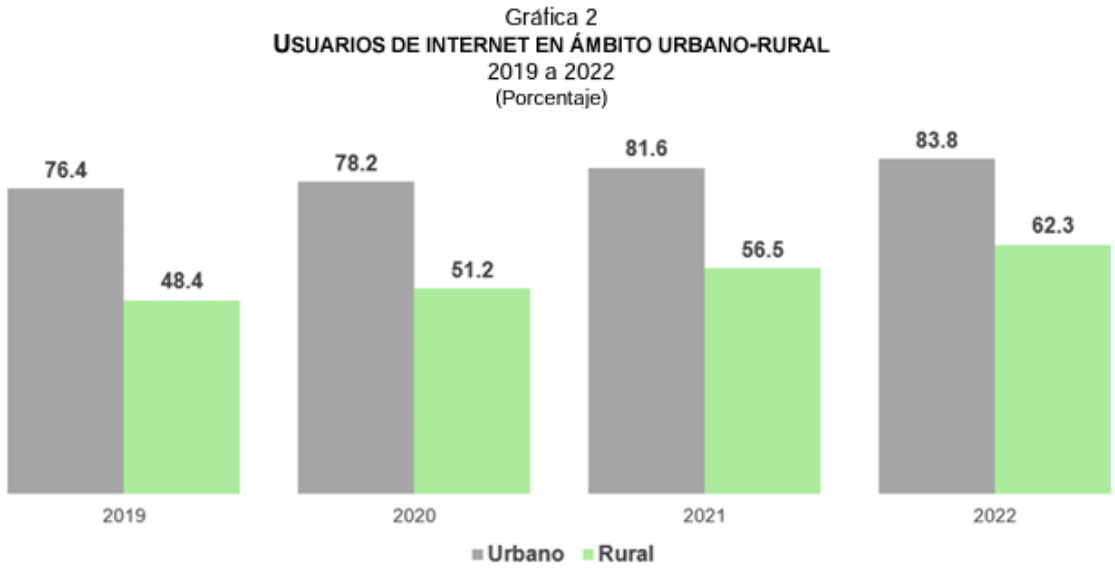
Ilustración 1. Usuarios de internet 2019 a 2022.



Fuente: ENDUTIH, 2022, p. 1.

En el ámbito urbano, en el rango de edad de la encuesta, un 83.8% de la población utilizó internet, en contraste con el 62.3% de la población establecida en una esfera rural. (ENDUTIH, 2022, p. 2)

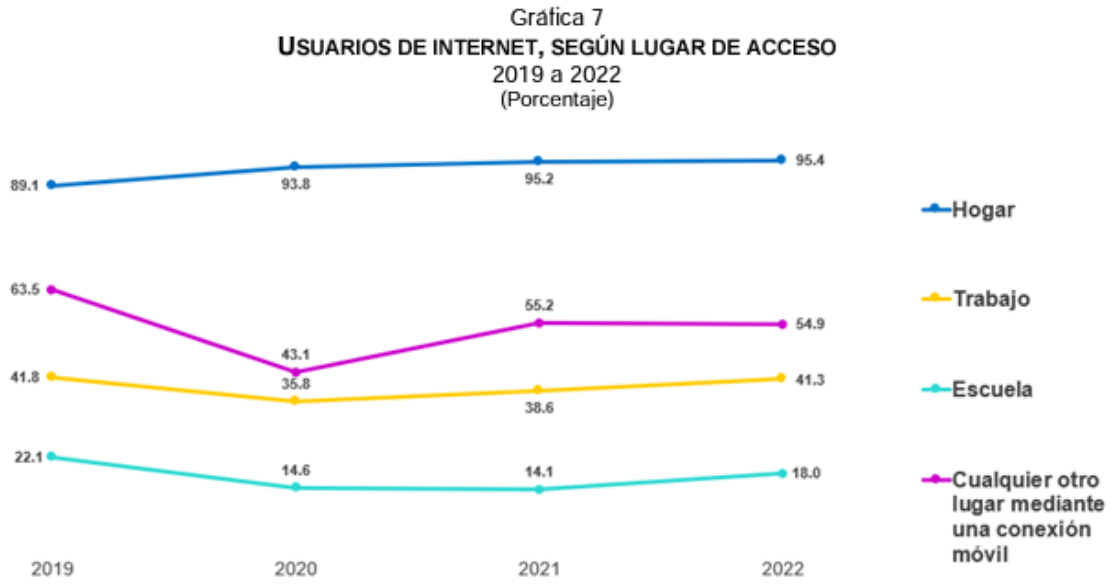
Ilustración 2. Usuarios de internet en ámbito urbano-rural. 2019 a 2022.



Fuente: ENDUTIH, 2022, p. 2.

La mayoría de los mexicanos encuestados tiene acceso a internet desde su hogar (95.4%), aunque también lo hacen desde su trabajo (54.9%), la escuela (41.3) y un porcentaje significativamente menor, desde cualquier otro lugar mediante una conexión móvil (18%). (ENDUTIH, 2022, p. 5)

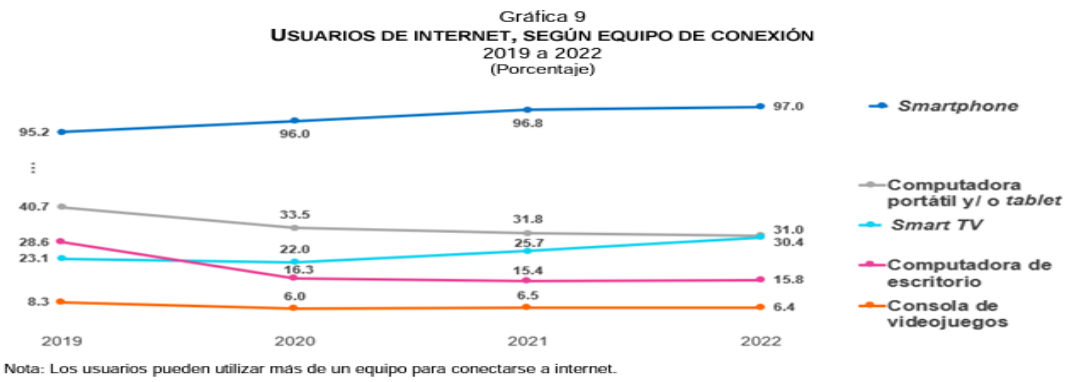
Ilustración 3. Usuarios de internet, según lugar de acceso 2019 a 2022.



Fuente: ENDUTIH, 2022, p. 5.

Del universo de personas encuestadas, un 97% tiene acceso mediante un teléfono inteligente. De forma complementaria a esta tecnología, un 31% manifestó tenerlo también desde una computadora portátil y/o tableta; un 30.4% desde su televisión inteligente; el 15.8% desde una computadora de escritorio y finalmente un 6.4% a través de una consola de videojuegos. (ENDUTIH, 2022, p. 6)

Ilustración 4. Usuarios de internet, según equipo de conexión 2019 a 2022.



Fuente: ENDUTIH, 2022, p. 6.

La Entidad Federativa con mayor cantidad de usuarios de internet es Baja California, con un 89.8%. La capital del país, Ciudad de México, se sitúa en

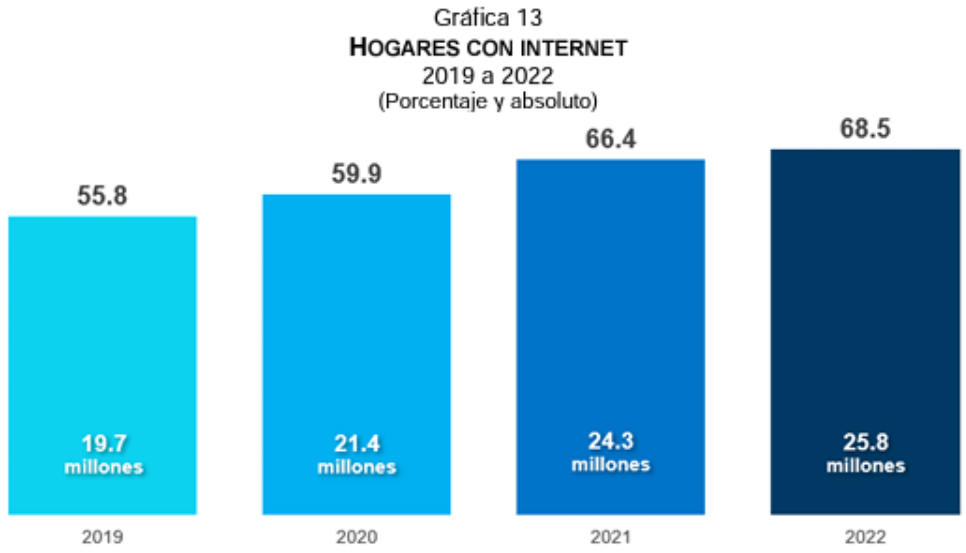
segundo lugar con un 89.7%. El último lugar lo ocupa Chiapas, con un 56.7%. (ENDUTIH, 2022, p. 10)

Ilustración 5. Usuarios de internet, según Entidad Federativa 2022.

Fuente: ENDUTIH, 2022, p. 10.

Por lo que hace a hogares con servicio de internet, únicamente un 68.5% cuenta con este. (ENDUTIH, 2022, p. 10)

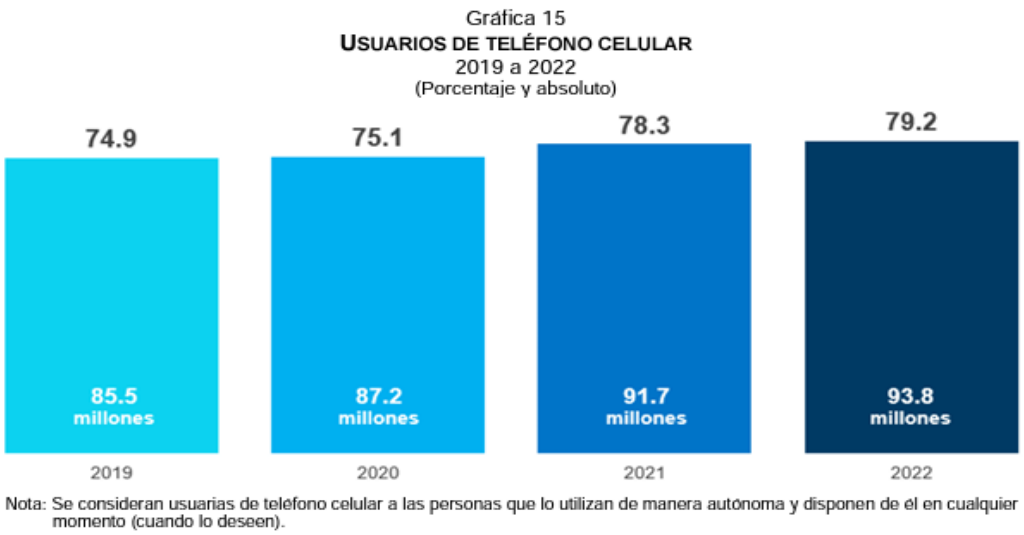
Ilustración 6. Hogares con Internet 2019 a 2022



Fuente: ENDUTIH, 2022, p. 10.

Un 79.2% de la población encuestada, es decir, 93.8 millones de personas, usa un teléfono celular. (ENDUTIH, 2022, p. 12)

Ilustración 7. Usuarios de teléfono celular 2019 a 2022



Fuente: ENDUTIH, 2022, p. 12.

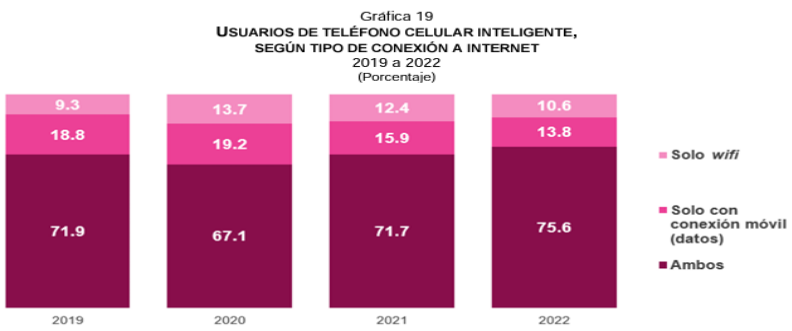
Del total de usuarios de teléfono celular, el 94.6% tiene al alcance a uno inteligente; un 5.2% usa uno común y apenas 0.2%, ambos tipos de teléfono. (ENDUTIH, 2022, p. 13)

Ilustración 8. Usuarios de teléfono celular, según tipo de equipo 2019 a 2022

Fuente: ENDUTIH, 2022, p. 13.

Del general de usuarios de teléfonos inteligentes, un 75%, tiene acceso a internet mediante conexión móvil (datos) y wifi; un 13%, únicamente a través de conexión móvil (datos) y el 10.6% a través de wifi, exclusivamente. (ENDUTIH, 2022, p. 15)

Ilustración 9. Usuarios de teléfono celular inteligente, según tipo de conexión a Internet 2019 a 2022



Fuente: ENDUTIH, 2022, p. 15.

Finalmente, 43.8 millones de personas, es decir, un 37% de la población encuestada se considera usuaria de computadora en México. De ellos, el 88.5% declara como su habilidad principal descargar contenidos de internet. En contraste, solo pueden programar en un lenguaje especializado un 17.4%. (ENDUTIH, 2022, p. 18)

Ilustración 10. Habilidades de los usuarios de computadora 2019 y 2022.

Fuente: ENDUTIH, 2022, p. 18.

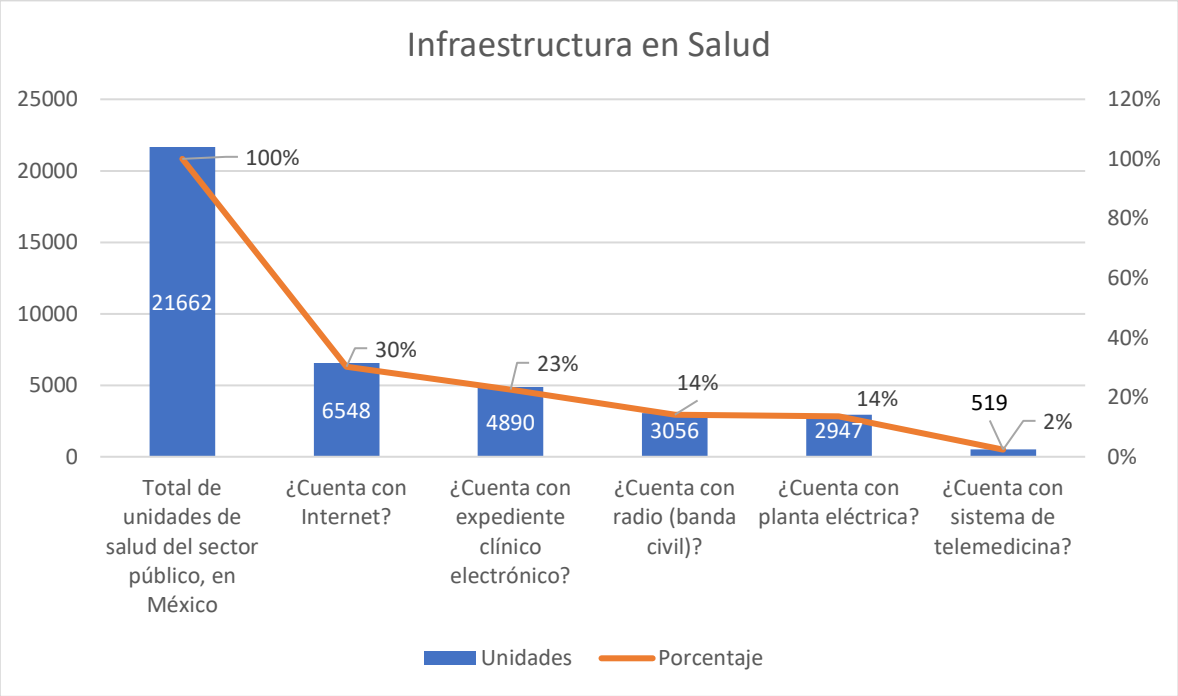
Por otra parte, la Dirección General de Información en Salud de la Secretaría de Salud del Gobierno de México, en su último Informe de Recursos de Salud Sectorial presentado en 2021 (DGIS, 2021), nos presenta los siguientes datos de accesibilidad de las unidades de salud de todos los niveles en el sector público del Sistema Nacional de Salud, en los siguientes rubros:

Tabla 1. Accesibilidad de las unidades de salud del sector público en México, a recursos tecnológicos hasta 2021

Descriptor	Total de unidades de salud del sector público, en México	¿Cuenta con Internet?	¿Cuenta con expediente clínico electrónico?	¿Cuenta con radio (banda civil)?	¿Cuenta con planta eléctrica?	¿Cuenta con sistema de telemedicina?
Unidades	21662	6548	4890	3056	2947	519
Porcentaje	100%	30%	23%	14%	14%	2%

Fuente: Elaboración propia, a partir del Informe de Recursos de Salud Sectorial 2021 de la Dirección General de Información en Salud de la Secretaría de Salud del Gobierno de México.

Ilustración 11. Accesibilidad de las unidades de salud del sector público en México, a recursos tecnológicos hasta 2021.



Fuente: Elaboración propia, a partir del Informe de Recursos de Salud Sectorial 2021 de la Dirección General de Información en Salud de la Secretaría de Salud del Gobierno de México.

Adicional a ello se consultó el Informe de avance y resultados 2022 del Programa Sectorial de Salud 2020-2024 de la Secretaría de Salud, derivado del Plan Nacional de Desarrollo 2019-2024, elaborado por el Gobierno de México y publicado en el Diario Oficial de la Federación el 12 de julio de 2019, que en su eje 2, Política Social, contiene al sub-eje denominado “Salud para toda la población”.

Este último, se desarrolla en el Programa Sectorial Derivado del Plan Nacional de Desarrollo 2019-2024, que en su Objetivo prioritario 3, llamado “Incrementar la capacidad humana y de infraestructura en las instituciones que conforman el Sistema Nacional de Salud, especialmente, en las regiones con alta y muy alta marginación para corresponder a las prioridades de salud bajo un enfoque diferenciado, intercultural y con perspectiva de derechos”, y contiene a la “Estrategia prioritaria 3.4 modernizar el sistema de información y comunicación con el propósito de garantizar información confiable y oportuna que facilite las decisiones en política pública, anticipe las necesidades de la población y favorezca la pertinencia cultural en los servicios brindados en el Sistema

Nacional de Salud" y como acciones puntuales relacionadas las que a continuación se enumeran (Diario Oficial de la Federación, 2020, p. 21):

- 3.4.1 Promover un Centro de Inteligencia en Salud, a partir de la reorganización de áreas para unificar los mecanismos relacionados con registro, conservación y almacenamiento de la información y evitar la fragmentación de la información en los diferentes niveles de atención en el sector.
- 3.4.2 Conformar un Padrón único de Salud, que permita identificar la confición de derechohabiencia de la población y su nivel de accesibilidad a los servicios de protección a la salud bajo el enfoque de redes integradas.
- 3.4.3 Fortalecer los mecanismos para la identificación y registro de datos personales, que consideren las disposiciones de la legislación vigente, que se evite la duplicidad de registros y favorezca el acceso y manejo de la información.
- 3.4.4 Articular los sistemas de información y comunicación existentes en el sector para procurar su unificación, conservación y aprovechamiento, especialmente para la conformación de plataformas y bases de datos confiables.
- 3.4.5 Implementar progresivamente tecnologías de información y comunicación tendientes a garantizar el funcionamiento de los sistemas de información, digitalización de expedientes e interoperabilidad interinstitucional, entre los diferentes niveles de atención en las instituciones que conforman el Sistema Nacional de Salud.

Sin embargo, no se encontraron datos para estos ejes en el Informe de resultados, por lo que inferimos que no se cuenta con acciones para dar cumplimiento al Plan Nacional de Desarrollo 2019-2024 o al Programa Sectorial de Salud 2022-2024.

Por lo que hace a la información de unidades de salud del sector privado, que también son parte del Sistema Nacional de Salud Mexicano, se encontraron dos fuentes.

La primera, el Directorio Estadístico Nacional de Unidades Económicas actualizado al año 2023, generado por el Instituto Nacional de Estadística y Geografía (INEGI), en el que pueden consultarse únicamente los datos de ubicación de las unidades económicas del sector salud, que incluye a consultorios, laboratorios, centros de atención, asilos o centros de planificación familiar, pero que por su naturaleza no nos proporciona datos de interés para esta investigación.

La segunda es un ranking elaborado por la empresa de consultoría Blutitude, la Fundación Mexicana para la Salud, A.C. y la Revista Expansión, titulado "Ranking Los Mejores Hospitales Privados de México, 2022". En este se seleccionaron hospitales privados de diversas bases de datos (no se especifican cuáles) pero que cumplieran con los requisitos de contar con página web y/o que contaran con la certificación del Consejo de Salubridad General, o que estuvieran inscritos en ese proceso de certificación. (Blutitude, Funsalud & Revista Expansión, p. 2)

Luego del análisis de todos los hospitales privados, se seleccionaron a los primeros quinientos que cumplieron con esos criterios, para ser evaluados mediante un instrumento elaborado con base en la metodología de Avedis Donabedian[4], "que combina más de 40 indicadores de una serie de fuentes externas oficiales y públicas distintas, una encuesta anónima de percepción entre médicos especialistas, la percepción de los pacientes así como de las aseguradoras". (Blutitude, Funsalud & Revista Expansión, p. 2).

[4] Avedis Donabedian "Desarrolló el enfoque de estructura, proceso y resultado, que se convirtió en la base para medir y mejorar la calidad de la atención sanitaria. Estas contribuciones están recogidas en *Evaluación de la Calidad de la Atención Médica* (1966), y se esforzó por definir todos los aspectos de la calidad en los sistemas de salud y los modelos propuestos para su medición; se encuentran en más de 100 artículos y 11 libros" (Fundación Avedis Donabedian, sin fecha).

La dimensión que nos interesa, tecnología, que equivale al 20% de la calificación total que se obtiene, se divide en los siguientes dominios (Blutitude, Funsalud & Revista Expansión, p. 6):

- Equipamiento básico, 30%.
- Equipamiento de alta especialidad, 60%.
- Digitalización de los servicios de salud (telemedicina), 2%.
- Expediente clínico electrónico en funcionamiento, 8%.

Como puede observarse, los últimos dos dominios no cuentan con un porcentaje significativo o de interés para obtener el total de la calificación. Igualmente, en el reporte no se especifican otros detalles de interés, como si el expediente clínico electrónico está certificado de acuerdo con lo que establece la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud, de 30 de noviembre de 2011.

De cualquier manera, reproducimos la tabla que contine a los primeros diez hospitales mejor evaluados, según este ranking.

Ilustración 12. Los Mejores Hospitales Privados de México 2022. Ranking General / Nacional.

Blutitude EXPANSIÓN FUNSALUD

LOS MEJORES HOSPITALES PRIVADOS DE MÉXICO 2022

RANKING GENERAL / NACIONAL

Posición 2022	Posición 2021*	Nombre Hospital**	Estado	Municipio/Ciudad***	Región	Puntaje general	Puntajes específicos				
							Talento (20%)	Tecnología (20%)	Procesos (30%)	Resultados (15%)	Percepción (15%)
1	2	Médica Sur	Ciudad de México	Tlalpan	Metropolitana	100.00	89.51	96.11	93.89	96.53	100.00
2	1	Centro Médico ABC Campus Observatorio	Ciudad de México	Álvaro Obregón	Metropolitana	99.36	100.00	90.24	100.00	96.99	77.27
3	5	Centro Médico ABC Campus Santa Fe	Ciudad de México	Cuajimalpa de Morelos	Metropolitana	90.40	81.10	76.74	100.00	99.23	62.92
4	6	Hospital Español	Ciudad de México	Miguel Hidalgo	Metropolitana	80.00	78.29	99.80	66.70	97.85	39.03
5	4	Christus Muguerza Hospital Alta Especialidad	Nuevo León	Monterrey	Norte	79.01	55.40	84.67	79.16	98.69	58.09
6	10	Hospital Zambrano Hellion Tecsalud	Nuevo León	San Pedro Garza García	Norte	75.36	90.17	100.00	48.30	98.71	30.14
7	8	Hospital San José Tecsalud	Nuevo León	Monterrey	Norte	72.33	90.15	86.04	51.74	95.43	26.57
8	16	Centro Médico Dalinde	Ciudad de México	Cuauhtémoc	Metropolitana	66.73	45.15	93.28	68.53	95.25	8.71
9	14	Hospital San Javier Guadalajara	Jalisco	Guadalajara	Occidente	65.86	29.93	97.30	66.93	94.30	22.33
10	28	Centro Médico Puerta de Hierro Andares	Jalisco	Zapopan	Occidente	64.01	34.35	80.52	69.67	98.21	18.23

Fuente: Blutitude, Funsalud & Revista Expansión, 2023.

En otro orden de ideas, es importante mencionar que la Organización de las Naciones Unidas (2022) desarrolla el Índice de Desarrollo de Gobierno Electrónico, que calcula el desarrollo de los servicios público digitales. En él, México ocupa el lugar 61, con 0.73 puntos. La media mundial es 0,5988 y la del continente americano, 06341. (Fundación Telefónica & Taurus, 2021, p. 261)

Finalmente, The Networked Readiness Index 2022 (Dutta & Lanvin, 2022, pp. 28, 31), que mide 131 economías a través de los datos de preparación digital teniendo en cuenta el impacto positivo que los países tengan en la economía, así como en la calidad de vida de sus habitantes, sitúa a México en el lugar sesenta con una puntuación de 51.33, identificándolo como un país de ingreso medio-alto en el continente americano. (Dutta & Lanvin, 2022, p. 33)

El pilar de tecnología, que incluye lo relacionado al acceso, contenido y su desarrollo futuro ocupa el puesto 63; el pilar denominado población, que toma en cuenta a los individuos, negocios y gobierno se encuentra en el lugar 67; en gobernanza, pilar que se compone con los subpilares de confianza, regulación e inclusión baja al 72 y en impacto, que considera a la economía, calidad de vida y la contribución al desarrollo sustentable, sube a la posición 42. (Dutta & Lanvin, 2022, p. 37)

1.1.2 España

El país europeo cuenta con la “Estrategia España 2050. Fundamento y propuestas para una Estrategia Nacional de Largo Plazo”, elaborado por el Ministerio de la Presidencia en 2021 y la “Estrategia de Salud Digital del Sistema Nacional de Salud”, elaborado por la Secretaría General de Salud Digital, Información e Innovación para el Sistema Nacional de Salud de 2 de diciembre de 2021. En este último documento, se prevén líneas para implementar la Estrategia de Salud Digital y como objetivos, los siguientes:

- 5.2.1 Personas y Salud.
- 5.2.2 Procesos de Valor
- 5.2.3 Información interoperable y de calidad

- 5.2.4 Innovación y atención sanitaria en Salud Pública

La estrategia de salud digital, pensada para desarrollarse de 2021 a 2026, cuenta con un proyecto bien definido, aunque no deja de reconocer que cuenta con diversos riesgos, tales como la inexistencia de un modelo de gobernanza y ya implementado, que se presenten resistencias a su adopción; la multiplicidad de estrategias digitales autonómicas; el incumplimiento de plazos de ejecución de proyectos; recursos humanos limitados a nivel nacional y reducidos en las Comunidades autonómicas; la falta de aceptación de los proyectos por parte de los profesionales de la salud y los usuarios del sistema; que las soluciones propuestas sean demasiado complejas para su aplicación[5]; falta de sostenibilidad económica (financiación europea) o tecnológica; que se presenten conflictos de intereses entre las competencias territoriales; la falta de estándares o que éstos no sean heterogéneos; la falta de mecanismos de rendición de cuentas, criterios éticos, de calidad o deontológicos y finalmente, una laxa estrategia de ciberseguridad. (Secretaría General de Salud Digital, Información en Innovación para el Sistema Nacional de Salud, 2021, pp. 52, 55, 56).

Por el contrario, se reconocen como oportunidades la experiencia adquirida de los actores del Sistema Nacional de Salud español para colaborar entre sí, con espacios bien definidos; el acompañamiento e impulso de la Unión Europea y de la Organización Mundial de la Salud para la implementación de estrategias de digitalización en esta materia, así como la disponibilidad de financiación en un periodo suficiente para implementar la estrategia. (Secretaría General de Salud Digital, Información en Innovación para el Sistema Nacional de Salud, 2021, p. 56).

En cuanto a datos de digitalización y acceso tecnologías de la población española, nuevamente tomamos como referencia a The Networked Readiness Index 2022 (Dutta & Lanvin, 2022, pp. 28, 31), que sitúa a España en el lugar

[5] A mayor abundamiento, Calavia (2022), enfatiza que el 57.6% de los profesionales de la salud de atención primaria tiene dificultades para visualizar pruebas y diagnósticos de los pacientes que realice otro especialista, en su turno, así como que las desigualdades de acceso entre servicios son significativas entre comunidades autónomas.

veintiséis con una puntuación de 66.51, identificándolo como un país de ingreso alto en Europa. (Dutta & Lanvin, 2022, p. 32)

En el pilar de tecnología, que describe el acceso, contenido y su desarrollo se encuentra en el lugar el 28; su población, pilar que toma en cuenta a los individuos, negocios y gobierno se encuentra en el lugar 25; en gobernanza que incluye el estudio de los subpilares confianza, regulación e inclusión desciende dos lugares, al 27 y en impacto, que considera a la economía, calidad de vida y la contribución al desarrollo sustentable, sube al 25. (Dutta & Lanvin, 2022, p. 36)

Por su parte y complementando lo anterior la Fundación Telefónica y Taurus (2023, p. 399) ya exponían en su informe “Sociedad Digital en España 2023”, que la proporción de población de este país que tiene al menos habilidades digitales básicas es del 55%, pero que llegará al 70% en 2030 y se espera que alcance el 100% en 2040.

Para mejorar esas competencias digitales y cerrar la brecha digital existente, el Gobierno de España (2021, p. 12) cuenta con el Plan Nacional de Competencias Digitales, que tiene su fundamento en cuatro pilares que desarrollen estas habilidades, a saber, primero en toda la ciudadanía; otro que se enfoca en la población activa (empleados y en paro, para la mejora de la empleabilidad y la calidad del trabajo desarrollado); para especialistas en tecnologías de la información y finalmente, las correspondientes al sector educativo que tienen como objetivo cambiar los paradigmas de enseñanza y aprendizaje entre la población española.

Así, con base en los datos del Informe sobre el último Índice de Economía y Sociedad Digital (DESI), publicado por la Comisión Europea en 2021 (Gobierno de España, 2021, p. 13), puede observarse que España se encuentra en el lugar once, con una puntuación total de 57,5.

De esta suerte, en el Plan citado se nos explica que el 43% de las personas entre 16 y 74 años carecen de competencias digitales básicas; que aumentó el

porcentaje de especialistas en tecnologías de la información hasta un 3.2%, que lo pone muy cerca de la media europea de 3.9%. También incrementó a un 4% la proporción de personas que se graduaron en este ámbito y finalmente, solo un 1.1% de empleados en tecnologías de la información son mujeres. (Gobierno de España, 2021, p. 15.)

Ilustración 13. Capital humano español en materia de tecnologías de la información.

	ESPAÑA			UE
	DESI 2018	DESI 2019	DESI 2020	DESI 2020
	Valor	Valor	Valor	Valor
2a1 Competencias digitales, al menos nivel básico % Personas	55% 2017	55% 2017	57% 2019	58% 2019
2a2 Competencias digitales por encima de nivel básico % Personas	32% 2017	32% 2017	36% 2019	33% 2019
2a3 Conociemientos de software, al menos a nivel básico % Personas	58% 2017	58% 2017	59% 2019	61% 2019
2b1 Especialistas en TIC % Empleo total	3,0% 2016	2,9% 2017	3,2% 2018	3,9% 2018
2b2 Mujeres especialistas en TIC % Empleo femenino	1,0% 2016	1,0% 2017	1,1% 2018	1,4% 2018
2b3 Titulados en TIC % Graduados	4,0% 2015	3,9% 2016	4,0% 2017	3,6% 2017

Fuente: Gobierno de España, 2021, p. 15.

Además, el 45% de la población española carece de competencias en esta materia y un 8% de ella nunca ha usado Internet. (Gobierno de España, 2021, pp. 14, 16).

1.2 Concepto y antecedentes doctrinarios y legales de la portabilidad.

Hoyos (2017, p. 143), considera que no es concebible una sociedad sin personas y personas sin derechos. Sin embargo, se enfrenta una crisis de los fundamentos por la velocidad con la que los avances tecnológicos ocurren, pero que difícilmente pueden ser reguladas con oportunidad por esta misma circunstancia.

Expresa Bobbio (1991, pág. 79), que además de las dificultades jurídico políticas la tutela de los derechos humanos se enfrenta con las inherentes al propio

contenido de estos derechos, pero para su realización son necesarias condiciones objetivas que no dependen de la buena voluntad de quienes los proclaman ni de la buena disposición de quienes presiden los medios para protegerlos. Lo que parece fundamental en una época determinada ya no lo es en otro contexto cultural o temporal. Es la imposibilidad de su realización uno de los mejores argumentos en contra de los derechos humanos, es decir, que se trata de un problema político, no filosófico: o se trata de justificar su existencia, si no de protegerla y garantizar luego, su ejercicio.

A mayor abundamiento señala Cotino (2020, p. 18), que los riesgos e impactos generados por los avances tecnológicos han obligado a evolucionar al "derecho a que le dejen a uno en paz",[6] a uno que desde su construcción doctrinaria y legal garantice la autodeterminación informativa del titular de los datos personales.

Así, "la teoría de la autodeterminación informativa no limita únicamente la recolección y transmisión de los datos, sino que define y protege los derechos del titular de los datos […] y es el origen teórico de la portabilidad de los datos" (Deng, 2021, p. 375).

A este respecto, la portabilidad de datos, como cualquier otro derecho que, para ser garantizado, externalizado o ejecutado requiere de la tecnología, expresada por ejemplo en sistemas interoperables, viene a resignificar la característica de la universalidad de los derechos humanos por su carácter instrumental para a su vez garantizar otros derechos como lo es el de la salud, materia de esta investigación.

Con el desarrollo de la tecnología, cualquier información aun y cuando se trate de una de naturaleza tan delicada como lo es la relativa al estado de salud, puede ser procesada, almacenada y transmitida a terceros que, en un principio, parecería que no tienen injerencia en su tratamiento, por lo que se pone en grave riesgo a su titular, ante la inminente violación a su esfera íntima.

[6] El mismo "*right to be alone*" que formularon Warren y Brandeis en 1890.

Pérez Luño (2012, p. 92), nos recuerda que se ha perfilado una doctrina del Tribunal Constitucional Español con una doble consecuencia en orden al sistema constitucional de los derechos fundamentales; primero un instituto de garantía o derecho instrumental tendente a tutelar el derecho de la intimidad frente a cualquier abuso informático; también el reconocimiento del derecho a la intimidad como uno autónomo frente a la libertad informática, garantizado a través del *habeas data* que, como complementa Troncoso (2003, p. 236) se entiende como "un conjunto de instrumentos procesales -acceso, rectificación y cancelación- que garantiza que la persona dispone de un control sobre sus datos personales y, por tanto, una protección sobre su identidad personal".

El derecho a la portabilidad de datos personales, por tratarse de uno de reciente positivización, encuentra su antecedente en la necesidad de los usuarios de servicios digitales de trasladar su lista de amigos, direcciones de correo electrónico y otro tipo de datos personales que brindan al hacer uso de ellos (Zanfir, 2012, p. 1).

Singapur en 1997 fue pionero de la portabilidad del número telefónico y el método fue rápidamente difundido a Estados Unidos y Japón, permitiendo al usuario mejorar su experiencia y promover la competencia de los operadores y las empresas del mercado […] lo que rápidamente se extendió a otros ámbitos tales como el Internet, herramientas de comunicación, de búsqueda o archivos digitales. (Deng, 2021, pp. 375, 376)

Otro antecedente importante es el "Proyecto de Portabilidad de Datos", cuya creación e impulso por compañías tales Google, Facebook, LinkedIn o Microsoft, entre otras, en 2007, perseguía la finalidad de volver posible este mecanismo (Bozdag, 2018, p. 1). Sin embargo, aunque cuenta con gran relevancia como antecedente, esta investigación está centrada en el análisis del derecho positivizado en las normas de protección de datos personales, por lo no hacemos referencia a la portabilidad de datos comprendida en el artículo 6, del Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de

noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

Además, como antecedente directamente ligado a la importancia que reviste que el derecho a la portabilidad se garantice de forma adecuada, tenemos a la ciencia ciudadana como la interpreta Quinn (2018, p. 1) en el entendido de que reviste gran utilidad que los datos sean portados por su propio titular, teniendo la potestad de transferirlos a diversas instituciones de investigación, lo que ahora es posible lograr por los avances tecnológicos y de una forma diferente a la que el derecho de acceso nos faculta, para no solo transmitirlos, sino reunirlos, agruparlos y estudiarlos de formas distintas a las tradicionales, mediante la interacción de personas con intereses similares, debiendo de cumplir con requisitos tales como la capacidad de registrarlos, de almacenarlos, de acceder a ellos y de que puedan transferirse.

Si bien es cierto que autores como Egan (2019, p. 3) identifican a la portabilidad como un principio que permite disponer de los propios datos personales para compartirlos a otro proveedor de servicios, incentivando la competencia de servicios en línea y que nuevos emerjan, otros autores como Krämer *et al.*, (2020, p. 9) afirman que la portabilidad de datos no producirá mayor o menor competencia e innovación en los mercados digitales por sí misma, más bien dependerá de en qué medida esa innovación sea fomentada. Por su parte, en el Proyecto de Portabilidad de Datos (s.f.) se le considera como una capacidad de las personas de volver a usar sus datos personales en aplicaciones interoperables; y autores que como Ursic (2018, p. 59) la consideran como una regla de la transferencia de datos.

No cabe duda de que se trata de un derecho fundamental reconocido ya en diversas disposiciones legales y que, como indica Cotino (2020, p. 18), debe dársele forma jurídica a la soberanía digital que resulta de los avances tecnológicos, incluyendo en su diseño “las facultades de propiedad o similares

que permitan monetizar[7] a los sujetos su contribución a la economía digital con la materia prima de sus datos personales", ya que estos y su facilidad de tratamiento, "constituyen indefectiblemente poder" (Rebollo, 2020, p. 29).

1.3 Marco legal

1.3.1 Orden jurídico mexicano.

En el Estado Mexicano, la portabilidad se asume como derecho distinto al del ámbito de la protección de los datos personales, en tres materias distintas:

1. Según la Ley Federal de Telecomunicaciones y Radiodifusión de 14 de julio de 2014, la portabilidad es el derecho que tienen los usuarios de conservar el mismo número de teléfono al cambiarse de concesionario o prestador de servicio (artículo 3, fracción XLIV). El derecho consiste en:

    a. Conservar de forma gratuita el número de teléfono celular si se cambia de compañía.
    b. Recibir la orientación de los proveedores para llevar a cabo la portabilidad, que deberá llevarse a cabo a más tardar en 24 horas a partir de la solicitud.
    c. La portabilidad solo puede realizarse en el mismo servicio (de móvil a móvil) y en la misma modalidad, sin que los proveedores puedan inhibir la garantía del derecho con prácticas tales como el bloqueo de las terminales.

2. De acuerdo con la Circular 3/2012 del Banco México, y con el artículo 18 de la Ley para la transparencia y ordenamiento de los servicios

[7] "Admitir la posibilidad de comerciar con nuestros datos personales conlleva también aceptar que sea legítimo intercambiar datos personales por medicamentos, por servicios sanitarios o por un descuento en una póliza de seguro o, incluso para conseguir un trabajo o mantenerlo. Este planteamiento, que sitúa la protección de datos personales en la esfera del derecho de propiedad —los datos personales como una *cuasi* propiedad, como diría Esser, siguiendo tanto a los juristas romanos como a los del *Common Law*—, y que se manifiesta en convertir el consentimiento del interesado en el principio jurídico fundamental, genera una enorme brecha, no sólo social sino de derechos, entre los pobres que comercian con sus datos personales y los ricos que no se ven obligados a compartir sus datos personales. Este planteamiento convierte la privacidad en un lujo y condena a los pobres a no tener privacidad." (Troncoso, 2020, p. 33)

financieros, de 15 de junio de 2007, los usuarios de estos servicios cuentan con el derecho de portabilidad o transferencia de la cuenta de nómina al banco de su preferencia, en la que pueden recibir los depósitos correspondientes de su salario, pensión o prestaciones de carácter laboral (Condusef, s/f).

Este servicio puede ser solicitado en cualquier sucursal del banco de la predilección del usuario. El prestador de servicios financieros no puede solicitar requisitos adicionales a la que establece la Circular 3/2012; no pueden cobrar comisiones por el ejercicio de este derecho, pero sí podrán aplicar los cargos correspondientes al pago de créditos a favor del banco o bien, si se han domiciliado los recurrentes de servicios, créditos o bienes. (Condusef, s/f)

3. En materia de servicios para la administración de fondos para el retiro (Afore) y con fundamento en el Convenio sobre portabilidad de derechos para reconocer la trayectoria laboral de los trabajadores cotizantes, firmado entre el Instituto Mexicano del Seguro Social (IMSS), la Comisión Nacional del Sistema de Ahorro para el Retiro (Consar) y el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) (Consar, 2023), los trabajadores afiliados a cualquiera de estas instituciones cuentan con el derecho de portabilidad que les “permite unificar las cotizaciones de los trabajadores que se desempeñaron tanto en el sector público, como en la iniciativa privada, mejorando el cálculo de pensión ya sea ante el ISSSTE o el IMSS bajo la Ley 73” (Pensionaplus, 2023).

   Está prevista la implementación de un sistema automatizado de portabilidad para agilizar el trámite aproximadamente en septiembre de 2023. (Consar, 2023).

1.3.2 Orden jurídico comunitario y español.

En 2007 fue expedida la Carta de Derechos de los usuarios de la red, un documento no vinculante en el que se establecían derechos fundamentales para los usuarios de internet y deberes para los proveedores de esos sitios. (Somaini, 2018, p. 169)

Igualmente, se ha discutido la conveniencia de que la portabilidad de datos se regule en la legislación de protección al consumidor en lugar de la de protección de datos personales. (Somaini, 2018, p. 169), pero fue negociado de manera exitosa en el seno del Consejo de la Unión Europea cuando fue publicado el 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.

En el Diario Oficial de la Unión Europea de 28 de noviembre de 2018, fue publicado el Reglamento (UE) 2018/19807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea, que en lo que a nosotros interesa, también contempla a la portabilidad entre sus líneas.

Así, desde su objeto que se describe en el artículo uno, contempla a la portabilidad de datos para los usuarios profesionales[8] como una de las características que garantiza la libre circulación de este tipo de datos.

En su artículo seis se mandata que la Comisión Europea debe fomentar y facilitar la elaboración de códigos de conducta y deberá garantizar que sean elaborados

[8] De acuerdo con el artículo 3 del reglamento que se analiza en este apartado, un usuario profesional se distingue del usuario por la finalidad del uso o solicitud que hace del tratamiento de datos. El primero lo realiza para fines relacionados con su actividad comercial, negocio oficio, profesión o función, y en el caso del segundo, el tratamiento no especifica finalidad. Tampoco debemos confundirlo con el usuario o titular de datos personales, que utiliza o solicita un servicio de tratamiento de datos pero de los de carácter personal, es decir, los que pueden hacerle identificado o identificable, y cuya regulación jurídica se encuentra en el Reglamento (UE) 2016/679, del Parlamento Europeo y el 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.

involucrando a todos los interesados tales como las pymes y empresas emergentes, usuarios y proveedores de servicios de la nube del sector que se trate.[9]

Estos, como instrumentos de autorregulación fomentarán una economía de datos competitiva con base a los principios de transparencia e interoperabilidad y de estándares abiertos que incluya aspectos tales como:

a. Mejores prácticas para facilitar el cambio de proveedores de servicios y la portabilidad en un formato de uso común, estructurado, de lectura automática y abierto, esto último si fuera solicitado por el proveedor que reciba los datos.

b. Que los usuarios profesionales cuenten con garantías mínimas de información detallada clara y transparente de forma previa a la firma del contrato de tratamiento de datos para facilitar el cambio de proveedor, de ser necesario.

c. Que los enfoques del régimen de certificación faciliten la comparación de los productos y servicios teniendo en cuenta las normas de orden nacional o internacional aplicables, entre los que pueden incluirse la gestión de calidad, de seguridad de la información, de la continuidad del negocio y medioambiental.
d. Finalmente, los planes de comunicación que, con un enfoque multidisciplinar, sirvan para concientizar a los interesados acerca del código de conducta.

1.3.3 HIPPA

En Estados Unidos se encuentra vigente desde 1996 la Health Insurance Portability and Accountability Act of 1996 (HIPPA), de carácter federal, que

9 Los códigos debían realizarse a más tardar el 29 de noviembre de 2019 y ser aplicados el 29 de mayo de 2020.

establece la necesidad de crear estándares nacionales cuyo objeto consiste en proteger los datos personales de los pacientes de ser transmitidos sin su consentimiento o conocimiento.

A su vez, el Reglamento de la Ley, implementado por el Departamento de Salud y Servicios Humanos del Gobierno de los Estados Unidos, contiene las disposiciones para su implementación. Estas regulaciones, contienen el derecho a la portabilidad de los datos de salud. (Centers for Disease Control and Prevention, 2018).

1.4 Antecedentes doctrinarios y legales del derecho a la portabilidad de los datos personales.

El derecho a la portabilidad es uno que apenas tuvo reconocimiento legal en la segunda mitad de la década pasada. Sin embargo, previo a ello fueron garantizados los derechos de acceso, rectificación, cancelación y oposición, que ya encontraban sustento doctrinario con mayor antigüedad.

Por ejemplo, ya en 1976, Atkinson (p. 145), los identificaba y conceptualizaba:

“uno, cómo se informa al individuo que se tiene información sobre él y cómo se da el tratamiento: la cuestión de la información previa. Esto implicará la consideración de la factibilidad y utilidad de guías para el ciudadano sobre los sistemas de registro que contienen información personal y las reglas bajo las cuales operan e implicará la consideración de otros métodos para notificar a las personas sobre estos asuntos. También debemos tener en cuenta […] el derecho de acceso a la información sobre la fuente y el uso de los datos. La segunda área problemática que debemos examinar es la mejor manera de dar al individuo el derecho a inspeccionar la información que se tiene sobre él y a corregir datos inexactos. Este es el derecho a impugnar y el derecho para presentar objeciones. Esto, sugiero, debe incluir una evaluación de las respectivas ventajas y desventajas, incluido el costo, de permitir la inspección de los registros y la impresión; y un examen de las consideraciones especiales que atañen a la historia clínica ya la información de inteligencia y demás que afecten a la

seguridad del Estado, el orden público y la prevención de delitos. Creo que en este punto debemos tener en cuenta el riesgo para la privacidad que puede resultar del acto mismo de hacer que la información sea accesible. En tercer lugar, debemos prestar atención a lo que se debe hacer para depurar los registros de datos inexactos u obsoletos y asegurarle al individuo que esto se ha hecho."

Braibant (1976, p. 148) concordaba con lo referido: "un ciudadano debe saber lo que otros saben de él para que actúe acorde a ello. Ante todo, un ciudadano debe estar en condiciones de cuestionar esa información, ya sea porque es inexacta, incompleta o desactualizada, o bien porque la persona que posee la información no tenía derecho a recopilarla y a conservarla."

La importancia del reconocimiento de estos derechos, que ahora extendemos al de portabilidad, recae en reestablecer el equilibrio del poder entre el titular de los datos y quien los posee y les da tratamiento, lo que le da sustancia al *habeas data* que se reproduce en las diversas legislaciones de la materia (Braibant, 1976, p. 149)

Braibant (1976, p. 153) considera que el objetivo principal del ejercicio del derecho de acceso a los propios datos personales es el de ejercer, de ser necesario, el de rectificación, teniendo en cuenta dos posibilidades. La primera, que los datos a los que se pretende acceder y, por tanto, posiblemente rectificar, sean hechos incontrovertibles; la segunda, que se trate de opiniones sobre el comportamiento o el carácter: "Para esta categoría de datos, la Ley de los Estados Unidos de 1971 ofrece una solución interesante, que recuerda el principio general consagrado en la Ley Alemana; el sujeto del expediente podrá presentar una breve declaración que contenga sus objeciones, que se adjuntará a su expediente y se comunicará a terceros, a menos que estas objeciones se consideren frívolas e irrelevantes; para que la declaración no sea demasiado larga y, en consecuencia, costosa para el administrador de datos, este último puede solicitar que se limite a cien palabras siempre que ayude al sujeto del archivo a redactarla claramente. Así, el expediente asume una forma de

"adversario" en el sentido procesal del término, lo que da un valor añadido a su contenido y garantiza la protección del ciudadano."

De esta forma, si el titular de los datos quiere ejercer cualquiera de los otros derechos, primero debe saber qué se conoce de él, siendo entonces el derecho de acceso la base para el resto; igualmente, el de rectificación constituye el valor de los datos y una premisa para el de portabilidad, por lo que puede inferirse que el ejercicio de todos ellos está íntimamente relacionado ya que responden a un objetivo único, es decir, a brindar una mayor autonomía del titular de los datos respecto a éstos, y a promover la integración de beneficios sociales y personales (Deng, 2021, p. 382).

Otros antecedentes de importancia podemos encontrarlos en la Ley de la República Digital de Francia, publicada el 7 de octubre de 2016, que garantiza este derecho; el programa Midata que se lanzó en 2011 en el Reino Unido para facilitar a los consumidores el acceso a sus datos personales en un formato electrónico y portable.

A su vez, la Administración de Barack Obama implementó una serie de programas denominados "Mis Datos", en 2010, que se encontraban enfocados a diversos sectores, tales como el de la salud o el bancario. (Ishii, 2018, p. 339)

Finalmente, no olvidamos mencionar que autores como Elfering (2019, p. 20), analizan el derecho de portabilidad de datos desde tres dimensiones: la protección de datos personales, el derecho del consumidor y la ley de competencia económica. Para este trabajo, nos enfocaremos en la primera de ellas, donde se ha fijado el objeto de estudio de esta investigación.

1.4.1 Orden jurídico mexicano.

El derecho de protección de datos personales se encuentra previsto en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917, que también nombra explícitamente a los de acceso, rectificación, cancelación y oposición (ARCO).

En el caso de los titulares de datos personales tratados por responsables denominados como sujetos obligados por pertenecer al orden público en México, además cuentan con el derecho de portabilidad, que solo se garantiza a través de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, pero no a nivel constitucional. Sin embargo, su desarrollo procedimental es similar, en los dos ámbitos que regulan las leyes recién citadas.

A continuación, se desarrollan los derechos en mención, excepto el de portabilidad, que se estudiará en la segunda parte, y el procedimiento que les es común a todos ellos, hasta al derecho materia de esta investigación.

1.4.1.1 Derecho de acceso

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010 únicamente menciona que el titular de los datos personales tiene derecho a acceder a estos y nuevamente, se establece su derecho de conocer el aviso de privacidad al que se condiciona el tratamiento.

A mayor abundamiento, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 21 de diciembre de 2011, establece que el derecho de acceso consiste en que el titular obtenga del responsable, la información relacionada con las condiciones y generalidades del tratamiento de los datos y la obligación de proporcionar acceso a esa información.

El derecho se garantiza cuando el responsable pone a disposición del titular los datos solicitados, en un plazo de quince días, ya sea que este acuda a revisarla a las instalaciones del responsable; o bien, a través de mecanismos tales como copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos o cualquier otra tecnología de la información prevista en el aviso de privacidad y en formatos legibles o comprensibles para el titular. Sin embargo, previo acuerdo

con este último, el responsable podrá proporcionar la información en medio distinto al previsto en el aviso de privacidad.

A su vez, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, se establece que el derecho consiste en acceder a los datos que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades en las que se lleva a cabo su tratamiento. Su finalidad es conocer qué información personal es detentada por terceros y si se encuentra correcta y actualizada, así como los fines de tratamiento.

Los Lineamientos generales de protección de datos personales para el sector público, de 19 de diciembre de 2017, establecen de manera específica que se da por garantizado el derecho de acceso cuando el titular tiene a su disposición de manera gratuita los datos personales previa acreditación de su personalidad o la de su representante, a través de medios de consulta directa en el sitio en que se encuentren o mediante la expedición de copias simples, certificadas, a través de medios magnéticos, ópticos, sonoros, visuales u holográficos o cualquier otra tecnología que el titular determine en un plazo de quince días y previo pago de los derechos correspondientes[10].

Si la solicitud se reitera en un periodo de doce meses tendrá un costo no mayor a tres días de salario mínimo vigente en la Ciudad de México. Se tendrá un plazo no menor a quince días hábiles para su consulta.

1.4.1.2 Derecho de rectificación

Tanto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010, como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, observan que el derecho de rectificación consiste en que la persona titular de los

[10] Hay que aclarar que se trata de días hábiles y derechos por la reproducción de la información, no por consultarla, acceder a ella o conocerla, según lo que se establece en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017.

datos o su representante legal, debidamente acreditado, solicite la corrección de sus datos si estos son inexactos o se encuentran desactualizados.

Se deben indicar las enmiendas a realizar, aportando la documentación que avale la petición y el responsable podrá ofrecer diversos mecanismos para facilitar el ejercicio del derecho, de acuerdo con el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 21 de diciembre de 2011.

Finalmente, en los Lineamientos Generales de Protección de Datos Personales para Sujetos Obligados, de 19 de diciembre de 2017, se considera que la obligación de rectificar los datos personales se dará por cumplida en el momento en el que el responsable notifique al titular, previa acreditación de su personalidad o de la de su representante legal, una constancia mediante la que se acredite la corrección solicitada en el plazo de quince días, debiendo señalar como mínimo los datos del titular tales como su nombre completo, los datos objeto de la rectificación y la fecha en que sucedió.

1.4.1.3 Derecho de cancelación

El titular podrá solicitar la cancelación de sus datos en los archivos, registros, expedientes y sistemas del responsable, a fin de que ya no estén disponibles, según la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017. Además de los requisitos generales para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición o portabilidad, el titular debe señalar las causas que motiven su solicitud.

En los Lineamientos Generales de Protección de Datos Personales para Sujetos Obligados, se considera que la obligación de cancelar los datos personales se dará por cumplida en el momento en el que se notifique al titular o su representante mediante constancia por escrito, los documentos, archivos, registros, expedientes y/o sistemas de tratamiento donde se encuentran los datos personales, el periodo de bloqueo si fuera el caso, las medidas de

seguridad implementadas y las políticas, métodos y técnicas utilizadas para la supresión definitiva de la información, en un plazo de 15 días.

Por lo que hace a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010, se prevé que el derecho de cancelación se puede ejercer en cualquier momento, a lo que proseguirá un periodo de bloqueo y posteriormente de supresión de los datos.

Sin embargo, debe ser advertido al titular que en los diversos casos que prevé la ley, el responsable debe conservarlos para dar cumplimiento a las responsabilidades inherentes a su tratamiento, por lo que el periodo de bloqueo deberé ser equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la ley aplicable en la materia. Por ejemplo, en el caso de los contenidos en el expediente clínico, la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012, prevé la conservación de este documento, en soporte físico o electrónico, durante cinco años.

Al respecto, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010 contempla como excepciones a la obligación de la cancelación de los datos personales si se refieren a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento; si deben ser tratados por disposición legal.

Estos plazos jamás deberán exceder el tiempo que se considere estrictamente necesario para cumplir las finalidades para las que fueron recabados los datos personales, teniendo siempre en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.[11]

[11] Por ejemplo, Troncoso (2006, p. 72) considera que, íntimamente relacionado con el derecho de supresión, se encuentra el principio de calidad de la información que "implica el expurgo y la destrucción de aquellos documentos e informaciones que forman parte de la historia clínica y que ya no son necesarios". Sin embargo, coincidimos con el autor en tanto recomienda seguir criterios de expurgo estrictos y, añadimos, ante cualquier duda, consultar antes de dar de baja información. En el ejemplo que propone, acerca de "que en la historia clínica conste que a una mujer se le dispensó una píldora del día siguiente hace varios años" estableciendo como criterio

1.4.1.4 Derecho de oposición

Con el fin de evitar un daño a su persona o bien, si no desean que su información personal sea utilizada para ciertos fines o por ciertas personas, los titulares de los datos personales podrán ejercer este derecho aclarando al responsable cuáles son las finalidades a las que se opone, para que se garantice el derecho si se comprueba que se cuenta con causa legítima y se halla procedente la solicitud.

En este caso, deberá crearse una base de datos llamada listado de exclusión[12], definida como aquella donde se registra de forma gratuita la negativa del titular al tratamiento de sus datos personales en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 21 de diciembre de 2011.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, contempla dos supuestos en los que el titular puede oponerse al tratamiento de sus datos: si siendo lícito el tratamiento le causa un daño o perjuicio y si sus datos personales son objeto de un tratamiento automatizado que le produzca consecuencias jurídicas no deseadas o afecte de forma significativa sus intereses, derechos o libertades y que mediante estos

---

que ese tipo de información debe ser cancelado antes de cumplir el término forzoso de cinco años, más exactamente, "a partir de la fecha en que la administración de otra píldora no afecta su salud", no coincidimos, sobre todo por las circunstancias en las que el Sistema Nacional de Salud mexicano opera, en que las anotaciones realizadas en expedientes clínicos físicos o electrónicos son poco menos que exactas, y los profesionales de la salud llegan a ser omisos, incluso. Y no es que pugnemos por la conservación de datos inútiles en detrimento del principio de calidad y exactitud, sino que primero tendrían que establecerse mecanismos que coadyuven en el correcto llenado del expediente clínico, para luego, implementar los que nos permitan mantener la información permanentemente actualizada. Por otra parte, consideramos que conservar ese tipo de datos no es inexacto, más bien da cuenta de la historia de la salud del paciente, que se va plasmando a lo largo del tiempo, por lo que valdría incluso reflexionar acerca del plazo de conservación, para que se acerque más al modelo de la Historia Clínica Única Uruguaya, que se emite al nacer la persona y concluye su vida archivística al morir esta.

[12] Los responsables pueden crear listas propias para incluir los datos de quienes manifiesten su oposición al tratamiento de sus datos, para sus productos, de terceras personas y por sector. La inscripción deberá ser gratuita, otorgando constancia de que fue efectuada.
Adicionalmente, está previsto en la Ley Federal de Protección al Consumidor, de 24 de diciembre de 1992, el Registro Público de Consumidores; en la Ley de Protección y Defensa al Usuario de Servicios Financieros, de 9 de marzo de 2018, el de usuarios, aplicables a los titulares de datos de esos sectores especializados, ambas mexicanas.

mecanismos evalúen, analicen o predigan su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento, según su artículo 47.

Además de los requisitos generales para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad, el titular debe señalar las causas que motiven su solicitud.

En los Lineamientos generales de protección de datos personales para el sector público, de 19 de diciembre de 2017, se abunda en la obligación de cesar el tratamiento de los datos personales por parte del responsable, que se dará por cumplida en el momento en el que éste notifique al titular o su representante una constancia en la que señale que ha ocurrido esa acción en el plazo de quince días.

.

1.4.1.5 Procedimiento de ejercicio

Tanto la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010, establece que, para su ejercicio no se requiere de forma previa desplegar alguno de ellos, ni se impide el de otro; pero el responsable cuenta con la obligación de resguardar los datos de tal forma que se permita ejercitar los derechos comentados en los tiempos y formas que la ley dispone y de manera gratuita, ya que únicamente se cobran los gastos de envío o la reproducción de las copias simples o en otros formatos o bien, la certificación de los documentos. El cobro no podrá ser mayor a la recuperación del costo del material correspondiente.

Adicionalmente, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, establece que si el titular proporciona el medio de soporte donde se le entregue la información solicitada no deberá efectuarse cobro alguno y que también será gratuita su reproducción siempre que no exceda de veinte hojas simples; sin embargo, el cobro puede exceptuarse atendiendo las circunstancias socioeconómicas de solicitante.

Tampoco pueden establecerse mecanismos para el ejercicio de derechos ARCO que impliquen un costo para el titular.

El legislador mexicano, ha considerado que puedan ejercer los derechos que en ella se garantizan el titular o su representante legal debidamente acreditados y en cualquier momento.

Para ello, será necesario interponer una solicitud que contenga el nombre del titular y un medio para recibir la respuesta, adjuntando los documentos que acrediten su identidad o su condición de representante, la descripción clara de los datos personales y cualquier elemento que facilite la localización de los datos personales. En el caso de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, se añade a lo anterior el área responsable que trata los datos personales, de tener el dato preciso.

Si fuera el caso además se indicarán las modificaciones a realizarse y se aportará la documentación que sustente la corrección o actualización de los datos. Si la solicitud fuera oscura o irregular, el responsable cuenta con cinco días hábiles para solicitarle al titular que se aclare y este, a su vez, contará con diez días adicionales para aportar los elementos necesarios o se tendrá por no presentada, de acuerdo con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010.

Así, la respuesta deberá recaer en un plazo máximo de veinte días hábiles contados desde la fecha en que recibió la solicitud para comunicarle al interesado si la misma procedió o no. Podrá ser ampliado en igualdad de tiempo, por una sola ocasión. Si la solicitud procedió, el responsable tendrá un máximo de quince días hábiles para llevar a cabo las gestiones que se hubieran solicitado. Este periodo también puede ser ampliado en igualdad de condiciones, una sola vez.

En el ámbito de los particulares, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010 prevé, la

solicitud de protección de derechos, que sólo el titular o el representante debidamente acreditado pueden presentar en caso de:

1. No haber recibido respuesta a la solicitud hecha ante el responsable.
2. Si no se otorga el acceso a los datos o se hace en un formato incomprensible.
3. Si el responsable se niega a efectuar las rectificaciones a los datos solicitados.
4. Si se considera que la información es incompleta o no corresponde a la solicitada.
5. Si el costo por reproducción es excesivo.
6. Si se niega la cancelación de los datos o si se continúa con el tratamiento a pesar de haber procedido la oposición.

En el caso de la negativa a revocar el consentimiento, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010 prevé que puede interponerse una denuncia ante el INAI, quien a través del pleno iniciará un procedimiento de verificación de considerarlo procedente. Esta denuncia de tratamiento indebido deberá contener como mínimo el nombre y domicilio del interesado, la relación de los hechos en los que se basa la denuncia, así como los elementos de prueba y el nombre y domicilio de quien se denuncia.

En general el procedimiento de verificación tiene una duración máxima de 180 días hábiles, que también puede ser ampliado por una sola ocasión y por la misma temporalidad y concluirá con una resolución del INAI donde se determinará el incumplimiento o no de la ley, así como las medidas que adoptará el responsable en cuanto a manejo de datos se refiere. Si hubiera infracciones a la ley, se iniciará el procedimiento de imposición de sanciones para el que se tienen cincuenta días hábiles y es susceptible de ser ampliado en una sola ocasión y por periodo igual, para dictar resolución a este respecto.

En contra de una resolución del INAI, procede un juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa. Para una debida atención se

sugiere a quienes la prestan llevar a cabo un análisis detallado de los procesos internos del negocio o la organización para identificar y reconocer el ciclo de vida de los datos personales tratados.

A la par se deberán reconocer las áreas de la organización involucradas en el tratamiento de datos y clasificar éstos de tal manera que se permita su identificación oportuna ante una solicitud de derechos ARCO y se implementarán controles que faciliten la conservación y resguardo de los archivos físicos o electrónicos de datos personales.

También se propone el diseño y habilitación de un procedimiento interno de gestión de solicitudes de derechos ARCO y establecer al menos una ventanilla de atención, así como un mecanismo interno de atención a quejas o inconformidades en materia de privacidad.

Para los responsables previstos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, el plazo inicial para dar respuesta a las solicitudes de ejercicio de derechos de acceso, rectificación, cancelación, oposición y portabilidad es también de veinte días, pero puede ser ampliado hasta por diez días más si las circunstancias lo ameritan, cuestión que deberá justificarse y serle notificada al titular. Pero si el ejercicio del derecho es procedente, debe hacerse efectivo en un plazo de quince días a partir de que le fue informada la respuesta al titular.

Únicamente se puede restringir el ejercicio de estos derechos por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. Tampoco procederá si el solicitante no es el titular de los datos o el representante no se encuentra acreditado para ello, si no posee los datos solicitados, si el ejercicio de los derechos lesiona los de un tercero, si existe un impedimento legal o la resolución que restrinja el ejercicio de estos derechos; o bien si los derechos, salvo el de acceso, han sido previamente ejercidos.

En caso de que el responsable de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017 sea incompetente, se hará de conocimiento al titular en un plazo de tres días contados a partir de la presentación de la solicitud. Si se declara la inexistencia de los datos, deberá hacerlo mediante una resolución del Comité de Transparencia.

También son causales de incompetencia del responsable en el orden público, que la cancelación u oposición hayan sido realizados, que el sujeto obligado no cuente con las facultades o atribuciones para requerir los datos sobre los que se pretenden ejercer los derechos de mérito; si los datos son necesarios para cumplir con obligaciones legales adquiridas por el titular, si en ejercicio de su atribuciones legales el sujeto obligado lleva a cabo un tratamiento necesario y proporcional para la conservación de la integridad, estabilidad y permanencia del Estado mexicano y si los datos son parte de la información de entidades sujetas a la regulación y supervisión financiera del sujeto obligado en cumplimiento al ejercicio de sus facultades y atribuciones.

Lo anterior no exime al responsable del tratamiento de otorgar una respuesta. Además, los Lineamientos generales de protección de datos personales para el sector público, de 19 de diciembre de 2017, prevén el envío de datos personales o constancias que los contengan por correo certificado o medios electrónicos únicamente si se ha acreditado fehacientemente la personalidad del titular de los datos o su representante, dejando constancia de ese hecho. En ningún momento podrá realizarse si se trata de datos personales de menores de edad o de personas fallecidas.

Ante la falta de respuesta del trámite o bien, la negativa del sujeto obligado para el ejercicio de los derechos, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, establece como medio de garantía secundario para el titular de los datos el recurso de revisión , que podrá ser interpuesto dentro de los quince días siguientes a que fue notificada la respuesta o que haya vencido el plazo sin obtenerla, ante el organismo garante local o la unidad de transparencia.

Esta solicitud debe presentarse dentro de los quince días hábiles siguientes de haber recibido la respuesta del responsable, a través de un escrito libre al INAI o por correo certificado, mediante los formatos que este expide para tales fines o en un futuro, mediante el sistema electrónico a implementarse.

Entre sus requisitos mínimos se incluyen el nombre del titular o su representante, copia de identificación oficial del titular o del representante y en el caso de éste último, documento que acredite su calidad de tal; domicilio para oír y recibir notificaciones; el nombre del responsable ante el que se presentó la solicitud de ejercicio de los derechos ARCO; copia de la solicitud y la respuesta a la misma, que dan origen a la inconformidad; las razones de esta o los actos que la motivan; si se deriva de una falta de respuesta deberá presentarse también la copia del acuse de la solicitud; las pruebas que sustenten el dicho del solicitante y cualquier otro documento que considere prudente presentar. Igualmente se acompañará por copias para el traslado y para el tercero interesado, en su caso. Si faltara alguno de los requisitos se tienen cinco días para subsanarlos, en caso contrario, se tendrá por no presentada.

Antes de dictar resolución de este último recurso, puede buscarse una conciliación entre las partes, procedimiento que no podrá durar más de 25 días entre citaciones y prevenciones. De no conseguirse un arreglo entre las partes, deberá continuarse con la sustanciación del recurso, que deberá ser resuelto en un plazo no mayor de cuarenta días, plazo que puede ampliarse solo una vez, hasta por otros veinte días.

Sin embargo, la conciliación no precederá si se encuentran involucrados menores de edad y se han vulnerado alguno de los derechos garantizados en la Ley General de los Derechos de Niñas, Niños y Adolescentes, de 4 de diciembre de 2014.

El responsable además, podrá manifestar lo que a su derecho convenga ante el Instituto Nacional o bien el de la entidad federativa que corresponda, para que, junto con las pruebas ofrecidas lleve a cabo la valoración correspondiente y se

emita la resolución mediante la cual se confirmará, modificará o revocara la respuesta del responsable o bien, se deseche o sobresea la solicitud por improcedente; en un plazo máximo de cincuenta días hábiles que pueden ser ampliados por igual temporalidad, siempre que se justifique.

En contra de la resolución al recurso de revocación emitida por el organismo garante local, podrá ser interpuesto ante el INAI un recurso de inconformidad en un plazo de quince días a que fuera notificada la resolución y deberá resolver en un plazo no mayor a treinta días contados a partir del día siguiente a la interposición del recurso.

Si no lo hiciere, la resolución impugnada se entenderá por confirmada. Las resoluciones del INAI son vinculantes, definitivas e inatacables para los responsables y los organismos garantes, pero los titulares pueden impugnarlas a través de la interposición del Juicio de amparo.

1.4.2 Orden jurídico comunitario y español.

En Europa, los derechos de acceso, rectificación, supresión, al olvido, de limitación de tratamiento, a no ser objeto de decisiones automatizadas y a la portabilidad, están garantizados en los Reglamentos (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 2018/1725, del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, así como en la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales de 6 de diciembre de 2018[13], que además prevé la existencia de este derecho en servicios de redes sociales y servicios equivalentes.

[13] Su artículo 17 determina que su ejercicio se llevará a cabo de acuerdo con lo que establece el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

A diferencia del caso mexicano, la legislación europea limita su aplicabilidad frente a los responsables que traten datos personales en el ejercicio de sus funciones públicas por lo que no puede ejercerse si la base de la legitimación del tratamiento de los datos es la necesidad de cumplir con una obligación legal aplicable al responsable, o de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.

El Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos, de 08 de noviembre de 2001, prevé como derechos de los interesados los de:

1. No ser objeto de una decisión que la afecte significativamente sobre la base exclusiva de un tratamiento automatizado de datos sin que se tengan en cuenta sus opiniones, excepto si el ordenamiento en el que se prevé el tratamiento cuenta con las medidas adecuadas para la garantía de sus derechos, libertades e intereses legítimos.
2. Obtener en periodos razonables de tiempo, sin demora o gastos excesivos, previa solicitud, la confirmación de que se tratan sus datos personales a que se comuniquen, así como información acerca de su origen, su periodo de conservación y cualquier otra que el responsable deba hacer de conocimiento para garantizar el principio de transparencia en su tratamiento.
3. Recibir una explicación, previa solicitud del motivo subyacente al tratamiento de los datos cuando se apliquen los resultados de ese tratamiento.
4. De oponerse en cualquier momento, con motivo de su situación, al tratamiento de sus datos, con excepción de la existencia de motivos legítimos para ello que predominen a sus intereses, derechos y libertades fundamentales.

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.

5. Obtener de forma gratuita y pronta la rectificación o el borrado de sus datos si el tratamiento se produce en contravención del Convenio.
6. Disponer de un recurso para la protección de sus derechos si no se cumplen obligaciones complementarias tales como la de adopción de medidas que demuestren que el tratamiento se lleva a cabo con arregla al Convenio, no se realice bajo los conceptos de privacidad por diseño y por defecto.
7. De beneficiarse sin importar su nacionalidad o residencia, de la asistencia de una autoridad de control para el ejercicio de sus derechos.

El plazo establecido por los Reglamentos (UE) 2016/679 y 2018/1725, es de un mes para la contestación de solicitudes del interesado, siempre fundadas y motivadas, debiendo facilitarle los mecanismos para solicitar, interponer y obtener la respuesta a su solicitud de forma gratuita en la medida de lo posible. El plazo puede prorrogarse hasta por dos meses siempre que se justifique por la complejidad y el número de solicitudes recibidas.

Ante la falta de respuesta del responsable, es este quien debe informarle al interesado en un plazo no mayor a un mes las causas de su negativa y el derecho que tiene de presentar una reclamación ante el Supervisor Europeo de Protección de Datos y de interponer un recurso judicial.

La única excepción a esta situación es cuando se encuentre establecido en los Reglamentos (UE) 2018/1725 y 2016/679 que la decisión sea necesaria para la celebración o la ejecución de un contrato entre el interesado y el responsable, si se autoriza por la legislación o se base en el consentimiento explícito del interesado.

El Reglamento (UE) 2016/679, también contempla la facultad del responsable de allegarse de la información que considere pertinente para confirmar la identidad del interesado que ejerce sus derechos. Este Reglamento también faculta al responsable del tratamiento para que en caso de que las solicitudes sean infundadas o excesivas por resultar repetitivas, a cobrar una cantidad razonable para cubrir los costes administrativos que le permitan dar respuesta o bien,

puede negarse a atender la solicitud, siempre teniendo éste la carga de probar dicha circunstancia.

En cuanto a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, contempla en su título tercero como derechos de los interesados los de transparencia e información al afectado, acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad. Esta Ley Orgánica reconoce el derecho de los interesados de ejercerlos por sí mismos o a través de su representante legal o voluntario.

En cuanto a las disposiciones de carácter general para su ejercicio, la Ley Orgánica 3/2018 establece las que siguen:

1. El responsable debe informar al interesado acerca de los medios que pone a su disposición para el ejercicio de los derechos, que deberán ser accesibles y no podrán ser denegados solo porque el interesado opte por un medio distinto.
2. El encargado cuenta con la facultar de tramitar, por cuenta del responsable, las solicitudes de ejercicio de los interesados sí así lo hubieren pactado en el acto jurídico que le vincule.
3. El responsable tiene la obligación de demostrar que ha cumplido con la sustanciación del procedimiento de los derechos.
4. Si el régimen de tratamiento, por tratarse de una materia determinada, contara con una legislación especial que resulte aplicable al ejercicio de los derechos enunciados, se estará a lo dispuesto por esa legislación.
5. Los titulares de la patria potestad pueden ejercer en representación de los menores de catorce años estos derechos.
6. Las actuaciones llevadas a cabo por el responsable, para la garantía de estos derechos, serán gratuitas.

1.4.2.1 Derecho de acceso

El 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 los que respecta

al tratamiento de datos personales y a la libre circulación de estos datos, establece que el objetivo de ejercer el derecho de acceso por el interesado será el de conocer si el responsable está tratando o no sus datos personales y de ser así, el acceso a esos datos y además a información como los fines del tratamiento, las categorías, destinatarios y plazo previsto de conservación de esos datos; la existencia del derecho de rectificación, supresión, limitación u oposición del tratamiento; del derecho a presentar una reclamación ante las autoridades de control y, si lo datos no se obtuvieron del interesado, cualquier información disponible sobre el origen.

El Comité Europeo de Protección de Datos (2022, p. 2) afirma que el objetivo principal del derecho de acceso es brindar a los interesados información "suficiente, transparente y fácilmente accesible para verificar la licitud y exactitud del tratamiento", lo que facilitará el ejercicio del resto de derechos, sin que esto constituya una condición para ello, como tampoco lo es el dar a conocer los motivos para su ejercicio.

Además, sostiene la importancia de diferenciarlo de derecho de acceso a la información pública. En cuanto a su alcance, el cuerpo colegiado es contundente es en establecer que se define por la solicitud realizada, sin una interpretación demasiado restrictiva, ya que pueden brindarse datos de terceros que se encuentren involucrados en ciertas acciones, como en el caso de un historial de llamadas telefónicas (Comité Europeo de Protección de Datos, 2022, p. 3).

El Comité es enfático en afirmar (2022, p. 2) que no es facultad del responsable del tratamiento "analizar si el ejercicio del derecho de acceso ayudará a verificar la legalidad del tratamiento o a ejercer otros derechos y debe dar trámite salvo que se intente ejercer por procedimiento distinto al establecido", pero debe facilitar los canales de comunicación adecuados para la recepción de este tipo de solicitudes.

A mayor abundamiento, el Comité (2022, p. 2) identificó como elementos del derecho de acceso:

1. Obtener la confirmación de si los datos corresponden o no al titular que pretende tener acceso, es decir, comprobar su exactitud.
2. Tener acceso a esos datos personales.
3. Conocer y cuestionar las condiciones del tratamiento de los datos.

Así, el Comité Europeo de Protección de Datos (2022, p. 3), recomienda "dosificar" esa información, de resultar abrumante por la cantidad que se daría, por lo que considera adecuado brindarla por capas, enfocada por niveles que deberán ser proporcionados al mismo tiempo si el titular así lo requiere.

El responsable se encuentra obligado a brindar una copia de la información, pero si se requirieran adicionales, puede cobrar una tarifa que cubra los gastos administrativos; si se presenta la solicitud por medios electrónicos, se privilegiará que la respuesta sea a través de estos.

A su vez, el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la UE considera que la finalidad del ejercicio de este derecho es el de conocer y verificar la licitud del tratamiento incluyendo los datos relativos a la salud contenidos en las historias clínicas. En tratándose de una gran cantidad de información, se procurará aquella que es de utilidad conocerse en relación con los fines de su tratamiento.

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, mandata que se seguirá lo establecido en el Reglamento (UE) 2016/679, pudiendo prevenir al interesado para que aporte la información referente a los datos específicos que necesita, y se considerará como cumplida cuando el responsable facilite el acceso al solicitante a través de un sistema remoto, directo y seguro que garantice permanentemente el acceso a toda la información solicitada[14], lo que se comprobará con la comunicación

[14] Para ejemplificar la obligatoriedad de garantizar este derecho de acceso a los propios datos personales, en este caso contenidos en la historia clínica, a través de la Resolución de la Agencia

respectiva donde conste el hecho. Esa solicitud también deberá cumplir con el principio de proporcionalidad, para no recopilar datos de manera excesiva (Comité Europeo de Protección de Datos, 2022, p. 3). El cumplimiento de lo anterior no limitará el derecho que tiene el interesado de solicitar los datos que no se encuentren en este tipo de sistemas.

Las solicitudes se consideran repetitivas cuando concurren más de una en el plazo de seis meses, siempre que no exista causa legítima. Si se elige un medio distinto de respuesta al que se ofrece y este tiene como resultado un coste desproporcionado, la Ley orgánica 3/2018, establece que la solicitud se tendrá por excesiva, y el interesado deberá que asumir los costos de su solicitud, por lo que el responsable solo deberá dar contestación sin dilación.

1.4.2.2 Derecho de rectificación

Los Reglamentos (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 2018/1725, del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, definen al derecho de rectificación como aquél que tiene el interesado de obtener sin dilación indebida del responsable, la corrección de los datos personales inexactos de los que sea

Española de Protección de Datos identificada como R/00679/2021, correspondiente al expediente TD/00205/2021, incoado contra Dentoestetic Centro de Salud y Estética Dental, S.L. por la falta de respuesta a la solicitud de acceso, en su considerando quinto expresa la autoridad de control de forma contundente que "Las normas antes citadas no permiten que pueda obviarse la solicitud como si no se hubiera planteado, dejándola sin la respuesta que obligatoriamente deberán emitir los responsables, aún en el supuesto de que no existan datos del interesado en los ficheros de la entidad o incluso en aquellos supuestos en los que no reuniera los requisitos previstos, en cuyo caso el destinatario de dicha solicitud viene igualmente obligado a requerir la subsanación de las deficiencias observadas o, en su caso, denegar la solicitud motivadamente indicando las causas por las que no procede considerar el derecho de que se trate. Por tanto, la solicitud que se formule obliga al responsable a dar respuesta expresa, en todo caso, empleando para ello cualquier medio que justifique la recepción de la contestación". Por supuesto, la AEPD resolvió contra el responsable del tratamiento, instándole a dar contestación o bien, justificando la insistencia de los datos personales. El mismo criterio se sostiene en la Resolución R/00211/2021, del expediente TD/00033/2021.

titular, pero además llaman a completar aquellos datos que por sus características lo necesiten, incluso mediante declaración adicional.

La Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales, además de lo anterior, establece que el afectado deberá acompañar su solicitud de cualquier documentación que acredite la necesidad de rectificar los datos, ya sea porque resulten inexactos o incompletos en relación con la finalidad para la que fueron recabados.

1.4.2.3 Derecho de supresión (el derecho al olvido, según el Reglamento 2017/679)

Por su parte, el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la UE, considera que el titular cuenta con el derecho de supresión o del olvido de sus datos personales si:

1. Ya no son necesarios para los fines de su recolección.
2. Si los titulares han revocado su consentimiento, particularmente si este fue prestado siendo menor de edad al considerar que por este hecho no se era consciente de las consecuencias de externarlo.

Además de lo anterior, el 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos contempla como causales para su garantía:

1. El tratamiento ilícito de sus datos.
2. Si los datos deben suprimirse para cumplir una obligación legal.
3. Si los datos se obtuvieron para colmar la oferta de un servicio de la sociedad de la información.

Sin embargo, los datos no serán susceptibles de ser suprimidos si:

1. Se está ejerciendo el derecho a la libertad de expresión e información.
2. Para cumplir una obligación legal.
3. Por razones de interés público en el ámbito de la salud pública.
4. Con fines de archivo en interés público.
5. Con fines de investigación científica, histórica o similares estadísticos.
6. Para la formulación, el ejercicio o la defensa de reclamaciones.

Igual se establece como necesario extender este derecho para llegar a convertirse en el de olvido en el entorno virtual, si el responsable hizo pública esa información, indicando la supresión de todo enlace a ellos, copias o réplicas de los datos, siempre que se tomen medidas razonables que se tengan a disposición para realizarlo. [15]

De esta suerte, el derecho al olvido "abre a personas físicas un procedimiento para instar de buscadores en línea la retirada de resultados obtenidos tras búsquedas efectuadas a partir del propio nombre"[16], con el objetivo de evitar el perfilamiento digital y para evitar la conservación de datos que resulten incompatibles con los fines, esto último derivado de que, por el tiempo de su

[15] Antonio Troncoso Reigada, en 2015 (pp. 67, 68), realiza comentarios acerca de la Sentencia del Tribunal Supremo, de 15 de octubre de 2015, dictada a propósito del derecho al olvido digital de los médicos. Argumenta que no se trata de que el motor de búsqueda no sea programado para indexar, sino que el editor de la página web tiene la responsabilidad de dilucidar cuál publicación preserva el interés público y por lo tanto, es susceptible de seguir siendo difundida, haciendo referencia a aquellas noticias contenidas en hemerotecas digitales. Esta decisión, continúa el autor, debe tomarla una persona y no ser automatizada. También destaca la importancia de observar el principio de presunción de inocencia en los procedimientos en los que se vean envueltos profesionales de la salud, toda vez ser vital para el desempeño de su profesión, interpretando incluso más allá de la Sentencia que "se puede defender incluir en las hemerotecas digitales herramientas de no indexación frente a los motores de búsqueda generales en relación con las informaciones sobre imputaciones de médicos que finalmente obtengan una Sentencia absolutoria. […] El problema es que la rápida accesibilidad en Internet de informaciones relativas a imputaciones de negligencia profesional a médicos […] lesiona gravemente el honor y la intimidad de los profesionales. En el caso que la Sentencia sea condenatoria, entiendo que esta información tiene relevancia pública y debe ser publicada en un medio de comunicación. Existe en este caso un interés público".

[16] Dada la naturaleza de la cuestión, concordamos con Cotino (2014, p. 430) en tanto menciona que las soluciones al problema de la ponderación del derecho de datos personales contra las libertades informativas en internet tendrían que ser de carácter global o por lo menos, continental, dado el alcance de las tecnologías de la información, teniendo siempre presente que cualquier información de interés público goza de protección legal.

conservación, se vuelvan no pertinentes o excesivos (García Mexía, 2020, p. 962).

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, prevé la acción del bloqueo de los datos no solo cuando proceda su supresión, sino también en el supuesto de su rectificación, definiéndolo como la identificación y reserva de los datos personales a través de la adopción de medidas técnicas y organizativas que impidan su tratamiento incluyendo que puedan ser visualizados, con la excepción de ser puestos a disposición de autoridades jurisdiccionales, las de protección de datos, el Ministerio Fiscal o las Administraciones Públicas competentes, pero únicamente por el plazo de prescripción de las posibles responsabilidades derivadas del tratamiento, que es de cinco años contados desde el alta de cada proceso asistencial (AEPD, 2022).

Si el bloqueo resulta un esfuerzo desproporcionado, el responsable deberá hacer un copiado seguro de la información constando en un soporte documental que permita acreditar su autenticidad, la fecha de bloqueo y que la información no ha sido manipulada.

Algunas excepciones que para el ejercicio del derecho pueden ser establecidas por las autoridades de control en el ámbito de sus competencias, son:

1. Si con su cancelación se obstaculizan las actuaciones judiciales o administrativas relacionadas con obligaciones fiscales, la actualización de las sanciones administrativas y la investigación y persecución de delitos.
2. Si son necesarios para proteger los intereses jurídicos del titular, para realizar una acción de interés público o para cumplir con una obligación adquirida legalmente por el titular.
3. Si son objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, con la condición de que sea realizado por un profesional de la salud sujeto a un deber de secreto profesional.

Si se hubieren cumplido las finalidades de tratamiento y no existiera algún impedimento legal, debe procederse a la cancelación de los datos, previo bloqueo, para finalmente suprimirlos. El responsable deberá documentar que ha cumplido con los plazos de conservación[17] a los que la ley de la materia específica le obligue.

Al llevar a cabo la cancelación, el responsable debe dar aviso al titular y, además, deberá dar noticia a los terceros a los que haya transmitido los datos, previo a la solicitud recibida, de que esta ha tenido lugar, para que este último proceda a garantizar este derecho.

[17] La AEPD (2020) se pronuncia al respecto de qué sucede con las historias clínicas de un médico que ha fallecido, teniendo como punto principal de su análisis de la "perspectiva del derecho a la protección de datos sobre qué debe hacerse con las historias clínicas propiedad de un facultativo que ha cesado su actividad, y en qué medida le afecta dicha situación a la consultante respecto de aquellas historias clínicas de los pacientes "compartidos" con la clínica que solicita la opinión de la autoridad reguladora. En ese sentido, se parte de la base de tratarse de datos personales de salud, especialmente protegidos por su naturaleza y con lo que concluyen que:

1. "Existe la obligación de conservación de las historias clínicas durante al menos cinco a los desde la última inscripción. (En ese sentido resuelve el TD-00267-2020, por medio del que la hija de un paciente fallecido en una Residencia solicita la supresión los datos de un informe incluido en la historia clínica de su padre, cuestión que le es negada por no haber cumplido con el plazo mínimo de conservación (AEPD, 2022).
2. Hay un deber de cooperación en la creación y mantenimiento de la historia clínica ordenada estructurada de un modo cronológico secuencial que abarque los acontecimientos derivados de la asistencia al paciente.
3. Existe un deber de responsabilidad activa en la gestión y custodia de las historias clínicas informada por el principio de confidencialidad." (AEPD, 2020, p. 7)
   […]
4. Los herederos del facultativo fallecido se convierten en responsables del tratamiento con las obligaciones correspondientes, por lo que "son responsables de la conservación y seguridad de las historias clínica, como mínimo, cinco años contados desde la fecha de alta de cada proceso asistencial" y "[…] será a quienes corresponda atender, y en su caso, satisfacer, el ejercicio de los derechos previstos en la normativa, como el derecho de acceso, cuya materialización dependerá de distintos factores…" (AEPD, 2020, p. 13) tales como que sean los herederos profesionales de la medicina, pues si fuera el caso, la AEPD considera que es el único supuesto en que podrían satisfacerse los derechos de mérito toda vez que su garantía es exclusiva del facultativo fallecido. En caso contrario, sugiere la AEPD acudir con un facultativo, con lo que deberían atender el supuesto de comunicación o cesión de datos o bien, mediante la figura de encargado de tratamiento, de acuerdo con su conveniencia. También sugiere la posibilidad de acudir a los colegios profesionales de médicos donde, al amparo de la relación jurídica, podrían ofrecer determinados servicios que tienen previstos para los facultativos que han cesado su práctica profesional.
5. Por lo que hace a los pacientes que el facultativo fallecido compartiera con la clínica donde prestó sus servicios, será corresponsable solamente si cuentan con un acuerdo o contrato vinculantes en que se determinen las responsabilidades tocantes a las obligaciones en la materia. En caso de no serlo, la Clínica deberá comunicar ese hecho a los herederos del facultativo, así como a los afectados, para que puedan llevar a cabo lo que a su derecho consideren conveniente.

Es importante mencionar que, si se tratara de datos de nacimientos, deberán añadirse los resultados de las pruebas biométricas, médicas o analíticas para determinar el vínculo de filiación entre la madre y su producto. Si se trata de la prestación de servicios consecuencia de violencia ejercida a menores de edad, debe también especificarse la circunstancia. Estos datos no se suprimen o destruyen y en caso de fallecimiento del paciente, sino que se conservan en los archivos definitivos de la Administración que corresponda (AEPD, 2022).

Además de lo descrito en el párrafo anterior, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece que, si la supresión deriva del ejercicio del derecho de oposición, el responsable puede conservar los datos de identificación del titular que ejerció el derecho con el objetivo de evitar el tratamiento a futuro con fines de mercadotecnia directa.

1.4.2.4 Derecho de limitación del tratamiento y a no ser objeto de decisiones automatizadas

El derecho a la limitación del tratamiento se encuentra contemplado en los Reglamentos (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 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, en términos de que el titular tendrá derecho de ejercerlos si:

1. Se impugna la exactitud de los datos personales en el plazo en que se permita verificar que están completos y exactos;
2. El tratamiento es ilícito, pero se ejerce la limitación y la supresión.
3. Si el responsable no requiere conservar los datos pues las finalidades han sido cumplidas, pero el titular necesita que sean conservados para el ejercicio de sus derechos.

4. Si el titular se opone al tratamiento en lo que se verifica si los motivos son legítimos.

Cabe hacer mención que el responsable debe informar acerca de la limitación del tratamiento con anterioridad a que se ejecute, acción que en los ficheros automatizados debe realizarse a través de medios técnicos.

En este derecho también se contempla el de oposición a que los datos personales sean objeto de tratamiento para cumplir con una función realizada en interés público o en el ejercicio de funciones y atribuciones del responsable, pero también de la elaboración de perfiles que pueden derivar en la toma de decisiones automatizadas[18]. Específicamente el Reglamento (UE) 2016/679, otorga el derecho a oponerse en todo momento, si el tratamiento tiene por objeto la mercadotecnia directa.

También, podrá ejercerlo contra del tratamiento con fines de investigación científica, histórica o estadística, por motivos relacionados con su situación particular, con la excepción de si se realiza para dar cumplimiento a una misión realizada por razones de interés público.

Si el tratamiento se encuentra limitado, según la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, debe constar en los sistemas de información del responsable.

1.4.3 Derechos digitales

[18] Hamon *et al* (2022, p. 73) sostienen que "Las técnicas actuales de aprendizaje automático, en particular las basadas en el *deep learning*, no pueden establecer vínculos causales claros entre los datos de entrada y las decisiones finales. Esto representa una limitación para proporcionar razones exactas y legibles para humanos detrás de decisiones específicas, y presenta un serio desafío para la provisión de explicaciones satisfactorias, justas y transparentes. Por lo tanto, la conclusión es que la calidad de las explicaciones podría no considerarse una garantía adecuada para los procesos automatizados de toma de decisiones en virtud del RGPD. En consecuencia, se deben considerar herramientas adicionales para complementar las explicaciones. Estos podrían incluir evaluaciones de impacto algorítmicas, basadas en principios de IA más amplios y nuevos desarrollos técnicos en IA confiable. Esto sugiere que eventualmente los enfoques descritos deberían ser considerados como un todo."

Autores como Deng (2021, p. 384), afirman que la información personal no solo se refleja en el mundo físico, sino también en el virtual, convirtiéndose así en datos de la red. Cotino (2018, p. 2348), a través de documentos tales como la Declaración conjunta sobre libertad de expresión e internet de 2011, asevera que la interrupción del acceso a internet o su negativa, son medidas extremas que en principio no encuentran justificación en razones de orden público o seguridad nacional, salvo que en el segundo supuesto hayan sido ordenadas por la justicia o no existan medidas menos restrictivas, lo que apoya la importancia de positivizar este tipo de derechos adaptados a la realidad del avance tecnológico que se vive.

Incluso enfatiza el autor (2019, p. 44) que, tanto la ética como el derecho deben brindar un mejor acompañamiento a este tipo de avances tecnológicos a través de diversas herramientas, como el cumplimiento normativo por diseño y defecto, así como la adecuación de códigos y políticas de ética y gobernanza que incluyan a los principios de dignidad, protección de derechos, beneficencia y no maleficencia, así como justicia, libertad, autonomía del ser humano, explicabilidad y transparencia para hacer frente a la autonomía artificial, trabajando los profesionales del derecho en conjunto con los creadores de los avances tecnológicos.

Su importancia es tal que autores como Rallo (2020, p. 44) consideran que su posivitización garantiza “la subordinación de la tecnología al individuo” con el fin de preservar su dignidad, no con la intención de coartar el uso de nuevos dispositivos, sino más bien su finalidad ulterior es la de obligar al aparato estatal a garantizar el acceso a esas tecnologías para, a su vez, hacer lo mismo con el libre desarrollo de la personalidad de la población que abarca también al mundo digital como medio de expresión.

Así, además de un sólido marco jurídico, Rebollo (2020, p. 44) cree indispensable que, como complemento a este primer elemento, exista una estructura social consolidada con un carácter globalizado, elementos que, sumados al Estado, podrán hacer en conjunto que las libertades y derechos de los que se habla sean ejercidos por sus destinatarios naturales.

Esto, en opinión de Cotino (2020, p. 88, 90) no sucede en España pues su inserción en la legislación de este país "implica una regulación vacía sin contenido normativo […] claramente insuficiente y que genera gran inseguridad jurídica […] que se quiere enmendar con una *carta de derechos digitales*, de dudoso alcance"; mientras que García (2020, pp. 962-964) asegura que a pesar de la positivización de los derechos digitales, será complicado que entre la población se comprenda a nivel práctico las exigencias del 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.

La Ley Orgánica de 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales contiene un título que a los ojos del derecho positivo mexicano resulta de interés y novedad. Es el concerniente a los derechos de la era digital, por no considerarlos el orden jurídico del país americano en una codificación única y tampoco incluir a todos los que la primera sí contempla. Estos se describen en la Tabla 2.

Tabla 2 - Derechos digitales reconocidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de 06 de diciembre de 2018

Derecho digital	Artículo de la Ley Orgánica 3/2018, que lo prevé	Concepto
Neutralidad de internet	80	Los usuarios tienen derecho a la neutralidad de internet, por lo que los proveedores de esos servicios proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos y económicos.
Acceso universal a internet	81	Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población, en especial para personas con necesidades especiales. Se procurará la superación de la brecha de género y generacional, en el ámbito personal y profesional. Se atenderá la realidad específica de los entornos rurales.

Seguridad digital	82	Los usuarios cuentan con derecho a la seguridad digital de las comunicaciones que transmitan y reciban a través de internet, debiendo informarles los proveedores de servicios de los derechos que tienen.
Educación digital	83	Este derecho se garantiza mediante la plena inserción del alumnado en la sociedad digital y procurando el aprendizaje para que su incursión se realice respetando la dignidad humana y los derechos fundamentales. Para lograrlo, las administraciones educativas deben incluirlo en su currículo y se capacitará al profesorado.
Protección de los menores en internet	84	Quien ejerza la patria potestad o la tutela de los menores de edad procurarán que estos usen de forma equilibrada y responsable los dispositivos digitales y los servicios de la sociedad de la información para la garantía del desarrollo de su personalidad y la preservación de su dignidad y derecho fundamentales. En ese sentido, el uso o difusión de imágenes o información personal de este grupo etario puede ser considerado una intromisión ilegítima, por lo que podría intervenir el Ministerio Fiscal para determinar las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996 de 15 de enero, de Protección Jurídica del Menor.
Derecho de rectificación en internet	85	Se reconoce que cualquier persona tiene derecho a la libertad de expresión en Internet y que los responsables de redes sociales y servicios equivalentes deben adoptar las medidas necesarias que permitan la garantía de este derecho además de publicar que la noticia original no refleja la situación actual del individuo que ejerció el derecho, permaneciendo visible junto con la información original.
Derecho a la actualización de informaciones en medios de comunicación digitales	86	Cualquier persona puede pedir de manera fundada que los medios de comunicación digitales incluyan un aviso de actualización que sea visible, junto a las noticias que le conciernan si la información publicada no refleja su situación actual por haber concurrido circunstancias luego de esa publicación, por lo que sería perjudicada; sobre todo si se trata de suceso de orden penal.
A la intimidad y uso de dispositivos digitales en el ámbito laboral	87	Los trabajadores y empleados públicos tienen derecho a la protección de su intimidad en el uso de dispositivos digitales puestos a disposición por su empleador. Aunque este puede acceder a los contenidos derivados de su uso, solo podrá hacerlo para controlar el cumplimiento de las obligaciones inherentes y de garantizar la integridad de los equipos, así como establecer criterios de uso respetando siempre la intimidad de los empleados, informándoles en todo momento de sus derechos y condiciones de uso.
A la desconexión digital	88	Los trabajadores y empleados públicos tienen derecho a la desconexión digital que les permita garantizar fuera de su horario laboral en respeto a su tiempo de descanso, permisos, vacaciones, intimidad personal y familiar, con énfasis especial a aquellos que presten sus servicios en la modalidad a distancia.
A la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo	89	Los empleadores pueden tratar imágenes obtenidas en sistemas de cámaras o videocámaras para el control de sus trabajadores, en el marco de la legislación que los rige, debiendo informar previo a que suceda a estos últimos y en ningún caso se podrá grabar el sonido o llevara cabo videovigilancia en lugares destinados para el descanso o esparcimiento de los trabajadores.

		Se permite la grabación del sonido siempre que se demuestre la relevancia de los riesgos para la seguridad de las instalaciones, personal o bienes.
A la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral	90	Los empleadores pueden tratar los datos obtenidos a través de sistemas de geolocalización para ejercicio de funciones de control de los trabajadores en el marco de las normas que les rigen, pero siempre informando de manera previa que ocurrirá este tratamiento, así como de las características de los dispositivos y de sus derechos ARCO y de limitación del tratamiento.
Derechos digitales en la negociación colectiva	91	Los convenios colectivos podrán establecer garantías adicionales a los derechos y libertades relacionados con el tratamiento de datos personales de los trabajadores y la preservación de sus derechos digitales en el ámbito laboral.
Protección de datos de los menores en internet	92	Cualquier persona física o jurídica que desarrolle actividades con menores de edad deberán garantizar la protección del interés superior del menor y sus derechos fundamentales en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información. Si se tata de redes sociales, además deberán contar con el consentimiento del menor, su tutor o quien ejerza la patria potestad, según sea el caso.
Al olvido en búsquedas de internet	93	Cualquier persona tiene derecho a que los motores de búsqueda en internet eliminen de las listas de resultados los enlaces publicados que contengan información relativa siempre que sea inexacta, inadecuada, no pertinente, no actualizada o excesiva o bien, por el paso del tiempo deban ser consideradas como tales, atendiendo a los fines que propiciaron su tratamiento, el tiempo transcurrido y la naturaleza de interés público de la información. Igualmente, aunque se ejerza este derecho, no se impide el acceso a la información de mérito a través de criterios de búsqueda distintos.
Al olvido en redes sociales y servicios equivalentes	94	Toda persona tiene derecho a suprimir sus datos personales de redes sociales, mediante su solicitud, ya sea que se hayan proporcionado por sí mismo o a través de terceros, siendo en este último supuesto que además deberán ser inadecuados, inexactos, no pertinentes, no actualizados o excesivos. Se procederá la supresión si las circunstancias personales evidencias la prevalencia de sus derechos por sobre la publicación de los datos, exceptuando lo que hayan sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas. Si se trata de información facilitada durante la minoría de edad de una persona, no importando quien facilitó los datos, bastará con la simple solicitud del titular de los datos para que se proceda sin dilación a su supresión.
Portabilidad en servicios de redes sociales o equivalentes	95	Los usuarios de estas tecnologías tienen derecho a recibir y transmitir los contenidos que hayan proporcionado a los prestadores de esos servicios, o bien, a que estos últimos los transitan directamente a otro prestador designado por el usuario siempre que sea posible técnicamente, pudiendo conservar copia de esa información si resulta necesaria para el cumplimiento de una obligación legal.

Testamento digital	96	Se establecen las condiciones para acceder a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas. En ese sentido, pueden solicitar acceso las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos, así como brindar instrucciones acerca de su utilización, destino o supresión. Sin embargo, no podrán eliminarse o modificarse si el fallecido lo prohibió expresamente o así lo establezca la legislación. El albacea o el designado para ello también puede solicitar el acceso a los contenidos para dar cumplimiento por sí a las instrucciones del fallecido. Si el fallecido fuera un menor de edad, los representantes legales o el Ministerio Fiscal podrán ejercer esta facultad. Si ha fallecido una persona con discapacidad, además de los contemplados en el párrafo anterior pueden ejercer la facultad los que hayan sido designados para el ejercicio de funciones de apoyo. Las personas legitimadas pueden decidir acerca del mantenimiento o eliminación de perfiles personales excepto si el fallecido haya decidido cuestión diferente, que tendrá que ser acatada. Si se solicita la eliminación del perfil, el responsable deberá hacerlo sin dilación. Además, se observarán las normas aplicables de las comunidades autónomas en el ámbito de su aplicación.

Fuente: elaboración propia a partir del texto de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Es importante mencionar el trabajo que está realizando el Congreso Constituyente de la República de Chile, que en su proyecto para la nueva Constitución está incluyendo, a través de la iniciativa “Chile Digital”, la regulación de la inteligencia artificial, así como los derechos a la privacidad, a la protección de datos personales, su rectificación y olvido; a la alfabetización y educación digital; de acceso a los datos públicos con fines de investigación, innovación y desarrollo, así como la obligación de garantizar el acceso universal a las redes digitales de información, así como a los servicios que se otorgan, garantizando su neutralidad. (TRENDTIC, 2022)

En México, el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917, contempla que el Estado cuenta con la obligación de garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, lo que contempla también la banda ancha e Internet, a través de mecanismos de competencia efectiva en la prestación de esos servicios. Lo anterior, a través de

la reforma publicada en el Diario Oficial de la Federación, de fecha 11 de junio de 2013.

También en México, la Ley Federal de Telecomunicaciones y Radiodifusión de 14 de julio 2014, hace énfasis en la garantía de esos derechos para la consideración de quién resulta beneficiario de concesiones de radiodifusión. Igualmente, contempla en su artículo tercero, fracción XLIII, la creación de una Política de inclusión digital universal a través del Poder Ejecutivo Federal, con el objetivo de brindar acceso a este tipo de tecnologías, especialmente a los sectores poblacionales de mayor vulnerabilidad, con el objetivo de cerrar la brecha digital entre los diferentes niveles socioeconómicos. En su capítulo VI, garantiza la neutralidad de las redes, a la que todos los concesionarios deberán someterse.

Es importante mencionar que este Plan no ha sido elaborado por el Gobierno de México, tan es así que en 2021 (inciso III), únicamente fue publicado en el Diario Oficial de la Federación el Acuerdo por el que se da a conocer el Programa de Conectividad en Sitios Públicos 2020-2021 de la Secretaría de Comunicaciones y Transportes, que en lo medular refiere que “promueve el acceso a Internet y a la banda ancha como servicios fundamentales para el bienestar y la inclusión social en el territorio nacional”, pero no se han elaborado ni publicado los lineamientos específicos para llevarlo a cabo.

Finalmente, el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, a través de su Comisión de Datos Personales, actualmente elabora una propuesta denominada “Carta de derechos de la persona digital. Código de buenas prácticas”. (Arévalo, 2022).

Segunda parte. El derecho de portabilidad de los datos personales.

2.1 Orden jurídico mexicano

En México, el derecho a la portabilidad de datos personales no se encuentra garantizado en la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917 como los derechos de acceso rectificación, cancelación y oposición.

Se trata de un derecho oponible exclusivamente de los entes públicos de gobierno, y se positiviza en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017. Las reglas para su ejercicio y garantía se encuentran en los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, emitidos por el Sistema Nacional de Transparencia.

En contraposición, aún no se ha regulado lo respectivo en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, de 5 de julio de 2010.

El Sistema Nacional de Transparencia mexicano (2018) ha identificado como principales diferencias entre los derechos de acceso y de portabilidad, las siguientes:

Tabla 3 - Diferencias entre el derecho de acceso y el de portabilidad.

Derecho de acceso a datos personales	Portabilidad de datos personales
Los datos personales se pueden encontrar en formatos físicos y/o electrónicos.	Los datos personales únicamente se encuentran en ambientes electrónicos o automatizados.
Se ejerce independientemente de la causa de legitimación del tratamiento de los datos personales, es decir, con el consentimiento del titular o por la actualización de alguna causal de excepción para no obtener éste.	Se ejerce cuando el tratamiento de datos personales se base exclusivamente en el consentimiento del titular o en un contrato.
El titular tiene derecho de acceder a todos sus datos personales que obren en los archivos, registros, expedientes y/o sistemas en posesión del responsable.	Sólo son portables aquellos datos personales que el titular proporciona directamente al responsable de forma activa y consciente y los metadatos asociados al tratamiento de éstos.

El derecho de acceso a datos personales no implica transferir los datos personales a otro responsable.	Una de las modalidades de la portabilidad de datos personales se traduce en que el titular puede solicitar la transmisión de sus datos personales, en un formato estructurado y comúnmente utilizado, a un sistema en posesión de otro responsable.
La reproducción de los datos personales puede ser en copias simples, medios electrónicos, sonoros, visuales, holográficos o cualquier otra tecnología.	La reproducción de los datos personales exclusivamente puede realizarse en un formato estructurado y comúnmente utilizado, que implique su reutilización o aprovechamiento de éstos.

Fuente: Sistema Nacional de Transparencia (2018). Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Como puede observarse, el Sistema Nacional de Transparencia identifica como principales diferencias el medio en que se encuentran soportados los datos, pues en el caso del derecho de acceso pueden estarlo en cualquiera, pero para el ejercicio de la portabilidad se requiere que se almacenen en medios electrónicos o automatizados.

Por lo que hace a la legitimación del tratamiento, en el primer caso se ejerce independientemente de esta circunstancia, pero la portabilidad se limita al consentimiento o una relación contractual. Lo mismo sucede a la forma en como el responsable obtuvo los datos, ya que el titular obtiene acceso independientemente de esta circunstancia, pero solo pueden ser objeto de portabilidad los datos que haya proporcionado directamente, así como los metadatos asociados.

Por último, la modalidad en que el derecho puede ser ejercido y la forma en que los datos serán reproducidos para entregarlos, en el ejercicio del derecho de acceso no encuentra limitación, pero en el de portabilidad necesariamente hablamos de un formato electrónico estructurado y comúnmente utilizado que implique la reutilización o aprovechamiento de los datos.

2.1.1 Objeto y alcance

De acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, se trata de un derecho cuyo ejercicio persigue dos objetivos. El primero es que el titular de los datos obtenga

del responsable del tratamiento, una copia de los datos personales que le ha proporcionado en un formato electrónico estructurado y comúnmente utilizado, características que le permitirán seguir usándolos, sin que lo impida el responsable a quien se dieron los datos en primer lugar.[19, 20]

La segunda es que el titular pueda transmitir esos datos personales a otro responsable, siempre que se cumplan a su vez dos condiciones, a saber:

- Que el tratamiento esté basado en el consentimiento del titular o en un contrato.
- Que la información sea conservada en un sistema de tratamiento automatizado y que también sea comúnmente utilizado, siempre y cuando el titular haya proporcionado los datos personales de forma directa, según los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018.

2.1.2 Procedencia del ejercicio del derecho

Según los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, para que el responsable del tratamiento pueda dar garantía a este derecho deben cumplirse los siguientes requisitos de procedencia, en su totalidad.

Así, los datos personales:

[19] En ese apartado es conveniente citar los resultados del estudio realizado por Turner *et al* (2020, p. 17) en el que afirman que tal cual se encuentra formulado el derecho a la portabilidad, no resulta suficientemente claro para que el titular de los datos lo ejerza, pero tampoco para que los responsables del tratamiento transmitan los datos, sobre todo por la falta de información clara disponible para tal efecto, que va desde como ejercerlo hasta los detalles de la transmisión de la información. Puede consultarse completo, en: https://doi.org/10.1177/1461444820934033

[20] Resulta de interés la Guía 1/2022 acerca de los derechos del titular de los datos personales (derecho de acceso) emitida por el European Data Protection Board el 18 de enero de 2022, pues sugieren brindar al interesado la copia de los datos solicitados “como texto escrito, que podría estar en un formato electrónico de uso común, para que el interesado pueda descargarlo. Los datos se pueden proporcionar en una transcripción o en un formulario siempre que toda la información esté incluida y este hecho no cambie o altere el contenido”.

1. Deberán ser tratados por medios automatizados o electrónicos, en un formato estructurado y comúnmente utilizado.
   Sin embargo, la positivización de este derecho en la legislación mexicana, no supone que el responsable del tratamiento cuente con la obligación de dar tratamiento de los datos personales a través de la tecnología indispensable, con el solo propósito de garantizarlo.
2. Se encontrarán en posesión del responsable ante el que pretende ejercerse el derecho.
3. Deberán concernir al titular o bien, a personas físicas que, teniendo un interés jurídico, se encuentren vinculadas con una persona fallecida.
4. Debieron haber sido proporcionados directamente al responsable por su titular, de forma activa y consciente, al realizar un trámite o usar un servicio, ya sea de manera física o mediante un dispositivo tecnológico.

El ejercicio de este derecho no deberá afectar los derechos y libertades de terceros.
Si se desea ejercer este derecho en el contexto de la transmisión de los datos personales a un responsable receptor, siempre que el tratamiento tenga como base la suscripción de un contrato o el consentimiento del titular, además de lo recién enumerado, deberá demostrarse que se cumple con alguna de las siguientes condiciones:

1. Que exista una relación jurídica entre el responsable receptor y el titular de los datos.
2. Que se cumpla un mandato judicial.
3. Si el titular pretende ejercer un derecho.

Además, según los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, al titular de los datos personales deberá proporcionársele en el aviso de privacidad integral, la información relativa a la posibilidad que tiene de ejercer este derecho, incluyendo además la clasificación de los datos que sean técnicamente portables, los formatos estructurados y comúnmente utilizados para ese fin, así como cualquier información relacionada para solicitarlo,

independientemente de que los datos hayan sido obtenidos del titular o a través de un tercero.

Finalmente, es de relevancia mencionar que el ejercicio del derecho a la portabilidad sea ejercido para transmitirlos a un responsable distinto, no cesa o concluye la relación entre el titular y el responsable que en primer lugar ha tratado los datos personales, por lo que "el titular podrá seguir utilizando o beneficiándose del servicio o programa proporcionado por el responsable al que hubiere facilitado los datos personales".

2.1.2.1 Información derivada, inferida, creada o generada por el responsable.

Los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, imponen a los responsables de tratamiento la obligación de procesar, filtrar, extraer, seleccionar y diferenciar la información que es objeto de portabilidad. Por ello, contemplan de manera específica la información que no puede ser objeto de portabilidad:

1. La inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento llevado a cabo por el responsable a los datos personales proporcionados directamente por el titular. En el supuesto se incluyen los datos sometidos a procesos de normalización, recomendación, categorización, creación de perfiles u otros similares o análogos.
2. Los pseudónimos; con la excepción de que se vinculen indubitablemente al titular y, por lo tanto, le identifiquen o le vuelvan identificable, siempre que el titular cuente con datos adicionales que permitan su individualización e identificación.
3. Aquellos datos que hayan sido disociados de tal forma que no puedan asociarse al titular o permitir su identificación, con la excepción de aquellos que puedan asociarse al titular al ser procesados posteriormente.

2.1.3 Reglas específicas para el ejercicio del derecho

Los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, establecen como sujetos obligados a los mismos que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, por ser un derecho que se haya consagrado en ella.

Es decir, que en México se encuentran obligados a garantizar este derecho cualquier autoridad, dependencia, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, tribunales administrativos y fideicomisos y fondos públicos, todos ellos de los órdenes federal, estatal y municipal cuando sea el caso, así como partidos políticos, siempre y cuando cuenten con sistemas en los que se lleve a cabo el tratamiento, que generen los formatos estructurados y comúnmente utilizados que requiere el ejercicio de este derecho.
Es importante mencionar que la legislación en materia de datos personales, se aplica sin perjuicio de la que tenga por objeto integrar los servicios digitales en trámites y servicios públicos, y para compartir o reutilizar plataformas y sistemas de información en cuya posesión se encuentren los tres órdenes de gobierno.

Al ser el derecho a la portabilidad uno de los garantizados por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, para ejercerlo se prevé el mismo procedimiento que para los derechos de acceso, rectificación, cancelación y oposición, descritos en el apartado de antecedentes del derecho que es materia de nuestro estudio.

Sin embargo, los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, imponen como requisitos adicionales para su ejercicio:

a. Que el titular haga la petición de solicitar una copia de sus datos personales en un formato estructurado y comúnmente utilizado o bien, la solicitud de que el responsable transmita sus datos personales al

responsable receptor;

b. Si se encontrara en una situación de emergencia, deberá hacer esa solicitud específica con la finalidad de que sean considerados los plazos establecidos para tal efecto.
c. Por último, en caso de solicitar que los datos sean transmitidos a otro responsable, deberá aportar los datos del receptor, además del documento mediante el que se acredite la relación jurídica entre el titular y el responsable, así como el cumplimiento de una disposición legal o el derecho que pretende ejercer.

Recuérdese que la solicitud no es procedente tratándose de información derivada, inferida, creada o generada por el responsable.

En el caso de que el titular decida ejercer el derecho a través de la modalidad de obtención de la copia de los datos personales, puede acompañar a su solicitud del medio de almacenamiento; si no lo hiciera, el responsable debe proporcionarlo añadiendo el costo razonable que implique este hecho; aclarando que el ejercicio del derecho, por disposición legal es gratuito.

Si es el responsable quien provee del medio físico de almacenamiento, deberá comunicar este hecho en la respuesta dirigida al titular, así como el costo al que asciende, quien deberá efectuar el pago en un plazo similar, remitiendo el comprobante a más tardar el día siguiente de realizado. Sin embargo, también le comunicará que tiene un plazo de tres días contados a partir de la recepción de la notificación para aportar el medio de almacenamiento.

El plazo para dar respuesta a la solicitud del titular es de veinte días hábiles según lo que establece la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017. Sin embargo, de acuerdo con los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, en caso de que el derecho de portabilidad se pretenda ejercer en el contexto de una emergencia, el plazo de respuesta no debe exceder de diez días

contados a partir del día siguiente de la recepción de la solicitud, sin posibilidad de prorrogarlo.

A su vez, se contempla un plazo de siete días hábiles para hacer efectiva su garantía del derecho por parte del responsable, una vez que se determine como procedente la solicitud realizada. Es decir, que ambos términos se reducen a la mitad: de veinte a diez días para responder a la solicitud; y de quince a siete días para hacerlo efectivo.

Cualquiera de los supuestos descritos implica que los datos deben ir cifrados durante su transmisión, y se designará a una persona que vigile el cumplimiento de las condiciones, normas, procedimientos y obligaciones técnicas previstas. La Unidad de Transparencia del responsable receptor deberá notificar a la del transmisor y al titular de los datos la recepción de la información a más tardar al día siguiente de haber recibido a información.

De esta forma, la portabilidad se considera efectiva si el titular o su representante ha recibido copia de sus datos personales en un formato estructurado y comúnmente utilizado que le permita seguir tratándolos o bien, habiéndose notificado que el responsable transmisor ha comunicado al responsable receptor los datos conforme a sus instrucciones.

Si el titular no acudiera a recoger la respuesta a su solicitud, la Unidad de Transparencia tendrá a su disposición la copia de sus datos por sesenta días a partir del siguiente en que fue notificado. Pasado este tiempo, el responsable deberá dar por concluida la atención de la solicitud y procederá a borrar los datos personales portables mediante estrategias seguras que permitan su supresión definitiva, dejando a salvo el derecho del titular para presentarle nuevas solicitudes.

Ante la ausencia de respuesta por parte del responsable o bien, por no estar de acuerdo con ella, el titular, su representante o quien acredite el interés jurídico o legítimo respecto a los datos personales de fallecidos, pueden interponer los medios de impugnación previstos en la Ley General de Protección de Datos

Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, para los derechos de acceso, rectificación, cancelación y oposición y que ya fueron descritos en apartados anteriores.

2.1.4 Normas técnicas y procedimientos para la transmisión de datos personales

Los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, se imponen normas técnicas para la portabilidad de datos personales, a saber:

1. Implementación de mecanismos, medios y procedimientos idóneos para que el titular obtenga sus datos personales, ya sea de forma personal o por vía electrónica o de descarga establecidas en los sitios web o tecnologías establecidas para ese fin.
2. Informar oportunamente al titular acerca de los formatos en que pueden serle entregados o transmitidos los datos, teniendo la posibilidad de elegirlo de existir diversas opciones que cumplan con los requisitos técnicos establecidos para tal efecto.
3. De ser posible, garantizar la interoperabilidad del formato en el que se entreguen o transmitan los datos personales para que su comunicación y reutilización sea uniforme y eficiente.
4. Mantener la capacidad de interoperar de los servicios con otros sistemas como cualidad con la que deberán ser diseñados. También deberán ser adoptados protocolos y estándares que procuren el intercambio de información con independencia del lenguaje de programación o la plataforma en la que hayan sido creados.

Al mismo tiempo, los Lineamientos recién invocados imponen una serie de condiciones técnicas que resultan de cumplimiento obligatorio para los responsables del tratamiento, tanto transmisor como receptor, de forma previa a la transmisión de datos personales en el contexto del ejercicio del derecho a la portabilidad:

1. Adopción de protocolos, herramientas, aplicaciones o servicios para enlazar y comunicar los datos personales.
2. Establecimiento de medidas de seguridad de carácter administrativo, físico y técnico para el ejercicio del derecho a la portabilidad. Los lineamientos enumeran de forma enunciativa a la autenticación de usuarios, conexiones seguras o la transmisión de datos cifrados.
3. Establecimiento de mecanismos de autenticación para el envío y recepción de los datos personales, exclusivos para la garantía de este derecho.
4. Instauración de controles para la obtención de evidencia del envío, recepción e integridad de los datos objeto de portabilidad.
5. Que los sistemas o plataformas electrónicas utilizadas para la transmisión de los datos objeto de portabilidad, cuenten con un registro de las operaciones realizadas con este fin, por ejemplo, las personas autorizadas para transmitir o recibir los datos personales, la fecha y hora del acontecimiento, el resultado de la operación o cualquier otra que dé cuenta del uso de esas tecnologías.

2.2 Orden jurídico comunitario y español

En la Unión Europea, los Reglamentos (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 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, establecen en su exposición de motivos, que el derecho a la portabilidad tiene como objetivo el reforzamiento del control de los datos del interesado, a través de la transmisión de esta información a otro responsable, siempre que su tratamiento se lleve a cabo en un formato estructurado, de uso común, de lectura mecánica e interoperable.

Teniendo en cuenta el ámbito de validez de cada Reglamento, a continuación, se elabora una tabla comparativa que expone la positivización del derecho:

Tabla 4. La regulación del derecho a la portabilidad en la Unión Europea

	Reglamento (UE) 2016/679	**Reglamento (UE) 2018/1725**
Ámbito de aplicación	Se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. También, al tratamiento de datos personales de interesado que residan en la Unión por parte de responsables o encargados no establecidos ahí, siempre que tenga que ver con la oferta de bienes y servicios o el control de su comportamiento.	Se aplica al tratamiento de datos personales por parte de todas las instituciones y organismos de la Unión.
Objetivo del derecho a la portabilidad	Para reforzar el control del interesado sobre sus propios datos, cuando el tratamiento se efectúe por medios automatizados.	Para reforzar el control del interesado sobre sus propios datos, cuando el tratamiento se efectúe por medios automatizados.
Artículo	20	22
Derecho	1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.	1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado.
	2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.	2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, o a responsables del tratamiento distintos de las instituciones y organismos de la Unión, cuando sea técnicamente posible.
Mecanismo de ejercicio	Se entenderá sin perjuicio del ejercicio del derecho al olvido o de supresión. Es decir, que ejercer el de potabilidad, no es sinónimo de que los datos deban suprimirse automáticamente. El derecho de portabilidad no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes	Se entenderá sin perjuicio del ejercicio del derecho de supresión o al olvido. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una función realizada en interés público o en el ejercicio de potestades públicas conferidas al responsable del tratamiento.

	públicos conferidos al responsable del tratamiento.	
Limitaciones en el ejercicio	No afectará negativamente derechos y libertades de otros. No puede ejercerse si el tratamiento tiene una base jurídica distinta del consentimiento o el contrato	No afectará negativamente derechos y libertades de otros. No puede ejercerse si el tratamiento tiene una base jurídica distinta del consentimiento o el contrato
Tratamiento de los datos personales	En un formato estructurado, de uso común de lectura mecánica e interoperable	En un formato estructurado, de uso común de lectura mecánica e interoperable
Procedencia de ejercicio	Si el interesado facilitó los datos personales y: a) - el tratamiento esté basado en el consentimiento dado por el interesado para uno o varios fines específicos. - o el interesado dio su consentimiento explícito para el tratamiento de datos personales de categorías especiales con uno o más de los fines especificados, siempre que la prohibición pueda ser levantada por este. - o el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. y b) el tratamiento se efectúe por medios automatizados.	Si el interesado facilitó los datos personales y: a) - el tratamiento esté basado en el consentimiento dado por el interesado para uno o varios fines específicos. - o el interesado dio su consentimiento explícito para el tratamiento de datos personales de categorías especiales con uno o más de los fines especificados, siempre que la prohibición pueda ser levantada por este. - o el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. y b) el tratamiento se efectúe por medios automatizados.
Obligaciones del responsable	No crea la obligación de adoptar o mantener sistemas d tratamiento que sean técnicamente compatibles. Sin embargo, se les alienta a crear formatos interoperables que permitan la portabilidad de datos.	No crea la obligación de adoptar o mantener sistemas d tratamiento que sean técnicamente compatibles. Sin embargo, se les alienta a crear formatos interoperables que permitan la portabilidad de datos.

Fuente: Elaboración propia a partir de los datos de los Reglamentos (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 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos

A su vez, Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, positiviza este derecho y prevé que su ejercicio deberá hacerse de acuerdo a lo dispuesto en el Reglamento (UE) 2016/679.

2.3 Marco conceptual y naturaleza del derecho a la portabilidad de los datos personales.

Ni la legislación ni la doctrina ofrecen un concepto exacto del derecho de portabilidad de datos personales, más bien describen los requisitos necesarios para su ejercicio y que se refieren en los siguientes apartados. Sin embargo, en 2015, el Supervisor Europeo de Datos Personales lo describió como "permitir que el titular o usuario decida qué pasa con sus datos personales" (Somaini, 2018, p. 172).

Gill & Metzger (2022, p.3), explican el derecho a la portabilidad como un "subgrupo de derechos del derecho de acceso a los datos personales, que especifica las modalidades de este último: particularmente, la portabilidad requiere una copia de los datos que serán transferidos fuera del espacio de control del responsable del tratamiento en un formato estructurado, comúnmente utilizado y de lectura de máquina común que permita ser procesado en un futuro y hacer uso de él. Sin embargo, no necesariamente se considera como modalidad de su ejercicio, poner a disposición de terceros los datos personales; y la mayoría de derechos de portabilidad permiten la modalidad directa, entre responsables del tratamiento, mientras el titular de los datos es quien tiene el derecho de solicitar la portabilidad de esa información."

Chassang *et al* (2018, p. 298), así como Vanberg, A., & Ünver, B. (2017, p. 2), coinciden en que se trata de una parte del derecho fundamental de protección de datos personales, que amplía al de acceso al mundo digital ya que no se trata de mejorar el acceso y accesibilidad a los datos personales al empoderar a su titular, sino que se espera que, al mismo tiempo sea una herramienta de impulso de la economía de datos.

Abundan en este argumento De Hert *et al* (2018, p. 194, 201), al argumentar que este derecho es el reflejo de un valioso trabajo de desarrollo y difusión que, centrado en el usuario, mejorarían su privacidad, así como la posibilidad de disfrutar lo que denominan "riqueza inmaterial" entendida como los datos personales en el entorno de la economía de datos. En consecuencia, la

portabilidad es un elemento imprescindible para consolidar la propiedad de los datos personales en un escenario de fusión, esto es, que el derecho a la portabilidad deberá verse como amalgama de la diversidad de servicios digitales, convirtiéndolos así en segmentos interoperables del internet de las cosas.

De opinión similar es Somaini (2018, pp. 164, 173), quien defiende que el derecho a la portabilidad de datos personales convertirá a los interesados en sujetos activos que, al ejercerlo, reutilizarán sus datos en un entorno que teniéndolos como centro, promueve el intercambio ágil de información y la fácil elección de proveedores de servicios que deberían estar diseñados para satisfacer las necesidades particulares del titular, ya que se ha estudiado su comportamiento para tal efecto. Es decir, que el ejercicio del derecho de portabilidad tiene como objetivo la reutilización de los datos personales, con lo que se equilibra la relación entre el titular y el responsable del tratamiento.

Krämer *et al* (2020, p. 6) afirman que la finalidad de garantizar este derecho es dotar de mayores capacidades de control al titular acerca de sus propios datos personales si es que el tratamiento se lleva a cabo a través de medios automatizado, que les permita reutilizarlo o bien transmitirlo a un responsable distinto, con lo que coinciden autores como Zanfir (2012, p. 1) al señalar que su garantía reduce las dificultades que los titulares de los datos tienen para autodeterminarse.

De la misma opinión es Elfering (2019, p. 7), que agrega que la positivización de este derecho tiene además el objetivo de incentivar la competición como una herramienta para disminuir el bloqueo del consumidor y brindarles, a su vez, mayor control sobre sus datos personales.
A mayor abundamiento, este derecho permitiría a los usuarios de servicios digitales llevar consigo los datos que han ido acumulando de un servicio a otro que se ajuste mejor a sus necesidades (Van der Auwermeulen, 2017, p. 59), por lo que, al ser una herramienta de circulación de la información, se trata de un derecho instrumental al dar estructura al flujo de datos personales a través de la legislación que lo positiviza (Somaini, 2018, p. 174).

En consecuencia, los interesados podrán portar la identidad digital que se ha ido construyendo para un producto o servicio en particular y que se ve como la continuación de la personalidad física del individuo. Esta cuestión, que a la larga deberá ser regulada, es la raíz del derecho a la portabilidad, según Zanfir (2012 p. 3) y Ursic (2018, p. 42) pues su ejercicio tiene como consecuencia natural el libre desarrollo de la personalidad[21,22] en un entorno distinto al tradicional, y cuya expresión inicial ya hemos estudiado en apartados anteriores al referirnos a los derechos digitales garantizados en España, por ejemplo.

De esta suerte, que el derecho a la portabilidad se haya positivizado tiene como objetivo adicional desarrollar confianza en la actividad económica que se lleva a cabo en ambientes digitales para a su vez, incentivar el desarrollo económico, además de que se propiciará la interacción de los usuarios al frenar los monopolios, para así, atraer nuevos usuarios (Van der Auwermeulen (2017, p. 68).
Así, los prestadores de servicio no tendrían otra opción que desarrollar mejores estrategias que ofrezcan una experiencia al usuario basada en la confianza en el servicio que recibe y de cómo se tratan sus datos (Datum Future, 2019, p. 12).

Los responsables también tendrían oportunidades tales como diversificar y mejorar la oferta de servicios y productos, o de incluir también tecnología tal como la Inteligencia Artificial, lo que el consumidor adoptaría con total naturalidad. (Gille *et al,* 2020, pp. 1, 2).

[21] Desarrolla la idea de las autoras citadas Gans (2018, p. 19) en “The Hamilton Project” y va más allá, proponiendo no solo que se porten los datos, sino que se garantice el derecho a la portabilidad de la identidad, lo que haría posible para su titular trasladarse entre plataformas digitales, sin abandonarlas y mitigaría los costos de esta acción. Para ello, deberán permitir la transferencia de, por ejemplo, comunicaciones entre plataformas distintas, indiscriminadamente. Así, serían los desarrolladores quienes asumirían los costos, pero al mismo tiempo, permitiría que se desarrollaran tecnologías que alcanzaran esta finalidad, siendo las redes sociales un excelente campo de desarrollo de esta idea, previo a su exportación para distintos fines. Esto, según el autor, permitiría equilibrar los costos de la implementación con los beneficios potenciales.

[22] No está por demás recordar, en este punto, a Rodatà (1976, p. 140) que insiste en que la persona puede fallar en comprender la magnitud misma del peligro que representa el uso de esos datos por parte de las organizaciones como consecuencia del enorme desequilibrio de poder entre el individuo aislado y las grandes organizaciones de recolección de datos es perfectamente obvio: bajo estas condiciones, es pura ilusión hablar de "control".

Por su parte Lynskey (2020, p. 499) afirma que positivizar este derecho, por una parte, afirmará la autodeterminación informativa del titular o interesado, empoderándolo ante el responsable del tratamiento, con lo que se reducirían los costos de cambio y se promovería la competencia al limitar las barreras de entrada a los mercados digitales. Esto incentivará la creación de nuevos productos y mejorará el flujo de los datos personales.

De forma similar opina Puccinelli (2017, p. 16), pues considera a la portabilidad de los datos personales como un elemento indispensable de la nueva economía digital y del gobierno abierto. Con su positivización en la norma se propicia el intercambio de información en formatos interoperables, sin embargo, este hecho también pone de manifiesto la falta de implementación de diversas medidas como normas técnicas, modalidades y procedimientos que permitan la garantía debida del derecho y la custodia efectiva de los datos personales.

Abona a lo anterior las afirmaciones de Datum Future (2019, p. 2). Esta organización argumenta que los conceptos de control y propiedad de los datos personales no serán del todo comprendidos ni significantes para sus titulares hasta que estos puedan disponer de su información, a través de la portabilidad, de manera segura y ágil. Por lo tanto, el objetivo de la garantía de este derecho es brindar al interesado mayor control sobre su información personal, promoviendo de forma indirecta la interoperabilidad y evitando los monopolios y mercados de datos[23].

[23] Malgieri & Custers (2018, p. 289) analizaron la importancia que podría tener para el interesado contar con el derecho a conocer el valor de sus datos personales, bajo el argumento de que "la mercantilización de las identidades digitales es una realidad emergente en la economía basada en datos y, por otro lado, las personas no parecen ser plenamente conscientes del valor monetario de sus datos personales." Con lo anterior, se vería empoderado para ejercer otro derecho, el de autodeterminación informativa, que le faculta para incluso monetizar sus datos, cuestión que ya sucede, pero de la que difícilmente los titulares obtienen un beneficio. Los autores concluyen que, aunque los modelos de venta que analizaron no brindan "una alternativa viable para aumentar la conciencia y el control de los titulares" además de que no son compatibles con el 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, tampoco proporcionan con claridad el control que se busca. Sin embargo, lo consideran una alternativa interesante para explorar, que se encuentra con obstáculos tales como "elegir un método de fijación de precios, cuestiones relacionadas con el control y el consentimiento y cuestiones relacionadas con la gobernanza y la aplicación; así como los problemas morales tales como la mercantilización de los derechos

No obstante, autores como Florez y Blind (2020, p. 2), así como Lam y Liu (2020, p. 2) piensan que este derecho tendrá efectos ulteriores a los descritos, por ejemplo, el de obligar a las plataformas a implementar soluciones técnicas para el ejercicio del derecho que podría además de generar competencia, el riesgo de que el titular de los datos abandone la plataforma. Otro efecto es que, por el contrario, la plataforma se vuelva confiable para el usuario, tanto el servicio como su proveedor, por lo que permanezca voluntariamente consumiendo el servicio, tal cual afirma Van der Auwermeulen, (2017, p. 60).

Sin embargo, los responsables del tratamiento no deberían considerar esta situación como una amenaza, sino como la oportunidad de innovar y mejorar los productos y servicios ofrecidos y a la vez, incrementar su prestigio y presencia en el mercado[24]; por lo que los servicios y proveedores más transparentes en el tratamiento de los datos, deberían ser los elegidos por usuarios cada día más informados y que ejercen su autodeterminación informativa (Van der Auwermeulen, 2017, p. 60).

humanos inalienables y no negociables y el potencial refuerzo de las disparidades existentes en la sociedad y los problemas cognitivos, como no darse cuenta de la presión de la información proporcionada, no comprender dicha información y el hecho que las personas no pueden cambiar su comportamiento incluso cuando están debidamente informadas.
Nos inclinamos, sobre todo, por el obstáculo moral, en tanto los derechos de autodeterminación informativa, a la privacidad y a la protección de datos personales son una de las expresiones más puras de la dignidad humana al salvaguardar una de las formas de autodeterminación de la persona, por lo que consideramos que sería tanto como vender parte de su dignidad.
Sin embargo, reconocemos que es una situación que debe estudiarse y regularse toda vez que la situación ya sucede. Destacamos entonces, la anonimización de los datos personales en tanto que es justamente ese vínculo con un sujeto, identificado o identificable, de donde obtienen su valor y son susceptibles de ser protegidos por la regulación de la materia.

[24] Al respecto, un estudio realizado por Krämer y Stüdlein (2019, p. 99) presenta un modelo de dos periodos, en el que un responsable de tratamiento es monopolista en el primero, pero en el segundo compite contra un responsable nuevo en el mercado. Sostienen que sin la posibilidad de portar datos se divulgan menos, pero incita a los clientes a proporcionarlos en mayor volumen, lo que conduce a mayores costos. Con la garantía del derecho, el responsable monopólico revelaría más datos y se reforzaría la posición en el mercado del segundo responsable. Sin embargo, consideran que el primero, aunque bajará los costos de sus servicios, los empeorará, toda vez que su variable estratégica es la de reflejar los costos operativos en el precio que pagan los consumidores. El modelo muestra algunas consecuencias no deseadas de este derecho, como la disminución de la competitividad del responsable transmisor, y que el derecho a la portabilidad reducirá la cantidad de datos recopilados que se determinarían por variables como el precio y el nivel de divulgación, revelando más información del usuario.

Quinn (2018, p. 6), a su vez, considera trascendental para el ejercicio del derecho dos elementos. El primero, que existe el derecho a recibir información en un formato legible por máquina y el segundo, que se otorga el derecho al interesado para solicitar la transferencia directa de sus datos personales a un responsable distinto de con quien mantiene la relación originaria, por considerarla más conveniente.

El derecho a la portabilidad se reconoce como consecuencia de que las empresas y plataformas se vuelven cada vez más poderosos por el crecimiento de los silos de datos (Kuebler-Wachendorff *et al*, 2021, p. 265) que resultan de gran utilidad ya que permiten el acceso a una gran cantidad de información, potenciando su utilidad desde el punto de vista económico (Krämer *et al*, 2020, p 9). Con ello, se logra fortalecer la soberanía de los interesados y que en ejercicio de su autodeterminación informativa participen en la economía de datos al decidir en qué condiciones proporciona su información personal.

La garantía del derecho de portabilidad resultará útil para evitar la retención de los datos personales, siempre que el interesado cuente con el conocimiento para ejercer este derecho (Comisión Europea, 2017, p. 1).

Lenard, (2020, p. 1), Lam y Liu (2020, p. 2), así como Van de Auwermeulen (2017, p. 2), opinan que este derecho facilita la multiplicación de la competencia[25] al diversificar a los sujetos que ofrecen productos y servicios similares, pero también aumenta el valor de los datos al provocar que se brinden más por la facilidad de replicarlos, con lo que coincide la Autoridad de Protección de Datos de Singapur (2019, p. 3). Sin embargo, esta situación pone a los responsables de tratamiento en desventaja, pues la garantía del derecho permite a los interesados cambiar de servicios tanto como prefieran, lo que deprecia el

[25] Engels (2016, sin página) publicó un estudio acerca de los efectos de la portabilidad de datos en la competencia de las plataformas en línea. En él, encuentra que los mercados tienen un riesgo alto de abuso de poder y que este derecho debe interpretarse de forma matizada para evitar efectos adversos sobre la competencia y la innovación, por la exigencia de que los datos sean portátiles en un formato estructurado de uso común. El autor afirma que la positivización del derecho impone cargas inequitativas y excesivas a las pequeñas empresas, al propiciar el uso de una sola tecnología durante un periodo de tiempo relativamente prolongado.

valor de los datos *per se* ya que dejan de pertenecer en exclusiva a un solo responsable.

Tanto Deng (2021, p. 385) como Elfering (2019, p. 27) consideran que debe discutirse acerca de la naturaleza del derecho de portabilidad, para determinar si pertenece como derecho de datos a la categoría de derechos de la personalidad, o bien, a la de derechos de la propiedad. A su vez, Ishii (2018, p. 350), argumenta que, si la portabilidad de datos encuentra su fundamento en la protección de datos, el derecho debe estar estructurado con el titular de los datos como su epicentro para brindarle autodeterminación, y limitando su alcance a los datos personales.

Autores como Somaini (2018, p. 171), Bistolfi & Scudiero (2016, p. 607) afirman que la portabilidad de datos consiste, esencialmente, en la facultad de los individuos de volver a usar sus datos a través de aplicaciones interoperables, con la finalidad de que pueda expresar libremente su personalidad y disfrutar su derecho a la autodeterminación informativa, a través de mecanismos que le permitan transferir por sí mismo o a través de terceros su información personal. Es decir, que la importancia del derecho está en que el titular o usuario de los datos tenga control efectivo de su información.

Vanberg, A. (2018, sin página) y Datum Future (2019, p. 5) identifican dos tipos de portabilidad. La primera, bilateral, en la que los datos se comunican directamente de un responsable a otro. La segunda, denominada multilateral, en la que los interesados pueden transmitir los datos a varios intermediarios o servicios similares que fueron creados específicamente para facilitar, en nombre del usuario, su transferencia a otros responsables que ofrecen servicios similares, que pueden ser consolidados o combinados.

Elfering (2019, p. 20), entiende a este derecho como uno que comprende a su vez, dos distintos: el de recibir y transferir datos personales, o lo que denomina portabilidad indirecta; y el derecho de transmitir esta información de un responsable a otro, o la portabilidad directa.

A su vez, la portabilidad indirecta también contiene otros dos derechos: le derecho de recibir sus datos personales y el de transmitirlos a otro responsable, sin que el responsable que tenía primero los datos obstaculice esta acción (Elfering, 2019, p. 20). Por otra parte, De Hert *et al* (2018, p. 197) y Somaini (2018, p. 165), consideran que el derecho a la portabilidad se compone a su vez, de tres derechos: el primero, el que tiene el titular de los datos de recibir sin obstáculos sus datos personales; el segundo, a transmitirlos a otro responsable del tratamiento y finalmente, el que tiene a que sus datos se transmitan directamente entre controladores, es decir, sin mediar su intervención, siempre que sea técnicamente realizable.[26]

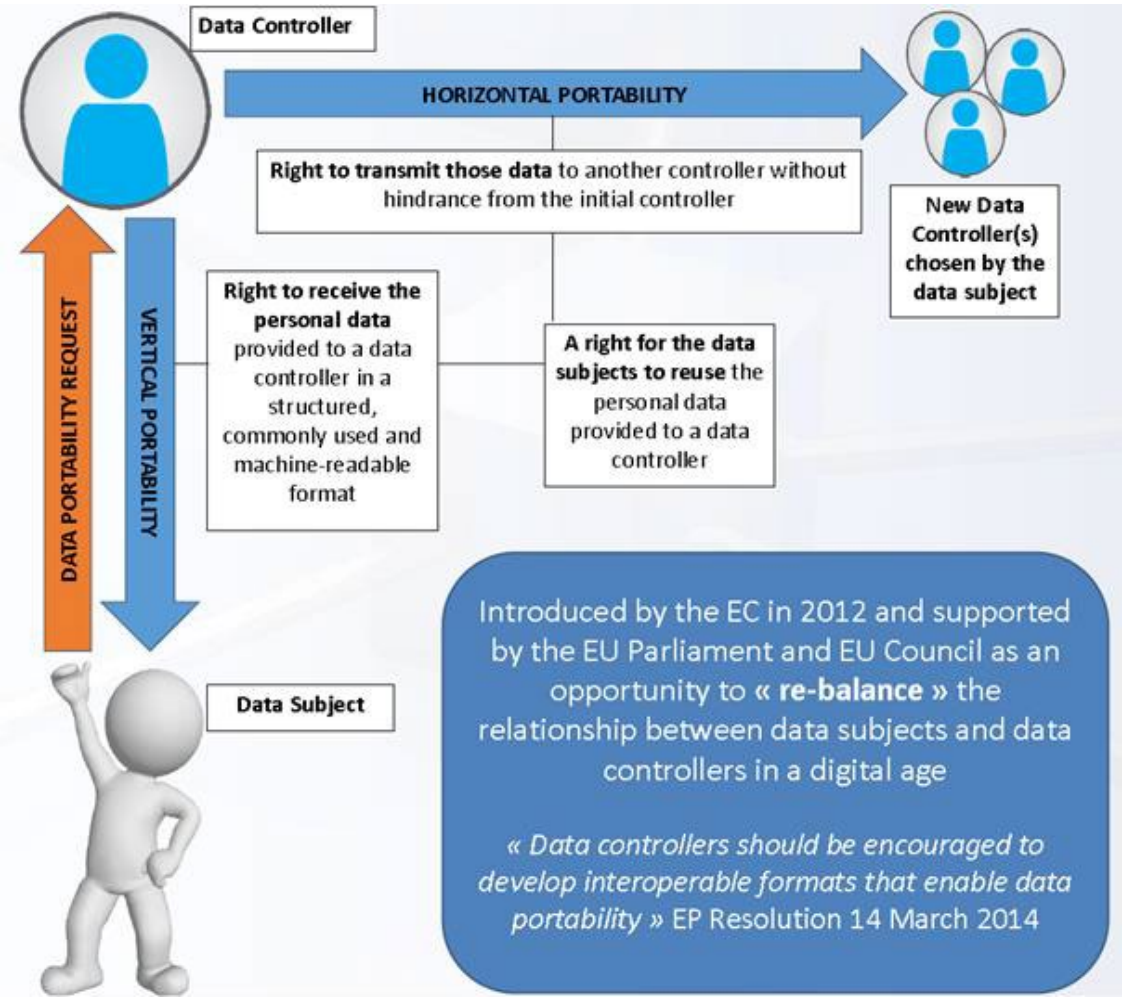
No obstante, los criterios descritos, concordamos con la teoría que exponen Chassang *et al* (2018, p. 298), quienes conciben al derecho a la portabilidad de datos personales como uno que se puede ejercer de forma vertical u horizontal, dependiendo de la preferencia del interesado. Es decir que, si solicita que sus datos se transmitan de responsable a un segundo responsable, nos encontramos ante la portabilidad horizontal. Si, por el contrario, solicita que la información le sea entregada, será portabilidad vertical.

Como resulta notorio, el criterio de los autores toma como eje rector a los responsables del tratamiento de los datos, pues en el primero de los casos los equipara en ese nivel de control que ejercen sobre la información, por lo que considera que se encuentran en una relación equitativa de poder con respecto al tratamiento de la información.

En cambio, la relación vertical se empodera el titular de los datos al recibir, en el formato ya descrito, su información personal, para transmitirla o reutilizarla de acuerdo con sus necesidades y sin mediar intervención de un tercero, como explica en el siguiente esquema.

[26] Para Somaini (2018, p. 165), la verdadera innovación consiste en la posibilidad de que exista una transferencia directa entre responsables del tratamiento, elegidos por el titular o usuario, siempre que sea técnicamente posible realizarlo.

Ilustración 14 - Descripción general del derecho de portabilidad de datos personales en el 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.



Fuente: Chassang et al (2018, p. 299).

Este último punto se encuentra relacionado con lo que implica el ejercicio del derecho. En el caso del de acceso, no necesariamente tendrá como finalidad transferir la información obtenida, acciones que no se encuentran restringidas más que por las limitaciones que la legislación establezca (Chassang *et al*, 2018, p. 300); mientras que el de portabilidad tiene como característica intrínseca su retransmisión y reaprovechamiento, de forma vertical y horizontal y para las finalidades que ya han sido explicadas, encontrando ambos además de otras

causas, límites en su ejercicio en el respeto a los derechos y libertades de terceros.

Es más, el Centre for Information Policy Leadership (CIPL, 2017, p. 1), considera hasta la emisión de su informe, que se trata de un nuevo derecho "sin historial significativo de aplicación práctica e implementación por parte de la industria […] y que no es obvio que […] tenga un valor añadido en respeto de los datos o datos personales".

La AEPD (2017, p. 22) considera que la portabilidad de datos es un complemento del derecho de acceso y que este actuaría como límite máximo al que puede referirse el primero: mientras el de acceso se refiere a la totalidad de los datos objeto de tratamiento sin importar la legitimación de esta acción, el de portabilidad únicamente procede si el interesado ha manifestado su consentimiento al tratamiento de los datos personales o existe una relación contractual, y ahí es donde se encuentra la limitación del espectro de datos que pueden ser objeto de portabilidad.

La federación Bancaria Europea (2017, p. 6) recomienda diferenciar el alcance del derecho a la portabilidad frente al de acceso, siendo más limitado el primero en cuanto a la cantidad de datos personales a obtener se refiere.

De acuerdo con el Grupo de Trabajo del Artículo 29 (2017, p. 5), este resulta crucial pues además de coadyuvar con su capacitación y participación lo que evitará la retención, el derecho que nos ocupa se formuló con el objetivo de innovar para llevar a cabo intercambios de datos de forma segura y eficiente que permitirá el enriquecimiento de los servicios y experiencias de los titulares que son sus consumidores.

Se trata de una herramienta que, entre otros objetivos, persigue el respaldo de la libre circulación de los datos personales en la Unión Europea, suscitando una mayor competencia entre los responsables del tratamiento y facilitando el intercambio de información entre estos lo que, a su vez, originará el desarrollo de nuevos servicios para consolidar un mercado único digital (Grupo de Trabajo el Artículo 29, 2017, p. 3). Si bien es cierto que no se regula la competencia,

también lo es que incidirá en ella por las características del ejercicio de este derecho.

Tanto el Grupo de Trabajo del Artículo 29 (2017, p. 3) como la AEPD (2017, p. 22), reconocen como su propósito que el titular de los datos cuente con más control acerca de los datos personales que le conciernen y su manejo responsable, en lo que consideramos se trata de fortalecer al derecho que tiene de autodeterminación informativa, al involucrarlo directamente en la tenencia y transmisibilidad de su información a otro responsable, en los términos que mejor le convengan en entornos informáticos.[27]

Sin embargo, el Grupo de Trabajo del Artículo 29 (2017) reconoce algunos elementos básicos del derecho, partiendo de la definición que ofrece el 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos y que a la letra dice “el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado [...]”.

Así, como el primero de ellos está el de recibir un subconjunto de datos personales que le conciernan, así como a almacenarlos para un uso posterior, que puede o no implicar su transmisión a un responsable de tratamiento distinto.

En ese sentido, el Grupo de Trabajo del Artículo 29 (2017, p. 5) lo comprende como un derecho complementario al de acceso, que además de conocer la información le permitirá al titular disponer de ella y gestionarla sin depender de

[27] Scheibner *et al* (2021, p. 56), hacen un análisis muy interesante acerca del importante papel que juegan los derechos de los pacientes para la gobernanza de los expedientes clínicos electrónicos de carácter nacional. Son enfáticos en que este tipo de herramientas deben ser realizados alrededor de la ponderación de los límites de los derechos de los pacientes a la luz de los principios bioéticos de Beauchamp y Childress, que son los que usan para su estudio, con un marco jurídico lo suficientemente consolidado pero flexible que permita a sus sujetos obligados reaccionar para adaptarse a la nueva realidad tecnológica.

una persona ajena y de la manera en que le sea más conveniente, lo que asumimos como una de las expresiones del derecho de autodeterminación informativa.

Otro de los elementos es el derecho que tiene el titular de, si así lo desea, transmitir sus datos a otro responsable de tratamiento, a través del primer responsable o bien, a obtenerlos y luego que el propio titular realice tal acción. De esta forma, podemos observar que no se establece un derecho general a la portabilidad, sino que deberá cumplirse alguna de las circunstancias descritas como supuestos de procedencia, por lo que los responsables no cuentan con la obligación de ofrecer la portabilidad (Grupo de Trabajo del Artículo 29, 2017, p. 10).

Además, según lo considera el Grupo de Trabajo del Artículo 29 (2017, p. 9), el responsable deberá satisfacer la solicitud del titular a cabalidad, por lo que este puede inconformarse de no encontrarse conforme con la forma en que le fue garantizado el derecho.

Quinn (2018, p. 16) reconoce importantes diferencias y limitaciones a este derecho. En el primer caso, se diferencia del de acceso porque mediante el de portabilidad, además de proporcionarse información inteligible, deberá ser suministrada en un formato interoperable, más no compatible por las dificultades que ello implica. Van der Auwermeulen (2017, p. 60), por su parte, realiza importantes acotaciones acerca de las desventajas que supone su positivización y garantía, entre las que menciona que sería perjudicial para la privacidad dado el poco control que pueden ejercer los usuarios sobre sus datos como consecuencia de la opacidad reinante en el proceso de portabilidad, así como su desconocimiento acerca del ejercicio de su derecho a la autodeterminación informativa y la protección de datos personales, exponiéndolo a riesgos como el fraude de identidad. Además, considera al riesgo de violentar la propiedad intelectual de los responsables del tratamiento ya que no se ha identificado en la legislación de forma precisa, cuál información es sujeta de portabilidad de la que no, teniendo un mayor problema aquellas compañías cuyos servicios se basan enteramente o en su mayoría en el tratamiento de datos personales.

A mayor abundamiento, Geiregat (2022, p. 514, 515) argumenta que la regulación de la propiedad intelectual impide la garantía del derecho a la portabilidad, ya que operacionalizarlo puede significar la violación de la legislación en esta materia. En consecuencia, no se impedirá el monopolio del mercado, lo que es contrario al objetivo de la positivización de este derecho.

Datum Future (2019, p. 5) identifica a su vez algunas barreras para su ejercicio, tales como que no existe una obligación clara de recibir datos mediante estos mecanismos, lo que podría generarles importantes gastos para implementar la tecnología que les permita leer la información portada; también que los usuarios se resisten al ejercicio de su derecho sobre todo por ignorancia, idea con la que coinciden con Van der Auwermeulen (2017, p. 57) y Zanfir (2012, p. 2) acerca de lo importante que es la confianza en el proveedor de servicios y los que ofrece, así como la transparencia con la que se tratan los datos personales.

Para fortalecer este derecho, que de entrada autores como Ursic (2018, p. 42) consideran endeble desde su origen normativo, se propone su ejercicio de cuatro formas: estableciendo control sobre las transferencias de datos personales; permitiendo el uso y reutilización de los datos personales; aprobando un mejor entendimiento de los flujos de datos y finalmente, que se facilite la equidad y se fomente el libre desarrollo de la personalidad, incrementando así el ejercicio del derecho a la transparencia en el tratamiento de los datos, como elemento complementario.

En relación a lo señalado, Lynskey (2020, p. 506) identifica que el fortalecimiento de los protocolos de seguridad de los datos personales es el mayor de los desafíos para garantizar el ejercicio de este derecho, habilitando, por ejemplo, controladores programados para identificar dudas razonables de la identidad de quien quiera ejercer el derecho, con el objetivo de confirmarla. Además, considera importante la realización de una evaluación de impacto en la que deberán identificarse estas áreas de oportunidad.

Por lo anterior, autores como Zanfir (2012, p. 3) argumentan que, si bien el objetivo principal el derecho a la portabilidad es el libre desarrollo de la personalidad, el medio idóneo para lograrlo será a través de procesos técnicos directamente relacionados a la protección de los datos personales que, al mismo tiempo, garanticen que los responsables del tratamiento compitan equitativamente entre sí. De forma similar argumentan (Krämer *et al.*, 2020, p. 10) en tanto consideran la portabilidad continuada como una regla que de manera proporcional habilite a los titulares de los datos la transferencia de sus datos personales y no personales en tiempo real.

Engels (2016, p. 4) asevera que el responsable debe asegurarse antes de llevar a cabo la transmisión de los datos, que tanto él como el receptor, ha adoptado las herramientas indispensables para enlazarse y comunicarse eficientemente, así como las medidas de seguridad necesarias, los mecanismos de autenticación establecidos exclusivamente para este fin, así como los medios relativos al control del envío, recepción e integridad de los datos personales.

También deberán determinarse con claridad, cuáles son las plataformas electrónicas o sistemas que se utilizan para portar datos en formatos estructurados y comúnmente utilizados, los que deberán ser capaces de emitir un registro de cualquier operación realizada, incluyendo lo relacionado a los sujetos que intervienen y la temporalidad en que tuvieron lugar. (Engels, 2016, p. 4)

Particularmente, el Grupo de Trabajo del Artículo 29 (2017, p. 15), indica que los responsables deberán garantizar que distinguen el derecho de portabilidad de otros, mediante el cumplimiento del principio de información, incluyendo también la relativa al ejercicio de este derecho, lo que deberá mostrarse de forma previa al cese de la relación jurídica con el interesado, ya que así se le ofrece la posibilidad de evaluar el destino que desea darle a los datos personales sobre los que ejerce titularidad. Igualmente, se recomienda a los responsables receptores brindar la información relacionada a distinguir los datos que son susceptibles de ser portados. Esta acción afianza la autodeterminación informativa de los interesados, pues se limitan los riesgos y se colabora en

procurar la exactitud y calidad de los datos personales. Así, no podría ser argumentado como obstáculo para la garantía del derecho a la portabilidad cualquier imposibilidad técnica que no haya sido advertida de forma pública y previa (Vanberg, 2018, sin página).

La legislación europea que estudiamos también prohíbe que se menoscabe el derecho de obtener la supresión de los datos personales, lo que, al mismo tiempo, no implica que estos se supriman en el contexto de la ejecución de un contrato. El Grupo de Trabajo del Artículo 29 (2017, p. 8) aclara que el titular de los datos puede continuar usando los servicios del responsable después de ejercido su derecho a la portabilidad y que esta acción no propicia ni la supresión automática de la información, ni la modificación de su periodo de retención y conservación original. Es decir, que mientras el responsable transmisor continúe tratando los datos personales, el titular puede ejercer los derechos aparejados, incluyendo el derecho al olvido.

Según De Hert *et al* (2018, p. 202) la garantía de los derechos que se abordan en el párrafo anterior propicia una competencia real entre proveedores de servicios y evita, a su vez, la monopolización de Internet al establecer como buena práctica el uso de plataformas multinivel o bien, de formatos interoperables. En estos supuestos, el centro del modelo será siempre el titular de los datos personales y quienes lo operarían, serían los proveedores de servicios, que son responsables del tratamiento de los datos.

En este sentido, es pertinente comentar que de acuerdo con el criterio del Grupo de Trabajo del Artículo 29 (2017, p, 8), luego de que el responsable receptor tenga ya los datos personales, se le consideran como facilitados directamente por el interesado y, en consecuencia, pueden ser objeto de portabilidad siempre que se cumpla con los requisitos de procedencia que ya hemos expuesto.

2.3.2 La interoperabilidad y lo formatos estructurados y comúnmente utilizados

Ursic (2018, p. 50) considera que se utilizan estos términos, sin definir, con el propósito de que la legislación permanezca tecnológicamente neutral, independientemente de qué tecnología se utilice para dar cumplimiento a este mandato legal. Sin embargo, añade, puede convertirse en un obstáculo para la correcta transferencia de la información al no establecerse las condiciones y requisitos mínimos necesarios para llevar la tarea a cabo. Es más, la interoperabilidad será el elemento clave para la implementación de la portabilidad, pues a su vez propiciará la ejecución de nuevos servicios desarrollados en beneficio de los consumidores y, en consecuencia, nuevas oportunidades de mercado y ventajas competitivas podrán ser alcanzadas por los prestadores de servicios digitales (Datum Future, 2019, p. 6; De Hert *et al*, 2018, p. 194; Wang & Shah, 2017, p. 20).[28]

Indarte (2012, p. 320) identificó tres tipos de interoperabilidad:

1. La sintáctica u operativa, que se refiere a la que resulta básica para

[28] En España se encuentra vigente el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. En él, se regulan, según su artículo 1, "los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica."
Incluso en la Unión Europea se cuenta con el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que deroga la Decisión (UE) 2015/2240, que establece la dotación financiera para ese programa cuyo objetivo consiste de acuerdo con su considerando 14 "en apoyar la transformación digital de la industria y favorecer un mejor aprovechamiento del potencial industrial de las políticas de innovación, investigación y desarrollo tecnológico, en beneficio de los ciudadanos y las empresas en toda la Unión, incluidas sus regiones ultraperiféricas y sus regiones económicamente desfavorecidas. El Programa debe estructurarse en cinco objetivos específicos que reflejen los ámbitos de actuación clave, a saber: informática de alto rendimiento; inteligencia artificial; ciberseguridad y confianza; capacidades digitales avanzadas, y despliegue y mejor uso de la capacidad digital e interoperabilidad. En todos esos ámbitos de actuación clave, el Programa también debe tener como objetivo una mayor adecuación entre las políticas de la Unión, los Estados miembros y las regiones, y la puesta en común de recursos privados e industriales para incrementar la inversión y desarrollar sinergias más sólidas. Además, el Programa debe reforzar la competitividad de la Unión y la resiliencia de su economía".
Tanto la UNE-EN ISO 13606, como la NOM-024-SSA3-2012, fueron creadas no con el objetivo de especificar los requisitos con los que debe cumplir el expediente clínico, si no para establecer la arquitectura que el soporte documental deberá tener para propiciar el intercambio de información entre distintos prestadores de servicios sanitarios, para lo cual contar con interoperabilidad semántica, para lo que se necesita contar con información sanitaria normalizada que exprese la actividad a registrar en la interfaz estructurada.

operar el resto, pues se establece un nivel semántico común para que la información pueda ser enviada y recibida, sin que ello signifique que sea interpretada de forma efectiva.

2. Por lo que hace a la semántica, es aquella que permite la interpretación y uso correctos de la información que se intercambia y la autora cree que se trata del objetivo a alcanzar. A su vez, la divide en la de procesamiento distribuido y global cuya diferencia principal estriba en "los estándares que aplican y en la forma en que están diseñados los sistemas" (Indarte, 2012, p. 321).

    a. La de procesamiento distribuido es la forma más común y se refiere a la implementación de sistemas que generan información para comunicarla a otro, que la procesará con la finalidad de generar algún resultado de valor.
    b. El procesamiento global, implica la capacidad de los sistemas de comunicarse entre sí, al mismo tiempo que pueden interpretar lo transmitido de manera correcta, sin que su diseño persiguiera ese objetivo y que como hemos reflexionado las diversas legislaciones establecen como requisito no obligatorio en el tema.

3. Finalmente, la interoperabilidad organizativa hace referencia a la capacidad que tendrá el sistema de interpretar la información siempre que se le hayan especificado las reglas del sector de que se trate, ya que "es la única forma de tener un nivel de visión de toda la institución mediante la definición formal de sus componentes y de la información que generan y consumen" (Indarte, 2012, p. 321).

En ese sentido se pronuncia el Grupo de Trabajo del Artículo 29 (2017, p. 18), pues contempla que los casos han de evaluarse individualmente para saber si se cuenta con los medios que hagan viable la portabilidad de datos, es decir, que en un principio será un formato interoperable; si bien es cierto que el receptor no se encuentra obligado a aceptarlo ya que pueden existir diferencias técnicas, en

cuyo caso se expondrá al interesado esta dificultad, lo que se considerará como una negativa a atender la solicitud.

Así, antes de externarla, los responsables deben valorar opciones para garantizar el derecho, tales como la transmisión directa del conjunto de datos, hacerlo en partes o bien, mediante una herramienta automatizada que permita elegir los datos que resulten pertinentes. (Grupo de Trabajo del Artículo 29, 2017, p. 18).

A su vez, los responsables pueden ofrecer mecanismos tales como la descarga directa de los datos o bien, la transmisión a otro responsable mediante una interfaz de programación de aplicaciones, el uso de un almacén de datos personales, contar con un tercero de confianza para su custodia, almacenamiento o concesión de permiso para su aprovechamiento por otro responsable y para procurar su transferencia, según sugiere la Comisión Europea (2017, p. 1).

A pesar de los requisitos que la norma europea impone, lo cierto es que no establece condiciones específicas acerca del formato en que los datos deben transmitirse, por lo que diferirá dependiendo del sector que se trate. Sin embargo, deberá procurarse la garantía del derecho a la portabilidad, por lo que deberán ser de lectura fácil pero no necesariamente compatibles, aunque si interoperables como exigen las legislaciones estudiadas.

Autores como Quinn (2018, p. 7) consideran que algunos límites al concepto de "legibilidad de la máquina" deben ser considerados en la garantía de este derecho, siendo más bien cautos en su interpretación, ya que no se impone la obligación al responsable de garantizar que los datos sean compatibles con todos los fines imaginables, lo que afirma podría ser un "elemento disuasorio para el procesamiento de datos en general" y que debe contemplarse más bien, como una responsabilidad compartida. También deberá ser cuidadoso en valorar en qué grado el formato utilizado dificultará la reutilización de esos datos al titular, explicando en todo caso las causas y conveniencia de lo decidido. Sin embargo, precisa que el procesamiento de metadatos adicionales no supone una

justificación legítima solo para garantizar la portabilidad de los datos a futuro, alentando aun así la cooperación entre los miembros de diversos sectores para establecer normas y formatos interoperables ajustados a sus necesidades y a los requisitos de garantía de este derecho.

De esta suerte, y siendo la portabilidad en opinión del Grupo de Trabajo del Artículo 29 (2017, p. 20) un tratamiento adicional y complementario al declarado inicialmente toda vez que no se lleva a cabo para lograr fines distintos a los señalados, esto debería incitar a los responsables a mantener de forma permanente los datos exactos y actualizados, para facilitar la tarea.

Por lo que hace a las condiciones técnicas, ya Lueders (2004, p. 9) recomendaba como criterio indispensable que el software a adquirir o desarrollar, debía ser uno mediante el que se garantizara la compatibilidad con estándares abiertos, concepto que hace referencia, según el mismo autor, al "conjunto de reglas y especificaciones que describen colectivamente el diseño o las características de funcionamiento de un programa o dispositivo, siendo publicado y puesto a disposición de la comunidad técnica de forma gratuita"; en contraste al código fuente abierto que se entiende como "un programa en el cual el código fuente está disponible para el uso del público en general y/o para la modificación de su forma de diseño original", por lo que, al no ser un estándar abierto si bien puede interoperar, no quiere decir que tendrá implementados los mismos estándares que otros programas de código abierto.[29]

Zanfir (2012, p. 4) propone analizar la importancia de la computación en la nube como medio para garantizar la portabilidad de datos pues contrario a lo que se

[29] Recordemos lo que Rodatà (1976, pp. 141, 142) nos advertía acerca de si es posible desarraigar las infraestructuras informáticas de la sociedad: "esto no significa que deba mirarse a la tecnología como un valor en constante progreso, reemplazando la ideología del *laisser-faire* por una *laisser-innover*; tampoco significa que pueda ocultarse el aspecto "totalitario" de la esta tecnología, enmascarándolo detrás de un velo de eficiencia. Si el objetivo a alcanzar es implementar el mejor uso posible del que se considera el recurso básico más importante de la sociedad futura, el camino a seguir es aquel que, […] conduzca a la expansión del poder colectivo. […] Esta es la cuestión central, porque el hecho de que las tecnologías de la información sean exclusivas de sujetos privilegiados, ya sean públicos o privado, tiene una consecuencia evidente: la de aumentar las posibilidades de la discriminación y los desequilibrios de poder dentro de una organización social."

supone, no aminorará la privacidad ni la protección de los datos, sino que se incentivaría la implementación de mejores y adicionales medidas de seguridad y en consecuencia, se fortalecería la autodeterminación informativa al facilitar y robustecer el acceso y control que sobre sus datos tienen sus titulares, además de ser necesario el trabajo legislativo correspondiente con lo cual, según la autora, incluso volverá visible la importancia que tiene el derecho de protección de datos personales.

2.3.2 Obligaciones del responsable del tratamiento para la garantía del derecho a la portabilidad de los datos personales.

Contrario a lo que podríamos inferir, la positivización del ejercicio de portabilidad no le impone al responsable la obligación de conservar la información y darle tratamiento a través de formatos estructurados y comúnmente utilizados, con la finalidad de garantizar este derecho. Consideramos que debería ser previsto lo contrario, toda vez que se trata de un derecho nuevo que responde a la necesidad que tienen los titulares de los datos de acceder y contar con sus datos personales aún y con los avances tecnológicos que se han presentado, es decir, para garantizarlo en otra modalidad que la tradicional.

Además de cumplir con los principios de protección de los datos personales, tanto los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018; así como los Reglamentos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 ponen especial énfasis en el relativo a la información, pues mandatan que deberá proporcionársele en el aviso de privacidad integral, la relativa a la posibilidad que tiene de ejercer este derecho, incluyendo además la clasificación de los datos que sean técnicamente portables, los formatos estructurados y comúnmente utilizados para ese fin, así como cualquier información relacionada para solicitarlo, independientemente de que los datos hayan sido obtenidos del titular o a través de un tercero.

Aunado a lo anterior, que la portabilidad sea ejercida y los datos transmitidos a un responsable distinto, no cesa o concluye la relación entre el titular y el responsable que en primer lugar ha tratado los datos personales. Aunque los Reglamentos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 también contemplan esta disposición, si alientan desde su exposición de motivos a que los responsables adopten formatos interoperables que permitan el ejercicio de este derecho.

El Grupo de Trabajo del Artículo 29 (2017, p. 7) reconoce que la garantía de este derecho impone la obligación a los responsables de tratar los datos personales del interesado de acuerdo con sus deseos, pues no es un derecho que tenga como límite aquellos datos que puedan ser útiles o relevantes en el contexto de servicios similares prestados por sus competidores. Además, interpreta que al actuar en nombre del titular, el responsable transmisor no es responsable del tratamiento que dé a los datos el responsable receptor, pues no fue él quien decidió quien dará tratamiento a esa información; sin embargo, deberá proporcionar garantías suficientes para asegurar que actúa a su nombre.

Egan (2019, p. 9) identifica tres tipos de transferencias dirigidas por los titulares de los datos y usuarios de los servicios. La primera, las abiertas, en las que los titulares que ejerzan el derecho reciban sus datos y puedan comunicarlos sin ninguna limitación o control, salvo las que existan en la ley a cualquier proveedor de servicios, y sin que en responsable transmisor y el receptor cuenten con relación jurídica alguna.

La segunda categoría es la de transferencias condicionadas, en la que el titular de los datos puede solicitar y recibir sus datos para transferirlos a cualquier responsable receptor que cumpla con ciertas condiciones impuestas por el transmisor y su relación jurídica existe únicamente para dar cumplimiento a este tipo de solicitudes, por lo que incluso tienen la capacidad de portar datos entre servicios, sin intervención del titular de los datos.

Por último, la autora conceptualiza a la transferencia entre socios, en la que los usuarios del servicio pueden recibir sus datos y transferirlos a un receptor con el que el responsable del tratamiento tiene una relación que va más allá de dar cumplimiento a este tipo de acciones, sino que persiguen la integración de sus características con los productos de la otra, como sucede con las diversas plataformas del Grupo Meta.

El Grupo de Trabajo del Artículo 29 (2017, p. 7) tampoco considera que el responsable transmisor tenga la obligación de comprobar la calidad[30] de los datos personales de forma previa a realizar la portabilidad o de retenerlos más tiempo del necesario o especificado por que exista la probabilidad de que recibirán una solicitud de ejercicio de este derecho. En el primer caso, datos deberían ser ya exactos y actualizados, cumpliendo con los principios de tratamiento establecidos en la norma de protección de datos personales.

De igual manera el Grupo de Trabajo del Artículo 29 (2017, p. 7) argumenta que, para garantizar este derecho, el responsable deberá contemplar la existencia de procedimientos específicos que respondan a su naturaleza particular. Si se cuenta con un encargado, en el contrato donde se formalice esta relación deberán establecerse clausulas específicas que contengan la obligación de asistir al responsable para tal efecto. Si existiera más de un responsable involucrado, en el instrumento deberán limitarse con claridad las obligaciones concernientes a cada uno.

De lo que sí resulta responsable el receptor de los datos es de garantizar que los datos portados son pertinentes y no excesivos para la nueva finalidad de tratamiento y por ello no se encuentran obligados a recibir los datos personales

[30] Abona a lo anterior el informe del Centre for Information Policy Leadership (2017, p. 5, 6) en tanto recomienda establecer mecanismos para que el responsable pueda asegurarse de los datos que el usuario quiere que sean portados, pues no hacerlo, podría generar cargas innecesarias por la gran cantidad de información que se puede tener acerca de una persona. Este organismo considera, incluso, que el responsable receptor no debería ser responsable de garantizar la pertinencia de los datos recibidos, idea con la que discrepamos, toda vez que esta obligación se traduce en la de garantizar el principio de minimización y proporcionalidad, que de cualquier forma debe cumplirse al referirse a un tratamiento de datos con un responsable nuevo y distinto al que originariamente tenían los datos, y que, además, dio origen al ejercicio del derecho de portabilidad.

o todos los que le sean transmitidos (Grupo de Trabajo del Artículo 29, 2017, p. 8). Igualmente, deberá establecer las condiciones de su tratamiento que deberán estar apegados a los principios de protección de datos, debiendo borrar aquellos que resulten excesivos a la brevedad.

En general, el Grupo de Trabajo del Artículo 29 (2017, p. 22, 23) recomienda a los responsables colaborar con el titular de los datos mediante el establecimiento de estrategias que mitiguen los riesgos en su transmisión; por ejemplo al garantizar que se entregan de forma segura a la persona adecuada como el uso de información adicional para la autenticación; o para que los usuarios almacenen de forma adecuada y segura sus datos personales en sus sistemas, al recomendarles el uso de un formato apropiado, herramientas de cifrado y otras medidas de seguridad para tal fin.

De lo descrito, el Centre for Information Policy Leadership (2020, p. 2), concluye que el ejercicio excesivo del derecho de portabilidad de datos puede abrumar a la competencia y dar cargas excesivas a los responsables de tratamiento al exigirles esfuerzos desproporcionados[31] a nivel tecnológico, sobre todo en aquellas áreas donde el ejercicio del derecho no representa ventajas reales o un valor añadido para el titular de los datos.

Al mismo tiempo, Quinn (2018, p. 14) reflexiona acerca de la obligación que tiene un responsable de tratamiento a transferir datos fuera de Europa, donde no se cuentan con las garantías conocidas para el procesamiento de datos, sobre todo porque considera que el artículo 20 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no contempla de forma explícita este supuesto y porque los artículos correspondientes a la transferencia de datos no se refieren tampoco a ser aplicables a la portabilidad, por lo que considera probable que se nieguen a garantizarla. La Federación

[31] El Centre for Information Policy Leadership en el informe citado (2020), propone al modelo "pull" como una solución factible para el responsable de los datos, que consiste en que ambas partes acodarían un procesamiento adecuado de los datos antes de que sean transferidos y al mismo tiempo, no se requiere que los responsables de tratamiento comprendan de qué forma llevan a cabo esta acción sus competidores, lo que a su vez representa un incentivo para desarrollar el mejor mecanismo y así, ganar nuevos clientes.

Bancaria Europea (2017, p. 3) hace hincapié en que los titulares de los datos deberían estar plenamente consciente de que estas cuestiones al ejercer su derecho.

En ese sentido, resulta de relevancia conocer las conclusiones del estudio realizado por Kuebler-Wachendorff *et al* (2021, p. 269, 270), en el que se demuestra que, a pesar de tener ya tres años de positivizado, al momento de la publicación de su artículo, su ejercicio y garantía no ha alcanzado el potencial que se tenía previsto, ya que menos de uno de cada cuatro de responsables de tratamiento ofrecieron a sus clientes la posibilidad de ejercer la portabilidad de sus datos, por lo que consideran, es necesario que se implementen los mecanismos necesarios para que se incentive a los titulares para el ejercicio de su derecho, pues apenas lo conocen y menos lo utilizan.

Para este último punto, reflexionan acerca de la conveniencia de realizar estudios centrados en desarrollar la conciencia de los titulares de los datos para aumentar su autodeterminación informativa y que ejerzan su derecho y que se explique la brecha entre las preocupaciones por conservar su privacidad y cómo se comportan en la realidad, es decir, si la conducta desplegada corresponde a los temores experimentados en este tema y acerca de cuál es su percepción de los servicios que ofrece y también del propio responsable.

2.3.2.1 La seguridad de la información para la garantía del derecho a la portabilidad de los datos personales

De acuerdo con Somaini (2018, p. 177), los datos se vuelven accesibles como consecuencia de que la portabilidad sea obligatoria. Esto se enfrenta al principio de seguridad, ya que los responsables de tratamiento no suelen garantizarla de manera equivalente a la exposición que sufren los datos personales por ejemplo, como consecuencia de su flujo nacional o transfronterizo. Como alternativa para solucionar cuestiones relacionadas, nos sugiere a las API (interfaces de programación de aplicaciones, por sus siglas en inglés).

Krämer *et al,* (2020, p. 7) y Urquhart *et al* (2017, p. 323) abogan también por el uso de este tipo de interfaces, entre la que destacan los sistemas de información de productos (PIM, por sus siglas en inglés), con los que se potencia el uso de la interoperabilidad ya que los usuarios controlarían la forma en que se accede y comparte la información al incrementar la transparencia acerca de su tratamiento y eficientar el ejercicio del derecho, mejorando el proceso desde la interposición de la solicitud hasta la disminución de los tiempos de respuesta.

El Grupo de Trabajo del Artículo 29 (2017, p. 14), sugiere que en el proceso de portabilidad se consideren dos aspectos. Primero, que la transmisión de la información, por sí misma, requiere medidas de seguridad suficientes para proteger su integridad. Segundo, que el responsable del tratamiento se asegure de transmitir la información al responsable destinatario correcto, tomando las medidas de seguridad pertinentes para lograr ambos de forma exitosa.

Sin embargo, autores como Bozdag (2018, p. 4) afirman que cumplir con las medidas de seguridad que la normativa solicita, -tales como mecanismos de autenticación avanzados, establecer un número límite de veces para ejecutar una solicitud de portabilidad en un límite de tiempo determinado, notificar al titular de los datos o el establecimiento de una cantidad máxima de datos que puedan ser objeto de portabilidad por jornada-, contravienen de manera directa al requisito de que el ejercicio de este derecho debería darse sin obstáculos. Los requerimientos de medidas de seguridad serán descritos en los siguientes apartados, con mayor detalle.

2.3.2.1.1 Orden jurídico mexicano

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 5 de julio de 2010, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, establece la obligación del responsable de establecer y mantener medidas de seguridad que podrán ser administrativas, técnicas y físicas. A través de estas, se protege a los datos personales de sufrir daño, pérdida, alteración, destrucción o bien, de que sean usados, se tenga acceso o su tratamiento no autorizado. La

obligación consiste en establecer políticas y programas de seguridad y un sistema de supervisión y vigilancia implementado de forma bianual, aunque si se realizan modificaciones sustanciales deberá reflejar la actualización realizada de inmediato.

A través de las medidas administrativas, se implementan la gestión, soporte y revisión de la seguridad a nivel organizacional, así como la identificación y clasificación de la información y la formación del personal en la materia.

Las medidas físicas se encuentran orientadas a la prevención de accesos no autorizados, daños o interferencia a instalaciones físicas, áreas críticas de la organización, equipo e información; la protección de equipos situados dentro o fuera de las instalaciones; la garantía de eliminación de datos de forma segura y proveer mantenimiento a los equipos, independientemente de para ello se emplee o no la tecnología.

Por último, las medidas técnicas serán aquellas cuyo resultado medible y que utilizan la tecnología para garantizar el acceso a las bases de datos por usuarios identificados y autorizados, sobre todo aquellos que lo necesitan para el desempeño de sus funciones; para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros y para la gestión de comunicaciones y operaciones de los recursos informáticos para el tratamiento de los datos personales.

El establecimiento de las medidas de seguridad puede ser por cuenta propia del responsable o mediante la contratación de un tercero *ex profeso*. Cualquiera sea la forma que se decida, deben determinarse considerando el riesgo inherente por tipo de dato personal y su sensibilidad: el desarrollo tecnológico, las consecuencias de su vulneración si llegara a ocurrir y si sucedieron previamente, el número de titulares, el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales para un tercero no autorizado para su posesión y cualquier factor que incida en el nivel de riesgo.

La ley federal estipula que las medidas de seguridad no deberán ser menores a las que se mantengan para el tratamiento de la información y también deberán tomar en cuenta el riesgo que existe, las consecuencias que pueden sufrir los titulares, la sensibilidad de los datos y el desarrollo tecnológico con que se cuente al momento de establecerlas.[32] En iguales términos se establece en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017.

También es importante señalar que la legislación federal establece la obligación de informar al titular de los datos de manera inmediata de cualquier vulneración de seguridad[33] ocurrida en cualquier fase del tratamiento de los datos personales que pueda resultar en una afectación de sus derechos patrimoniales o morales, para que pueda tomar las medidas que a su derecho convengan. La legislación general por su parte concede un plazo máximo de 72 horas para informar al titular, contadas a partir de la confirmación de la vulneración de seguridad, pero también deberá informar por escrito al Organismo Garante[34]. Lo anterior, a efecto de determinar si hubo afectación a los derechos patrimoniales[35] o morales[36] del

[32] Tómese como ejemplo la sanción de €10,000.00 impuesta por el Garante per la protezione dei dati personali, a un médico que para entregar sus recetas, había adoptado como método el colgarlas fuera de su ventana con pinzas para la ropa, sin sobre o método que ocultara su contenido y que puede consultarse completa en Ordinanza ingiunzione - 28 ottobre 2021 [9716887] - Garante Privacy

[33] En la Guía 9/2022, de la notificación de brechas en la seguridad de datos personales según el RGPD, adoptada el 10 de octubre de 2022 por el Comité Europeo de Datos Personales, se emiten recomendaciones y ejemplos para la notificación de este tipo de incidentes en diversos ámbitos.

[34] Según el artículo 67 de los Lineamientos generales de protección de datos personales para el sector público, de 19 de diciembre de 2017, deberá informarse, cuando menos la hora y fecha de la identificación de la vulneración; la hora y fecha del inicio de la investigación sobre la vulneración; la naturaleza del incidente o vulneración ocurrida; la descripción detallada de las circunstancias en torno a la vulneración ocurrida; las categorías y número aproximado de titulares afectados; los sistemas de tratamiento y datos personales comprometidos; las acciones correctivas realizadas de forma inmediata; la descripción de las posibles consecuencias de la vulneración de seguridad ocurrida; las recomendaciones dirigidas al titular; el medio puesto a disposición del titular para que pueda obtener más información al respecto; el nombre completo de la o las personas designadas y sus datos de contacto, para que puedan proporcionar más información al Instituto, en caso de requerirse y cualquier otra información y documentación que considere conveniente hacer del conocimiento del Instituto.

[35] Cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

[36] Cuando la vulneración esté relacionada, de manera enunciativa más no limitativa, con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto

titular, según el artículo 67 de los Lineamientos generales de protección de datos personales para el sector público, de 19 de diciembre de 2017.

El titular deberá conocer la naturaleza del incidente, los datos personales comprometidos, las recomendaciones que haga el responsable para proteger sus intereses, las acciones correctivas realizadas de forma inmediata y las fuentes de información en la materia. El responsable, a su vez, debe implementar las acciones correctivas, preventivas y de mejora que eviten que la vulneración se repita, dando cuenta de ello en una bitácora para los responsables, prevista en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017.

Como consecuencia a la notificación de una vulneración de seguridad, según la Ley Federal, el INAI podrá realizar las investigaciones que considere pertinentes pues en su caso, podría iniciar un procedimiento de verificación y después podría establecer una sanción si el caso lo ameritara. También puede emitir recomendaciones no vinculantes en materia de seguridad de los datos, como herramienta proactiva y orientadora para los responsables del tratamiento en este tema.

Entre las acciones que la legislación mexicana, tanto la federal como la general, contempla para establecer y mantener la seguridad de los datos están las de elaborar un inventario de datos personales y sus sistemas de tratamiento, la determinación de funciones y obligaciones de los responsables o encargados del tratamiento, elaborar un análisis de riesgo y de brecha, el establecimiento de medidas de seguridad diseñadas para el caso concreto y la elaboración de un plan de trabajo para su implementación así como de las que del estudio resulten faltantes, llevar a cabo revisiones, auditorías, capacitación del personal involucrado y el registro de los medios de almacenamiento de los datos personales.

---

físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

Los responsables deben actualizar las medidas de seguridad si se modifican las medidas o procesos de seguridad por la revisión de la política de seguridad, si las finalidades de tratamiento se modifiquen de tal suerte que también cambie el nivel de riesgo, si los sistemas de tratamiento fueron vulnerados o exista cualquier afectación a los datos personales. Sin embargo, esta acción debe ser realizada cuando menos cada año, tratándose de datos personales sensibles.

Tanto en la ley federal como en la general, se considera como vulneración de seguridad la destrucción, copia, uso, acceso, tratamiento, alteración o modificación no autorizados; la pérdida, el robo, extravío y el daño de los datos personales. Estas deberán informarse al titular en cuanto se confirme que han ocurrido y deberá implementar las acciones necesarias para revisar la magnitud de la afectación, para que se tomen las medidas que a su derecho convengan.

2.3.2.1.1 Orden jurídico comunitario y español

Para cumplir adecuadamente con el principio de seguridad, se establecerán y mantendrán las medidas técnicas, físicas y administrativas[37, 38], que permitan proteger los datos contra pérdida, daño, alteración, destrucción o el uso, acceso o tratamiento no autorizado, preferentemente contemplándolo desde el diseño de la política de privacidad -lo que Bygrave, (2022, p. 175) llama “seguridad por diseño” que debe considerar automáticamente que se le incluya por defecto- e incluso, desde la del establecimiento.

[37] Sirve como ejemplo la Resolución de la AEPD R/02909/2015, correspondiente al Procedimiento No. AP/00029/2015, para estudiar los límites del principio de seguridad, pues al haber confirmado con datos provistos por el ente responsable que un facultativo no autorizado tuvo cientos de accesos comprobados a la historia clínica de una paciente, sin que los haya detectado y mucho menos adoptado alguna medida que permitiera corregir el fallo de seguridad, por lo que este tipo de acontecimientos también permiten concluir la falta de aplicación del principio de seguridad, pues en palabras de la propia Agencia (2022), su sistema debería ser uno “que permita, no solo conocer los registros de todos los accesos que se realizan a cada una de las historias clínicas de sus pacientes, sino también que permita, por medio de la revisión periódica de esa información, la detección de problemas tales como los accesos injustificados. Con ello se garantizaría la seguridad de los datos de carácter personal y se evitaría su alteración, pérdida, tratamiento o acceso no autorizado, en definitiva, unas medidas de seguridad adecuadas que garanticen el derecho fundamental a la protección de datos personales.”

[38] Piñar (2018, p. 108) abunda diciendo que, la ciencia jurídica y la técnica deben practicarse éticamente, pues “ante la innovación tecnológica hemos de volver a los principios, a lo esencial, pues de otro modo corremos el riesgo de movernos en un escenario cambiante, improvisando soluciones que terminan por quedar obsoletas antes incluso de ser plenamente aplicadas, desbordadas por la evolución, inmisericorde para el derecho, de los avances de la técnica.”

Con esa idea concuerda Troncoso (2018, p. 142) en tanto interpreta que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, no contiene el listado de medidas a observar, sino que cede la responsabilidad de establecerlas al responsable del tratamiento, que sabrá cuáles son las que mejor se adecúan a su situación, a través del principio de responsabilidad proactiva.

El Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 prevé a su vez, la obligación de implementar medidas de seguridad adecuadas contra la destrucción accidental o no autorizada, la pérdida accidental, el acceso, modificación o difusión no autorizados de los ficheros automatizados.[39]

Las medidas de seguridad del tratamiento que los Reglamentos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 contemplan para su aplicación, son:

1. La seudonimización y el cifrado de los datos.
2. La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento de forma permanente.
3. La capacidad de restaurar la disponibilidad y el acceso a los datos de forma rápida si hubiera un incidente físico o técnico.[40]

[39] De la importancia de su implementación en estructuras críticas del sector sanitario hacen un estudio Marjopoulou y Papakonstantinou (2021), en el que sostienen que la seguridad debe estar incluida por diseño y defecto para aprovechar todos los beneficios que la digitalización ha traído al campo de la salud, todo ello desde la uniformización de la legislación aplicable, lo que permitirá reducir la vulnerabilidad de las infraestructuras y por lo tanto, garantizar en mejor y mayor medida la privacidad y protección de datos personales de los usuarios de los sistemas de salud.

[40] Acerca de este particular, Troncoso (2021, p. 47), apunta que toda vez que el Reglamento (UE) 2016/679 no establece medidas específicas para su cumplimiento, sino que por el contrario, deja en consideración del responsable del tratamiento las que han de adoptarse, el legislador se alejó del modelo jurídico del Derecho continental europeo para acercarse al *Common law*, que revisa cada caso particular, toda vez que el responsable deducirá las medidas a poner en práctica de las evaluaciones de impacto o estudios que realice.

Para lo anterior, deberán tenerse en cuenta siempre el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos humanos.[41]

Los Reglamentos (UE) 2016/679 y 2018/1725, también contemplan la obligación del responsable de avisar a la autoridad, en este caso el Supervisor Europeo de Protección de Datos, de una violación a la seguridad de los datos personales.[42] Deberá hacerse de manera inmediata o en la medida de sus posibilidades, pero sin mediar demora, dando cuenta de la naturaleza del incidente, el número de afectados, la categoría de los datos, los relativos al delegado de protección de datos, así como las consecuencias que se estima pueden suceder, así como las medidas adoptadas para contener el suceso. La obligación también contempla documentar este tipo de incidentes, efectos y las medidas correctivas, debiendo avisar también al delegado de protección de datos.

El aviso también deberá darse al interesado mediante un lenguaje comprensible, salvo que las medidas aplicadas no permitan el conocimiento de los datos por haberse cifrado o hacerlo ininteligibles, garanticen que ya no exista la posibilidad de que se den circunstancias que los pongan en alto riesgo o bien, esto suponga un esfuerzo desproporcionado, ante lo que debería emitir un comunicado público para dar noticia de lo sucedido. El Supervisor Europeo o la autoridad de control, dependiendo del caso, podría obligarle a hacerlo en caso de ser omiso.

[41] A su vez, en la Exposición de motivos de la Recomendación CM/Rec(2019)2 del Comité de Ministros del Consejo de Europa, de 27 de marzo de 2019, realizada a los Estados miembros sobre la protección de los datos relacionados con la salud, se sugiere que las medidas de seguridad deben centrarse en la disponibilidad de los datos, su integridad y la auditabilidad del sistema que los almacena.

[42] Para finalizar este apartado, resulta conveniente citar a Troncoso (2006, p. 88) en tanto hace la diferenciación de la cesión de datos contra el incumplimiento del deber de secreto, atendiendo a sí el acceso a esa información tiene la finalidad de llevar a cabo un tratamiento por parte de terceros. De esta suerte, si no hubiera una custodia adecuada de los archivos o bien, si se produce un acceso no autorizado, el autor lo considera una violación al deber de seguridad y no el segundo de los supuestos.

2.3.3 Información que es objeto del ejercicio del derecho a la portabilidad.

Según la legislación analizada, en todos los casos nos encontramos con que la información que puede ser objeto de portabilidad son los datos personales de los interesados[43], siempre y cuando su tratamiento esté legitimado por la base del consentimiento o una relación contractual. También se condiciona a que esa información debe estar conservada en sistemas que permitan generar formatos estructurados y comúnmente utilizados, que permitan su intercambio por ser compatibles, o por medios automatizados, como lo reconoce el Grupo de Trabajo del Artículo 29 (2017, p. 10).

Otros datos excluidos de transmisión a causa del ejercicio de este derecho son los protegidos por la propiedad intelectual y los secretos comerciales, que si bien es cierto se encuentran protegidos, ante una solicitud deberán negarse estos, pero no los que efectivamente correspondan a quien pretende ejercer su derecho a la portabilidad (Grupo de Trabajo del Artículo 29, 2017, p. 14).

Por ello, el Grupo de Trabajo del Artículo (29, p. 20) afirma que la portabilidad supone un alto "nivel de abstracción de cualquier formato interno o propietario. Como tal, la portabilidad de los datos supone un estrato adicional del tratamiento de los datos por parte del responsable, con el fin de extraer los datos de la plataforma y filtrar los datos personales que no estén incluidos en el ámbito de la portabilidad, tales como datos inferidos o datos relacionados con la seguridad de los sistemas."

En este supuesto, es decir, de los datos procedentes de la aplicación de técnicas de *know how* del responsable (AEPD, 2017, p. 23), se entiende que quedan excluidos los que así hayan sido obtenidos, sin que puedan excluirse del ejercicio del derecho los proporcionados directamente por el titular o aquellos que resulten derivados directamente del desarrollo del servicio, es decir, los que surjan como

[43] "Los datos más valiosos provienen de los propios usuarios, que aportan datos tanto directamente como a través de su actividad en la plataforma" (Gans, 2018, p. 5).

consecuencia de esta causa, pero no así los que sean producidos intencionalmente por el responsable mediante las técnicas referidas.

Sin embargo, la información inferida deberá ser otorgada mediante el ejercicio del derecho de acceso, aunque no del de portabilidad (Datum Future, 2019, p. 4). Sostiene la misma opinión Quinn (2018, p. 9) aunque también cree que ese tipo de datos podrían ser de especial interés para cuestiones sanitarias o de investigación científica, ya que puede implicar el descubrimiento de correlaciones y relaciones que serían de inmensa utilidad, idea con la que coincidimos. Van der Auwermeulen (2017, p. 70) hace esta distinción y considera que la información estadística producto de los servicios digitales, al no estar relacionada con los interesados no cae en el supuesto.

Sin embargo, los datos tales como los perfiles de vendedores de plataformas digitales si debiesen ser portables, refiriéndose específicamente al sistema de puntuación y retroalimentación que reciben por el servicio que brindan, toda vez que si bien es cierto son producto de la inferencia que hace el prestador de ese servicio de otros datos, también lo es que en ellos se refleja su actividad y aprovechamiento como vendedor (Van der Auwermeulen, 2017, p. 70), es decir, que dan cuenta de su resultado desarrollando ese trabajo, pues como Ursic referencia (2018, p. 57), el propósito del Grupo de Trabajo del Artículo 29 no era restringir el uso de los datos personales, sino el de inhibir su explotación comercial.

Se contrapone a este ejemplo el de los avatares generados por ciertas aplicaciones de juegos, información que considera no debería ser portable toda vez que si bien el usuario elige las características que le permiten autodeterminarse en ese espacio virtual, también lo es que se trata de unas desarrolladas por completo por el autor de la plataforma y que contará con esas mismas opciones de expresión personal en cualquiera otra donde se registre e interactúe. (Van der Auwermeulen, 2017, p. 70)

Por su parte, la Federación Bancaria Europea (2017, p. 4) considera indispensable que solo los datos proporcionados por el titular sean portados, ya

que los inferidos o derivados del tratamiento de los responsables cuentan con un valor añadido que les da esta acción, con lo que sus competidores se beneficiarían injustamente. De igual importancia es la definición de la factibilidad técnica para llevar a cabo la transferencia de datos, de tal suerte que se procure la estandarización y portabilidad directa entre responsables.

En el mismo sentido se pronuncia el Grupo de Trabajo del Artículo 29 (2017, p. 11) y el Centre for Information Policy Leadership (2017, p. 7) al referir que únicamente los datos que se consideren personales, es decir, que nos permitan identificar o hacer identificable a un individuo son objeto de portabilidad, por lo que como habíamos visto en el capítulo anterior, aquellos datos que no se clasifiquen como personales no se encuentran en la esfera de protección de la legislación en la materia, lo que incluye a los seudónimos siempre que se cuente con los identificadores correspondientes que los relacionen con su titular. Lo anterior se entiende toda vez que, en su definición, el derecho únicamente ampara aquella información que fue proporcionada directamente por el interesado. [44]

Sin embargo, la AEPD (2017, p. 23) aclara que este derecho no hace referencia únicamente a datos actuales o que se traten en un momento presente, sino que deberán tenerse en cuanta los que hayan sido facilitados por el titular o bien, los obtenidos por el responsable como consecuencia del uso del producto o servicio contratado, ya que la limitación de este entendimiento desprende de su esencia

[44] Así lo consideró también la Agencia Española de Protección de Datos en su Resolución de fecha 03 de diciembre de 2019 que emitió al expediente TD-00195-2019, resultado de la reclamación que una persona presentó frente a Telefónica de España. S.A.U., mediante la que exigía que se le facilite la totalidad de información que la política de privacidad de la empresa señala como objeto de portabilidad. La AEPD le instruye a la empresa la interpretación amplia de los dispuesto en el Reglamento 2016/679 acerca de los datos personales que le incumben a la reclamante y considera que la portabilidad se llevó de forma incompleta pues no se ha incluido información que se también ha proporcionado la propia titular de los datos de forma directa al hacer uso del servicio contratado. Sin embargo hacen la diferenciación con los datos de tráfico y localización de los que se consideran en la Ley 9/2014 de 9 de mayo General de Telecomunicaciones, por lo que hace a las “visitas a la Web”, pues estas deben conservarse con el único ánimo de transmitirlas si le son requeridas por autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales por un periodo de doce meses a partir que se dio la comunicación, aunque la Directiva 2006/24/CE permite reducirla a seis meses o ampliarla a dos años, por lo que, considera la AEPD, la única obligación que se establece es la descrita y no una diversa, por lo que según la resolución los titulares “no cuentan con derecho a la portabilidad de los datos de tráfico conservados por las operadoras a los efectos previstos en la Ley 25/2007”.

a la portabilidad y sobre todo, al control de la información que debe tener su titular que fue uno de los objetivos por el que se dotó de reconocimiento al derecho.

Con esta idea coinciden Chassang *et al* (2018, p. 306) toda vez que, sobre todo tratándose de investigación clínica, es prácticamente imposible proporcionar todos los datos necesarios al comienzo de la relación jurídica por la propia naturaleza del tratamiento. Por esa limitación, es que autores como Lam y Liu (2020, p. 2) nos advierten de que los responsables del tratamiento pueden ofrecer como servicio adicional a sus clientes el proporcionarles el análisis de sus datos, pues recordemos que el resultado no puede portarse, lo que en su opinión puede monopolizar su relación con ese responsable como proveedor de servicios.

A su vez, los Reglamentos (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, establecen que, si los datos personales objeto de la portabilidad conciernen a más de un interesado, el derecho a recibirlos se entiende sin perjuicio de los derechos y libertades del resto de los titulares, de conformidad con los dictados de estas disposiciones jurídicas.

El Grupo de Trabajo del Artículo 29 (2017, p. 13) también considera que los responsables pueden ubicarse en el supuesto de que los datos que deban portar incluyan información de terceros y concluye que debe permitirse conocer esa información puesto que da cuenta de cómo se relaciona el interesado que ha solicitado el ejercicio del derecho. Sin embargo, el responsable receptor debería evitar el tratamiento de esos datos para finalidades que afecten los derechos y libertades de terceros, eliminándolos incluso si se hará uso de ellos para finalidades distintas a las de origen.

Igualmente, si se van a tratar, debe señalarse la base jurídica para tal efecto, siendo responsabilidad del interesado los obtenidos por este derecho y que las decisiones acerca del tratamiento no las tome el responsable de los datos, por lo que para evitar este tipo de consecuencias los datos deberían permanecer

bajo el control exclusivo del interesado que ejerció la portabilidad, utilizándolos únicamente para necesidades personales o domésticas, no pudiendo utilizar un nuevo responsable este tipo de datos para sus propios fines, como los de mercadotecnia o para enriquecer el perfil del tercero sin su consentimiento (Grupo de Trabajo del Artículo 29, 2017, p. 13).

Resulta una buena práctica por parte de los responsables facilitar las herramientas necesarias para que los interesados decidan los datos que desean recibir, transmitir y excluir (Grupo de Trabajo del Artículo 29, 2017, p. 14), lo que, en nuestra opinión, coadyuvaría a consolidar la autodeterminación informativa de los titulares de los datos y a conseguir el objeto para el que este derecho fue reconocido. Contraria a esta idea es la de la Federación Bancaria Europea (2017, p. 7), pues reflexiona que esta práctica va más allá de la intención del legislador y que en su campo específico, deben establecerse estrategias para prevenir y detectar el lavado de dinero y otras conductas similares, cuestiones a las que la portabilidad de esos datos específicos no abonaría en el cumplimiento del interés legítimo de tratamiento de los datos personales, para lograr las finalidades descritas.

Además de lo anterior, el Grupo de Trabajo del Artículo 29 (2017, p. 9) contempla el caso de que otras leyes de la Unión Europea prevea lo relativo a otros tipos de portabilidad, por lo que el responsable deberá atender con cuidado las solicitudes que reciban y revisar si se refiere a la portabilidad de datos personales con arreglo a la legislación en esa materia o bien, si el interesado o su representante hacen referencia a la de otro sector, en cuyo caso las normas en materia de protección de datos personales no resultan aplicables. Si fuera el caso contrario, la legislación específica aplicable al sector que se trate de ninguna manera anula a la de protección de datos, sino que el derecho deberá garantizarse en ese marco, por lo que sugieren evaluar los casos individuales para saber hasta qué punto la legislación específica puede afectar el ejercicio de este derecho en el contexto de la protección de los datos personales.[45]

[45] Como puede verse ejemplificado en la Resolución N°. R/00552/2019 y el Informe 0195/2017, de la Agencia Española de Protección de Datos, que en su interpretación de los casos sometidos

2.3.3.1 Datos inferidos

Por lo que hace a la información inferida, creada o generada por el responsable del tratamiento de los datos, el Grupo de Trabajo del Artículo 29 (2017, p. 12) considera que tampoco puede ser portada, por lo que lo único que podría proporcionarse al titular son aquellos datos que denominan brutos, es decir, aquellos que no han sido procesados o interpretados en la elaboración de perfiles como consecuencia de su análisis, tales como aquellos que facilite por sí de forma activa y consciente, así como aquellos que se obtienen en virtud del uso o servicio o dispositivo por parte del titular.

En ese sentido, se consideran datos inferidos y deducidos aquellos que, si bien tienen que ver con el titular de los datos, son creados por el responsable a partir de los que este ha proporcionado al inicio de su relación jurídica y, por definición legal, no se encuentran comprendidos entre los que pueden ser considerados al ejercer el derecho de portabilidad. (Vanberg, A., 2018; Grupo de Trabajo del Artículo 29, 2017, p. 12).

Para explicar el origen de los datos, Kuebler-Wachendorff *et al* (2021, p. 265, 266) diferencian entre los obtenidos directamente de su titular, los que pueden ser observados al recopilarse por tecnología de sensores y que Krämer *et al* (2020, p. 8) especifican que dado su origen, muy pocas compañías pueden obtenerlos por el tipo de tecnología que se requiere para ello.

Los inferidos, por otra parte, comprenden los generados a partir de aquellos que se reciben y observan. A su vez, los datos predichos hacen referencia al análisis indirecto de la realidad, resultando en pronósticos de la conducta del titular. Continúan con el segundo supuesto, acerca de la transmisión de la información mediante un formato estructurado, de uso común y de lectura mecánica, que consideran como los requisitos mínimos para facilitar la interoperabilidad de los datos, que debe plantearse para salvar los obstáculos tecnológicos en el ejercicio

a su consideración utilizan como herramientas para precisar el alcance del ejercicio del derecho las legislaciones específicas en materia de telecomunicaciones y bancaria, respectivamente.

del derecho. Así, los datos facilitados por el interesado pueden incluir los que "guarden relación con la actividad del interesado o que se derivan de la observación del comportamiento de una persona, pero no los datos que resultan del análisis posterior de dicho comportamiento" (Grupo de Trabajo del Artículo 29, 2017, p. 12).

Por estas razones, De Hert *et al* (2019, p. 198), Chassang *et al* (2018, p. 298) y Elfering (2019, p. 18) piensan que el análisis para determinar los límites del ejercicio del derecho debería ser casuístico, para diferenciar desde el principio cuáles son los datos susceptibles que portar, con lo cual creemos que deberán implementarse estrategias de privacidad por diseño y defecto para facilitar la tarea. A mayor abundamiento en las conclusiones de su estudio, Kuebler-Wachendorff *et al* (2021, p. 270), explican que sería ampliamente beneficioso aumentar el alcance de los datos que pueden ser portados, incluyendo los inferidos, pues ayudaría a empoderar al titular de los datos y solicitar nuevos servicios o bien, personalizarlos. Deberán tener en cuenta siempre la clasificación de los datos que se traten y efectuando las mejores prácticas para garantizar la seguridad pero también para la agilización del ejercicio del derecho, lo que para ellos incluye la implementación de incentivos, la regulación específica en la materia e incluso, la educación a la población para el mejor aprovechamiento y garantía de este derecho, por lo que, en consecuencia, incentivaría la autodeterminación informativa del titular de los datos, facilitando su transferencia y promoviendo la innovación basada en los datos.

De opinión similar son Urquhart *et al* (2017, p. 322), quienes identifican como beneficios de ampliar el rango de datos objeto de portabilidad fomentar la publicación de literatura especializada acerca de cómo se usan los datos recolectados para generar respuestas o aplicaciones creativas y útiles que permitan su mejor aprovechamiento por parte del usuario, empoderándolo. En sentido contrario opina Deng (2021, p. 378, 379), quien asegura que el alcance de los datos proveídos por el titular o interesado no puede ser dilatado a voluntad, por lo que los datos inferidos por medio de lo que denomina "especulación relevante", derivada de los datos que el interesado proveyó y que son resultado una deducción subjetiva realizada por el proveedor del servicio en

el ejercicio de su profesión y basada en el análisis, no pueden ser considerados como datos personales proporcionados por el interesado. Una opinión similar nos brinda acerca de los datos de terceros que no deberían ser incluidos en la respuesta de la solicitud del ejercicio del derecho.

Gill & Metzger (2022, pp. 7, 9, 10), critican el alcance de los datos que pueden ser objeto de portabilidad, señalando que se trata de una de las grandes insuficiencias del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ya que se encuentra limitado a los datos personales proveídos por el interesado y limitado a la relación contractual, considerando también que existe incertidumbre acerca de los derechos y libertados de terceros.

Para ello, los autores recién citados proponen que el término de datos inferidos también incluya los resultantes de la observación realizada al interesado o inferida de la observación o de los datos que este ha proporcionado conscientemente. Por ejemplo, los observados pueden ser los que el médico obtiene de la auscultación de su paciente y los inferidos, el diagnóstico resultante, ya que como bien señalan en el contexto del ejercicio del derecho a la portabilidad, ¿por qué los datos que pueden salvar la vida de su titular no pueden ser compartidos con terceros?

Bozdag (2018, p. 3-5), explica los retos que la diferenciación de datos brutos o proporcionados por el titular y los inferidos impone para el ejercicio del derecho. Los primeros son recolectados directamente del interesado y deberían ser susceptibles de portabilidad, mientras que los inferidos carecen de este rasgo por mandato de ley. En el caso de los datos de salud, el límite entre ambos tipos se vuelve difuso si el dato es producto de una combinación o incluye otros datos, como ejemplifica con la frecuencia cardiaca y el flujo sanguíneo o la tensión arterial; y argumenta que no está claro si al inferirse del primer dato, deban entonces ser objeto de portabilidad o si lo deban ser si se han recolectado individualmente. En todo caso, ¿cómo se hace esa diferenciación? Consideramos que hacer una anotación en el expediente clínico al respecto es una carga excesiva e innecesaria para el prestador del servicio sanitario.

Tercera parte. El ejercicio del derecho de portabilidad de los datos personales en el contexto del sistema sanitario.

3.1 Derechos tutelados.

3.1.1 Derecho a la protección de la salud.

La Organización Mundial de la Salud desde 1946 (OMS, 2007), conceptualiza a la salud como “un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades".[46]

Identificado como un corolario del derecho a la vida, el derecho a la salud se ha visto cristalizado y consolidado en los ordenamientos constitucionales del siglo XX, pues es fruto de los avances tecnológicos y de la ciencia médica, impactando a diversos aspectos, por ejemplo, la longevidad del ser humano. Valadez (2020, p. 13) estima que las consecuencias no solo influirán a la protección de la salud, sino que impactarán a las materias laboral, educativa, asistencial, habitacional y económica, lo que “obligarán a respuestas jurídicas imaginativas”, dada la dimensión y velocidad con la que los cambios se presentan cotidianamente.

Abunda Carbonell (2013, p. 9) al afirmar que la salud “es un componente determinante del desarrollo económico ya que se trata de un elemento inseparable del capital humano” y una “dimensión fundamental para explicar el bienestar de los seres humanos”, de tal suerte que, si este elemento se encuentra fuera de balance, resulta muy difícil disfrutar de una buena calidad de vida, pues como señala Ruiz (1985, pp. 3,4), “la salud es causa y efecto del desarrollo […] ha sido ámbito en el que se manifiestan las desigualdades que caracterizan a la región (Latinoamérica).”
Coincide Brena (2020, p. 15) al estimar que la salud es consecuencia “de la interacción de diversas variables ambientales, socioeconómicas, psicológicas y biológicas que inciden en el individuo y en la sociedad” por lo que su análisis y protección debe ser multidisciplinario ya que no se trata de un derecho que siendo fundamental se considere autónomo, por lo que resulta de utilidad e

[46]La cita procede del Preámbulo de la Constitución de la Organización Mundial de la Salud, que fue adoptada por la Conferencia Sanitaria Internacional, celebrada en Nueva York del 19 de junio al 22 de julio de 1946, firmada el 22 de julio de 1946 por los representantes de 61 Estados (Official Records of the World Health Organization, Nº 2, p. 100), y entró en vigor el 7 de abril de 1948. La definición no ha sido modificada desde 1948. (Recuperado de OMS. (2017). Preguntas más frecuentes. Febrero 20, 2017, de OMS Sitio web: http://www.who.int/suggestions/faq/es/)

interés que dichas acciones se lleven a cabo desde los diversos enfoques que ofrecen otros derechos tales como a una vida con calidad, a la dignidad, a la autonomía, a la integridad física y mental, a la intimidad o a la información.

Un concepto del derecho a la protección de la salud lo ofrece Moctezuma (2000, p. 17), al referir que "se puede conceptualizar al derecho a la protección de la salud como el sistema de normas jurídicas de derecho social que regula los mecanismos para garantizar la protección de la salud como bien supremo del hombre, a través de la delimitación del campo de la actividad gubernamental, con la finalidad de que sirva de medio para obtener justicia social." Kurzcyn a su vez (2019, pp. 895, 896) considera que la salud es el fundamento mediante el cual se ejercitan y resguardan todos los derechos humanos reconocidos que, mediante su característica de progresividad, indivisibilidad e interdependencia vuelve obligatorio que el Estado provea a través de los medios que considere adecuados, "de las mejores condiciones médicas en términos de calidad, eficacia y eficiencia".

La Suprema Corte de Justicia de la Nación de México (SCJN) (2016, p. 115), ha expresado acerca del derecho a la salud que "…se entiende como la obligación del Estado de establecer los mecanismos necesarios para que todas las personas accedan a los servicios de salud para obtener un determinado bienestar general integrado por el estado físico, mental, emocional y social de la persona, del que deriva el derecho fundamental a la integridad físico-psicológica." Y continúa, afirmado que su completa ejecución es indispensable para que las personas puedan ejercer otros derechos y libertades.

Sin embargo, autores tales como Medina (2016, p. 121) realizan una distinción entre el derecho a la salud y el de protección a la salud. Así, el primero, que considera se refiere a estar saludable, por definición interpreta que se trata de uno de imposible garantía por parte del Estado pues va más allá de sus posibilidades al no depender de este su pleno ejercicio. El segundo, sin embargo, se refiere a la salvaguarda de la salud a través de mecanismos institucionales y jurídicos -garantías primarias y secundarias- para que se pueda atender el

estado de salud de las personas, siendo que entre más alto sea su nivel, considera que más productiva será la sociedad.

En este sentido, la SCJN (2004, p. 40) abunda en la distinción en tanto se trata de un derecho –el de protección de la salud- prestacional positivizado en una norma programática, ya que para satisfacerse es necesario que el Estado preste un bien o un servicio y se encuentra establecido en una norma que dicta los términos en los que el legislador debe basarse para emitir normas secundarias que contienen los mecanismos de ejercicio y posterior garantía, de ser necesaria, por parte de la población. Esta correlación fue expresada en el artículo 25 de la Declaración Universal de Derechos Humanos, en los términos siguientes: “Todo ser humano tiene derecho a un nivel de vida que le permita a él mismo y a su familia gozar de salud y bienestar que incluyan la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios; tiene, asimismo, derecho a la seguridad en caso de desempleo, enfermedad, discapacidad, viudez, vejez u otros casos de pérdida de sus medios de subsistencia por circunstancias ajenas a su voluntad”.

Ferrajoli (2013, p. 395) expone los dos sentidos de este derecho que define como molecular. El primero es el derecho negativo de inmunidad, es decir, se prohíbe lesionar y por tanto se da una abstención de dañar la salud. El otro, positivo, que “dada su universalidad, sólo podrá ser garantizado a todos si sus garantías positivas se encomiendan a la esfera pública”, es decir, como obligaciones aspiracionales o derechos programáticos. De esta manera, considera que la privatización integral de la sanidad “equivale a la verdadera negación, más que a una violación del derecho fundamental a la salud” y que más bien, debería complementarse, que no sustituirse, con prestaciones de tipo privado, en la medida de las posibilidades de cada persona.

Como un derecho bidimensional, pero en sentido individual y social, lo considera la Primera Sala de la Suprema Corte de Justicia de la Nación mexicana, que a través de un criterio jurisprudencial sostiene que “el Estado tiene un interés constitucional en procurarles a las personas en lo individual un adecuado estado de salud y bienestar. Por otro lado, la faceta social o pública del derecho a la

salud consiste en el deber del Estado de atender los problemas de salud que afectan a la sociedad en general, así como en establecer los mecanismos necesarios para que todas las personas tengan acceso a los servicios de salud."[47]

En cuanto al orden jurídico internacional, podemos invocar los artículos 2° de la Convención Americana sobre Derechos Humanos y 10 del Protocolo de San Salvador, que mencionan

> Artículo 2. Deber de adoptar disposiciones de derecho interno.
> Si el ejercicio de los derechos y libertades mencionados en el artículo uno no estuviere ya garantizado por disposiciones legislativas o de otro carácter, los Estados parte se comprometer a adoptar, con arreglo a sus procedimientos constitucionales y a las disposiciones de esta convención, las medidas legislativas o de otro carácter que fueren necesarias para hacer efectivos tales derechos y libertades.

[47] DERECHO A LA PROTECCIÓN DE LA SALUD. DIMENSIONES INDIVIDUAL Y SOCIAL. La protección de la salud es un objetivo que el Estado puede perseguir legítimamente, toda vez que se trata de un derecho fundamental reconocido en el artículo 4o. constitucional, en el cual se establece expresamente que toda persona tiene derecho a la protección de la salud. Al respecto, no hay que perder de vista que este derecho tiene una proyección tanto individual o personal, como una pública o social. Respecto a la protección a la salud de las personas en lo individual, el derecho a la salud se traduce en la obtención de un determinado bienestar general integrado por el estado físico, mental, emocional y social de la persona, del que deriva otro derecho fundamental, consistente en el derecho a la integridad físico-psicológica. De ahí que resulta evidente que el Estado tiene un interés constitucional en procurarles a las personas en lo individual un adecuado estado de salud y bienestar. Por otro lado, la faceta social o pública del derecho a la salud consiste en el deber del Estado de atender los problemas de salud que afectan a la sociedad en general, así como en establecer los mecanismos necesarios para que todas las personas tengan acceso a los servicios de salud. Lo anterior comprende el deber de emprender las acciones necesarias para alcanzar ese fin, tales como el desarrollo de políticas públicas, controles de calidad de los servicios de salud, identificación de los principales problemas que afecten la salud pública del conglomerado social, entre otras. Tesis de jurisprudencia 8/2019 (10a.). Aprobada por la Primera Sala de este Alto Tribunal, en sesión privada de trece de febrero de dos mil diecinueve. Esta tesis se publicó el viernes 22 de febrero de 2019 a las 10:24 horas en el Semanario Judicial de la Federación y, por ende, se considera de aplicación obligatoria a partir del lunes 25 de febrero de 2019, para los efectos previstos en el punto séptimo del Acuerdo General Plenario 19/2013.

Artículo 10 Derecho a la Salud

1. Toda persona tiene derecho a la salud, entendida como el disfrute del más alto nivel de bienestar físico, mental y social.
2. Con el fin de hacer efectivo el derecho a la salud los Estados parte se comprometen a reconocer la salud como un bien público y particularmente a adoptar las siguientes medidas para garantizar este derecho:

a. la atención primaria de la salud, entendiendo como tal la asistencia sanitaria esencial puesta al alcance de todos los individuos y familiares de la comunidad;
b. la extensión de los beneficios de los servicios de salud a todos los individuos sujetos a la jurisdicción del Estado;
c. la total inmunización contra las principales enfermedades infecciosas;
d. la prevención y el tratamiento de las enfermedades endémicas, profesionales y de otra índole;
e. la educación de la población sobre la prevención y tratamiento de los problemas de salud, y
f. la satisfacción de las necesidades de salud de los grupos de más alto riesgo y que por sus condiciones de pobreza sean más vulnerables.

La Suprema Corte de Justicia de la Nación (2016, p. 116) incluso sostiene que el Estado Mexicano debe proporcionar protección especial a quienes se encuentran en vulnerabilidad por su situación de salud, a través de instalaciones en servicios de salud pública de calidad, “que disminuyan cualquier amenaza al derecho a la vida y a la integridad física”, como sería que exista el riesgo de contagiarse por enfermedades oportunistas.

En cuanto a lo que el numeral 12 del Pacto Internacional de Derechos Económicos, Sociales y culturales de 1966, establece, el máximo tribunal mexicano (2016, p. 116) ha interpretado que dado que el Estado mexicano lo ha ratificado y es parte, le impone obligaciones inmediatas para asegurar a la

población un nivel esencial del derecho a la salud y su cumplimiento progresivo para alcanzar su ejercicio pleno "por todos los medios apropiados, hasta el máximo de recursos que disponga", ya que se trata de un derecho cuyo disfrute permite alcanzar un estado de bienestar general, que incluye diversas variantes de bienes, servicios y condiciones para alcanzarlo, tales como acceso al agua limpia y potable, acceso a alimentos sanos y adecuados, vivienda, condiciones salubres en el espacio laboral y acceso a la educación e información sobre cuestiones relacionadas con la salud.

El artículo 12 en cita ha sido objeto también, de la Observación General 14[48] del Comité de Derecho Económicos, Sociales y Culturales de la ONU (2000) que

[48] Al respecto, el Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito mexicano, se ha pronunciado acerca de la forma idónea de cumplirla en el contexto nacional mediante la siguiente tesis aislada: DERECHO A LA SALUD. FORMA DE CUMPLIR CON LA OBSERVACIÓN GENERAL NÚMERO 14 DEL COMITÉ DE LOS DERECHOS SOCIALES Y CULTURALES DE LA ORGANIZACIÓN DE LAS NACIONES UNIDAS, PARA GARANTIZAR SU DISFRUTE. El Estado Mexicano suscribió convenios internacionales que muestran el consenso internacional en torno a la importancia de garantizar, al más alto nivel, ciertas pretensiones relacionadas con el disfrute del derecho a la salud, y existen documentos que las desarrollan en términos de su contenido y alcance. Uno de los más importantes es la Observación General Número 14 del Comité de los Derechos Sociales y Culturales de la Organización de las Naciones Unidas, organismo encargado de monitorear el cumplimiento de los compromisos asumidos por los Estados firmantes del Pacto Internacional de Derechos Económicos, Sociales y Culturales, del cual México es parte y el que, esencialmente, consagra la obligación de proteger, respetar y cumplir progresivamente el derecho a la salud y no admitir medidas regresivas en su perjuicio, absteniéndose de denegar su acceso, garantizándolo en igualdad de condiciones y sin condicionamiento alguno, debiendo reconocer en sus ordenamientos jurídicos, políticas y planes detallados para su ejercicio, tomando, al mismo tiempo, medidas que faciliten el acceso de la población a los servicios de salud, es decir, este ordenamiento incluye no solamente la obligación estatal de respetar, sino también la de proteger y cumplir o favorecer este derecho. En estas condiciones, ese cumplimiento requiere que los Estados reconozcan suficientemente el derecho a la salud en sus sistemas políticos y ordenamientos jurídicos nacionales, de preferencia mediante la aplicación de leyes, adoptando una política nacional de salud acompañada de un plan detallado para su ejercicio, cuando menos en un mínimo vital que permita la eficacia y garantía de otros derechos, y emprendan actividades para promover, mantener y restablecer la salud de la población, entre las que figuran, fomentar el reconocimiento de los factores que contribuyen al logro de resultados positivos en materia de salud; verbigracia, la realización de investigaciones y el suministro de información, velar porque el Estado cumpla sus obligaciones en lo referente a la difusión de información apropiada acerca de la forma de vivir y de alimentación sanas, así como de las prácticas tradicionales nocivas y la disponibilidad de servicios, al igual que apoyar a las personas a adoptar, con conocimiento de causa, decisiones por lo que respecta a su salud.
CUARTO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO. Amparo en revisión 19/2013. Juan de la Paz Jiménez y otro. 30 de mayo de 2013. Unanimidad de votos. Ponente: Jesús Antonio Nazar Sevilla. Secretaria: Ángela Alvarado Morales. Nota: Por ejecutoria del 23 de noviembre de 2016, la Segunda Sala declaró inexistente la contradicción de tesis 120/2016 derivada de la denuncia de la que fue objeto el criterio contenido en esta tesis, al estimarse que no son discrepantes los criterios materia de la denuncia respectiva. Datos de localización: publicación en el Semanario Judicial de la Federación y su Gaceta, Décima Época,

aborda la definición de aspectos fundamentales del derecho a la salud, enfatizándose en este texto aquéllos con injerencia directa en el tema que se estudia.

Como ya se dijo, el derecho a la salud tiene un contenido muy extenso que da pie a variadas acciones o conductas de omisión en aras de garantizarlo, pero se auxilia del ejercicio de otros derechos fundamentales que le sirven de instrumento para su garantía plena. De esta suerte, como el Comité lo menciona, el derecho a la salud no se entiende como el derecho a estar sano, sino como el derecho al disfrute de toda una variedad de beneficios, bienes, servicios y condiciones necesarios para alcanzar el más alto nivel posible de disfrute de este derecho. En consecuencia, enfatiza el Comité en el párrafo ocho, no es correcto que se considere únicamente como el derecho a estar sano.

Por ello, vale la pena detenerse en lo que Ferrajoli (2013, p. 293) insiste acerca de la efectividad del derecho a la salud que no puede, ni debe, "limitar a prever diagnósticos y tratamientos preventivos de carácter público y gratuito" ya que al tratarse de un derecho por demás complejo, encuentra múltiples expresiones para su garantía, verbigracia, a ser tratado adecuadamente, al acceso a servicios de salud convenientes, a ser informado acerca del pronóstico diagnóstico y tratamiento, en su caso; a participar en las decisiones terapéuticas, a expresar el consentimiento informado, a ser resarcido por eventuales daños e incluso, a morir con dignidad.

Ahora bien, regresando a lo que el Comité de Derecho Económicos, Sociales y Culturales de la ONU (2000, párrafo 12) señala en la recomendación de mérito, es claro en que el derecho a la salud goza de las características de disponibilidad, es decir, que cada Estado debe contar con un número suficiente de establecimientos, bienes y servicios públicos, centros de atención y programas de salud. De accesibilidad, cuando todo lo anterior resulta asequible a cualquier persona sin mediar discriminación y con facilidades geográficas y

libro XXV, tesis aislada I. 4o. A, 86 A, Tribunal Colegiado de Circuito, t. 3, octubre de 2013, p. 1759.

económicas. De aceptabilidad, si resultan respetuosos de la ética médica y culturalmente apropiados y adaptados al entorno donde se ofrezcan, respetando en todo momento la confidencialidad e intimidad de los usuarios del sistema de salud; finalmente de calidad, ya que además de los considerado en la característica anterior, los servicios médicos serán apropiados desde el punto de vista científico.

En el mismo párrafo considera también ciertos aspectos que deben atenderse para considerar que el Estado atiende correctamente la diferencia entre hombres y mujeres en el ámbito de la salud: los factores biológicos, socioeconómicos y la falta de respeto a la confidencialidad de la información médica, la cual, puede disuadir a la mujer de acudir a consulta. Lo anterior afecta negativamente en la atención médica que tiene que ver con el tratamiento de enfermedades de los órganos genitales, la utilización de métodos anticonceptivos o la atención de abortos incompletos o si ha sido víctima de violencia sexual.

En ese entendido, considera el Comité (2000, párrafo 14) que deben adoptarse medidas tendientes a garantizar la salud materna, reproductiva e infantil y las concernientes preventivas de accidente laborales y enfermedades profesionales (párrafo 15). En cuanto a la prevención de enfermedades y de forma directamente relacionada con la materia de esta investigación, se pronuncia a favor del establecimiento de programas de educación en salud (2000, párrafo 16) como una forma de garantizar el derecho de acceso a la información en esta materia. Todo ello, enmarcado en un ambiente sin discriminación[49] (2000, párrafo 19).

[49] El Pleno de la Suprema Corte de Justicia de la Nación Mexicana se pronunció a este respecto mediante la tesis aislada, publicada en el Tomo XXXIV del Semanario Judicial de la Federación y su Gaceta de agosto de 2011 en la página 29, que a continuación se reproduce: DERECHO A LA SALUD. IMPONE AL ESTADO LAS OBLIGACIONES DE GARANTIZAR QUE SEA EJERCIDO SIN DISCRIMINACIÓN ALGUNA Y DE ADOPTAR MEDIDAS PARA SU PLENA REALIZACIÓN. Del artículo 4o. de la Constitución Política de los Estados Unidos Mexicanos, según el cual toda persona tiene derecho a la salud, derivan una serie de estándares jurídicos de gran relevancia. El Estado Mexicano ha suscrito convenios internacionales que muestran el consenso internacional en torno a la importancia de garantizar al más alto nivel ciertas pretensiones relacionadas con el disfrute de este derecho, y existen documentos que esclarecen su contenido y alcance jurídico mínimo consensuado. Así, la Observación General número 14 del Comité de Derechos Económicos, Sociales y Culturales de la Organización de las Naciones Unidas, por ejemplo, dispone que el derecho a la salud garantiza pretensiones en términos de

Un tema especialmente importante es el que en el párrafo 32 enuncia acerca del principio de no regresividad[50]. Así el Comité de Derecho Económicos, Sociales y Culturales de la ONU (2000) únicamente consideraría justificable la aplicación de una medida regresiva siempre que el Estado acredite el estudio de cada opción disponible y que no resulta adecuada su aplicación. También deberán cuidarse de prohibir o impedir los cuidados preventivos, las prácticas curativas y

disponibilidad, accesibilidad, no discriminación, aceptabilidad y calidad de los servicios de salud y refiere que los poderes públicos tienen obligaciones de respeto, protección y cumplimiento en relación con él. Algunas de estas obligaciones son de cumplimiento inmediato y otras de progresivo, lo cual otorga relevancia normativa a los avances y retrocesos en el nivel de goce del derecho. Como destacan los párrafos 30 y siguientes de la Observación citada, aunque el Pacto Internacional de Derechos Económicos, Sociales y Culturales prevé la aplicación progresiva y reconoce los obstáculos que representa la limitación de los recursos disponibles, también impone a los Estados obligaciones de efecto inmediato, como por ejemplo las de garantizar que el derecho a la salud sea ejercido sin discriminación alguna y de adoptar medidas para su plena realización, que deben ser deliberadas y concretas. Como subraya la Observación, la realización progresiva del derecho a la salud a lo largo de un determinado periodo no priva de contenido significativo a las obligaciones de los Estados, sino que les impone el deber concreto y constante de avanzar lo más expedita y eficazmente posible hacia su plena realización. Al igual que ocurre con los demás derechos enunciados en el Pacto referido, continúa el párrafo 32 de la Observación citada, existe una fuerte presunción de que no son permisibles las medidas regresivas adoptadas en relación con el derecho a la salud.
Amparo en revisión 315/2010. Jorge Francisco Balderas Woolrich. 28 de marzo de 2011. Mayoría de seis votos. Disidentes. Sergio Salvador Aguirre Anguiano, Margarita Beatriz Luna Ramos, Jorge Mario Pardo Rebolledo, Luis María Aguilar Morales y Guillermo I. Ortiz Mayagoitia. Ponente: José Ramón Cossío Díaz. Secretarias: Francisca María Pou Giménez, Fabiana Estrada Tena y Paula María García Villegas Sánchez Cordero. El Tribunal Pleno, el cuatro de julio en curso, aprobó, con el número XVI/2011, la tesis aislada que antecede. México, Distrito Federal, a cuatro de julio de dos mil once.

[50] Nuevamente, el Alto Tribunal mexicano, a través de su Segunda Sala y mediante tesis aislada, se pronuncia acerca de las condiciones de garantía del derecho a la salud, al nivel más alto posible: SALUD. DERECHO AL NIVEL MÁS ALTO POSIBLE. ÉSTE PUEDE COMPRENDER OBLIGACIONES INMEDIATAS, COMO DE CUMPLIMIENTO PROGRESIVO. El artículo 2 del Pacto Internacional de Derechos Económicos, Sociales y Culturales prevé obligaciones de contenido y de resultado; aquéllas, de carácter inmediato, se refieren a que los derechos se ejerciten sin discriminación y a que el Estado adopte dentro de un plazo breve medidas deliberadas, concretas y orientadas a satisfacer las obligaciones convencionales, mientras que las de resultado o mediatas, se relacionan con el principio de progresividad, el cual debe analizarse a la luz de un dispositivo de flexibilidad que refleje las realidades del mundo y las dificultades que implica para cada país asegurar la plena efectividad de los derechos económicos, sociales y culturales. En esa lógica, teniendo como referente el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental contenido en el artículo 12 del citado Pacto, se impone al Estado Mexicano, por una parte, la obligación inmediata de asegurar a las personas, al menos, un nivel esencial del derecho a la salud y, por otra, una de cumplimiento progresivo, consistente en lograr su pleno ejercicio por todos los medios apropiados, hasta el máximo de los recursos de que disponga. De ahí que se configurará una violación directa a las obligaciones del Pacto cuando, entre otras cuestiones, el Estado Mexicano no adopte medidas apropiadas de carácter legislativo, administrativo, presupuestario, judicial o de otra índole, para dar plena efectividad al derecho indicado. Amparo en revisión 378/2014. Adrián Hernández Alanís y otros. 15 de octubre de 2014. Mayoría de tres votos de los Ministros Alberto Pérez Dayán, José Fernando Franco González Salas y Luis María Aguilar Morales. Ausente: Sergio A. Valls Hernández. Disidente: Margarita Beatriz Luna Ramos. Ponente: Alberto Pérez Dayán. Secretaria: Georgina Laso de la Vega Romero. Gaceta del Semanario Judicial de la Federación. Libro 12, noviembre de 2014, Tomo I, página 1192.

las medicinas tradicionales, lo que no significa que se deba tolerar la venta de medicamentos peligrosos[51] o la aplicación de tratamientos coercitivos, salvo casos en los que se justifique plenamente. Tampoco deberán limitarse el acceso a tratamientos anticonceptivos ni la participación de la población en los asuntos de la materia (Comité de Derecho Económicos, Sociales y Culturales de la ONU, 2000, párrafo 34).

Por lo que hace a la obligación de cumplimiento del Estado en sentido de facilitar el acceso a los servicios de salud, el Comité de Derecho Económicos, Sociales y Culturales de la ONU (2000) establece como medidas pertinentes las de garantizar la atención de la salud, lo que incluiría a la inmunización, aquellos factores determinantes para la conservación de la salud como la alimentación

[51] Sirva como ejemplo las consideraciones vertidas en la sentencia de la Corte Europea de los Derechos humanos dictada para el asunto Hristozov y otros contra Bulgaria, cuya versión final fue publicada el 29 de abril de 2013. En ella "los demandantes […] tratan de argumentar que, debido al pronóstico grave de su condición médica, se les debería haber permitido asumir los riesgos asociados a un producto experimental que podría salvarles la vida", interés que el tribunal considera como "la libertad de optar, como una medida a adoptar como último recurso, a un tratamiento no probado que puede conllevar riesgos, pero que los demandantes y sus médicos consideran apropiados dadas sus circunstancias, en un intento por salvar sus vidas". De los argumentos de la resolución, destaca particularmente que "actualmente, existe una tendencia clara en los Estados contratantes, a permitir bajo ciertas condiciones y de una forma excepcional, el uso de medicamentos no autorizados. Sin embargo, ese consenso no se basa en los principios establecidos en la legislación de los Estados parte. Tampoco parece extenderse a la forma precisa en que este uso debe ser regulado". Y de que "[…] el margen de apreciación que debe otorgarse al Estado demandado debe ser amplio, especialmente en lo que respecta a las disposiciones que se aprueban con el fin de lograr un equilibrio entre los intereses públicos y privados. Las autoridades búlgaras han optado por equilibrar los intereses contrapuestos, permitiendo a los pacientes que no pueden ser tratados satisfactoriamente con medicamentos autorizados, incluyendo a aquellos pacientes con enfermedades terminales como los demandantes, a obtener, en determinadas condiciones, medicamentos que no han sido autorizados en Bulgaria, pero que si han sido autorizados en otros países […]. Al parecer, este fue el motivo, por el que la Agencia de Medicamentos rechazó la petición de los demandantes […]. Esta solución inclina la balanza entre el potencial beneficio terapéutico y el riesgo del medicamento, a favor de este último, ya que los medicamentos autorizados en otro país, probablemente ya se hayan sometido a pruebas de seguridad y eficacia. Al mismo tiempo, esta solución, dejan a los medicamentos que aún se encuentran en diversas etapas de desarrollo, totalmente inaccesibles. En vista del amplio margen de apreciación de las autoridades en este ámbito, el Tribunal considera que […] no es tarea de un tribunal internacional, señalar a las autoridades nacionales competentes, el nivel de riesgo que es aceptable en tales circunstancias". Finalmente, la demanda fue declarada inadmisible. Para consultar la resolución completa, visitar: https://tinyurl.com/4k5z77es

adecuada, agua potable, servicios básicos de saneamientos y vivienda, así como condiciones de vida adecuada.
Sin embargo, también considera fundamental la formación apropiada y suficiente de facultativos en la materia y también el establecimiento de un sistema de salud público, privado o mixto. En el caso mexicano se cuenta con un sistema nacional que incluye a los sectores público, privado y social y cuyo análisis en comparación con el español será objeto de páginas posteriores de este capítulo. No menos importante se considera incentivar las investigaciones médicas, así como nuevamente, los programas de educación en salud y las campañas de información, todo lo que se incluye en el párrafo 36. (Comité de Derecho Económicos, Sociales y Culturales de la ONU, 2000)

Ahora bien en el sentido de promover, la obligación de cumplimiento se explica en el párrafo 37 de la recomendación, a través de la importancia de la promoción de medidas positivas por parte del Estado, que incluirán, entre otras, "fomentar la realización de investigaciones y el suministro de información" y la de "apoyar a las personas a adoptar, con conocimiento de causa, decisiones por lo que respecta a su salud", lo que consideramos podrá lograrse además con la mejora de la relación prestador-usuario, ambos del sistema de salud, si se vuelven eficientes los mecanismos de acceso al expediente clínico, situación de la que se expondrá su importancia en páginas sucesivas de esta investigación. (Comité de Derecho Económicos, Sociales y Culturales de la ONU, 2000)

Además de las señaladas, entre las obligaciones del Estado que resultan prioritarias se señalan en el párrafo 44, la de impartir educación y proporcionar acceso a la información relativa a los principales problemas de salud en la comunidad, con inclusión de los métodos para prevenir y combatir esas enfermedades y la de proporcionar capacitación adecuada al personal del sector salud, incluida la educación en materia de salud y derechos humanos. (Comité de Derecho Económicos, Sociales y Culturales de la ONU, 2000)

Ambas coadyuvan en el logro de la descrita en el párrafo anterior, y por medio de su desarrollo se privilegia la creación de conciencia del personal de salud y también del paciente, de que poseen derechos que pueden ejercer y sus

obligaciones para cumplir de manera mutua y en un ámbito de respeto a su contraparte y a las disposiciones legales que rigen su comportamiento. Resulta natural que una de las violaciones que establece el Comité es la de la ocultación deliberada de la información que reviste importancia fundamental para la protección de la salud o para el tratamiento (Comité de Derecho Económicos, Sociales y Culturales de la ONU, 2000, párrafo 50).

Se resalta la importancia de contar con una legislación marco, que otorgue mayor efectividad a la estrategia nacional para hacer realidad el derecho a la salud; esa normativa debe comprender cualquier aspecto relacionado y no sólo remitir en cada una de ellas a la legislación aplicable en la materia, evitando generar confusiones entre quienes pretenden ejercer los derechos, o bien buscar la aplicación de la ley (Comité de Derecho Económicos, Sociales y Culturales de la ONU, 2000, párrafo 56).

3.1.1.2 Orden jurídico mexicano

En México, el artículo 4° de la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917, además de garantizar el derecho de cualquier persona que se encuentre en el país y no cuente con seguridad social, a recibir de forma gratuita la prestación de servicios públicos de salud, medicamentos y cualquier insumo necesario al momento de requerir la atención, sin importar su condición social; ordena al legislador definir las bases y modalidades para el acceso a los servicios de salud a través de la legislación secundaria, así como la concurrencia entre la Federación y las entidades federativas en materia de salubridad general:

> *Artículo 4°. [...]*
> *Toda persona tiene derecho a la protección de la salud. La Ley definirá las bases y modalidades para el acceso a los servicios de salud y establecerá la concurrencia de la Federación y las entidades federativas en materia de salubridad general, conforme a lo que dispone la fracción XVI del artículo 73 de esta Constitución.*

Igualmente dispone, en el artículo 2°, apartado B, la obligación de asegurar el acceso efectivo a los servicios de salud de los pueblos indígenas. En otro orden de ideas, la Ley reglamentaria del artículo 4° Constitucional es la General de Salud, de 7 de febrero de 1984 y en el ámbito de lo local, las Leyes de Salud promulgadas en cada entidad federativa, estableciendo estas últimas las facultades que la entidad posee atendiendo a la concurrencia de acuerdo al artículo 124 de la Constitución Federal, es decir, que las facultades que no se concedan por esta a los funcionarios federales se entienden reservadas en virtud del principio de subsidiariedad a las entidades federativas o a la Ciudad de México, en el ámbito de la competencia de cada uno.

Estas legislaciones establecen como finalidades del derecho a la protección de la salud:

- El bienestar físico y mental del hombre para contribuir al ejercicio pleno de sus capacidades.
- La prolongación y el mejoramiento de calidad de la vida humana.
- La protección y el acrecentamiento de los valores que coadyuven a las condiciones de salud y que contribuyan al desarrollo social.
- La extensión de actitudes solidarias y responsables de la población para la preservación conservación, mejoramiento y restauración de la salud.
- El disfrute de los servicios que satisfagan las necesidades de la población y el desarrollo de la enseñanza y la investigación científica y tecnológica para la salud.

3.1.1.3 Orden jurídico comunitario y español

En el marco jurídico español, el derecho a la salud se encuentra previsto desde la Constitución de 1978[52] en su artículo 43:

[52] En la misma disposición normativa podemos encontrar positivizado la obligación de los poderes públicos de garantizar un sistema de servicios de salud a los ciudadanos durante la tercera edad (artículo 50), así como la salud y defensa de los consumidores (artículo 51).

1. Se reconoce el derecho a la protección de la salud.
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.
3. Los poderes públicos fomentarán la educación sanitaria, la educación física y el deporte. Asimismo, facilitarán la adecuada utilización del ocio. (sic)

A su vez, en el artículo 149.1. 16.ª del mismo ordenamiento, se establece la competencia exclusiva del Estado Español para establecer las bases y coordinación general en materia de sanidad.[53]

Por su parte, la Ley 14/1986, de 25 de abril, General de Sanidad, es la que tiene por objeto la regulación de cualquier acción que haga efectivo el derecho a la protección de la salud reconocido en el artículo de la Constitución General ya citado.

No obstante lo señalado la modificación de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud llevada a cabo a través del Real Decreto-ley 7/2018, de 27 de julio, sobre el acceso universal al Sistema Nacional de Salud, a través de su primer artículo modifica al 3 de la segunda norma señalada en la que, si bien es cierto que se reconoce como titulares a los mismos sujetos señalados en la legislación general, considera que aquellas personas que cuenten con el derecho de asistencia sanitaria en España, podrán ejercer su derecho de acceso en cumplimiento de los reglamentos comunitarios de coordinación de sistemas de Seguridad Social o de los convenios bilaterales que aborden el tema siempre que residan en el territorio o bien, en sus desplazamientos temporales, con las condiciones que esas normas jurídicas establezcan.

[53] Las competencias en esta materia están transferidas a las Comunidades Autónomas, lo que explicamos con amplitud en el epígrafe 3.3.2 El Sistema Nacional de Salud Español.

Este mismo Real Decreto-ley, establece que estos derechos podrán hacerse efectivos con cargo a los fondos públicos si el sujeto se encuentra en alguno de los siguientes supuestos, a saber: tener nacionalidad española y residencia habitual en territorio español; tener reconocido su derecho a la asistencia sanitaria en el país por cualquier otro título jurídico, aunque su residencia habitual no se encuentre en el país y siempre que un tercero no se encuentre obligado a su pago; finalmente, si se trata de una persona extranjera con residencia habitual y legal en España, que no tenga la obligación de acreditar la cobertura obligatoria de esta prestación por otra vía.

Quienes no se encuentren en los supuestos mencionados, pueden beneficiarse de esta prestación siempre que otorguen los emolumentos correspondientes por el servicio recibido, derivada de la suscripción de un convenio especial. Las personas con régimen de asistencia sanitaria beneficiarios de los regímenes especiales de la Seguridad Social mantendrán su régimen jurídico específico.

3.1.2 Derecho a la protección de datos personales.

3.1.2.1 Antecedentes. La intimidad y la privacidad.

El Diccionario de la Real Academia Española define a la intimidad como una "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia". A su vez, la privacidad la conceptualiza como "cualidad de privado" o bien, el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". Por otra parte, el Diccionario Oxford precisa que la voz intimidad hace referencia a "tener una relación cercana y personal con alguien"; y el vocablo privacidad, "al estado de encontrarse solo y no ser observado o interrumpido por otras personas", lo que sin duda nos recuerda a la tesis de Warren y Brandeis presentada en la revista Harvard Law Review, en 1890.

Es lo que Rodotà (2018, p. 89), considera como el *human enhacement*, es decir, el desarrollo de la condición humana "gracias a la eliminación de vínculos naturales y culturales que hace posible la ciencia, como una extensión de las oportunidades de la vida". Ya en 1976 (p. 135), el autor nos advertía que "el

cambio de motivación modifica el significado de la reivindicación de privacidad: en el primer caso, al negar la información necesaria para promover acciones sociales la privacidad aparece como un instrumento para potenciar los privilegios de un grupo; en el segundo, sirve para reaccionar contra autoritarismo y contra una política de discriminación basada en opiniones (o religiosas, gremiales, raciales, etc.). La privacidad, de esta manera, se convierte en un medio para permitir que todos los ciudadanos sean tratados por igual, de promover la igualdad y no de proteger los privilegios, rompiendo así por el vínculo identificador con la clase burguesa."

Como parte inherente al derecho a la intimidad consideramos a la identidad, que "se configura como el derecho a ser uno mismo y diferente a los demás", coincidiendo con la definición de Piñar (2018, p. 96). Así, el ser humano se identifica en el mundo físico a través de una serie de datos que lo proveen de una identidad pública, que lo diferencia de sus congéneres, siendo de tal importancia poseerla que sin ella se carece de personalidad y por lo tanto de derechos, según el autor señalado, por lo que "contar con una identidad es presupuesto para la propia dignidad de la persona, para ser titular de derechos y obligaciones, para tener una existencia en el mundo del Derecho y por lo tanto en el de los derechos". (Piñar, 2018, p. 96)

De esta forma, la intimidad será la interioridad de la persona, como disposición peculiar del ser humano a la introspección, a lo recóndito y secreto. La intimidad se identifica con la soledad y el aislamiento. Por ello, si su definición se amplía hasta llegar a la convivencia con otros, es cuando se considera jurídicamente relevante, pues el concepto original se limita a la soledad del individuo y el auto confinamiento personal y en todo caso, la conducta desplegada no afectaría la esfera jurídica de personas distintas al que ejerce ese derecho a la intimidad (Pérez Luño, 2012, p. 77).

Piñar (2018, pp. 98, 99) además, cree que existe una tensión entre la identidad pública que se nos da y la privada que asumimos, producto de "… los intentos del poder por controlar, definir y tergiversar la identidad de las personas y la lucha del ser humano por alcanzar la propia identidad. Los poderes públicos, no

siempre dictatoriales, se ha valido de la posibilidad de alterar, tergiversar o manipular la identidad de las personas para convertirlas en amigos o enemigos. […] El poder se basa en saber todo del otro […] y en que se sepa lo menos posible de quien lo ostenta, del que además se diseña una identidad inventada al objeto de doblegar el conocimiento de los súbditos."

Recordemos que, siendo una creación misma del ser humano, artificial, producto del pacto social que se ha creado para facilitar la convivencia pacífica y organizada, las normas jurídicas por las que se rige la humanidad idealmente deberán proyectar la libertad en tres sentidos que nos explica Bobbio (1991, p. 44) siempre que cuente con una esfera de actividad personal protegida contra la injerencia de todo poder externo, en particular del poder estatal; debe participar de manera indirecta o directa en la formación de las normas que deberán posteriormente regular su conducta en la esfera que no constituye su intimidad y finalmente, debería tener el poder de traducir en comportamientos concretos los abstractos que se han previsto en las normas constitucionales.

Así, de acuerdo con Bobbio, (1991, p. 122) "también la esfera de los derechos de libertad se ha ido modificando y extendiendo por efecto de innovaciones técnicas en el campo de la transmisión y difusión de las ideas y de las imágenes, y en relación con el posible abuso que de ellas se puede hacer y que era inconcebible cuando el mismo uso no era posible o técnicamente difícil. Y continúa Rodotà (1976, p. 139): "Se llega así a otro problema. ¿Qué tipo de control? Es evidente que en el panorama que hemos indicado la posibilidad de control no sólo sirve para tranquilizar a cada ciudadano en cuanto a la precisión y el uso correcto de los datos que le conciernen directamente, pero puede convertirse en un instrumento de equilibrio en la nueva distribución del poder que empieza a surgir. Este último resultado, sin embargo, no se lograría si la perspectiva de control se mantuviera solo de carácter individualista, limitándose todo el asunto a conceder ciudadanos individuales el derecho de acceso a grandes bienes públicos y archivos privados."

La visión cerrada de intimidad, identificada con el *ius solitudinis*, ha sido sustituida por una concepción activa y dinámica en la que se le entiende como

la posibilidad de conocer, acceder y controla las informaciones que conciernen a cada persona (Pérez Luño, 2012, p. 79). Es decir, como Valdez (2012, p. 76), señala con acierto, que "el derecho a la intimidad tiene por objeto la autodeterminación afirmativa".

Tenorio y Rivero (2012, p. 54) señalan que la autodeterminación informativa consiste "en el control y manejo de la información personal de manera autónoma e independiente por parte de los individuos"[54]. Al respecto, Piñar (2018, p. 97), refiere que "hay una identidad que se define en función de los elementos que cada uno quiere que se resalten o le definan" y la persona, a través de la privacidad, mantiene, reivindica o hace valer la identidad que nos representa o la que se posee en realidad. En sus palabras, "la privacidad permite controlar mi yo y expresar el yo que quiero transmitir a los demás" (Piñar, 2018, p. 98), por lo que la decisión acerca de lo que se trasluce de la propia vida está en manos del individuo que la vive.

Por ejemplo, Lara *et al* (2014, p. 13) clasifican a la privacidad en corporal, territorial, comunicacional, de la información o de protección de datos personales, de acuerdo con los ámbitos donde el ser humano se desarrolla y que además sirve para delimitar la esfera de su protección en dos ámbitos, el primero al retirar del ámbito público algunas "conductas, o manifestaciones de la persona, ya sea por su propia voluntad, por la ley o por la costumbre" y en segundo lugar si concurre un daño que sea inminente y conocido de suceder por la comunicación de esas conductas.

El acto de ser de una persona es tan intenso que resulta imposible que se le confunda con otros, por lo que su individualidad no se refiere a la intimidad en el

[54] Resulta interesante rescatar la clasificación de las preferencias fundamentales que, en respuesta al ensayo de Bobbio "Sobre el fundamento de los derechos humanos" realiza Giuliano Pontara (en Bobbio, 1991, p. 87), en la que las describe como aquellas condiciones necesarias para perseguir la satisfacción de cualquier otra o la realización de cualquier valor, fin o valor que se precise tener. Así, enumera a la preferencia de vivir más que la de no vivir; la de no ser sometido a graves sufrimientos gratuitos a más de la que ser sometido y la que interesa para efectos de este texto, la de poder decidir las preferencias de cada uno de forma autónoma y de perseguir su propia satisfacción sin ser sometidos a amenazas de frustración de estas tres preferencias fundamentales, sin amenaza a la propia vida, a la propia vida, a la propia salud y autonomía.

sentido de solitud que se ha señalado, si no a un carácter personal de ser, de no confundirse con otro individuo[55]. Así, la "identidad propia, la real en una democracia, o la que atribuye tasadamente la ley, es parte esencial del libre desarrollo de la personalidad y la dignidad humana" (Piñar, 2018, p. 100).

En el mismo sentido el Poder Judicial de la Federación de los Estados Unidos Mexicanos emitió la siguiente tesis aislada en materia civil, identificada con el número 168944[56], que en lo que nos interesa dice que "[…] tal derecho (el de la intimidad) atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia; asimismo garantiza el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia; lo que se traduce en el derecho de la autodeterminación de la información que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizar esa información." Así el derecho fundamental a la intimidad garantiza la libre expresión de la personalidad, que la persona pueda ser auténtica, fiel a sí misma, a sus convicciones y de esta forma alcanzar la plenitud del ser.

Troncoso (2020, p. 46), identifica claramente varias dimensiones de este derecho de autodeterminación informativa, como lo ha concebido el Tribunal Constitucional Federal Alemán:

1. Como derecho de estatus negativo, en tanto que su finalidad es evitar la recopilación de los datos por el aparato estatal.
2. Como derecho de libertad al oponerse a los tratamientos que lleven a cabo los poderes públicos.

[55] Sin embargo, Piñar (2018, p. 99) comenta, a propósito de las identidades falsas, que "condicionan la relación con el otro. La democracia se basa en que la identidad oficialmente pública esté configurada por los menos elementos posibles, mientras que la privada puede ser tan limitada o tan extensa como cada persona decida sin que por ello puedan derivarse consecuencias negativas para ella" (sic)

[56] DERECHO A LA INTIMIDAD. SU OBJETO Y RELACIÓN CON EL DERECHO DE LA AUTODETERMINACIÓN DE LA INFORMACIÓN. Localización: Novena Época. Instancia: Tribunales Colegiados de Circuito de los Estados Unidos Mexicanos. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación y su Gaceta. Tomo XXVIII, septiembre de 2008. Materia(s): Civil. Tesis: I.3o. C.695.

3. Como derecho fundamental, con un carácter defensivo, pero con dimensión objetiva e institucional para dotar al Estado de la obligación de impedir a través de la aprobación del marco jurídico, que se recopilen datos personales.[57]

En el mismo sentido fueron establecidos los principios básicos de la Comisión de Estudio sobre la Protección de la Intimidad creada en 1974 en los Estados Unidos, que interpretadas por Rebollo (2003, p. 223) indican:

1. Todo individuo tiene derecho a acceder a la información personal que le afecte, y especialmente a aquella que se encuentra en bancos de datos informatizados.
2. Todo individuo ha de tener la posibilidad y el derecho a controlar, de forma razonable, la transmisión de la información personal que le afecte.
3. La norma ha de regular necesariamente como garantía del derecho a la intimidad:
    a. El tiempo de conservación de los datos personales
    b. Las finalidades de tratamiento.
    c. Las garantías de calidad de la información (veracidad, integridad y actualidad).
    d. La prohibición de su revelación.

Adalbert Podlech (citado por Pérez Luño, 2012, p. 80), defiende que la intimidad, más que un estado de auto confinamiento supone una determinada calidad de la relación con los otros. Es decir, que se trata de una condición o calidad social de la persona, que es objeto de tutela constitucional en la medida en que ésta puede tener legítimo derecho a no revelar a los demás determinados aspectos de sus relaciones con otras personas, que el titular del derecho juzga deben permanecer en un plano reservado o privado, lo que constituye el núcleo de la

[57] Y añadiríamos, que más que evitar que se recopile esta información que resulta necesaria para el cumplimiento de funciones y atribuciones de las diversas dependencias, lo que se busca es impedir que se recolecten de forma excesiva y se utilicen para fines distintos.

autodeterminación informativa (informationelle Selbstbestimmung) y que se ve desarrollado con las nuevas facetas de la intimidad que en las sociedades avanzadas, requieren nuevos instrumentos de tutela jurídica, al darse el tratamiento de datos personales de manera automatizada.[58]

Sobre este asunto fue trazada la teoría de las esferas (Sphiirentheorie), que establece una protección gradual dependiendo del ámbito de desarrollo personal al que se haga referencia. Así, la denominada "íntima", corresponde al ámbito secreto de la persona, que no comparte con otro; la privada que determina a la dimensión de vida personal y familiar y, por último, la individual, que afecta a cuanto define la peculiaridad o individualidad de una persona (Pérez Luño, 2012, p. 81). Sin embargo, esta teoría se superó con la sentencia de 15 de diciembre de 1983 acerca de la Ley de censo de población, en la que la jurisprudencia alemana concibe la intimidad como autodeterminación informativa, es decir, como la libertad del ciudadano para determinar quién, qué y con qué ocasión puede conocer y/o utilizar los datos que le afectan,[59] pero también, para decidir acerca de las actividades que puede realizar para que su comportamiento resulte congruente con esa postura, pues, según Schwabe (2009, p. 96), "un

[58] Para el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº 45/2001 y la Decisión nº 1247/2002/CE., el titular cuenta con el derecho de no ser objeto de una decisión basada únicamente en el tratamiento automatizado que puede o no incluir la elaboración de perfiles que produzca efectos jurídicos en él o le afecte significativamente. Sin embargo, no podrá ejercerlo si la decisión es necesaria para la celebración o el cumplimiento de un contrato entre el titular y el responsable, si se encuentra autorizada en una normativa de la Unión o si se basa en el consentimiento expreso del titular.

[59] La sentencia BVerfGE 65, 1 [Censo de Población], fue dictada a razón del recurso de amparo constitucional interpuesto en contra de la Ley de Censo de Población, en 1982, que en lo sustancial solicitaban que esa ley se declarara anticonstitucional y que se ordenara la suspensión de la aplicación de la ley hasta que se resolviera el de mérito (Heredero, 1983). El Tribunal Constitucional Federal Alemán (Schwabe, 2009, p. 94) resolvió que "1. El derecho general de la personalidad […] protege a los individuos frente a la recolección, archivo, empleo y difusión ilimitada de sus datos personales. El derecho fundamental garantiza en esta medida la capacidad de los individuos, para determinar; en principio, la divulgación y empleo de sus datos personales. 2. Los límites a ese derecho a la "autodeterminación informativa" se admiten sólo con base en la prevalencia del interés general […] para su reglamentación el legislador debe tener en cuenta el principio de proporcionalidad. También está obligado a acatar las disposiciones procedimentales y organizatorias, que evitan el peligro de una violación del derecho a la personalidad. 3. Se debe diferencia entre los datos vinculados a la persona […] y aquellos que se encuentran destinados a fines estadísticos (para cuyo caso) no se puede exigir de forma estrecha y concreta que los datos estén vinculados a un fin determinado. 4. […] Para la seguridad del derecho a la autodeterminación de la información, se requiere para el desarrollo y organización de la recolección de datos de disposiciones complementaras, en consonancia con la Constitución".

ordenamiento social y un orden legal en el que los ciudadanos no pudieran conocer *quiénes, cuándo y en qué circunstancias* saben *qué* sobre ellos, serían incompatibles con el derecho a la autodeterminación de la información. […] Esto no sólo iría en detrimento de las posibilidades de desarrollo individual de los individuos, sino también de la comunidad, porque la autodeterminación es una condición funcional elemental de una nación democrática libre, fundada en la capacidad de sus ciudadanos para cooperar y actuar."

O, como refiriera Vidal (2020, p. 86) "si bien el derecho a la intimidad permite garantizar una esfera reservada de la persona, el derecho a la protección de datos atribuye un poder de disposición y control sobre la información personal, incluso cuando sea accesible a terceros". Además, ya Rodatà en 1976 (p. 130), aseveraba que, "al encontrar la raíz del poder de la información, así como aquellos que lo ejercen en realidad, no solo será posible desarrollar formas de contrarrestarlo y controlarlo, pero también para explotar las posibilidades ofrecidas por las tecnología informática[60], para tratar de implementar otras formas de gestionar ese poder, capaz de ofrecer a las libertades individuales aquellas posibilidades de expansión, lo que hubiera sido impensable hasta hace muy poco tiempo […] analizando las implicaciones que pueden tener en el contexto del sistema político."

Es por lo que, al delimitar al derecho a la intimidad se debe reconocer la frontera de los ámbitos público y privado. Así, mientras lo íntimo es todo aquello que se lleva a cabo en la esfera de mayor reserva, lo privado admite la intervención de las personas más cercanas al sujeto: se propone pensar, por ejemplo, en una relación afectiva se comparten momentos e ideologías inevitablemente, con otra persona, a la que se le permite ingresar en ese círculo personal y en el que, depende de cómo evolucione esa situación, se le compartirán detalles incluso

[60] Así, Piñar (2018, p. 101) considera que la identidad que se forja en el plano virtual se define de forma ajena a la persona que la posee, a través de los algoritmos donde se diseña, por lo que además de controlarla y vigilarla a través de estos mecanismos, pone en duda el derecho al libre desarrollo de la personalidad del titular de esos datos, lo que ocurre además por la relativa facilidad con la que estos pueden ser perfilados, ya que estas tecnologías "van a adecuar procesos a nuestros gustos, por lo que no será fácil objetar las indicaciones que de ello deriven".

del rubro personal, de lo íntimo. Como refiere Rebollo (2003, p. 222) podemos distinguir entonces entre dos tipos de intimidad, la física o clásica y la informativa, a la que hemos hecho referencia en este párrafo.

En cambio, el ámbito público es la cara que se da ante la sociedad: la presentación a los demás de la propia personalidad y muchas veces, lo que se desea se piense de sí mismo. Es un espacio caracterizado por la injerencia del mundo exterior en el área que se establece con tal carácter, donde se interactúa libremente y se permite la plena accesibilidad de entes totalmente ajenos al espacio privado. Es un espacio de expresión de lo que se considera adecuado.

De esta forma, Pérez Luño (2012, p. 82) propone 3 premisas para superar las polaridades dilemáticas de la intimidad:

1. Las formas en que la intimidad se manifiesta en un concepto único, pero también adaptable a la realidad en que las personas se desenvuelven.
2. El derecho a la intimidad consiste en garantizar la autodeterminación de una persona que ya no puede permanecer aislada, sino que debe relacionarse con otro y el poder público.
3. En consecuencia, el dilema entre una intimidad interna y auténtica y una intimidad externa alienada se torna inexistente, toda vez que ambos suceden de manera complementaria e inevitable, sin que haya detrimento a la garantía del derecho.

3.1.2.2 El derecho a la autodeterminación informativa y la protección de los datos personales.

En cualquiera de los foros descritos, el individuo debería ejercer de forma plena su autodeterminación informativa, entendida esta como la facultad de toda persona para tomar control sobre su propia información, ya que decide lo que da a conocer públicamente y lo que no; resuelve que comunica a aquellos que comparten el círculo de su privacidad y hasta donde les permite conocer su intimidad.

Muñoz (1996, p. 147, 148) considera que la intimidad se venía protegiendo, entendiéndola desde el aspecto negativo de la conservación de un secreto, esto es, que ciertos acontecimientos o aspectos de la vida de alguien no fueran conocidos más que por un grupo reducido de semejantes que tuvieran el privilegio de conocer la información. Sin embargo, también le reconoce un aspecto positivo a este derecho en el control del titular del dato para darlo a conocer a terceros, es decir, la autodeterminación informativa.

Para autores como Rodatà (1976, p. 139) el concepto de autodeterminación informativa es de tal relevancia que consideraba que "la obligación de suministrar datos, en efecto, no puede considerarse meramente como compensación de las prestaciones sociales que, directa o indirectamente, el ciudadano puede disfrutar. Los datos recogidos no sólo permiten organizaciones públicas y privadas para preparar e implementar sus planes, pero también permiten el crecimiento de nuevas formas de concentración de poder. En consecuencia, los ciudadanos tienen derecho a reclamar el control directo sobre esas personas que han adquirido un mayor poder, gracias a los datos suministrados a ellos."

Por lo anterior, como afirma Fernández (2021, p. 93), queda manifiesto que la interpretación que los tribunales europeo-continentales han dado de este derecho es tendente a su vinculación no con la intimidad como los norteamericanos han interpretado, si no con la dignidad y el libre desarrollo de la personalidad.

Así, Rodotà (2018, p. 90) explica que la "construcción de la identidad puede confiarse cada vez más a algoritmos, sustrayéndola a la decisión y al conocimiento individuales" ello por la colección de información acerca de las personas. Siguiendo el pensamiento del teórico italiano, la consecuencia será la apropiación de la identidad por terceros, alejándose de forma progresiva la identidad de la autonomía de la persona a la que pertenece, confundiéndose de tal suerte "hasta desaparecer la fuerza del humano en la construcción de sí

mismo", resultando para él complicada la propuesta de nuevas rutas para que las personas reinventen su identidad en los tiempos de la tecnociencia.[61,62]

Acerca de la identidad también reflexiona el Supervisor Europeo de Protección de Datos, a través de su Grupo Asesor en Ética, (2018, p. 30), que entre sus aportaciones expone, además de que la personalidad y los datos personales son inseparables la una de los otros por causa de la inviolabilidad de la dignidad humana. Como afirma Hernández (2018, p. 280, 281), la legislación que contiene la técnica regulatoria del tratamiento de los datos personales debe ser considerada como el medio por el que se garantiza ese derecho de autodeterminación informativa, que de ninguna manera "justificarían consecuencias tan inconvenientes para la extensión y refuerzo de la innovación tecnológica en el ámbito digital", que se relaciona directamente con la autonomía personal y a su vez, con su dignidad como persona. Es en relación con lo descrito que Cotino (2020, p. 38) considera que se está construyendo "un nuevo derecho de protección de datos, distanciándolo de la privacidad y la intimidad […] en ocasiones resulta absurdo, inviable o contraproducente desvincular la protección de datos de la privacidad que es su matriz y en la que sin duda se integra."

Rebollo (2003, p. 222) por su parte, identifica de manera clara las generaciones en las que se ha garantizado la protección de datos personales y que coinciden según su análisis, con el avance tecnológico. Así, "…una primera generación requiere la autorización previa de los bancos de datos; la segunda generación coincide con la garantía de los que con posterioridad han sido denominados datos sensibles, dada su incidencia en los derechos de la personalidad; y, por último, una tercera generación, que atiende a la imposibilidad de un control previo de los equipos, y de un control estático de los datos, y, por tanto, que tiene que prevenir su potencialidad y funcionalidad."

[61] *Vid.* por ejemplo *Self Sovereign Identity. A guide to privacy for your digital identity with Blockchain,* disponible en https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

[62] Por ejemplo, de acuerdo con Pérez Luño (2012, p. 99), el reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa tiende a la tutela de la intimidad de los datos sanitarios procesados a través de las nuevas tecnologías, o también de aquellos que tienen su origen en ámbitos de experimentación biotecnológicos.

Lo anterior deberá tenerse en cuenta al definir, aplicar e interpretar la norma, sobre todo cuando entendemos a la protección de datos personales como un derecho humano, por lo que según Hernández (2018, p. 285), deberá adoptarse "una visión de conjunto, que verifique hasta qué punto un tratamiento de datos de carácter personal arriesga que la autonomía personal resulte afectada", pues como ya identificaba el Grupo de Trabajo del Artículo 29 (2007, p. 4), el objetivo de las normas en materia de protección de datos es la protección "de las libertades y los derechos fundamentales de las personas físicas y, en particular, su derecho a la intimidad, en los que respecta al tratamiento de los datos personales".

Es decir, que "la técnica jurídica de la protección de los datos personales ante el uso de la informática nace y existe para hacer efectivo el derecho a la autodeterminación informativa" (Murillo de la Cueva, 1999, p. 53), cuya normativa al ser aplicada de manera estricta, no solo salvaguarda esta, si no también, la libertad personal, como instrumento para detener la injerencia y hasta abuso sobre los titulares de los datos, para obtener cualquier tipo de beneficio a su costa (Murillo de la Cueva, 2007, p. 18). El control que ofrece la positivización de este derecho se identifica a través de dos elementos, también descritos por Murillo de la Cueva (2007, p. 18), a saber, el consentimiento del titular de los datos como elemento legitimador de su obtención y tratamiento o en su defecto, la habilitación que la legislación dé para los fines de interés.

De esta suerte y como refiere Troncoso (2003, p. 245) "… el derecho fundamental a la protección de datos es, […] un derecho autónomo nuevo que protege a la persona -en especial, la propia información personal- frente a las tecnologías de la información y que, […] representa una concretización del derecho a la intimidad en los tratamientos de datos personales, […] es un instrumento de garantía de otros derechos fundamentales (a través de la atribución) a su titular (de) un haz de facultades que consiste en el poder jurídico de imponer a terceros la realización o la omisión de determinados comportamientos."

3.1.2.3 Derecho internacional.

Establecido entonces que nos encontramos frente a un derecho humano, la acción de plasmarle en diversos cuerpos normativos sin duda brinda la seguridad de su respeto y difusión como tal entre la población.

En su regulación, se tiene como constante el establecer que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación, en los diversos ordenamientos, como el Convenio para la protección de los derechos y las libertades fundamentales de 01 de junio de 2010 (artículo 8), el Pacto Internacional de Derechos Civiles y Políticos de 23 de marzo de 1976 (artículo 17) y la Convención Americana sobre Derechos Humanos (Pacto de San José) de 22 de noviembre de 1969, que lo contempla en el apartado 2 de su artículo 11.

Mención aparte merecen el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo, Francia, el 28 de enero de 1981 del Consejo de Europa de 28 de enero de 1981, así como su Protocolo Adicional relativo a las Autoridades de Control y a los flujos Transfronterizos de Datos, de 08 de noviembre de 2001[63], ya que se trata del primer instrumento internacional con carácter de vinculante para quienes lo hayan suscrito y ratificado. En éste se plasman los principios de la protección de datos personales, siendo trabajo de los firmantes desarrollarlos de manera particular.

Resultan también relevantes los principios establecidos en el Marco de privacidad del foro de cooperación económica Asia Pacífico (APEC) de 2015,

[63] Al que México se ha adherido recientemente a través del Decreto emitido por la Cámara de Senadores del Honorable Congreso de la Unión, en ejercicio de la facultad que le confiere el artículo 76 de la Constitución Política de los Estados Unidos Mexicanos de 05 de febrero de 2017, y que se publica en el Diario Oficial de la Federación el 12 de junio de 2018. Sin embargo, en México no se ha ratificado el Protocolo de enmienda del convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal hecho en Estrasburgo el 10 de octubre de 2018, pero sí lo ha hecho el Reino de España.

que tienen como fin el proteger la privacidad de información personal; prevenir la creación de barreras innecesarias al flujo transfronterizo de datos; fomentar la uniformidad por parte de empresas multinacionales en los métodos utilizados para la recolección uso y procesamiento de datos personales; fomentar los esfuerzos nacionales e internacionales para promover y hacer cumplir las disposiciones legales de protección de datos personales.

También son de importante mención los principios de licitud, exactitud, finalidad, acceso y no discriminación, que en materia de protección de datos personales y con ámbito de aplicación mundial fueron enumerados dentro de la Resolución 45/95 de 14 de diciembre de 1990, de la Asamblea General de las Naciones Unidas, acerca de los principios rectores sobre la reglamentación de los ficheros computarizados de datos personales.

3.1.2.4 Orden jurídico mexicano.

La autoridad de protección de datos mexicana (IFAI, ahora el Instituto Nacional de Transparencia, Acceso a la Transparencia y Protección de Datos, INAI, 2014, p. 2), ya asumía a la protección de datos personales como un derecho humano que reconocido en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, de 5 de febrero de 1917, "[..] que otorga el poder a toda persona física para que sus datos personales sean tratados de manera lícita y leal, a fin de garantizar su privacidad y derecho a la autodeterminación informativa, es decir, a decidir quién puede tratar sus datos personales y para qué fines."

En México existen dos leyes que garantizan el derecho de protección de datos personales, pero que están diferenciadas en su ámbito de aplicación que, aunque también podrá ser territorial, obedece antes a la calidad del sujeto que es responsable del tratamiento de los datos. Por lo tanto, si los datos personales son tratados por órganos gubernamentales, su actuar se verá regido por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, que es una disposición de orden público y aplicable a todo el país; y las entidades integrantes de la federación, debieron emitir legislaciones similares y armonizadas a la mencionada.

Esta Ley General, no cuenta con un reglamento que desarrolle su contenido, pero el INAI (2017) ha emitido los Lineamientos Generales de Protección de Datos Personales para el Sector Público que únicamente resultan aplicables a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, fideicomisos y fondos públicos, del ámbito federal y partidos políticos que en el ejercicio de sus atribuciones y funciones lleven a cabo tratamientos de datos personales de personas físicas, en términos de lo dispuesto en la Ley y los Lineamientos generales recién mencionados, así como al INAI y los organismos garantes en lo que respecta a la sustanciación de los recursos de inconformidad. Por lo que respecta al resto de los sujetos obligados, deberán atenerse a lo establecido exclusivamente por la ley en cita, o a la legislación reglamentaria general o en las entidades federativas que corresponda.

Por otra parte, si el responsable del tratamiento es un particular (quien por exclusión no pertenezca al sector público o reciba recursos públicos), debe regirse por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de 05 de julio de 2010 y su Reglamento de 21 de diciembre de 2011, no importa en qué entidad federativa resida, ya que únicamente el congreso federal tiene la facultad de legislar sobre este tema particular, según la fracción XXIX-Ñ, del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, de 05 de febrero de 1917.

El objeto de este cuerpo normativo es la protección de los datos personales en posesión de los particulares, para regular su tratamiento legítimo, controlado e informado a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Son sujetos regulados de esta ley los particulares, entendidos estos como personas físicas o morales de carácter privado que lleven el tratamiento de datos personales. No están sometidas a sus dictados las sociedades de información crediticia ni tampoco los particulares que recopilan información para uso exclusivamente personal, es decir que no la divulguen o comercialicen la información de mérito.

Entre otras restricciones que describe la legislación mexicana, tanto en el ámbito público como en el de los particulares, excluye de su ámbito de aplicación la información concerniente a las personas jurídicas; la que se refiera a personas físicas en su calidad de comerciantes y profesionistas y la de personas físicas siempre que presten sus servicios para alguna persona moral o física con actividades empresariales y/o prestación de servicios, tales como nombre, función o puesto desempeñado, domicilio, dirección electrónica, teléfono y fax, siempre y cuando su finalidad de tratamiento sea la de representación del empleador o contratista.

Igualmente, aunque respetando la expectativa razonable de privacidad, quedan excluidos del amparo de la norma aquellos datos personales que se obtengan de fuentes de acceso público, es decir, de aquellas en las que su consulta pueda ser realizada por cualquier persona sin mayor exigencia que el pago de una contraprestación, derecho o tarifa, como ocurre por ejemplo en los registros de estado civil o los públicos de la propiedad. Aunque también son considerados como tales los medios remotos o locales de comunicación electrónica, óptica y de otra tecnología siempre que el sitio donde los datos se alojen esté abierto a la consulta general; los directorios telefónicos; los diarios, gacetas o boletines oficiales y los medios de comunicación social, así como los registros públicos. No serán consideradas fuentes de acceso público tratándose de aquella información que en ella se contenga sea o tenga procedencia ilícita.

Por lo que hace a los sindicatos y cualquier persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal o municipal, tratará los datos personales en apego a la legislación de la materia para los particulares.

3.1.2.5 Orden jurídico comunitario y español.

De especial interés para nuestro estudio resultan los Reglamentos de la Unión Europea 2018/1725 de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos

datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE; el 2016/679 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 del Parlamento Europeo y del Consejo. [Parlamento Europeo y Consejo Europeo] de 24 de octubre de 1995 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales así como la Carta de los Derechos Fundamentales de la Unión Europea que además de buscar garantizar estos derechos, también persiguen el flujo de datos sin tantas restricciones, entre los países miembros. Se destaca en esta última, el reconocimiento del derecho de protección de datos personales como uno fundamental, pues han sido tomados en muchos casos como modelo a seguir para la legislación mexicana en la materia, por lo que su análisis también resulta de relevancia para nuestro estudio.

Los primeros dos, se aplican en conjunto y el Reglamento 2018/1725 tuvo que ser adaptado del similar 2016/679, aunque su ámbito de aplicación es específico al tratamiento de datos por instituciones y organismos de la Unión Europea en cualquier contexto. Sin embargo, se excluye lo relativo al de cooperación judicial en materia penal y cooperación policial.

Otro ordenamiento indispensable para la investigación es el Protocolo de enmienda del convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal hecho en Estrasburgo el 10 de octubre de 2018. Este señala como excepciones de su aplicación, si el tratamiento se prevé en un ordenamiento, respeta la esencia de los derechos y libertades y constituye una medida necesaria y proporcionada para la protección de la seguridad nacional y la defensa, la seguridad pública, intereses económicos y financieros importantes del Estado, la imparcialidad e independencia del poder judicial o la prevención, investigación y persecución de infracciones penales así como la ejecución de sanciones de este mismo orden; la protección del titular y de derecho y libertades de terceros, con énfasis en la libertad de expresión.

También se excluye de su protección al tratamiento de datos con fines de archivo siempre que sea por interés público o de investigación científica[64] o histórica, así como de estadística, siempre que no exista riesgo de vulneración de los derechos y libertades de los titulares de los datos. En este caso, deberán implementarse medidas técnicas y organizativas además del principio de minimización de datos para su adecuado tratamiento, de tal suerte que no se identifique a los titulares.

En el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la UE, se limita el ejercicio de los derechos relacionados con la protección de datos personales así como a los principios que rigen su tratamiento en situaciones necesarias para la salvaguardia de la seguridad pública, la investigación, prevención y enjuiciamiento de infracciones penales o la ejecución de las sanciones de la materia, la protección de la vida humana en respuesta a catástrofes naturales o de origen humano, la seguridad interna de las instituciones, para cumplir los objetivos de la política exterior y de seguridad común, por un importante interés económico de la Unión Europea, así como el mantenimiento de sus registros públicos por razones de interés público general, la protección del titular o de los derechos de terceros en las que se comprende la protección social, la salud pública y los fines humanitarios.

A su vez, entre las limitaciones que contempla el 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos están la seguridad del Estado y la pública, la defensa, la prevención, investigación, detección o enjuiciamiento

[64] Quinn (2021, p. 29), consideró en su estudio publicado en ese año, que entre más grande sea una base de datos, más probable será que contengan datos confidenciales. Además, esos datos "aparentemente inocuos y no personales de forma aislada pueden, cuando se procesan con otras formas de datos, revelar información que es personal y de naturaleza sensible". Para él resulta evidente que este problema no hará más que acentuarse, por lo que los investigadores deberán buscar bases legales para tratar este tipo de datos, además de la del consentimiento del titular de estos.

de infracciones penales o las ejecuciones de esta materia; objetivos importantes de interés público, la protección de la independencia judicial y de sus procedimientos; la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; la supervisión, inspección o reglamentación vinculada con la autoridad pública en casos de seguridad del Estado, interés público general y el último de los mencionados; la protección del interesado o de los derechos de terceros y la ejecución de demandas civiles.

En España, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales establece con arreglo al Reglamento (UE) 2016/679 que el tratamiento de datos personales se realiza fundado en el cumplimiento de una obligación legal exigible al responsable si una norma del Derecho de la Unión Europea o una con rango de ley así lo establece, pudiendo también imponer condiciones especiales al tratamiento dependiendo de la materia que se trate. Igualmente, solo puede considerarse el tratamiento con fundamento en una misión realizada en interés público o en ejercicio de los poderes públicos del responsable si esta deriva de una competencia atribuida por una norma con rango de ley. También excluye del ámbito de aplicación el tratamiento que una persona física realiza si coloca cámaras de videovigilancia dentro de su domicilio, sin embargo, la exclusión no se extiende a si contrata a una entidad especializada para ello, pues se entiende que, para llevar a cabo el objeto de su contrato, debe tener acceso a la información captada.

Tanto el 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos como el 2018/1725 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de 06 de diciembre de 2018 excluyen de su ámbito de garantía a los datos de personas fallecidas y el de personas jurídicas incluyendo a las empresas que se constituyen con esta figura, incluyendo también el nombre y la forma de la persona jurídica y sus datos de contacto.

3.2 El derecho de protección de datos personales como instrumento de garantía del de protección a la salud.

Para concluir estas líneas, nos permitimos retomar a Bobbio (1990, p. 114) en cuanto afirma que los derechos fundamentales son aquellos que permiten la realización de los otros derechos y que deben concretarse en su universalización y multiplicación. Lo anterior es así, ya que la cantidad de bienes considerados de tutelarse ha aumentado, la titularidad de sujetos distintos al ser humano ha sido ampliada y este último, ha encontrado la forma de concretar su destino en una sociedad democrática, con fundamento en la dignidad de las personas, en torno a quienes giran los artificios creados por ellos mismos que conocemos como derechos y sociedad (Rodotà 2014, p. 174).

Guastini (2001, pp. 223 y 224) reflexiona acerca de que los derechos sociales, como el de la salud se formulan como normas atributivas de derechos, pero no confieren ninguno ya que se limitan a ordenar al legislador que se persigan ciertos objetivos. Tampoco cuentan con un mecanismo para que este cumpla con su labor, pues “ningún juez constitucional puede anular la inexistencia de una ley”, pero sí anular la que “viole un derecho social”, siempre que se cumpla el supuesto de que el legislador formule alguna, lo que Bovero (2013, p. 15) considera un *ius imperfectum*, y continúa: “las normas que confieren derechos subjetivos, por sí mismas son insuficientes: deben ser complementadas con normas dirigidas a volver efectivos los derechos, estableciendo las garantías”.

Es así como, tanto el derecho a la protección de la salud, como el de protección de datos personales, primero son considerados como derechos fundamentales. Luego, convergen en la importancia que reviste la información para que ambos puedan ser garantizados. Es decir, para el prestador de los servicios de salud será indispensable obtener información veraz para ofrecer un diagnóstico, pronóstico y tratamiento; mientras que el usuario se beneficiará tanto si recibe voluntariamente información del prestador acerca de su estado de salud, como si ejerce su derecho de acceso a los datos que contiene su expediente clínico,

al tomar decisiones libres e informadas que impactarán directamente a su estado de salud.

De esta suerte, si bien es cierto que el derecho de protección de datos personales es independiente al de protección de la salud, en consonancia a la redacción que el legislador utilizó, el primero puede instituirse como mecanismo de garantía del segundo, al establecerse en la legislación secundaria los procesos que permiten acceder a la información relativa al usuario acerca de su estado de salud, es decir, los datos personales contenidos en el expediente clínico, que a su vez, también cuentan con garantías secundarias para asegurar que el derecho de protección de datos personales pueda ser ejercido por el sujeto. En consecuencia, este último se convierte en una de las garantías secundarias del derecho que el paciente tiene de ser informado acerca de su estado de salud.

3.3 Ámbito de ejercicio. Los Sistemas Nacionales de Salud.

Habiendo dejado claro la importancia y transversalidad del derecho a la salud, y que de él se desprenden diversas obligaciones de acción u omisión para verlo garantizado incluyendo el ejercicio de otros derechos fundamentales como los de acceso y protección a los datos personales, resulta importante conocer cuál es la estructura del sistema de salud mexicano y español, que es el ámbito en el que se ejercerán ambos.

3.3.1 El Sistema Nacional de Salud Mexicano.

Hasta principios del siglo XX, la participación del Estado Mexicano en asuntos de salud se limitó a actividades dirigidas al control de los bienes que tienen impacto sobre la salud y de las enfermedades en la población, a través de la Secretaría de Gobernación, al ser una de sus facultades. (Frenk y Gómez, 2015, pp. 21-31)

Los servicios curativos se limitaron a los que se proporcionaban a través de la Dirección General de la Beneficencia Pública y Privada, ya que los hospitales

eran espacios dedicados al amparo de huérfanos, hospedaje de peregrinos y asistencia de los indigentes, brindándoles ayuda material y espiritual al tiempo de excluírseles del resto de la sociedad por el peligro que supuestamente representaban. Los médicos trabajaban, sobre todo, en sus consultas privadas y acudían a las casas de sus pacientes, haciendo en ese entonces una verdadera labor de acompañamiento, enfatizando aquella relación paternalista donde la visión del profesional de la salud se imponía a los deseos, incluso, del propio afectado.

El proceso histórico de su composición a partir del siglo pasado se presenta en el siguiente cuadro de Frenk y Gómez (2015, p. 32), donde se representa la conquista de un derecho ciudadano y a partir de los cuales se presenta la práctica de la medicina en el ámbito hospitalario.

Tabla 5 Hitos en la historia contemporánea del sistema mexicano de salud.

1915	Inauguración del Hospital General de México
1917	Creación del Consejo de Salubridad General y el Departamento de Salubridad Pública, establecida en la Constitución
1939	Creación del Instituto de Salubridad y Enfermedades Tropicales
1943	Creación de la Secretaría de Salubridad y Asistencia, del Instituto Mexicano del Seguro Social (IMSS) y del primero de los Institutos nacionales de salud, el Hospital Infantil de México
1960	Creación del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE)
1979	Creación del Programa IMSS-Coplamar, hoy IMSS-Prospera (IMSS-P)
1983	Incorporación a la Constitución del derecho a la protección de la salud[65]

[65] Ya Ruiz (198, p. 6) daba cuenta de lo novedoso de la reforma constitucional del 03 de febrero de 1983: “El término Derecho a la Salud”, ingenuo y demagógico, quedó atrás ante el poder constituyente que utilizó el más sensato de Derecho a la Protección de la Salud” que consagra el elemento radical de ese derecho, el acceso universal a servicios de salud, sean éstos de atención médica, de salud pública o de asistencia social, como como más tarde clarificó el Congreso en la Ley General de Salud. […] El derecho a la protección de la salud, que no es accionable, que no goza de garantía jurisdiccional, viene a completar el contenido programático de la Constitución y a hacer explícito el proyecto social que ésta contiene. El nuevo derecho es respuesta a la dimensión de salud de la llamada cuestión social.” Y apunta que se indican las finalidades del derecho, los servicios de salud en el contexto de la economía mixta del México de la década de 1980, los servicios básicos y la integración del Sistema Nacional de Salud “bajo la rectoría de la Secretaría de Salubridad y Asistencia coordina a los servicios de salud públicos, sean estos federales, estatales y municipales, así como los que se presten en los sectores social y privado”, así como la distribución de las competencias en materia de salubridad general.

1984	Promulgación de la Ley General de Salud.[66]
1985	Inicio de la descentralización de los servicios de salud para la población no asegurada, que concluye en 2000 Creación de la Fundación Mexicana para la Salud
1987	Creación del Instituto Nacional de Salud Pública
1991	Creación del Programa de Vacunación Universal
1996	Creación del Programa de Ampliación de cobertura y del Programa de Educación, Salud y Alimentación (Progresa), hoy Programa de Inclusión Social "Prospera"
2001	Creación de la Comisión Federal de Protección contra Riesgos Sanitarios (Cofepris)
2003	Creación del Sistema de Protección Social en Salud, cuyo brazo operativo es el Seguro Popular

Fuente: Frenk y Gómez, 2015, p. 32

Así, el Sistema Nacional de Salud se encuentra sustentado en el Título Segundo de la Ley General de Salud, de 07 de Febrero de 1984, y en su integración no distingue entre personas físicas y morales ni públicas o privadas, pues no importando el ámbito al que pertenezcan, se consideran como partes a las dependencias y entidades de la administración pública federal y local, así como a las personas físicas y jurídicas de los sectores social y privado que presten servicios de salud, por los mecanismos de coordinación de acciones cuyo objeto es dar cumplimiento al derecho de protección de la salud.

El objetivo de creación del Sistema fue la persecución de objetivos tales como proporcionar a toda la población servicios de salud, priorizando tanto su mejora como la atención preventiva de problemas sanitarios que condicionen y causen daños a la salud, con estrategias enfocadas al grupo etario, sexo y factores de riesgo de a quienes se dirigen. Con ello, se contribuirá al desarrollo demográfico y armónico del país, al bienestar social de la población a través de servicios de asistencia social, promoviendo el desarrollo de la familia y la comunidad de todos

[66] Sigue Ruiz (1985, p. 7) explicando que el Programa Nacional de Salud incluido en la reforma señalada fue creado "como medio para dotar de efectividad al derecho a la protección de la salud […] en sus dos expresiones radicales: avanzar en la universalización de los servicios de salud y avanzar en el aseguramiento de una calidad mínima homogénea. Reconoce, sin embargo, algunos obstáculos que pueden llegar a impedir su cumplimiento, como las finanzas, los regímenes distintos de atención, los rezagos económicos y sociales, así como las diferencias culturales de los usuarios y prestadores de servicios.

los sectores de la población mexicana y del medio ambiente en que se desenvuelven.

También se busca promover el conocimiento y desarrollo de la medicina tradicional indígena en condiciones adecuadas, propiciando incluso la participación de los prestadores de servicio de salud en estas comunidades; de igual forma, propiciar la modificación de patrones culturales que determinen hábitos, costumbres y actitudes relacionados con la salud y el uso de los servicios que se presten para su protección. Otro de sus objetivos es el diseño de políticas públicas alimentarias y la creación de programas de atención para las víctimas y victimarios de acoso y violencia escolar, mediante el desarrollo e integración de las tecnologías de la información y las comunicaciones para ampliar la cobertura y mejorar la calidad de atención a la salud.

Una reforma importante al sistema fue la publicada en noviembre de 2019 en el Diario Oficial de la Federación, consistente en la desaparición del llamado "Seguro Popular", para sustituirlo con el Instituto de Salud para el Bienestar. Sin embargo, fue reformado nuevamente mediante decreto que modifica a la Ley General de Salud de 07 de febrero de 1984, para que en su lugar exista ahora el Servicio de Salud del Instituto Mexicano del Seguro Social para el Bienestar (IMSS-Bienestar), publicado el 29 de mayo de 2023, y que funcionará a través de convenios de coordinación y colaboración con los servicios de salud de las Entidades Federativas, que dará paso al Servicio Nacional de Salud Pública a consolidarse en 2024.

Respecto a las autoridades sanitarias mexicanas[67] la Ley General de Salud, de 07 de febrero de 1984 en su artículo 4, reconoce como tales al Presidente de la

[67] La autoridad sanitaria mexicana es una figura sui generis en la legislación. Resulta tan importante, que se establece en la fracción XVI del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, de 05 de febrero de 1917, dentro de las facultades que tiene el Congreso de la Unión para dictar leyes sobre salubridad general de la República.
Así, su potestad resulta ejecutiva y sus disposiciones deben ser obedecidas por las autoridades administrativas de todo el país. Un claro ejemplo resulta en caso de epidemias de carácter grave o riesgo de invasión de enfermedades exóticas en el país, tiene la obligación de dictar las medidas preventivas indispensables, que en un momento posterior serán sancionadas por el Presidente de la República.

República, el Consejo de Salubridad General, la Secretaría de Salud Federal y a los gobiernos de las Entidades Federativas.

El Sistema Nacional de Salud está coordinado por la Secretaría de Salud Federal, con la colaboración de los gobiernos de las Entidades Federativas en el ámbito de sus competencias y de los acuerdos de coordinación que celebren entre sí, organizando para el cumplimiento de ese propósito sistemas estatales de salud e incluso, estrategias que impliquen la descentralización de los municipios que así deseen hacerlo. De esta forma, a la Secretaría le compete dictar normas oficiales mexicanas en la materia; en cuanto al ámbito educativo, organizar y operar los servicios de salud en este sector; organizar y operar por sí o en coordinación el desarrollo temporal de acciones en las entidades federativas a su solicitud y en consonancia a sus acuerdos de coordinación; la promoción, orientación, fomento y apoyo de acciones en materia de salubridad general a cargo de las entidades federativas con sujeción a las políticas nacionales de la materia.

Igualmente le corresponde el ejercicio de la acción extraordinaria en materia de salubridad general, así como la promoción y programación del alcance y modalidades del sistema nacional de salud, desarrollando las acciones pertinentes para su consolidación y funcionamiento. Tiene también atribuciones de regulación, control y fomento sanitarios en lo que se refiere al control y vigilancia de los establecimientos de salud, cadáveres y personas, a través del órgano desconcentrado denominado Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS).

Los gobiernos de las entidades federativas, a su vez, deberán organizar, operar, supervisar y evaluar los servicios de salubridad general que se refieren el artículo tercero[68] de la Ley General de Salud, de 07 de febrero de 1984, acordando

Otro supuesto previsto en el mismo artículo es que si el Consejo de Salubridad General puso en vigor ciertas medidas contra el alcoholismo y la venta de sustancias nocivas, o bien, para prevenir y combatir la contaminación ambiental, serán revisadas con posterioridad por el Congreso de la Unión, si resulta de su competencia.

[68] II. La atención médica; II Bis La prestación gratuita de los servicios de salud, medicamentos y demás insumos asociados para personas sin seguridad social (lo cual se describirá a detalle en

previamente con la Secretaría lo conducente. También, contribuir a la consolidación del Sistema Nacional de Salud, así como el desarrollo de los estatales; la formulación y desarrollo de programas locales de salud; la elaboración de estadística local y la vigilancia del cumplimiento de la Ley General de Salud, de 07 de febrero de 1984, en el ámbito de su competencia. De forma conjunta, la Federación y las Entidades Federativas velarán por la prevención del consumo de narcóticos, atención de adicciones y persecución de los delitos contra la salud.

3.3.1.1 Los servicios de salud

El Título Tercero de la Ley General de Salud, de 07 de febrero de 1984 propone como concepto de servicios de salud cualquier acción realizada en beneficio del individuo y de la sociedad en general, que se encamine a proteger, promover y restaurar la salud de la persona y de la colectividad, clasificándolos en tres tipos, a saber: de atención médica, de salud pública y de asistencia social.

La garantía de su extensión progresiva, cuantitativa y cualitativa se encuentra supeditada a las prioridades del Sistema Nacional de Salud, particularmente entre la población que no cuente con afiliación a algún sistema de seguridad social. Entre los servicios que se consideran básicos, están la educación para la salud, el saneamiento básico, el mejoramiento de las condiciones sanitarias del

---

el apartado correspondiente al Instituto Nacional del Bienestar); IV. La atención materno infantil; IV Bis, El programa de nutrición materno-infantil en los pueblos y comunidades indígenas; IV Bis 1. La salud visual; IV Bis 2. La salud auditiva; IV Bis 3. Salud bucodental; V. La planificación familiar; VI. La salud mental; VII. La organización, coordinación y vigilancia del ejercicio de las actividades profesionales, técnicas y auxiliares para la salud; VIII. La promoción de la formación de recursos humanos para la salud; IX. La coordinación de la investigación para la salud y el control de ésta en los seres humanos; X. La información relativa a las condiciones, recursos y servicios de salud en el país. XI. La educación para la salud. XII. La prevención, orientación, control y vigilancia en materia de nutrición, sobrepeso, obesidad y otros trastornos de la conducta alimentaria, enfermedades respiratorias, enfermedades cardiovasculares y aquellas atribuibles al tabaquismo; XIII. La prevención y el control de los efectos nocivos de los factores ambientales en la salud del hombre; XIV. La salud ocupacional y el saneamiento básico; XV. La prevención y el control de enfermedades transmisibles; XVI. La prevención y el control de enfermedades no transmisibles y accidentes; XVII. La prevención de la discapacidad y la rehabilitación de las personas con discapacidad; XVIII. La asistencia social; XIX. El programa para la prevención, reducción y tratamiento del uso nocivo del alcohol, la atención del alcoholismo y la prevención de enfermedades derivadas del mismo, así como la protección de la salud de terceros y de la sociedad frente al uso nocivo del alcohol; XX. El programa contra el tabaquismo; XXVI Bis. El control sanitario de cadáveres de seres humanos; y XXVII Bis. El tratamiento integral del dolor.

ambiente, la prevención y control de las enfermedades transmisibles, no transmisibles y de los accidentes; la atención médica integral[69], la materno-infantil, la sexual y reproductiva, la mental, así como la prevención y el control de las enfermedades bucodentales, la disponibilidad de medicamentos y otros insumos esenciales[70], la promoción de un estado de vida saludable y la asistencia social a los grupos más vulnerables, destacando de forma especial a las comunidades indígenas y la atención médica a pacientes geriátricos.

Se consideran prestadores de servicios médicos[71] a cualquier institución de salud de carácter público, privado o social, así como los profesionales, técnicos y auxiliares que ejerzan libremente cualquier actividad relacionada con la práctica médica, según la definición ofrecida por el Decreto de Creación de la Comisión Nacional de Arbitraje Médico, de 06 de marzo de 1996, en su artículo tercero.

La Ley General de Salud, de 7 de febrero de 1984 incluye otra clasificación de los servicios de salud, en atención a quienes los prestan, por lo que pueden ser públicos a la población en general, a derechohabientes de instituciones públicas de seguridad social o los que con sus propios recursos o que reciban el encargo

[69] Esta comprende, según el artículo 27 fracción III y al 33 de la Ley General de Salud, de 07 de febrero de 1984, cualquier acción preventiva, curativa, de rehabilitación o paliativa, incluyendo a la atención de urgencias. La primera de ellas destaca la legislación, deberá incluir la realización de acciones de promoción y prevención para la protección de la salud, de acuerdo con la edad, sexo y determinantes físicos, psíquicos y sociales de las personas, que deberían realizarse en una sola consulta. Por lo que hace a las personas sin seguridad social, deberá garantizarse la prestación gratuita de servicios de salud, medicamentos y demás insumos asociados.

[70] Para ello se cuenta con un Compendio Nacional de Insumos para la Salud, que elabora el Consejo Nacional de Salubridad con la colaboración de la Secretaría de Salud, las instituciones públicas de seguridad social y aquellas que determine el Ejecutivo Federal, y al que deben ajustarse las instituciones públicas del Sistema Nacional de Salud. En él, se agrupan, caracterizan y codifican todos aquellos insumos que se consideran esenciales para la salud y la Secretaría de Salud garantizará su existencia permanente para que la población que los necesite pueda tener acceso a ellos. En este sentido, es la Secretaría de Economía quien fija los precios máximos de venta al público y asegurará su adecuada distribución y comercialización.

[71] En México, cualquier profesión en el campo de las ciencias médicas comprendidas en la Ley General de Salud, de 07 de febrero de 1984[71] requiere que para su ejercicio se cuente con título y cédula profesionales, debidamente expedidos, el primero por una institución educativa de las registradas ante la Secretaría de Educación Pública y la segunda, por la Dirección General de Profesiones de la misma Secretaría, así como certificados de especialización debidamente expedidos y registrados por la misma autoridad educativa. Por lo que hace a los profesionistas que realicen procedimientos quirúrgicos de especialidad, deberá además de contar con la cédula profesional correspondiente, la certificación oficial del Consejo de Especialidad Médica a la que pertenezca esa rama de la medicina.

del Poder Ejecutivo Federal presten las mismas instituciones a otros grupos de usuarios; los sociales y privados sin importar la forma de su contratación y cualesquiera otros que se presten de conformidad con lo que la autoridad sanitaria tenga a bien establecer.

Los primeros con todos los que se presten en establecimientos[72] públicos de salud y a los que acuda cualquier persona que los necesite, sin importar su nacionalidad y que se rigen por criterios de universalidad, igualdad, inclusión y gratuidad al momento de requerirlos, así como los medicamentos y demás insumos necesarios. En el caso de los derechohabientes de las instituciones de seguridad social que deseen tener acceso a los servicios descritos, podrán hacerlo, pero en términos de los convenios que entre esas instituciones se hayan suscrito.

Si bien es cierto que las instituciones de salud pública se rigen por el principio de gratuidad, también lo es que podrán cobrarse cuotas de recuperación a los usuarios de los servicios, que serán determinadas de acuerdo con su costo y las condiciones socioeconómicas de quien solicita el servicio. Se fundarán en principios de solidaridad social y debe exceptuarse su cobro cuando se demuestre que el usuario carece de los recursos para sufragarlas. No obstante, los extranjeros deberán pagarlas de forma íntegra, salvo en casos de urgencia. Además, a partir de 2005, todo menor de edad que no sea derechohabiente o beneficiario de alguna institución de salud será eximido del cobro de las cuotas desde su nacimiento hasta los cinco años, siempre que su familia se encuentre en un nivel de ingreso que corresponda a los tres últimos deciles establecidos por la Secretaría.

[72] Es importante mencionar que el Reglamento de la Ley General de Salud, de 07 de febrero de 1984 en materia de prestación de servicios de atención médica considera como establecimientos para la atención médica aquellos en los que se desarrollen actividades preventivas, curativas, de rehabilitación y de cuidados paliativos dirigidas a mantener y reintegrar el estado de salud de las personas y a paliar los síntomas del padecimiento; en los que se presta atención odontológica, de salud mental, servicios auxiliares de diagnóstico y tratamiento; las unidades móviles aéreas, marítimas o terrestres, del ámbito público, social o privado.

Por lo que hace a las instituciones de seguridad social, tales como el Instituto Mexicano del Seguro Social (IMSS) o el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE) por citar los ejemplos más representativos, se consideran servicios de salud aquellos que les son prestados a las personas que cotizan o hubieren cotizado conforme a sus leyes, así como a sus beneficiarios. Si son federales, deben coordinarse permanentemente con la Secretaría de Salud Federal. Entre otros, sus servicios comprenden la atención médica, la materno infantil, la planificación familiar, la salud mental, la promoción de la formación de recursos humanos, la salud ocupacional y la prevención y control de enfermedades no transmisibles y accidentes.

En cuanto a los servicios privados de salud se consideran así siempre que sean prestados por personas físicas o morales en las condiciones que convengan a los usuarios solicitantes y que se sujetan a los ordenamientos legales, civiles y mercantiles. Pueden ser contratados por el propio usuario o a través de sistemas de seguros individuales o colectivos. Se encuentran sujetas a las tarifas que establezca la Secretaría de Economía con opinión de la de Salud, ambas Federales. Si se tratara de personas de escasos recursos, la ley contempla que sus servicios deben ser gratuitos. Adicional a lo anterior, deben colaborar en la prestación de los servicios básicos de salud con especial atención en la educación, prevención y control de enfermedades transmisibles de atención prioritaria, planificación familiar y disponibilidad de insumos; proporcionar servicios de urgencias, notificar las enfermedades transmisibles a la autoridad sanitaria, proporcionar atención médica a la población en casos de desastre; colaborar en la formación y desarrollo de recursos humanos para la salud y desarrollar actividades de investigación. Los de carácter social son los que presten, ya sea directamente o mediante la contratación de seguros individuales o colectivos, aquellos grupos y organizaciones sociales a sus miembros y a sus beneficiarios. En cuanto a sus tarifas, se sujetan a las mismas disposiciones que los privados.

A partir de 2011, todo establecimiento que preste servicios de atención médica, no importando el sector al que pertenezca, debe contar de acuerdo con su grado de complejidad y nivel de resolución con un Comité Hospitalario de Bioética para

la resolución de problemas derivados de la atención médica que también promoverá la educación bioética permanente a sus miembros y al personal del establecimiento; y un Comité de Ética en investigación para evaluar y determinar los protocolos de investigación en seres humanos a cuyas recomendaciones es obligatorio dar seguimiento, siempre que se lleven a cabo actividades de investigación en seres humanos.[73]

Además de los comités, los establecimientos deben presentar el aviso de funcionamiento en el que se expresen las características y tipo de servicio que presta y en caso de ser privado, también señalará a su responsable sanitario, por lo menos con 30 días de anticipación al inicio de sus operaciones, quien además deberá contar con título, certificado o diploma con los que acredite los conocimientos necesarios y que cuentan con la obligación de establecer y vigilar del desarrollo de los procedimientos ofrecidos; vigilar la aplicación de las medidas de seguridad e higiene del personal a su cargo; atender las reclamaciones que se formulen por irregularidades en la prestación de los servicios sin perjuicio de la responsabilidad profesional en que pueda incurrirse; informar de las enfermedades de notificación obligatoria, adoptar las medidas de vigilancia epidemiológica, así como notificar al Ministerio Público o a las autoridades competentes de los casos en que se les requieran servicios de atención médica para personas con lesiones o signos que se presuman vinculados con la comisión de hechos ilícitos.

Es importante mencionar, que los establecimientos que tengan como finalidad la atención de usuarios que se internen para su diagnóstico, tratamiento o rehabilitación, y que también pueden tratar pacientes ambulatorios, así como llevar a cabo actividades de formación y desarrollo de personal para la salud y de investigación se consideran hospitales y atendiendo a su grado de complejidad pueden clasificarse como:

[73] Ambos Comités se sujetarán a las disposiciones de la Comisión Nacional de Bioética y deberán ser interdisciplinarios y e integrados por personal médico de distintas especialidades, así como por profesionales de la psicología, enfermería, trabajo social, sociología, antropología, filosofía o derecho que cuenten con la capacitación en bioética y además deberán contar con representantes del núcleo afectado de los usuarios de los servicios de salud.

a. Hospital general de segundo o tercer nivel para atención de pacientes si cuenta con las cuatro especialidades básicas de la medicina, es decir, cirugía general, gineco-obstetricia, medicina interna, pediatría y otras especialidades complementarias y de apoyo derivadas que prestan servicios de urgencias, consulta externa y hospitalización.

b. Hospital de especialidades, siendo aquellos de segundo o tercer nivel para la atención de pacientes de una o varias especialidades médicas, quirúrgicas o médico-quirúrgicas que presta servicios de urgencias, consulta externa, hospitalización y que deberá realizar a favor de los usuarios actividades de prevención, curación, rehabilitación y de cuidados paliativos, así como de formación y desarrollo de personal para la salud y de investigación científica.

c. Instituto, si se trata de un establecimiento de tercer nivel cuya actividad principal la constituye la investigación científica, la formación y el desarrollo de personal para la salud y que puede proporcionar servicios de urgencias, consulta externa, de hospitalización y de cuidados paliativos, a personas que tengan una enfermedad específica, afección de un sistema o enfermedades que afecten a un grupo etario.

Finalmente, cualquier establecimiento tiene prohibido la realización de ciertas acciones, de acuerdo con su actividad primordial. Por ejemplo, los responsables de establecimientos destinados al proceso de medicamentos no pueden prestar servicios de atención médica si no cuentan con la documentación que los acredite como profesionales de la medicina; la misma prohibición tiene el personal que labore en establecimientos destinados al proceso de órtesis y ayudas funcionales. Igualmente, el personal de cualquier establecimiento no puede celebrar contratos con el usuario respecto a la institución, exceptuando los que se relacionan con sus obligaciones económicas respecto de los servicios solicitados.

En otro orden de ideas, existen diversas definiciones de quienes se acercan a pedir, para sí o para terceros, atención médica. La Ley General de Salud, de 07 de febrero de 1984 considera como usuario de los servicios de salud a cualquier persona que los requiera y obtenga en cualquier sector, de acuerdo con las condiciones y conforme a las bases que para cada modalidad contempla la norma en cita y las que resultan vigentes y aplicables.

Por otro lado, la definición del vocablo paciente se encuentra en la NOM-004-SSA3-2012 Del expediente clínico, de 29 de junio de 2012, y le considera con esa condición a todo aquel usuario directo de la atención médica. En cambio, para el Reglamento de la Ley General de Salud en Materia de Prestación de Servicios de Atención Médica, de 14 de mayo de 1986, se trata de "toda aquella persona que para sí o para otro solicite la prestación de servicios de atención médica" es un demandante; un paciente ambulatorio "aquel usuario de servicios de atención médica que no necesite hospitalización" y "toda aquella persona que requiera y obtenga la prestación de servicios de atención médica" se considera usuario.

El numeral 3.58 de la Norma Oficial Mexicana NOM-035-SSA3-2012, En Materia de información para la salud de 30 de noviembre de 2011, lo define a la población usuaria como las "personas que utilizan al menos una vez al año los servicios de salud". Para efectos de esta investigación, por su acepción más amplia, será utilizada la penúltima de las enunciadas. Además de los que ya se han mencionado, entre algunos de los derechos con los que cuentan, están el de elegir a su médico tratante de forma libre y voluntaria; pero si se trata de su ejercicio en una institución de seguridad social, únicamente los asegurados, a su favor y el de sus beneficiarios podrán hacerlo, no así estos últimos. De igual forma, contarán con las facilidades que les permitan tener acceso a una segunda opinión acerca de su caso.

También tienen derecho ser informados y de consentir los procedimientos, diagnósticos terapéuticos y quirúrgicos que les sean indicados y aplicados, de manera libre y voluntaria, y de contar con su expediente clínico, así como de ser tratados con confidencialidad. Deberán apegarse a las reglamentaciones

internas de los prestadores de servicios, privilegiando en todo momento el buen uso de los materiales y equipos médicos a su alcance y disposición. En este sentido, por ejemplo, estos últimos regularán las modalidades de acceso a los servicios de salud, quienes para efecto de identificación de los usuarios pueden implementar registros biométricos y otros medios de identificación electrónica.

Los usuarios podrán involucrarse con los prestadores de servicios de los tres ámbitos, en acciones de promoción de hábitos saludables de conducta, prevención o tratamiento de problemas ambientales vinculados a la salud; como auxiliares voluntarios en tareas simples de atención médica y asistencia social, en la notificación de personas que requieran de estos servicios, la formulación de sugerencias para la mejora de los servicios; también mediante la información a las autoridades sanitarias acerca de efectos secundarios y reacciones adversas de los medicamentos consumidos ya sea por su consumo o por su disposición final y con información a las autoridades competentes de las irregularidades o deficiencias en la prestación de los servicios de salud.

Respecto al último punto, si los usuarios tuvieran alguna queja del servicio que les fue proporcionado, pueden presentarla ante el propio prestador de servicio o a las instancias que existan para tal fin por ejemplo los órganos internos de control o las Comisiones de Arbitraje Médico[74], en el ámbito de su competencia. De esta forma, los prestadores de salud deberán establecer los procedimientos de orientación, asesoría y los mecanismos necesarios para que los usuarios o promoventes las presenten, así como sus reclamaciones o sugerencias proporcionando esos servicios tanto en español y en la lengua materna de los usuarios pertenecientes a comunidades indígenas.

Igualmente, se prevé la concesión de la acción popular para denunciar ante las autoridades sanitarias cualquier hecho, acto u omisión que represente un riesgo o provoque un daño a la salud de la población, que podrá ejercitarse por

[74] De conformidad con el Decreto de Creación de la Comisión Nacional de Arbitraje Médico publicado en el Diario Oficial de la Federación del tres de junio de 1996, se trata de un órgano desconcentrado de la Secretaría de Salud, con plena autonomía técnica para emitir sus opiniones, acuerdos y laudos. Fue creada para contribuir a resolver los conflictos suscitados entre los usuarios de los servicios médicos y sus prestadores de servicios.

cualquier persona. Para darle curso, únicamente se necesita que el denunciante señale los datos para localizar la causa de riesgo. Específicamente, quienes sean beneficiarios de la prestación gratuita de servicios de salud, tienen derecho a recibir esos servicios sin discriminación y en condiciones de igualdad, de forma integral, con un trato digno y respetuoso y con atención de calidad; a recibir los medicamentos e insumos asociados de manera gratuita. Los derechos especificados en los párrafos anteriores también les están garantizados. Destaca especialmente el derecho de no cubrir ningún tipo de cuotas de recuperación o cualquier costo por los servicios de salud, medicamentos y demás insumos asociados.

En cuanto a sus obligaciones, se contemplan la de participar en acciones de educación y promoción para la salud y prevención de enfermedades; la de informarse acerca de los procedimientos que rigen el funcionamiento de los establecimientos que les brinden los servicios; a colaborar con el equipo de salud informando con veracidad y exactitud acerca de sus antecedentes, necesidades y problemas; a cumplir con las recomendaciones, prescripciones, tratamiento o procedimiento al que hay aceptado someterse; a informarse acerca de los riesgos y alternativas de los procedimientos terapéuticos y quirúrgicos que les sean indicados y de los de consultas y quejas; a dar un trato respetuoso a todo el personal prestador de servicios de salud, a los usuarios y sus acompañantes; a cuidar las instalaciones, colaborar en su mantenimiento, a hacer un uso responsable de los servicios y a proporcionar de manera fidedigna la información indispensable para su incorporación a este tipo de servicios.

Sin embargo, el beneficio podrá suspenderse si realizan acciones en su perjuicio o afecte intereses de terceros; se proporcione información falsa para determinar su condición laboral o de beneficiario de la seguridad social o bien, si el usuario se incorpora por sí o indirectamente, a alguna institución de seguridad social, federal o local.

3.3.1.2 El Sistema Nacional de Información en Salud.

El Reglamento de la Ley General de Salud, de 7 de febrero de 1984 en materia de protección social en salud, de 5 de abril de 2004, contempla la obligación de la Secretaría de evaluar integralmente el Sistema Nacional de Salud mediante la creación de un subsistema de información especializado que sea alimentado con la información de los Regímenes Estatales y de los recursos con los que el sistema sea financiado. Su fuente primaria de información será la contenida en el padrón de beneficiarios del Sistema Nacional de Salud y la de sus expedientes clínicos, elaborados de acuerdo con lo establecido en la Norma Oficial Mexicana NOM 004-SSA2-2012, del expediente clínico, de 29 de junio de 2012. Mediante este sistema, se proveerá la información actualizada a los servicios de consulta externa, urgencias y hospitalización de las especialidades consideradas básicas, a saber, gineco-obstetricia, cirugía general, medicina interna, pediatría y geriatría; así como la correspondiente a medicamentos e intervenciones cubiertas por el Fondo de Protección contra Gastos Catastróficos.

Toda la terminología será la señalada por la Norma NOM-035-SSA3-2012 en Materia de Información en Salud, de 30 de noviembre de 2011, cuyo objetivo es el de establecer los criterios y procedimientos a seguir para producir, captar, integrar, procesar, sistematizar, evaluar y divulgar la información en salud. Su observancia es obligatoria en todo el territorio nacional para todo aquel integrante del Sistema Nacional de Salud que preste servicio de atención a la salud en establecimientos fijos y/o móviles.

Como mecanismo para el cumplimiento de lo anterior, se contempla que esta norma regule al Centro de Inteligencia en Salud, que se constituye por un conjunto de procesos específicos para integrar, usar y explotar la información en materia de salud para presentar indicadores, así como estadísticas relevantes y prioritarias para la toma de decisiones en políticas públicas en la materia.

Como se ha visto, la información en materia de salud será utilizada con fines estadísticos por lo que se reitera la importancia de su estudio para conocer la forma en que se lleva a cabo su recopilación y posterior disociación y así conocer

si se cumple con los principios básicos de la protección de los datos personales durante este proceso. Así, toda la información que el Sistema Nacional de Salud genere deberá estar apegada a lo dispuesto en la legislación en materia de transparencia y protección de datos personales, que ya analizamos en apartados anteriores.[75]

En cuanto al flujo de información, establece que el Sistema Nacional de Salud, conforme a sus atribuciones, será el encargada de concentrar la información generada por el Sistema Nacional de Información e Salud (SINAIS) y el Sistema Nacional de Información Básica en Materia de Salud (SNIBMS), así como su órgano rector; dentro de la información que resulta relevante para su transmisión se encuentran aspecto tales como población y cobertura, recursos para la salud o nacimientos.

Esta deberá ser entregada por trimestre, semestre o de manera anual según sea el caso, además con desagregación por unidad médica, localidad, municipio y entidad federativa, lo que dependerá de las necesidades de la Secretaría, a través de los formatos y especificaciones determinados por cada componente del SINAIS en medios electrónicos o sistemas informáticos, además debe cumplir con los siguientes atributos de calidad, cuya medición, seguimiento y difusión se hará de acuerdo a los procedimientos establecidos por la Dirección General de Información en Salud (DGIS):

1. Oportunidad, es decir, que la información debe estar disponible de manera pronta, de manera proporcional a la fecha de ocurrencia del evento o desde la fecha de la solicitud.
2. Cobertura, en referencia a la proporción de la población objetivo, captada en un sistema de información.

[75] Por ser expedida en 2012, la Norma NOM-035-SSA3-2012 en Materia de Información en Salud, de 30 de noviembre de 2011 no contempla la observancia de la Ley General de Transparencia y Acceso a la Información Pública ni la General de Protección de Datos Personales e Posesión de Sujetos Obligados, que deberán ser cumplida en los términos y aplicabilidad correspondiente a partir de su entrada en vigor en los años 2016 y 2017, respectivamente.

3. Integridad, en tanto que la información será completa indicada por la proporción de la información faltante.
4. Validez, en referencia a la proporción de la información fuera de los rangos y valores permitidos.
5. Veracidad, respecto a la concordancia entre la información captada y la realidad.
6. Consistencia, de conformidad a la coherencia interna de la información contenida en cada sistema de información y a la coherencia externa entre sistemas.

La NOM-035-SSA3-2012, en materia de información en salud de 30 de noviembre de 2011, también define los lineamientos de recogida de información de diversos módulos tales como población, cobertura, recursos para la salud, recursos humanos, recursos físicos y materiales, infraestructura, equipo médico, recursos financieros, servicios para la salud, captando como mínimo los datos que ahí se señalan y que en el último de los módulos contempla datos del paciente y sobre la atención médica que le fue proporcionada, es decir, que se incluye el tratamiento de datos personales sensibles.

Para dar certidumbre de la veracidad de la información, ésta se cotejará desde el establecimiento de salud y se deberá capacitar a todo el personal involucrado en estos procesos. También serán informados de las implicaciones legales que pueden derivarse de la no observancia de la normativa correspondiente. En cuanto a los módulos de nacimientos, daños a la salud y mortalidad, los datos son recabados y sistematizados para fines epidemiológicos y estadísticos, de morbilidad, motivos de atención y planeación y asignación de recursos.

La norma dispone que la información publicada en el SINAIS es la única fuente oficial, por lo que deberá ser utilizada para integrar informes de carácter nacional o internacional; en cada uno de los niveles operativos de este sistema se deben adoptar las medidas necesarias para garantizar la seguridad de la información, evitar su alteración, pérdida, transmisión y acceso no autorizado. El uso y difusión de la información se sujeta a los principios de confidencialidad y reserva que establecen las legislaciones vigentes en la materia y que han sido referidas

en el cuerpo de este subtítulo, así como las que resulten aplicables en materia de transparencia y protección de datos personales.

3.3.2 El Sistema Nacional de Salud Español.

El Sistema Nacional de Salud se encuentra descrito en la Ley 14/1986 de 25 de abril, General de Sanidad, pero también, en la Ley 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud. La primera de ellas nos describe en su exposición de motivos el recorrido legislativo que ha seguido el país peninsular para implementar el sistema tal como se le conoce hoy en día y cita, entre sus antecedentes más importantes, los enunciados a continuación:

Tabla 6. Evolución histórica del Sistema Nacional de Salud Español.

1822	Proyecto de Código Sanitario	No prosperó por las disputas acerca de la exactitud científica de los medios técnicos en que pretendía apoyarse.
1855	Ley de 28 de noviembre de 1855	Consagra a la Dirección General de Sanidad.
1904	Real Decreto-Ley de 12 de enero de 1904	Aprueba la Instrucción General de Sanidad.
1934	Ley de Coordinación Sanitaria de 11 de junio de 1934	Primer intento de racionalización del sistema de salud.
1942	Ley de 14 de diciembre de 1942	Se constituye el Seguro Obligatorio de Enfermedad, bajo el Instituto Nacional de Previsión.
1944	Ley de Bases de 1944	La Dirección General de Sanidad se convierte en órgano supremo, con competencias para atender ´problemas sanitarios de la colectividad y de acciones de prevención, pero deja al margen la función asistencia y la salud individual.
1962	Ley de Hospitales de 21 de julio de 1962	Racionalización del sistema también en el ámbito de los servicios centrales, así como de la creación de numerosas Comisiones Interministeriales.
1974	Decreto 2065/1974, de 30 de mayo	Reestructuración del Seguro Obligatorio de Enfermedad.
1986	Ley 14/1986, de 25 de abril, General de Sanidad	Creación del Sistema Nacional de Salud.

Fuente: elaboración propia, a partir de la exposición de motivos de la Ley 14/1986, de 25 de abril, General de Sanidad.

De esta forma, a través de la Ley 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud se crea el Sistema Nacional de Salud español,

que se considera como el conjunto de los servicios de salud de las Comunidades Autónomas que se coordinan entre sí bajo el principio de integración consagrado en su artículo 50.

Si bien es cierto que en el capítulo I del su primer título habla del sistema de salud, orientado a la promoción de la salud y la prevención de las enfermedades, extendiendo la asistencia a la población española, en condiciones de igualdad efectiva y superando cualquier desequilibrio territorial y social, integrando en sus objetivos y actuaciones el principio de igualdad entre mujeres y hombres.

Su ámbito de aplicación se extiende a las prestaciones sanitarias, la farmacia, los profesionales, la investigación, los sistemas de información, la calidad del sistema sanitario, los planes integrales, la salud pública y la participación de ciudadanos y profesionales, con el seguimiento del Consejo Interterritorial y la Alta Inspección, de acuerdo con la Ley 16/2003.

Entre sus características fundamentales, se cuentan la de la extensión de sus servicios a toda la población; la de su organización adecuada para prestar una atención integral de la salud que comprenda su promoción, prevención, curación y rehabilitación procurando altos niveles de calidad; la coordinación e integración de todos los recursos sanitarios públicos en un dispositivo único y su financiación de las obligaciones por recursos de las Administraciones Públicas.

Se encuentra mandatado la organización y desarrollo de las acciones sanitarias por parte del Estado, las Comunidades Autónomas y las administraciones públicas competentes que deben crear sus Servicios de Salud, cuyas actuaciones deben apegarse a la promoción de la salud, la del interés individual, familiar y social a través de la educación sanitaria de la población; a la garantía de la prevención y no solo la curación de las enfermedades y a la de la asistencia sanitaria en cualquier caso de pérdida de salud; a la promoción de las acciones de rehabilitación funcional y reinserción social del paciente y a la ejecución de la integración del principio de igualdad entre mujeres y hombres para garantizar a su vez el de la salud. Al mismo tiempo, los servicios sanitarios obedecerán en

cuanto a su organización y funcionamiento a los principios de eficacia, celeridad, economía y flexibilidad.

También deberán desarrollarse acciones tales como la educación sanitaria para la mejora de la salud individual y comunitaria con las diferencias necesarias entre mujeres y hombres y con formación contra la discriminación de las primeras; la atención primaria integral de la salud que incluyan las curativas y rehabilitatorias; la asistencia sanitaria especializada, domiciliaria, hospitalización y rehabilitación; la prestación de productos terapéuticos precisos; los programas de atención a grupos poblacionales de riesgo; la promoción y la mejora de sistemas de saneamiento, abastecimiento de aguas, eliminación y tratamiento de residuos líquidos y sólidos, saneamiento y control del aires, vigilancia sanitarios y adecuación a la salud del medio ambiente.

De igual forma, deberán atender temas de orientación en materia de planificación familiar; promoción y mejora de la salud mental y laboral; el control sanitario y prevención de riesgos para la salud derivados de productos alimentarios, farmacéuticos y otros que pongan en riesgo la salud de las personas; la promoción y mejora de actividades de veterinaria de salud pública; la difusión de la información epidemiológica general; la formación del personal de salud; el fomento a la investigación científica; el control y mejora de la calidad de la asistencia sanitaria en cualquiera de sus niveles; el tratamiento de los datos estadísticos necesarios para el análisis respectivo y la promoción, extensión y mejora de los sistemas de detección de discapacidades, para su reducción o la intensificación de las ya existentes.

En consonancia con lo anterior, la Ley 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud, considera fundamental la realización de estudios epidemiológicos para orientar las políticas preventivas de los riesgos para la salud y la planificación y evaluación sanitaria, incluyendo para el mismo efecto la actividad básica de la veterinaria de salud pública. En cuanto a su catálogo de prestaciones, se comprende a las relacionadas a la salud pública, la

atención primaria[76], la especializada[77] y la sociosanitaria[78]; la atención de urgencias, la prestación farmacéutica, la ortoprotésica, de productos dietéticos y de transporte sanitario.

Su cartera común básica incluye todas las actividades asistenciales de prevención, diagnóstico, tratamiento y rehabilitación que se realicen en centros sanitarios o sociosanitarios, el transporte sanitario urgente, de tal suerte que se dé continuidad asistencial con enfoque multidisciplinar enfocado en el paciente, con la máxima garantía de calidad y seguridad en la prestación del servicio sanitario y también las condiciones de accesibilidad y equidad de todas las personas beneficiarias del Sistema Nacional de Salud.

La cartera suplementaria, por otra parte, contiene la prestación farmacéutica, ortoprotésica y con productos dietéticos, así como el transporte sanitario no urgente de prescripción facultativa. La cartera accesoria incluye las actividades, servicios o técnicas, sin carácter de prestación y que por lo tanto no se consideran esenciales o que son coadyuvantes o de apoyo para mejorar las patologías de carácter crónico y que se encuentran condicionadas a aportación y/o reembolso del usuario. La cartera de servicios complementaria de las

[76] Comprende la asistencia sanitaria a demanda, programada y urgente tanto en la consulta como en el domicilio del enfermo; la indicación o prescripción y la realización, en su caso, de procedimientos diagnósticos y terapéuticos; las actividades en materia de prevención, promoción de la salud, atención familiar y atención comunitaria; las actividades de información y vigilancia en la protección de la salud; la rehabilitación básica; las atenciones y servicios específicos relativos a las mujeres, que específicamente incluirán la detección y tratamiento de las situaciones de violencia de género; la infancia; la adolescencia; los adultos; la tercera edad; los grupos de riesgo y los enfermos crónicos; la atención paliativa a enfermos terminales; la atención a la salud mental, en coordinación con los servicios de atención especializada y la atención a la salud bucodental, de conformidad con la Ley 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud.

[77] La misma legislación establece que la atención sanitaria especializada comprenderá la asistencia especializada en consultas; la asistencia especializada en hospital de día, médico y quirúrgico; la hospitalización en régimen de internamiento; el apoyo a la atención primaria en el alta hospitalaria precoz y, en su caso, la hospitalización a domicilio; la indicación o prescripción, y la realización, en su caso, de procedimientos diagnósticos y terapéuticos; la atención paliativa a enfermos terminales; la atención a la salud mental; la rehabilitación en pacientes con déficit funcional recuperable. Se prestará, siempre que las condiciones del paciente lo permitan, en consultas externas y en hospital de día.

[78] La Ley 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud establece que la atención sociosanitaria se llevará a cabo en los niveles de atención que cada comunidad autónoma determine y en cualquier caso comprenderá a los cuidados sanitarios de larga duración, la atención sanitaria a la convalecencia y la rehabilitación en pacientes con déficit funcional recuperable.

comunidades autónomas deberá incluir por lo menos a la común en modalidad básica de servicios asistenciales, suplementaria y de servicios accesorios, aunque podrán incorporar la técnica, tecnología o procedimiento no contemplado en la común y deberán asumirlas con cargo a su presupuesto.

En cuanto a la atención de urgencia, esta se proporciona al paciente en cualquier caso de situación clínica que obliga a una atención sanitaria inmediata, en los centros sanitarios o fuera de ellos hasta en el domicilio del paciente, de manera permanente mediante la atención médica y de enfermería. Llama la atención que Ley 33/2011, de 4 de octubre, General de Salud Pública impone el deber de informar a los usuarios de los servicios, aunque únicamente del sistema sanitario público o los que a él se vinculen, sus derechos y deberes a los poderes públicos y no solamente a quienes forman parte del sistema. A los que, si cuentan con las prestaciones de este, tienen derecho a la información y documentación sanitaria y asistencial de conformidad con la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

Por lo que hace a otros derechos de los usuarios, se consideran el del respeto a su personalidad, dignidad humana e intimidad y a no ser discriminado; a ser informado sobre los servicios sanitarios a los que puede tener acceso y los requisitos para su uso; a la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones públicas o privadas, pero siempre que estas colaboren con el sistema público y a ser notificado de si los procedimientos a lo que se someta son susceptibles de utilizarlos para un proyecto docente o de investigación; a que le sea asignado un médico. También tienen derecho a participar en las actividades sanitarias a través de las instituciones comunitarias; a utilizar los mecanismos establecidos para interponer una reclamación o una sugerencia; a elegir el médico y los profesionales sanitarios y a obtener los medicamentos y productos sanitarios necesarios para la promoción, conservación o restablecimiento de su salud.

Si la atención primaria ha sido superada por el caso particular del usuario del sistema de salud, tiene derecho a ser atendido en los servicios especializados

hospitalarios. Abunda en este sentido la Ley 33/2011, de 4 de octubre, General de Salud Pública al establecer como derechos de los ciudadanos el de información, de participación, a la igualdad, a la intimidad, confidencialidad y respeto a su dignidad. También se establecen como derechos de los ciudadanos en el conjunto del Sistema Nacional de Salud, a disponer de una segunda opinión facultativa sobre su proceso, a recibir asistencia sanitaria en su comunidad autónoma de residencia y también la asistencia sanitaria del catálogo de prestaciones del Sistema en la comunidad autónoma en la que el ciudadano se encuentre desplazado.

Igualmente, la Ley 33/2011, de 4 de octubre, General de Salud Pública considera como obligaciones de los ciudadanos el cumplir con las prescripciones generales de naturaleza sanitaria; cuidar las instalaciones y colaborar en el mantenimiento de las instituciones sanitarias y responsabilizarse del uso adecuado de las prestaciones ofrecidas por el sistema sanitario. También impone como sus deberes el de colaboración para el desarrollo de las actuaciones de salud pública y para abstenerse de realizar conductas que impidan su ejecución; y el de comunicación para que den a conocer hechos, datos o circunstancias que constituyan un riesgo o peligro grave para la salud de la población a las autoridades sanitarias.

Las personas que no cuentan con el derecho a la asistencia[79] de los servicios de salud podrán acceder a ellos como pacientes privados. En la atención primaria los serán aplicadas las mismas normas sobre asignación de equipos y libre elección que al resto de los usuarios; por lo que hace a los servicios hospitalarios, el ingreso dependerá de una lista de espera única[80] que no diferirá de la

[79] Este tema se encuentra regulado en Real Decreto 576/2013, de 26 de julio, por el que se establecen los requisitos básicos del convenio especial de prestación de asistencia sanitaria a personas que no tengan la condición de aseguradas ni de beneficiarias del Sistema Nacional de Salud. Para acceder al convenio, los solicitantes deberán acreditar la residencia efectiva en España por un año inmediato anterior a la fecha de la solicitud, estar empadronadas en algún municipio competente para su suscripción y no tener acceso a un sistema de protección sanitaria pública por cualquier título. Las cuotas se establecen por rango diferenciado de edad y también, las causas de extinción de este convenio.

[80] El Real Decreto 1039/2011, de 15 de julio, por el que se establecen los criterios marco para garantizar un tiempo máximo de acceso a las prestaciones sanitarias del Sistema Nacional de Salud, para que pueda efectuarse en condiciones de igualdad efectiva, regula entre otras cosas,

condición del paciente y la facturación tendrá lugar como ingresos propios de los servicios de salud que se hayan solicitado en los centros correspondientes.

En cuanto a las competencias del Estado español, Ley 33/2011, de 4 de octubre, General de Salud Pública establece como exclusivas las de sanidad exterior y las relaciones y acuerdos sanitarios internacionales, en consonancia con el artículo 149.1. 16.ª de la Constitución Española, de 29 de diciembre de 1978. También podrá desarrollar acciones de análisis y medición de requisitos técnicos para el control sanitario del medio ambiente; el registro general de alimentos y de las industrias que los producen; la autorización de componentes alimentarios para regímenes especiales, detergentes y desinfectantes empleados en esa industria.

Además, desarrollarán actuaciones acerca de reglamentación, autorización y registro de medicamentos de uso humano y veterinario, así como de productos que puedan suponer un riesgo para la salud de las personas, así como de quienes los preparan, elaboran o fabrican; la aprobación y homologación de instalaciones y equipos de centros y servicios y también los que tengan que ver con extracción y trasplante de órganos, así como la homologación de programas de formación posgraduada, perfeccionamiento y especialización del personal sanitario.

De igual forma se hace referencia a los puestos de trabajo del personal para garantizar la igualdad de sus oportunidades laborales; los servicios de vigilancia y análisis epidemiológicos y de las zoonosis; el establecimiento de sistemas de información sanitaria y la realización de estadísticas de interés general; la

---

los tiempos de espera de las listas en mención. En su anexo, establece como tiempo máximo en días naturales 180, para cinco intervenciones quirúrgicas especializadas: cirugía cardíaca valvular y coronaria; cataratas y prótesis de cadera y rodilla.
Lo relativo al tratamiento homogéneo de la información sobre las listas de espera en el Sistema Nacional de Salud, lo regula el Real Decreto 605/2003 de 23 de mayo, que se publicó con la finalidad de establecer criterios, indicadores y requisitos mínimos, básicos y comunes en listas de espera de consultas externas, pruebas diagnósticas/terapéuticas e intervenciones quirúrgicas. De su aplicación quedan excluidas las consultas externas, las pruebas diagnósticas y terapéuticas e intervenciones quirúrgicas de carácter urgente, así como las de trasplantes de órganos (que dependen de su disponibilidad) y las producidas en situaciones de catástrofe, así como las no contempladas en la legislación vigente como prestaciones básicas y comunes del Sistema Nacional de Salud.

coordinación de las actuaciones para impedir o perseguir el fraude, abuso, corrupción o desviación de prestaciones o servicios sanitarios en el sector público y el establecimiento de medios y sistemas de relación para garantizar la comunicación de la información recíproca entre la administración sanitaria del Estado y las Comunidades Autónomas.

Por lo que hace a estas últimas, cuando dispongan de la organización de sus servicios de salud deben tener en cuenta las responsabilidades y competencias de las provincias, municipios y las administraciones territoriales intracomunitarias. Específicamente los ayuntamientos tienen las responsabilidades mínimas de control sanitario del medio ambiente, de industrias, actividades y servicios, transportes, ruidos y vibraciones; de edificios y lugares de vivienda y convivencia humana; de la distribución y suministro de alimentos, bebidas y demás productos; de los cementerios y la policía sanitaria mortuoria.

La Ley 41/2002 considera al paciente como "la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud", mientras que un usuario es "la persona que utiliza servicios sanitarios *de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria*". Así, tal como señala la Ley de Ordenación de las Profesiones Sanitarias (Ley 44/2003) y el Estatuto Marco del Personal Estatutario de los Servicios de Salud españoles, el ejercicio de las profesiones sanitarias se llevará a cabo con plena autonomía técnica y científica, sin más limitaciones que las establecidas por la Ley y los principios y valores contenidos en el Código Deontológico, teniendo derecho y obligación a una formación continuada.

Mención aparte merecen las actividades sanitarias privadas cuyo ejercicio libre se encuentra reconocido en los artículos 35 y 36 de la Constitución Española de 29 de diciembre de 1978, al igual que la libertad de empresa en este sector, en el numeral 38. Sin embargo, Ley 33/2011, de 4 de octubre, General de Salud Pública indica la imposibilidad de vincular a los hospitales y establecimientos del sector privado en el Sistema Nacional de Salud, aunque sí deberán someterse a

las mismas inspecciones y controles sanitarios, administrativos y económicos que los públicos.

En materia de salud pública, la Ley 33/2011, de 4 de octubre, General de Salud Pública considera que la vigilancia es el conjunto de actividades que se realizan para recoger, analizar, interpretar y difundir información relacionada con el estado de salud de la población y los factores que la condicionan para dar fundamento a las actuaciones en esta materia y deberán tomar en cuenta por lo menos las condiciones sociales y las desigualdades que incidan en la salud; los riesgos ambientales y sus efectos en la salud; la seguridad y riesgos alimentarios; las enfermedades no transmisibles; los riesgos relacionados con el trabajo y sus efectos en la salud; las enfermedades transmisibles, zoonosis y las emergentes; los problemas de salud relacionados con el tránsito internacional de viajeros y bienes; las lesiones y la violencia y otros problemas que resulten relevantes en la materia, mediante sistemas de alerta precoz y respuesta rápida que permitan la detección y evaluación de incidentes, riesgos, síndromes y enfermedades a través de la Red de Vigilancia en Salud Pública.

En cuanto a la Autoridad Sanitaria Estatal, también la Ley 33/2011, de 4 de octubre, General de Salud Pública es la que señala que lo es la persona titular del Ministerio de Sanidad, Política Social e Igualdad, los titulares de los órganos superiores y órganos directivos de ese ministerio con rango igual o superior al de Director General. Esta autoridad podrá dictar disposiciones y actuará mediante los órganos con competencia, en actividades públicas o privadas para proteger la salud de la población. Adoptará medidas de carácter general para coordinar y ejecutar las actuaciones de salud pública y las medidas de intervención especial en esta materia en situaciones de urgencia o necesidad, o bien ante circunstancias extraordinarias que representen un riesgo para la salud de la población y destacando que la ley establece que debe respaldarlo la evidencia científica disponible y que puede solicitar el apoyo, auxilio y colaboración de funcionarios públicos, instituciones u órganos administrativos para el ejercicio de sus funciones. En caso de urgente necesidad, también podrá solicitar el auxilio de las Fuerzas y Cuerpos de Seguridad del Estado o de agentes de la autoridad que cuenten con funciones de seguridad.

Otro órgano del Sistema Nacional de Salud es la Comisión de Recursos Humanos, que tendrá a su cargo actividades de planificación, diseño de programas de formación y modernización de sus recursos humanos y también definirá los criterios básicos de evaluación de competencias de los profesionales sanitarios, con arreglo a la Ley 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud. La preside el Ministro de Sanidad, teniendo representación las comunidades autónomas y con la participación del Foro Marco para el Diálogo Social y la Comisión Consultiva Profesional. La misma legislación considera como centros de investigación del Sistema Nacional de Salud los que designe este ministerio a propuesta del Instituto de Salud Carlos III o las comunidades autónomas.

El instituto en mención fomentará las redes de investigación cooperativa que actuarán como estructuras de investigación y consulta científica por lo que podrán acceder a financiación específica y participar en programas europeos de investigación.

3.4 El soporte documental de los datos personales en el ámbito sanitario. El expediente clínico.

3.4.1 Marco conceptual.

El expediente clínico es el documento más importante en el que se refleja la atención que el facultativo brinda al usuario de los servicios de salud. Cantero (s.f) lo define desde diversas perspectivas. Por ejemplo, como “el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial”. Sin embargo, apunta que desde el punto de vista médico puede comprenderse como “el relato escrito o verbal de la enfermedad del paciente y, por extensión, el documento en que aquel relato se recoge o refleja y se guarda o conserva”.

Galán a su vez, (2020) afirma categórico que se trata de “la biografía patológica de la persona” en la que se da cuenta de la relación entre el médico y su paciente, y por este hecho considera que se trata de una prueba fundamental del actuar del profesional de la salud no solo para observar que haya cumplido con la legislación sanitaria y la lex artis, sino también con otras legislaciones como la de protección de datos personales, por lo que se encuentra sujeta a cuando menos, la doble regulación que se señala. Así, en palabras del autor que bien podemos comprender aplicables no solo en materia de legislación sanitaria, como veremos a lo largo de la investigación,

El expediente clínico ostenta, por consiguiente, una enorme importancia a la hora de juzgar la responsabilidad profesional del médico, ya que, entre otros extremos, puede darnos la clave de la relación de causalidad de su actuar y el daño sufrido por el paciente en el curso de la terapia impuesta.

Así, se trata de un documento fundamental para el titular de los datos que ahí se contienen derivado de su naturaleza y al mismo tiempo, porque da constancia de las circunstancias en que ha sido brindada la atención médica, por lo que constituye una prueba extraordinaria que puede incluso, ayudar a la resolución de asuntos judiciales o administrativos, como consideran Sánchez y Abellán (2006, p. 7).

Para Cantoral (2012, pp. 117,118), la importancia jurídica del expediente clínico se puede explicar a través de los siguientes principios:

1. Confidencialidad, que hace referencia que las partes eviten accesos no autorizados de terceros para salvaguardar el documento.
2. Claridad e inteligibilidad. La autora (p. 118), como también señala Galán (2020) a lo largo de su obra, considera que “el fin primario del expediente clínico es facilitar en todo lo posible la asistencia sanitaria” y partiendo de esa premisa es que destaca la importancia de que la información en él contenida sea lo suficientemente clara y entendible para no generar retrasos y errores.

3. Tutela de los derechos del paciente. La elaboración de este documento debe hacerse de tal manera, que todos los derechos que puedan relacionarse con “el proceso asistencial o como consecuencia de este” (Cantoral, p. 118) deberían estar tutelados.
4. Veracidad. Ya que la información contenida en el expediente clínico permitirá el conocimiento acertado de la situación del paciente.
5. Complitud. Toda la información necesaria para la atención del paciente debe plasmarse en este documento. Igualmente se refiere a la forma en que debe asentarse, esto es, sin abreviaturas y que sea legible; además deberán incluirse en el registro todos los actos médicos practicados, o la manera de acceder a esa información.
6. Autenticidad del contenido. La autora lo relaciona con el deber de custodia y archivo de la institución o el personal sanitario a quien corresponda esta responsabilidad, para garantizar la inviolabilidad de su contenido, pero también, el derecho de acceso que el paciente tiene a la información en él contenida y que esta misma acción pueda realizarla el facultativo para que su proceso asistencial sea el adecuado.
7. Unidad e integración. En su resguardo, esto es, que exista un archivo a nombre de un solo paciente.

Galán (2020, pp. RB-4,10)[81] identifica como finalidad principal de este documento brindar con mayor facilidad la asistencia sanitaria solicitada de manera adecuada, aunque no deja de reconocer que posee fines tales como el “judicial, epidemiológico, de salud pública, de investigación de docencia e inspección, organización, planificación, evaluación, acreditación y funcionamiento del sistema sanitario”.

Conviene mencionar, sin embargo, antes de explorar la definición que la legislación vigente ofrece, que la mexicana prefiere el término “expediente clínico” al de “historia clínica”, este último utilizado ampliamente en la legislación internacional, como la española o la uruguaya, cuestión que obedece a que la

[81] Este es el formato de las páginas en la aplicación de la editorial Thomson Reuters Proview, mediante la que se consultó la versión electrónica de la obra de Galán.

historia clínica es parte integrante del expediente, según la Norma Oficial Mexicana NOM-004-SSA3-2012, Del *expediente* clínico de 29 de junio de 2012.

3.4.2 Expediente clínico en el Sistema Nacional de Salud Mexicano.

La Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012, ofrece una definición con mayor especificidad y bajo la denominación de expediente clínico, al conjunto único de información y datos personales de un paciente, que se integra dentro de todo tipo de establecimiento para la atención médica en los ámbitos público, privado y social que conforman al Sistema Nacional de Salud y la Norma Oficial recién citada lo considera como el instrumento que materializa el derecho a la protección de la salud.

Este documento tiene tal trascendencia, que el Reglamento de la Ley General de Salud, en materia de protección social en salud, de 5 de abril de 2004, lo señala como fuente primaria de información, junto con la contenida en el padrón del Sistema de Protección Social en Salud, y deberá ser integrado de acuerdo con la normativa aplicable, por cada uno de sus beneficiarios.

En él constan los registros, anotaciones, constancias y certificaciones correspondientes de las intervenciones que el personal de salud realiza para dar atención al paciente, apegado a las disposiciones jurídicas aplicables a través de documentos que pueden encontrarse en cualquier tipo de soporte, ya sea escrito, gráfico, imagenológico, electrónico, magnético, electromagnético, óptico, magnetoópticos o de cualquier índole.

Por otra parte, considera al resumen clínico como el documento elaborado por un médico, en el que se registran los aspectos relevantes de la atención médica de un paciente, contenidos en el expediente clínico y deberá contener como datos mínimos el padecimiento actual, diagnósticos, tratamientos, evolución, pronóstico y estudios de laboratorio y gabinete. Establecer la diferencia entre ambos documentos es importante ya que en esta la Norma Oficial Mexicana NOM-004-SSA3-2012 del expediente clínico, de 29 de junio de 2012, se prevé proporcionar el resumen clínico al titular de los datos personales; mientras que

el expediente, únicamente podrá ser proporcionado a las autoridades judiciales, órganos de procuración de justicia y autoridades administrativas, como autoridades competentes para solicitarlos.

De forma específica, se dispone la integración del expediente clínico en atención a los servicios genéricos de consulta general, de especialidad, de urgencias y hospitalización; pero si en un mismo establecimiento se proporcionan varios servicios, debe integrarse un único expediente por cada paciente en el que se harán constar los documentos que cualquier prestador de servicio genere al atenderle. Lo mismo sucede con las evidencias de atención que se generen en materia de odontología, nutriología, atención psicológica o similares y los de transfusión de unidades de sangre o sus componentes, que atenderán de igual forma lo dispuesto a en las Normas Oficiales Mexicanas correspondientes al tema que se trate.

Ahora bien, si en un mismo establecimiento se proporcionan diversos servicios, deberá integrarse un solo expediente por cada paciente, donde constará cualquier documento que sea generado por el personal sanitario que intervenga en su atención.

El expediente clínico en consulta general y de especialidad deberá contar como mínimo con la historia clínica, y debe contener en el orden que se citan, los apartados de:

1. Interrogatorio.
2. Exploración física.
3. Resultados previos y actuales de estudios de laboratorio, gabinete y otros.
4. Diagnósticos o problemas clínicos.
5. Pronóstico, indicación terapéutica y nota de evolución. Esta última deberá elaborarse de conformidad al estado clínico del paciente, cada vez que se le proporciona atención y debe describir su evolución y actualización del cuadro clínico, signos vitales, resultados relevantes de servicios auxiliares de diagnóstico y tratamiento, diagnóstico o problemas clínicos, pronóstico y tratamiento e indicaciones médicas.

6. La historia clínica deberá contemplar también un apartado donde conste la nota de interconsulta con la solicitud al médico especialista y los resultados de la consulta efectuada; la nota de referencia o traslado en caso de ser requerida.
7. Por lo que respecta a las notas médicas en el servicio de urgencias, estas deberán ser elaboradas por el médico que proporciona la atención y deberá señalar la fecha y hora del servicio, los signos vitales, el motivo de la atención, el resumen del interrogatorio, la exploración física y estado mental de requerirse.
8. Resultados relevantes de los estudios de los servicios auxiliares de diagnóstico y tratamiento que se hayan solicitado, los diagnósticos o problemas clínicos, el tratamiento y pronósticos, la nota de evolución, la de interconsulta, referencia o traslado, de ser necesarias.
9. Si fuera necesario un servicio de hospitalización, la nota médica deberá ser elaborada por el médico que ingresa al paciente al servicio y deberá incluir información referente a las circunstancias de entrada del paciente, sus signos vitales, un resumen del interrogatorio, exploración física y estado mental, resultados de estudios, tratamiento y pronóstico, historia clínica; notas de evolución, de referencia y traslado, preoperatoria elaborado por el cirujano que va a intervenir al paciente que como mínimo debe referir la fecha de la cirugía, diagnóstico, plan quirúrgico, tipo de intervención, riesgos, cuidados y plan terapéutico preoperatorio así como el pronóstico.
10. Las notas de hospitalización deben incluir también las preanestésicas de vigilancia y registro de ese servicio, la posoperatoria que mencione la técnica utilizada y los hallazgos transoperatorios, además del conteo de material, incidentes, accidentes, sagrado, transfusiones, personal interviniente y el plan de manejo y tratamiento postoperatorio inmediato, el pronóstico del paciente, el envío de piezas o biopsias quirúrgicas y cualquier hallazgo de importancia para el estado de salud del paciente, debiendo firmarla el responsable de la cirugía.
11. Las notas de egreso, que deberán contemplar la fecha de ingreso y egreso del paciente, el motivo por el que deja el servicio, su diagnóstico final, el resumen de la evolución de su salud y su estado actual, el manejo

que se le dio durante su estancia hospitalaria, si existe algún problema clínico pendiente, su plan de manejo y tratamiento, las recomendaciones pertinentes para su vigilancia ambulatoria, señalando los factores que supongan un riesgo para su salud; el pronóstico de su estado y si el egreso se debió a su defunción, habrá que indicar las causas que la originaron en concordancia a su certificado de defunción y de la necropsia hospitalaria de haberse realizado.

El expediente clínico también debe contener reportes del personal profesional y técnico que interviene en la atención del paciente, como el de enfermería, y otros documentos tales como las cartas de consentimiento informado, la de egreso voluntario, la de notificación al Ministerio Público para los casos en que sea necesario avisar a los órganos de procuración de justicia; también pueden incluirse otros documentos como las notas de defunción y de muerte fetal. Inclusive, desde nuestra perspectiva, será el lugar idóneo para resguardar los consentimientos informados para el uso y tratamiento de los datos personales que se traten y tengan que ver con la atención médica, en los supuestos en que proceda su otorgamiento de acuerdo con la legislación respectiva.

La Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012 establece que el prestador de servicios de salud deberá incluir en las notas clínicas de urgencia reportes del personal profesional y técnico, notas preoperatorias, preanestésica, vigilancia y registro anestésico, posoperatoria, nota de egreso consentimiento informado y cartas de consentimiento informado, cuya elaboración está sujeta a los requisitos mínimos que establece esta norma así como los eventos mínimos en los que se requiere su elaboración, lo que no excluye casos a los diversos presentados para los que no es obligatorio el empleo de formatos impresos. De forma optativa, el expediente contendrá cubierta o carpeta y hoja frontal, así como las notas que en su caso llegaran a generar los servicios de trabajo social, nutrición, la ficha laboral y los necesarios para complementar la información acerca de la atención

proporcionada al paciente. Si llegara a celebrarse un contrato para la prestación de servicios, debe constar en el expediente[82].

También, de conformidad con el Reglamento de la Ley General de Salud en materia de trasplantes, de 26 de marzo de 2014, correspondiente al orden jurídico mexicano, debe integrarse en este documento las evidencias necesarias que permitan comprobar la ausencia de ánimo de lucro y de hechos de coacción para llevar a cabo uno de estos procedimientos, como resultado del Comité Interno de Trasplantes; el receptor deberá contar con un expediente clínico de al menos seis meses de antigüedad previos a la realización del trasplante; si existe parentesco entre el donador y el receptor, en el expediente clínico debe agregarse la documentación original o su copia certificada o debidamente legalizada, por medio de la que se compruebe esta situación; finalmente en el expediente del donador debe registrarse el establecimiento de salud al que se destinaron los órganos, tejidos o células procurados, la fecha de esta acción y el nombre de la persona que fue responsable de su traslado, incluyendo los datos de su identificación oficial.

Además, debe tenerse e integrarse aquel documento donde conste de manera expresa y por escrito que se ha brindado un consentimiento debida y suficientemente informado al paciente de cualquier procedimiento al que se le someta. Lo anterior elevará la calidad de la atención que se brinda al hacer de la comunicación con el paciente una costumbre de la práctica médica, evitando

[82] Al interior de los establecimientos para la atención médica ambulatoria y hospitalaria del Sistema Nacional de Salud mexicano, se podrá evaluar la calidad del expediente clínico, a través de organismos colegiados internos o externos. Para tal efecto, podrán utilizar el Modelo de Evaluación del Expediente Clínico Integrado y de Calidad, y la evaluación podrá solicitarse por las personas físicas, morales, representantes legales o los facultados para ello en los establecimientos para la atención médica ambulatoria y hospitalaria de los Sistema Nacional de Salud. Su objetivo es asegurar que todos los pacientes que reciben atención médica cuenten con un solo expediente clínico integrado, dando a conocer los resultados de la evaluación al personal involucrado para que se apliquen las propuestas de mejora y se eleve la calidad de la atención médica y de la elaboración de ese documento. Entre los rubros que se evalúan se encuentran la calidad de los registros y cumplimiento del expediente clínico, su custodia, archivo, uso e integración, así como la calidad de la atención médica a través de los registros del expediente. Puede consultarse su guía operativa, así como los algoritmos de las ramas de interés en la página https://desdgces.salud.gob.mx/mecic/index.php/home, que retoma del Apéndice A Informativo de la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012 que establece la calidad de los criterios y cumplimiento normativo del Modelo del que se habla.

futuras controversias que debiliten o destruyan la relación entre el prestador de servicios médicos y el paciente.

3.4.3 La historia clínica en el Sistema Nacional de Salud Español.

En España, la historia clínica es regulada por la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. La define como el conjunto de documentos, cualquiera que sea su formato, que contiene los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial.

A su vez, el Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza, la nombra además historial médico, pero toma el mismo concepto ofrecido por Ley 41/2002. En este país se cuenta con un sistema automatizado en el que la historia clínica resumida es un documento electrónico, alimentado y generado de forma automática, actualizado en tiempo real, a partir de los datos que los profesionales incluyan en la historia clínica completa de cada paciente.

Según la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, el expediente clínico deberá contener los datos generales que siguen:

1. Tipo, nombre y domicilio del establecimiento y en su caso, nombre de la institución a la que pertenece.
2. Razón o denominación social del propietario o concesionario de ser el caso.
3. Nombre, sexo, edad y domicilio del paciente y demás datos que señalen las disposiciones sanitarias, atendiendo a los servicios genéricos de consulta general, de especialidad, urgencias y hospitalización.

En términos similares parece pronunciarse la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica en tanto contempla que la historia clínica, contendrá la identificación de los profesionales de la salud que han intervenido en los procesos asistenciales, con el objetivo de obtener la integración máxima que sea posible de la documentación clínica de cada paciente al menos en el ámbito de cada centro, lo que se detalla en el Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud.

El Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, contempla a los informes clínicos de alta, de consulta externa, de urgencias, de atención primaria, de resultados de pruebas de laboratorio, de pruebas de imagen, de cuidados de enfermería y de la historia clínica resumida. Sin embargo, las comunidades autónomas pueden establecer modelos propios de documento clínicos, pero que deben incluir todas las variables que se incluyen en el Real Decreto citado.

Esta disposición también resulta aplicable a los centros y dispositivos asistenciales que las Entidades de Seguro Libre pongan a disposición de mutualistas y beneficiarios de la Mutualidad General de Funcionarios Civiles del Estado, el Instituto Social de las Fuerzas Armadas y la Mutualidad General Judicial. Además, se destaca que cualquier documento clínico generado previamente a la entrada en vigor de este Real Decreto, se puede conservar en el estado en que se encuentre.

En lo que se refiere al contenido mínimo de la historia clínica, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, enfatiza el derecho que el usuario tiene de que quede constancia, por escrito o en el soporte técnico más adecuado de la información obtenida en los procesos asistencias de que fue objeto por lo que deberá contener la documentación relativa a:

1. La hoja clínico estadística
2. La autorización de ingreso el informe de urgencia.
3. La anamnesis y la exploración física.
4. La evolución.
5. Las órdenes médicas.
6. La hoja de interconsulta.
7. Los informes de exploraciones complementarias.
8. El consentimiento informado.
9. El informe de anestesia, el de quirófano o de registro del parto, el de anatomía patológica.
10. La evolución y planificación de cuidados de enfermería y su aplicación terapéutica.
11. El gráfico de constantes y el informe clínico de alta, de los que correspondan a la situación de procesos de hospitalización podrán ser exigidos en ese supuesto.

Si se trata de nacimientos, deben añadirse los resultados de las pruebas biométricas, médicas o analíticas para determinar el vínculo de filiación entre la madre y su hijo. Si se trata de la prestación de servicios consecuencia de violencia ejercida a menores de edad, debe también especificarse la circunstancia. Estos datos no se suprimen o destruyen y en caso de fallecimiento del paciente, se conservan en los archivos definitivos de la Administración que corresponda (AEPD, 2022).

3.4.4 La regulación del Expediente clínico electrónico del Sistema Nacional de Salud Mexicano.

En México, la Ley General de Salud, de 7 de febrero de 1984 establece en el artículo 109 bis como obligación de la Secretaría de Salud Federal la emisión de la normativa que deben seguir los sistemas de información de registro electrónico en salud (SIRES) que usen las instituciones del Sistema Nacional de Salud para

que se garantice la interoperabilidad procesamiento, interpretación y seguridad de la información que se contenga en los expedientes clínicos electrónicos. [83] También es un caso previsto en la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012, en la que se establece como opción al expediente tradicional físico la utilización de medios electrónicos, magnéticos, electromagnéticos, ópticos, magneto-ópticos o de cualquier otra tecnología para su integración, siempre que se tomen en cuenta los requisitos mínimos que la norma en comento establece para tal efecto.

De esta suerte, fue publicada en el Diario Oficial de la Federación la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud, de 30 de noviembre de 2012. Su observancia es obligatoria[84] en todo el territorio nacional

[83] Una aproximación al tema en México ha sido, la Iniciativa con Proyecto de decreto por el que busca reformarse el artículo 77 bis 9 de la Ley General de Salud, para la implementación de un registro de pacientes individual, así como la creación de un archivo electrónico de historias clínicas, que presentó el Senador Saúl López Sollano, del Grupo parlamentario Morena que se publicó el 15 de diciembre de 2020 en la Gaceta del Senado de la República Mexicana. En este documento, que encuentra su origen en la creación del INSABI para dar cumplimiento a las disposiciones que han surgido por esta acción. El Senador considera que contar con historias clínicas resulta esencial para "poder archivar y gestionar todo tipo de datos sobre la atención sanitaria del paciente y puede llegar a utilizarse para la investigación clínica epidemiológica" (§ 16). Igualmente enfatiza la importancia de su tratamiento confidencial, además de contar con un archivo por medio del que se pretende asegurar la implementación de redes de atención a la salud mediante:
1.- Un intercambio de opiniones por medios electrónicos entre médicos de distintos hospitales referentes a un diagnóstico, padecimiento o distintas funciones médicas que se le pueda dar a este intercambio de información, respetando el cuidado de las medidas de seguridad, confidencialidad y profesionalismo que establece la Ley.
2.- Facilitar la obtención de datos para medios estrictamente de control de epidemias y usos médicos que establece la Ley General de Salud.
3.- Contar con un registro de los padecimientos del paciente para mejorar los diagnósticos y con ello un mejor resultado en los servicios de salud implementados por los institutos y clínicas que pertenecen a la Secretaría de salud. (§ 18 a 20)
Lo anterior, a través de la adición del siguiente párrafo al artículo que se pretende modificar: "Los establecimientos que presten servicios de salud, como lo marca la presente Ley, estarán obligados a tener y conservar el expediente de historial clínico digital de cada paciente, así como a compartirlo con las diversas instituciones de Salud." (§28) La iniciativa completa puede consultarse en https://tinyurl.com/y2cnzrc6

[84] Para su interpretación y aplicación armónica, se sugiere la consulta de las Normas Oficiales Mexicanas NOM-035-SSA3-2012, En materia de Información en Salud, de 20 de noviembre de 2011; la Norma Oficial Mexicana NOM-004-SSA3-2012, Del expediente clínico, de 29 de junio de 2012; y la NOM-017-SSA2-2012, Para la vigilancia epidemiológica, de 19 de febrero de 2013. A esta última no se hace referencia en el presente texto toda vez que dentro de sus objetivos se encuentra la recogida y difusión de información resultado de la vigilancia epidemiológica de acuerdo a los apéndices informativos A, B y C que ella misma establece y que contemplan información desagregada, es decir, que solo muestran datos estadísticos, que si bien es cierto

para cualquier establecimiento que preste servicios de atención médica que formen parte del Sistema Nacional de Salud y que adopten un Sistema de Información de Registro Electrónico para la Salud, como lo es el expediente clínico electrónico. Igualmente, resulta vinculante para toda aquella persona física o moral que cuente en el país con derechos de propiedad, uso, autoría, distribución y/o comercialización de los sistemas referidos. Los Sistemas de Información de Registro Electrónico para la Salud (SIRES) son aplicables indistintamente si se trata de los sectores público, privado y social del Sistema Nacional de Salud.

De acuerdo con esta Norma Oficial, corresponde a la Secretaría de Salud Federal establecer el marco jurídico al que se sujetarán los SIRES para garantizar la obtención, tratamiento y seguridad de la información que se contiene en esos sistemas. Como sucede con el expediente clínico, los prestadores de servicios de salud -haciendo referencia los establecimientos- son solidariamente responsables junto con el personal que preste sus servicios de la observancia estricta de la normativa aplicable, no importando su forma de contratación.

Tanto los establecimientos como los prestadores de servicio médico deben garantizar la confidencialidad de la identidad de los pacientes, la integridad y confiabilidad de la información clínica así como establecer las medidas de seguridad que estimen adecuadas para evitar el uso ilícito que pueda lesionar al titular de la información, y nuevamente remite a las disposiciones jurídicas aplicables, que se expondrán en el apartado de la legislación especializada en materia de protección de datos personales.

---

resulta de gran importancia conocer la forma en la que el procedimiento se lleva a cabo, este tendrá que ser desarrollarse a partir de la adecuada recolección y tratamiento de los datos personales que se asientan en un expediente clínico o expediente clínico electrónico y que se transmiten entre prestadores de servicios de salud para cumplir con lo establecido en dicha norma, que no va más allá de enfatizar que los criterios y procedimientos para la obtención de la información para el monitoreo son los que define la autoridad sanitaria “en los manuales correspondientes”, por lo que se enfatiza el estudio de otros cuerpos normativos que tratan este tema con mayor especificidad. Este punto será desarrollado con mayor profundidad en los capítulos en que se aborde el derecho a la portabilidad y el reporte de los resultados de la investigación.

Se atenderán los principios éticos y científicos que orientan la práctica médica. Su difusión al paciente, familiares, representante legal o terceros se hará de conformidad a la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012, pues la Norma que se comenta contempla el cambio de plataforma en que la información se expresa. Inclusive hace referencia a la posibilidad de intercambiar información a través de los SIRES de conformidad a la legislación vigente en 2012, es decir, a la Ley Federal de Transparencia y Acceso a la Información Pública, cuestión que ahora está regulada por Ley General de Transparencia y Acceso a la Información Pública, de 4 de mayo de 2015, y de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017; así como las Leyes de Transparencia y protección de datos personales de las entidades federativas armonizadas a las generales.

Se prevé la posibilidad de aplicar sanciones en caso de la revelación de la información contenida en los SIRES sin autorización expresa, aunque no especifica el medio de prueba idónea de dicha expresión del titular de la información o de quien tenga facultad legal para decidir por él, de acuerdo con las disposiciones legales aplicables, por lo que deberá analizarse cada caso. Sin embargo, debe recordarse que, de conformidad a la legislación vigente en materia de protección de datos personales, el tratamiento de datos personales sensibles, como los de salud, requiere para su tratamiento de un consentimiento expreso y por escrito del titular, por lo que el responsable del tratamiento deberá ser cuidadoso respecto de las finalidades para las que recaba y trata esa información, y analizar a qué base legitimadora de tratamiento se encuadra su acción.

Los prestadores de servicios de salud son responsables del mantenimiento de los SIRES para que la información bajo su resguardo sea íntegra, confiable y se encuentre disponible en todo momento, siendo responsables de que los registros permanezcan completos e inalterados por agentes externos. Resulta interesante mencionar que se reitera la posibilidad de llevar a cabo intercambio de la información en marco de los convenios o acuerdos que entre ellos existan,

siempre que sea con el objetivo de toma de decisiones o la prestación de servicios de salud integrados.

La Secretaría de Salud Federal será quien coordine la elaboración de Guías y Formatos que orienten a los prestadores de servicios para el intercambio de información. Estos son documentos técnicos cuyo objetivo es especificar el detalle de esa acción con independencia de los procesos que se den al interior de los establecimientos o entre prestadores de servicio. Incluyen como mínimo el alcance de tipos de sistemas, tipos de prestadores de servicios de salud y tipos de intercambio para los que aplica; el diccionario de variables, donde se distingue el tratamiento confidencial, catálogos y reglas de validación; la conformación del documento electrónico, mensaje de datos o servicio; el mecanismo de interconexión basado en estándares, así como ejemplos, referencias y bibliografía.

Los prestadores de servicios de salud pueden elegir para el intercambio de información los estándares que mejor les convenga, siempre que se sujeten a lo dispuesto por la norma en comento. Para llevar a cabo cualquier tipo de intercambio de información, los prestadores de servicios de salud deben desarrollar estos documentos electrónicos estructurados e inalterables. Los datos mínimos de identificación se reducen a la Clave Única de Registro de Población (CURP), nombre y primer y segundo apellido si cuenta con este último.

De utilizar los SIRES, los prestadores de servicios deben implementar un sistema de gestión de seguridad de la información, de acuerdo con lo contemplado en la legislación en materia de transparencia y protección de datos personales, así como de los estándares en materia de seguridad de la información con el objetivo de asegurar la confidencialidad, integridad, disponibilidad, trazabilidad y no repudio de la información en salud. En este sistema deberá resguardarse y registrarse cualquier información derivada de la prestación de servicios de salud en forma de documentos electrónicos y deben permitir la firma electrónica avanzada del profesional de salud para toda aquella información que así se determine en el sistema de seguridad correspondiente. Como medida de seguridad mínima deberán contemplar un usuario y contraseña y mecanismos

de autorización basados en roles; para eficientar el intercambio de información deberán ser implementados mecanismos de autenticación, cifrado y firma electrónica avanzada.

Los SIRES deben permitir la exportación de la información del paciente con base a lo dispuesto en materia de transparencia y protección de datos, utilizando las Guías y Formatos que hemos considerado anteriormente; así como implementar controles sobre los consentimientos del titular de la información o quien legalmente se encuentre facultado en consonancia con las disposiciones legales ya citadas.

Por último, es relevante señalar que la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de Información de Registro Electrónico para la Salud, de 30 de noviembre de 2011, contempla un procedimiento por medio del cual se realiza la Evaluación de la Conformidad para certificar el cumplimiento de los SIRES por parte de los obligados señalados en términos de lo que ella misma establece[85]. Para proporcionar una ruta de implementación de este instrumento, la Dirección General de Información en Salud de la Secretaría de Salud Federal mexicana (en adelante, DGIS, 2011), publicó el Manual del Expediente Clínico Electrónico.

Este Manual se publicó como herramienta de interpretación de la NOM-024-SSA3-2020, que precedió a la NOM-024-SSA3-2012, que se encuentra en vigor. Sin embargo, la Dirección General de Información en Salud no ha actualizado el documento y se continúa citando por los facultativos que instrumentan la aplicación de los SIRES en México. Afirma que esta innovación en la gestión de la información de los usuarios de los servicios de salud responde a problemáticas tales como:

1. La dispersión de su información que no se apega a los estándares de las Normas Oficiales Mexicanas en la materia;

[85] El estatus de la certificación de los SIRES, de conformidad a la NOM-024-SSA3-2012, puede consultarse en la página http://dgis.salud.gob.mx/contenidos/intercambio/sires_certificacion_gobmx.html

2. La falta de referencias documentales para los facultativos, que impiden, según el diagnóstico de la DGIS que estos emitan un diagnóstico oportuno y sin retrasos o apegado a las guías de práctica clínica;
3. Los largos tiempos de espera de los procedimientos de referencia y contrarreferencia.
4. La duplicidad de estudios de laboratorio e imagenología por la falta de comunicación de los resultados dentro de la institución o entre ellas.
5. Los trámites que deben realizarse para solicitar un estudio.
6. La dificultad para realizar un diagnóstico asistido por un especialista mediante la telemedicina.

Además, identifica como problemáticas a nivel institucional la cantidad de expedientes clínicos en formato físico y su espacio de almacenamiento; el sistema de su identificación que suele diferir entre instituciones, lo que dificulta el intercambio de la información contenida; la falta de capacitación del personal que maneja el archivo y los altos costos en materiales, infraestructura y personal que permita la operación idónea del sistema de archivo.

De esta suerte, los beneficios de su implementación incluyen el aumento de las acciones de prevención entre la población, así como de la seguridad de los pacientes y la reducción de los eventos adversos, los costos hospitalarios, por tratamiento o estudios innecesarios o redundantes; el acceso ágil y sencillo de la información contenida; la reducción de tiempos dedicados a actividades administrativas; se facilita la integración del documento y su acceso y por lo tanto, la asistencia médica se agiliza y se mejora la calidad en el servicio; pero también se optimiza la obtención y consulta de la información para finalidades de actividad clínica, epidemiológica, docente, de administración de recursos e investigación.

Pero la Dirección General de Información en Salud de la Secretaría de Salud mexicana cita ventajas que no encontramos diversas a las que tendría actualmente si los facultativos se apegaran a la normativa existente en la materia, por ejemplo, el ahorro de tiempo en la consulta del expediente, debido

al registro de toda la información del paciente en su unidad médica, ya que esta puede ser compartida con la de otras unidades médicas, pues en ocasiones hay que remitir al paciente a sitios especializados para realizarse pruebas específicas.

La confidencialidad con la que se maneja el sistema de los expedientes clínicos electrónicos fortalece la relación entre el médico y el paciente, pues está basada en la confianza y en el secreto profesional ya que garantiza la seguridad de la información. Existe una tendencia por parte de los pacientes que va en ascenso: la disposición de expedientes médicos en caso de ser necesario, transferirlos a otra institución. Incluso, el paciente puede usar el expediente clínico electrónico como prueba documental en alguna disputa legal por inconformarse con la calidad del servicio médico recibido. (DGIS, 2011, p. 23)

Al mismo tiempo esta guía identifica que los principales componentes funcionales con que debe contar el expediente clínico electrónico (DGIS, 2011, p. 15) son de administración de órdenes y resultados; para manejo de medicamentos, solicitudes para atención de pacientes, referencia y contra referencia o perfiles de diagnóstico, entre otros; de gestión administrativa y clínica y de salud pública.

Además, señala que este tipo de documentos electrónicos tienen dos elementos que los constituyen: el software y el hardware. En el primer caso, se compone de la aplicación médica, que facilita la interacción entre médicos y enfermeras que actúa como un gestor de correos electrónicos; de almacén de datos para el resguardo digital de la información, con las medidas de seguridad pertinentes, que deberán contar con un plan de respaldo y manejo de contingencias para “asegurar la continuidad del servicio e integridad de la información. También debe contar con políticas de control de acceso y mecanismos de seguridad informática que garanticen la confidencialidad de la información” (DGIS, 2011, p. 17).

Deben también contemplarse aplicaciones complementarias para visualizar datos de imagenología, estudios de laboratorio, administración de interconsultas;

el sistema operativo que controla las bases de datos y una plataforma de interoperabilidad e información, que, la DGIS considera que es un elemento que no forma parte integral del sistema de expediente clínico electrónico, pero que puede complementarlo.

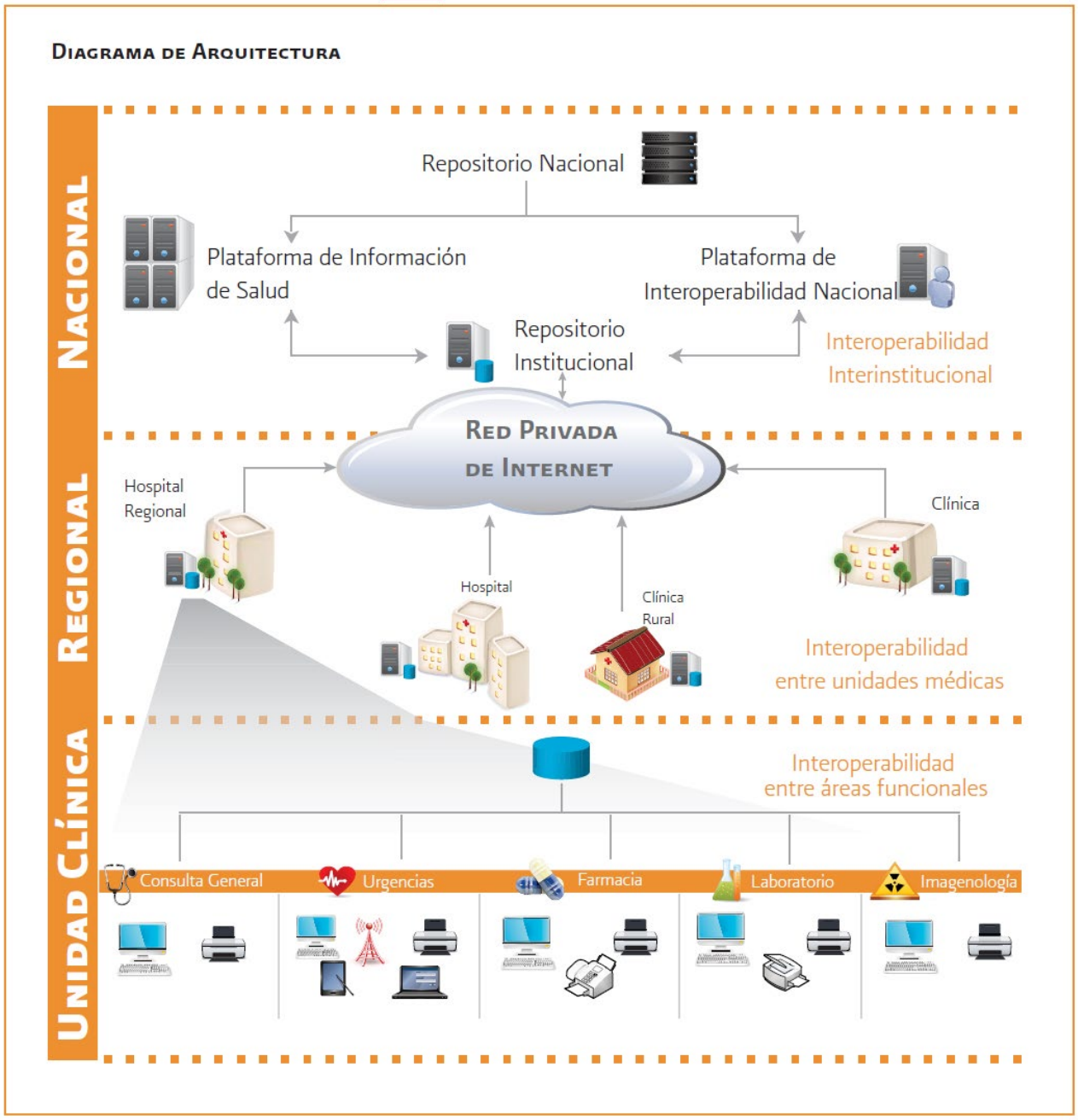
Para Comandé, Nocco y Peigné (2015, p. 200) “los sistemas de historia clínica electrónica son elementos fundamentales de los sistemas sanitarios modernos, ya que pueden asegurar una mayor calidad y seguridad de las historias clínicas en comparación con los modos tradicionales de cotejo, almacenamiento y transmisión de información. Del mismo modo, pueden facilitar el acceso a los registros al tiempo que garantizan altos estándares de protección y seguridad para los datos de atención médica y la privacidad individual.”

En nuestra opinión, el último elemento debería ser parte esencial de este tipo de plataformas, pues permite el ejercicio de otros derechos como el de portabilidad, acceso y protección de datos personales, que a su vez coadyuvan al ejercicio y garantía del de la salud del usuario, lo que en la guía parece considerarse esencial en el diseño de arquitectura de la plataforma, como puede apreciarse en los esquemas que se presentan.

Ilustración 15 - Diagrama de arquitectura de la interoperabilidad entre instituciones y/o regiones.

Fuente: DGIS, 2011, p. 18

Ilustración 16 - Diagrama de arquitectura de la interoperabilidad entre instituciones y/o regiones.



Fuente: DGIS, 2011, p. 18

Por lo que hace a la parte física o hardware, la DGIS (2011, p. 17,18) consideró que sus módulos esenciales son el equipo de cómputo o terminal mediante la que el profesional de la salud ingrese e interactúe con los datos; componentes periféricos tales como impresoras, escáneres, lectores biométricos o no-breaks; sistema de red que resulte adecuado para garantizar la conectividad del sistema

y los servidores apropiados para el almacenamiento, soporte e intercambio de la información. Para lograr este cometido el método más común es la mensajería Health Level Seven (HLS).

Todo esto deberá ser implementado en cinco niveles. El primero, es el puesto de consulta individual, después se considera a las unidades de salud; luego al nivel hospitalario; después al regional o metropolitano y finalmente a los ámbitos nacional e internacional. Desde el primero debería ser considerada como característica esencial del sistema que sea homologado, es decir, que permita llevar a cabo mediante la interoperabilidad el intercambio de información de los pacientes y con un sistema de seguridad óptimo para la clase de información que se contiene.

Para llevar a cabo la implementación del sistema deberá realizarse un estudio de factibilidad, la gestión del presupuesto y posterior selección del proveedor; posteriormente implementar la infraestructura tecnológica y el software adecuados, para posteriormente capacitar al personal involucrado y finalmente, se dará paso a la operación de los procesos, al soporte y actualización tanto del software como de los procesos y procedimientos realizados para su ejercicio.

3.4.5 La regulación de la historia clínica electrónica en el Sistema Nacional de Salud Español.

Para el Grupo de Trabajo del Artículo 29 (2007, p. 4), la historia clínica electrónica es el documento que contiene el estado de salud física y mental, idealmente desde el nacimiento hasta la muerte del titular de los datos, para facilitar su acceso para brindar atención médica u otros fines relacionados. Se trata de una estrategia que incrementa la calidad del tratamiento de los datos y de la eficacia de los tratamientos, así como del suministro de los datos para el control de calidad, estadísticas y planificación en los sistemas nacionales de salud.

La AEPD (2017, p. 7) considera que la historia clínica electrónica no es otra cosa que la versión digital de la historia clínica, por lo que debe operarse como un registro unificado y personal, que se archiva en soporte clínico y cuyo contenido

es multimedia para lo que deberán utilizarse tecnologías de la información y comunicaciones para hacer posible la integración de la información ahí contenida en un Sistema de Información Clínica. En cuanto al proyecto de Historia Clínica Electrónica del Sistema Nacional de Salud español, tiene como objetivo garantizar el acceso a la historia clínica resumida, de acuerdo con el anexo correspondiente que contiene los datos mínimos del Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, y que ya ha sido referenciado con anterioridad.

A diferencia de la situación en el país latinoamericano, el Instituto de Información Sanitaria (2010, p. 4) refiere que todas la Comunidades Autónomas tienen implementado el sistema de Historia Clínica Electrónica que, si bien es cierto cumple con la meta de eficientar el proceso de atención al paciente, también lo es que como ya fue anotado, no ha sido creado para brindar información "fuera del ámbito geográfico donde su información se ha generado". Por ello la importancia de la instauración del Sistema de Historia Clínica Digital, como "instrumento de cohesión del sistema sanitario español" (Instituto de Información Sanitaria, 2010, p. 6) y que para cuya institución el Ministerio de Sanidad se ha basado en la lógica asistencial de los ciudadanos que requieren asistencia sanitaria fuera de su Comunidad Autónoma; el de dar cumplimiento al derecho de recibir atención sanitaria de calidad en condiciones de igualdad efectiva, poniendo a disposición la información esencial de los pacientes.

También se hace referencia a esa misma necesidad de los facultativos de la salud de contar con la información debida para cumplir con la responsabilidad inherente a su ejercicio profesional, dando cumplimiento al mandato de las leyes 16/2003, de 28 de mayo, de cohesión y calidad en el Sistema Nacional de Salud y 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, de establecer los sistemas necesarios para tener acceso a la información de los pacientes que exista en diversos servicios de salud, a través de un solo punto.

Por ello sus objetivos generales son la garantía para el ciudadano del acceso vía plataforma de información a sus datos de salud, propios o de su representado, además de a los profesionales sanitarios, a través de mecanismos ágiles y fáciles, protegiendo de manera permanente esta información de personas no autorizadas, mediante un sistema con medias de seguridad[86] adecuadas. (Instituto de Información Sanitaria, 2010, p. 10)

La gran aportación de este Sistema es la Historia Clínica resumida, pues dada su finalidad, su actualización debe ser automática en aras de la efectiva garantía del derecho a la protección a la salud del ciudadano y del acceso a sus datos, pudiendo descargar los que estén disponibles o incluso imprimirlos. El ciudadano puede verificar quién ha accedido a sus datos, para comprobar cuáles han sido legítimos, para lo que tendrá disponibilidad de en qué momentos se ha realizado el acceso, desde qué servicios de salud, centro sanitario, el facultativo que lo hizo y por supuesto, que documento se ha consultado.

Otra característica que nos parece notable, pues es evidencia de que se garantiza el derecho de autodeterminación informativa del paciente, es que este puede limitar el acceso a parte de sus datos de salud a algunos de los profesionales que le atienden (Instituto de Información Sanitaria, 2010, p. 17) que si bien es cierto ha causado polémica, el Instituto de Información Sanitaria lo considera exento de tal, ya que solo se trata del ejercicio por medios automatizados de la puesta a disposición de la información de salud del paciente a otro facultativo, a través de una historia clínica física. Sin embargo, antes de poder activar la funcionalidad, se advierte al ciudadano de que el proceso de diagnóstico y terapéutico puede verse afectado pues el profesional no contará con toda la información disponible acerca de su estado de salud, por lo que, si este último la considerara imprescindible, se informará al paciente acerca de esta circunstancia para que permita su visualización.

[86] Se enlistan a la identidad de las personas autorizadas con anterioridad, la autenticidad de los agentes que dicen actuar en representación de los autorizados, la garantía del no repudio al acceso, la privacidad de la información que se intercambia y su integridad, según el Instituto de Información Sanitaria (2021)

Un evento importante que tomar en cuenta para el ejercicio de este derecho es la capacidad del paciente para decidir, por lo que en el caso de que confluya una situación de urgencia en la que se requiera una actuación impostergable, el profesional puede visualizar esa información cuya vista se ha impedido, pero se dejará evidencia de tal acceso, con lo que se garantiza en una situación extrema la garantía del derecho a la protección de la salud. (Instituto de Información Sanitaria, 2010, p. 18)

En el Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria y transfronteriza, se establece que España aplicará los estándares nacionales, europeos e internacionales de comunicación de la Historia Clínica Electrónica o de sus componentes. Por ello, se debe elaborar una evaluación de impacto con el objetivo de que se garantice que el tratamiento intensivo al que pretenden someterse los datos personales se justifique, primero y se realice apegado a la legislación vigente. Es más, autores como Hamon *et al* (2022, p. 72) han propuesto esta herramienta como la adecuada para complementar el cumplimiento del deber de información a usuarios de ambientes automatizados.

Así y para finalizar, coincidimos con Comandé, Nocco y Peigné (2015, p. 200) quienes en su estudio encontraron que la gestión eficaz del expediente clínico electrónico “podría satisfacer las nuevas necesidades en los servicios de salud” pero la presión para reducir los costos ya sea en el ámbito público o privado, pueden llevar a sacrificar su efectividad y funcionalidad en torno a la garantía del derecho a la protección de datos personales.

3.4.6 La interoperabilidad y los formatos estructurados y comúnmente utilizados en el contexto del ámbito sanitario.

Sin la interoperabilidad el derecho de portabilidad de datos personales perdería el sentido ya que la información no podría circular libremente, por lo que depende por completo de la adopción de estándares que la hagan realidad, como afirman Bistolfi & Scudiero (2016, p. 607, 609).

Existen soluciones tecnológicas que hacen posible la interoperabilidad, entendida como la transmisión de datos entre sistemas de información heterogéneos, de la que uno de sus aspectos es la interoperabilidad semántica. Uno de los pasos imprescindibles para alcanzarla es definir por acuerdo, el conjunto de datos que, por su relevancia, deben estar contenidos en los diferentes informes clínicos que describen los procesos de atención sanitaria realizados a ciudadanos concretos en cualquier centro o servicio del Sistema Nacional de Salud. Esta homogeneidad es uno de los elementos de normalización que facilitan el intercambio entre sistemas diferentes al servicio de los ciudadanos.

Además de la contribución que supone la normalización de los contenidos de cara a hacer posible la interoperabilidad entre sistemas de información distintos, la instauración de modelos básicos, contrastados por expertos, como instrumento para recoger y presentar la información clínica de manera estandarizada, permite garantizar una homogeneidad en los contenidos de los documentos clínicos en el sistema sanitario público que facilita su comprensión y la más rápida localización de la información, tanto a los pacientes como a los profesionales sanitarios, con independencia del territorio donde deban ser atendidos o donde se haya generado la información.

También deberá garantizar si fuera posible, la interoperabilidad del formato en que se entreguen los datos personales para que estos puedan ser utilizados o comunicados uniforme y eficientemente, procurando que sus sistemas y servicios mantengan la capacidad de interoperar con otros. Esta es una cualidad que deberá preverse desde su diseño y para su ciclo de vida para que el intercambio de información exista independientemente del lenguaje de programación o plataforma en la que se desarrolle, pues lo que es técnicamente posible para un responsable, puede no serlo para otro. (Vanberg, 2018; sin página). Así, como sostiene Veil (2018, citado por Elfering, 2019, p. 21) “la expresión ‘formato estructurado’ es probablemente incorrecta”. No es el formato en el que se respalda la información lo que debe ser estructurado, sino los datos personales para cumplir con el objetivo de volver a usar esa información (Elfering, 2019, p. 21).

La interoperabilidad, menciona Engels (2016, p. 4) no debe confundirse con la portabilidad, pues la primera va más allá de la segunda, al ser su objetivo la interconexión de los usuarios independientemente de la plataforma que utilicen, pero la segunda, implica tomar los propios datos y enviarlos a una plataforma distinta para no comenzar con el perfil de usuario desde una etapa inicial. Indarte (2012, p. 317), considera a la interoperabilidad como una de las características esenciales de los sistemas de información en salud, ya que permite "la comunicación transversal y longitudinal a lo largo de la estructura de los servicios de salud, garantizando la confidencialidad y la integridad de la información intercambiada y su acceso oportuno"; lo que a su vez asume como un desafío que de ser superado, permitiría "una gestión efectiva, eficiente y eficaz centrada en los ciudadanos".

Tal es su importancia que, continúa la autora, este concepto no debe analizarse solo desde el punto de vista informático, sino también del de salud en el que se ven involucrados principalmente tanto los profesionales de la salud como las autoridades que la regulan ya que, si se hace de forma correcta, se evitaría perder información valiosa acerca del estado de salud de los usuarios y a su vez, hacer menor cualquier riesgo potencial para ellos al impedir que el profesional de la salud tome decisiones basadas en información incompleta o parcial. (2012, p. 318).

Indarte (2012, p. 327) propone que, para lograr esa meta, deberían atenderse los presupuestos mínimos tales como la normalización del registro de usuarios, la identificación de las instituciones prestadoras de servicios de salud, así como el conjunto de actos médicos, fármacos y servicios que se brindan a los usuarios y que se realizan en el sistema, usando codificaciones internacionales[87] para facilitar la tarea, además del establecimiento de los estándares necesarios para

[87] Entre los sistemas de normalización que sugiere la autora, se encuentran la Clasificación Internacional de Atención Primaria (CIAP2), la Clasificación Internacional de Enfermedades elaborada con propósitos epidemiológicos y estadísticos (CIE9 o CIE10), la Nomenclatura Sistematizada de Medicina (Systematized Nomenclature of Medicina SNOMED CT).

que los sistemas se comuniquen[88]. Este trabajo debería ser realizado por profesionales sanitarios en conjunto con aquellos que lo sean en la gestión de datos e información, entendiendo que, si los estándares se cumplen, se beneficia directamente el titular de los datos en tanto le ofrecen un servicio de calidad y al mismo tiempo, le garantizan su derecho de protección de datos personales en sus diversas vertientes (Marco y Salvador, 2017, pp. 2, 29 y 37).

3.4.7 Datos inferidos en la historia clínica y las anotaciones subjetivas.

Muñoz (1996, p. 153), considera esencial establecer la frontera entre qué es propiedad del facultativo y qué del usuario. Si fuera obra intelectual del primero, podría disponer de ella a voluntad sin contar con el consentimiento del segundo, quién ha sido su fuente de información. Como señala, en la historia clínica se encuentra testimonio de la actividad intelectual del profesional que bien podría ser considerada "propiedad intelectual y digna de protección en cuanto derecho del médico […] pero todo esto va referido a la intimidad del paciente, y me parece que, por mucho que se le pueda atribuir al médico en su derecho a su propiedad intelectual, lo que no puede es utilizarla en contra o lesionando el derecho a la intimidad del paciente."

Para Galán (2020, p. RB-4-14), este documento es parte del fichero denominado historia clínica y por ello, el responsable de su tratamiento es la persona física o jurídica que decide acerca de su finalidad, contenido y uso del tratamiento por lo que este hecho determina su titularidad, de conformidad a la legislación española reglamentaria en materia de protección de datos de carácter personal.

Autores como Cantero (s.f), dan cuenta de tres teorías que responden a esta interrogante:

[88] Para este caso, Indarte (2012, p. 307) considera adecuados la Mensajería HL7 que facilita el intercambio de información clínica o contable y administrativa, DICOM para el intercambio de imágenes médicas digitales, la CEN/ISO 13606 para los documentos clínicos digitales, CDA que es un estándar HL7 para documentos clínicos de cualquier naturaleza y el OpenEHR como un modelo de referencia de fuente abierta para sistemas de historia clínica. Igualmente considera adecuado el modelo Integrating Healthcare Entrerprises (IHE) para definir el conjunto de perfiles que harán común los estándares, seguridad y trazabilidad de las actividades del sistema, pero nos advierte que cada uno será útil según el nivel de complejidad de aplicación para el que se necesite.

a. Es propiedad del paciente, toda vez ser su fuente de información, lo que le otorgaría su titularidad. A este argumento se suma el de la contraprestación que el paciente paga por la atención médica, que no resulta aplicable en todos los casos, como lo estudiaremos en la tercera parte de esta investigación.
b. Es propiedad del médico, sobre todo si se trata del ámbito privado y si el facultativo trabaja para una institución, esta ostenta la propiedad. Esto no quiere decir que el paciente no pueda acceder a la información, sino que lo hace con algunas limitaciones. Otra vertiente de esta teoría sostiene que propiedad del médico por ser producto de su proceso intelectual, por lo que pasa a ser su propiedad.
c. Posición integradora. En ella se sostiene que el propietario del documento es el centro sanitario o el facultativo en el que este es el "titular de su aportación intelectual y administrador del interés de terceros allí registrados" y el paciente, "el titular de la intimidad en ella reflejada".

El Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud, es claro en el anexo VIII, mediante el que se establecen el conjunto de datos mínimos de la historia clínica resumida, que el facultativo puede hacer anotaciones de sus observaciones libres subjetivas, pero únicamente acerca de valoraciones sobre hipótesis diagnósticas no demostradas, de la sospecha acerca de incumplimientos terapéuticos, sospecha de tratamientos no declarados, de hábitos no reconocidos, de haber sido víctima de malos tratos o de comportamientos insólitos, con la única justificación de dar cuenta de sus evaluaciones siempre que resulten de interés legítimo para el manejo de los problemas de salud por otro profesional. A *contrario sensu*, el Grupo de Trabajo del Artículo 29 (2007, p. 8) apunta que la información incluida en el expediente clínico lo fue por ser relevante para la atención médica, por lo que, de no serlo, no debería haberse incluido, por lo tanto, se debe considerar el acceso ilimitado.

El paciente nunca ha poseído su expediente clínico, pero con los avances tecnológicos, se encuentra a punto de convertirse en uno de sus tenedores

materiales, al menos en México, aunque como analizaremos en la tercera parte de nuestra investigación, esto ya sucede en la Unión Europea. Determinar la propiedad de este documento, independientemente de su soporte documental, resulta, según Romeo y Castellano (1993, p. 14) de capital importancia para establecer procedimientos de descubrimiento de datos y para el derecho de acceso a este documento por parte del usuario, que sí resulta el titular de esos datos.

Para dirimir esta cuestión, los autores nos proponen dos escenarios. El primero, en el que los médicos no tienen derechos intelectuales sobre este documento y el segundo, en que se argumenta que se cuenta con derechos intelectuales de quienes elaboran estos documentos, en tanto se trate de la información derivada de los elementos recopilados, por ejemplo, el diagnóstico, el pronóstico, las valoraciones y apreciaciones acerca del estado de salud del paciente y resulta la idea por medio de la que se niega al paciente el derecho de acceso a su propia historia clínica.

De esta manera, consideran los autores citados que si el facultativo invocara su derecho de autor, no tendría contenido pues únicamente recopila información en el soporte documental que utilice pero no es el creador original de este último, si bien es cierto que anota las deducciones producto de su ejercicio mental y de su preparación académica, no debe confundirse “con la facultad y deber de evitar que la información de la historia clínica será tratada o transmitida a persona no autorizada o para fines ilegítimos”. (Romeo y Castellano, 1993, p. 14)

Continúan razonando que este documento está conformado por elementos de distinta naturaleza desde el punto de vista de la relevancia que puedan alcanzar ante la ciencia jurídica, como ya se ha identificado a lo largo de este capítulo, entre los que se incluyen y son relevantes “las anotaciones subjetivas del médico en relación con las reacciones y actitudes del paciente, que son de especial importancia en algunos casos” (Romeo y Castellano, 1993, p. 14) y que sostienen, son los que únicamente pueden ser objeto de consideración como creación científica y por lo tanto, del derecho de propiedad intelectual.

Además, consideran que, si se trata de actividades desarrolladas en una institución, ya sea pública o privada, la titularidad corresponde a esta; si bien es cierto que el facultativo tiene control sobre el uso que terceros puedan dar al documento, transmitiendo los derechos de explotación al centro para que pueda desarrollar la actividad para la que fue creado, por lo que consideran que el paciente no puede demandar que le sea proporcionado el documento original.

Sánchez y Abellán (2006, p. 25) sostienen que los facultativos pueden impedir el acceso a las anotaciones subjetivas que se incluyan en el expediente clínico, sin embargo, este tipo de comentarios deben ser anotados siempre que cuenten con trascendencia clínica. Para estos autores, se definen como "las reflexiones e impresiones transcritas en los documentos de anamnesis y evolución clínica por los profesionales sanitarios encargados de la asistencia de los pacientes y cuyos destinatarios son los profesionales involucrados en la asistencia".

Para Comandé, Nocco y Peigné (2015, p. 201), se daría un fenómeno de "explosión de litigios" en materia de responsabilidad médica, al ver confirmado en su estudio del "riesgo de percibir la innovación técnica como un camino para erradicar los errores en la medicina", dotando de importancia a la investigación del "grado de precisión e integridad de los datos que se requieren a los profesionales", por la marcada exposición del trabajo de estos gracias al acceso a las historias clínicas.

Con esta idea coincide Fajardo (2011, p. 309, 310), quien sostiene la opinión que nosotros hemos visto reflejada en la generalidad de los facultativos con quienes convivimos por razones laborales, esto es, que "es indispensable resguardar cierta información contenida en el expediente clínico, en especial aquella que pueda afectar a terceros o incluso la propia salud del paciente" y también que lo ideal sería proteger cierta información contenida en el expediente clínico, ya que el acceso total, irrestricto o indiscriminado al mismo, puede repercutir negativamente en la actividad médica, generando un esquema en el que prive la desconfianza y se propicie el ejercicio de la medicina defensiva".

Igualmente opinaba Porfirio (2006, pp. 35, 36), en su calidad de presidente de la Academia Mexicana de Cirugía, primero acerca de que considera al expediente clínico el documento en el que se registra el quehacer del médico. Es, como vemos, muy alejado de la posición centrada en el paciente o usuario de los servicios de salud que predomina tanto en la legislación como en la doctrina.

De esta situación daba cuenta Gómez (2006, pp. 11, 12), por lo que hace a los profesionales sanitarios mexicanos, acerca de lo que denominaba "la vieja idea patrimonialista de que a los documentos generados u obtenidos por el gobierno sólo tengan acceso los servidores públicos que la generan, es decir, los médicos trabajadores del Estado" pero que "el gobierno mexicano ya no puede sostener el principio de que su responsabilidad de resguardar los archivos le otorgaba un derecho de propiedad sobre los mismos, incluso en demérito del titular del expediente médico". Considera que garantizar el derecho de acceso al expediente clínico es de tal importancia que "un corolario de ésta (una existencia digna) es […] el libre acceso a sus propios expedientes e historiales clínicos".

La Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012 parece coincidir con ese criterio, en tanto prevé únicamente proporcionar información verbal al paciente, a quien ejerza la patria potestad, la tutela, representante legal a familiares o autoridades competentes. Igualmente contempla brindar un resumen clínico u otras constancias del expediente clínico -pero no el expediente completo- siempre que se solicite por escrito, aunque no establece alguna formalidad especial más que ésta.

Sin embargo, la misma Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012 es clara en reconocer al paciente como titular de los datos que proporciona a los profesionales de la salud para su atención, los cuáles, así como los que permiten su identificación, son considerados como confidenciales, cuestión que se ha considerado por los creadores de esta regulación como ratificación y consolidación del principio ético del secreto profesional.

A su vez, el criterio de Galán (2020, R-B4.14), con el que coincidimos, es que no debe impedirse el acceso a este tipo de anotaciones, que ni siquiera deberían incluirse ya que en muchos casos se trata de expresiones inadecuadas y sin trascendencia para documentar la atención brindada. Por ello, considera que, si esas anotaciones resultan de interés para el tratamiento del paciente, no debería negársele el acceso a su contenido, con el objetivo de que "pueda obtener un conocimiento lo más completo posible de su estado de salud, así como del alcance y finalidad del tratamiento pautado en su caso… la reserva a tales anotaciones subjetivas debe oponerse […] por el facultativo concreto autor de las mismas y no por el centro sanitario que custodie las mismas."

En este sentido parece estar redactada la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012, que establece claramente que la propiedad del expediente clínico la ostenta la institución o el prestador de servicios médicos que los genera si no pertenece a una institución. De lo que es propietario el paciente, es de los datos personales e información que aporta y que se encuentra contenida en dicho documento, en su carácter de beneficiario de la atención médica que se recibe: esa titularidad se le reconoce para la protección de su salud y la confidencialidad de sus datos. Claramente se establece que deben permanecer en manos de su propietario por un periodo mínimo de cinco años, contados a partir de la fecha del último acto médico por tratarse de un conjunto de documentos elaborados en interés y beneficio del paciente.

Con la misma postura se pronunció el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que mediante el comunicado INAI-317-2017 expresó que "la titularidad de los datos personales contenidos en un expediente clínico es del paciente, no de los hospitales ni médicos o profesionales de la salud, y éste cuenta con ciertos derechos relacionados con esa información, como el derecho a solicitar una copia de su expediente y a la confidencialidad de sus datos personales" [89].

[89] El comunicado completo puede consultarse en https://tinyurl.com/5fca5h5f

Por la misma temporalidad el legislador se ha pronunciado respecto de la conservación del expediente clínico en establecimientos para el internamiento de enfermos, en el Reglamento de la Ley General de Salud en materia de prestación de servicios de atención médica de 14 de mayo de 1986; además, añade la obligación del manejo de este documento únicamente por personal autorizado, aunque no especifica de cuál se trata. Esto último hace referencia al expediente clínico "vivo" como lo denomina Troncoso (2006, p. 86), sin embargo, pasado el plazo y convirtiéndose este documento en uno "pasivo", el autor sugiere que estos documentos "deben archivarse como regla general separando los datos identificativos de los documentos clínicos, como medida de seguridad, sin perjuicio de la investigación genética, científica, epidemiológica y docente.

La Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico, de 29 de junio de 2012, continúa estableciendo que cualquier prestador de servicio de salud debe integrar y conservar el expediente clínico y en caso de formar parte de un establecimiento de salud éste será solidariamente responsable respecto del cumplimiento de la obligación descrita independientemente de la forma de contratación del personal. Se puede integrar en medios electrónicos, magnéticos, electromagnéticos, ópticos magnetoópticos o de cualquier otra tecnología, en términos de la Norma Oficial Mexicana NOM-024-SSA3-2012 Sistemas de información de registro electrónico para la salud. Intercambio de información en salud, de 30 de noviembre de 2011.

En el ordenamiento jurídico español, la Ley 41/2002, de 14 de noviembre de 2022, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, se establece una responsabilidad similar, pues estipula que cada centro archivará las historias clínicas de sus pacientes, aunque no necesariamente en su soporte documental original, como mínimo cinco años contados a partir de la fecha del alta de cada proceso asistencial si bien es cierto que se considerará cada caso específico.

En lo referente a los datos relacionados con el nacimiento del paciente, sus pruebas biométricas, médicas o analíticas para determinar la filiación con la

madre, no serán destruidos y una vez conocido su fallecimiento, deberán trasladarse a los archivos definitivos de la administración que correspondan, donde se les dará conservación bajo las medidas de seguridad que la legislación de protección de datos disponga, además de su conservación y la recuperación de la información, así como los mecanismos de autenticidad de su contenido y las modificaciones que pueda sufrir por su propia naturaleza y para su reproducción futura, adoptando las medidas técnicas y organizativas adecuadas para su archivo y protección que viten su destrucción o pérdida accidental. Estas disposiciones serán aplicables en general a toda la documentación clínica que se genere y los datos solo podrán ser comunicados previa solicitud del órgano jurisdiccional dentro del proceso penal o en caso de reclamación o impugnación judicial de la filiación materna.

También se establece el deber de cooperar en la creación y el mantenimiento de la documentación clínica de forma ordenada y secuencial. Si el servicio se presta de forma individual, será en esa modalidad en que hagan responsables los profesionales sanitarios de la gestión y custodia de la documentación de referencia. Llama la atención que la Ley española establece como un derecho del paciente, los relacionados con la custodia de la historia clínica. Sin embargo, Cantero (s.f) considera que más que la propiedad de la historia clínica debería aclararse quien cuenta con acceso a ella.

3.4.8 Ejemplos de buena práctica.

3.4.8.1 El Espacio Europeo de Datos Sanitarios

Sin lugar a duda, un caso de estudio de relevancia es el del Espacio Europeo de Datos Sanitarios (EEDS). De muy reciente creación, apenas en mayo de 2022 fue presentada ante la prensa por la Comisión Europea esta iniciativa que sin duda llama la atención, por prometer ser la solución al facilitar el acceso de los datos entre los países miembros de la Unión Europea ya sea por parte de sus titulares, las personas que proveen los servicios de atención médica e incluso investigadores públicos y privados.

Además, el anuncio público se dio con base a las propuestas de Ley de Gobernanza de Datos y la Ley de Datos y con el respaldo de legislación de obligatorio cumplimiento como el 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos o la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

De esta suerte, la Comisión Europea (2022) manifiesta que el proceso e implementación de esta iniciativa se vio acelerado por la reciente emergencia sanitaria por la enfermedad COVID 19, que puso en evidencia la necesidad de eficientar las comunicaciones y la puesta a disposición de datos sanitarios para hacer frente a lo sucedido.

En ese sentido, se propone al EEDS como la solución que, en la medida de lo posible, permita salvar los obstáculos que se presentan al intercambiar este tipo de información, al ser una herramienta que, para este fin, "establece reglas claras, normas y prácticas comunes, así como infraestructuras y un marco de gobernanza para el uso de los datos sanitarios electrónicos por parte de los pacientes y para finde de investigación, innovación, elaboración de políticas, seguridad de los pacientes, estadística o reglamentación" (Comisión Europea, 2022).[90]

También, es relevante mencionar la importante inversión que la Unión Europea realizará para llevará a cabo este proyecto, pero también los beneficios esperados, pues, aunque se ha destinado un presupuesto de 12,000 millones de euros por parte de los Estados Miembros, a los que se suman 810 millones de euros de parte de la Comisión Europea (2012), se estima un ahorro de 11,000

[90] Kiseleva y de Hert (2021, p. 21) han encontrado cuatro áreas legales de gran importancia que pueden necesitar de regulación específica para el correcto funcionamiento del Espacio Europeo de Datos Sanitarios: normas sobre la prestación de asistencia sanitaria en los Estados miembros; protección de datos personales en la prestación de asistencia sanitaria y la investigación médica; control y uso de datos no personales y el marco regulatorio sobre inteligencia artificial.

millones de euros a lo largo de 10 años, gracias a los beneficios que se detallan a continuación.

El público objetivo a beneficiarse en un primer momento es cualquier persona en la Unión Europea en su calidad de usuario de la atención médica, ya que según la propuesta, podrán ejercer los derechos concernientes a sus datos sanitarios de forma plena (acceso, rectificación, cancelación o supresión, oposición y portabilidad), empoderándolos de tal suerte que se ejerza su derecho a la autodeterminación informativa.

Si embargo, el EEDS está diseñado para facilitar el trabajo de los profesionales de la salud por la interoperabilidad incluida desde el diseño de la plataforma que garantiza el acceso transfronterizo al historial médico de los pacientes, haciendo más eficiente el gasto público y la atención brindada al evitar la duplicidad de atención o pruebas realizadas al usuario del servicio, por ejemplo, lo que necesariamente deriva en la mejora de la calidad de la atención que se provee.

Esta misma característica beneficiará el trabajo de las personas que se dediquen a la investigación, los reguladores en el ámbito de la salud y los gobiernos, pues podrán obtener los datos sanitarios, de acuerdo con la Comisión Europea (2022), a través de la creación de un organismo de acceso a esta información que tendrá como misión la garantía de la privacidad de los pacientes. También la industria farmacéutica está considerada en esta propuesta, ya que se establecerá un mercado de historias clínicas electrónicas en la Unión Europea que será regulado homogéneamente, en el que la interoperabilidad y la seguridad deberán ir incluidas por diseño y por defecto, debiendo los fabricantes certificar que dan cumplimiento a las normas correspondientes (Comisión Europea, 2022).

Entre otras iniciativas que se verán impactadas de manera positiva por el intercambio de la información, está el Plan Europeo de Lucha contra el Cáncer, la Estrategia Farmacéutica para Europa y el Programa de Investigación sobre Salud y Medio Ambiente para Europa (HERA, por sus siglas en inglés). Para ello, el EEDS ampliará la gobernanza de los datos, regulando el uso secundario, es decir, “la reutilización de datos sanitarios agregados por parte de, por ejemplo,

profesionales de la investigación y de la innovación, responsables políticos y operadores de la industria", (Comisión Europea, 2022) para lo que se conformarán dos infraestructuras digitales que permitan hacer interoperable el intercambio de datos para usos primarios y secundarios de manera transfronteriza.

Esta infraestructura, denominada "My health @ EU", consiste en el servicio de recetas electrónicas y dispensaciones en este mismo mecanismo, para que las personas obtengan su medicación en cualquier establecimiento que se encuentre en países miembros de la UE. El otro servicio es el de acceso a los historiales resumidos de los pacientes mediante los que se proporcionarán datos generales de trascendencia, tales como las enfermedades que se cursan, alergias o antecedentes y a largo plazo, también los resultados de los exámenes de laboratorio o gabinete, así como la historia clínica, todo ello en la lengua materna del facultativo que esté brindando la atención en ese momento. Estos mecanismos serán implementados en 2025, en al menos veinticinco países (Comisión Europea, 2022).

Para garantizar lo descrito, se propone la publicación de la Ley de Gobernanza de Datos[91] y se creará el Consejo del Espacio Europeo de Datos Sanitarios, que estará conformado por los representantes de las autoridades sanitarias digitales, así como los nuevos organismos de acceso a los datos sanitarios de los Estados de UE, la Comisión Europea y observadores (Comisión Europea, 2022).

No obstante, sobre todo lo concerniente al acceso a los datos por personas y/o entidades ajenas a la relación médico-paciente, se contará con medidas de seguridad tales como el acceso y descarga de datos anonimizados, que sean procesados en entornos cerrados y seguros y solo para fines específicos que

[91] Fue recientemente aprobada el 16 de mayo de 2022 por el Consejo Europeo, pero entrará en vigor en 15 meses contados a partir de su publicación en el Diario Oficial de la Unión Europea. Entre sus principales novedades, están, "la cesión de datos del sector público para su reutilización, en los casos en que esos datos estén sujetos a derechos de terceros; el intercambio de datos entre empresas a cambio de algún tipo de remuneración; la cesión de datos personales con ayuda de un «intermediario de datos personales», cuya labor consistirá en ayudar a los particulares a ejercer los derechos que les confiere el Reglamento General de Protección de Datos (RGPD); la cesión de datos con fines altruistas". (Comisión Europea, 2020).

busquen el beneficio común (Comisión Europea, 2022), a través del diseño institucional y legislativo que se ha citado con anterioridad.

Uno de los retos más importantes que la Comisión Europea ha identificado para que el EEPD se consolide, es la diversa madurez que los miembros de la UE tiene respecto al uso de las tecnologías para dar tratamiento a los datos de salud, pues algunos de ellos cuentan con un avance en el nivel de digitalización importante, sobre todo en materia de interoperabilidad, mientras que once países aún siguen utilizando medios no electrónicos para brindar el servicio[92]. Por lo que hace al tratamiento de datos con fines de investigación, apenas trece de los países han comenzado a establecer sistemas nacionales que los centralicen para facilitar su acceso.

Finalmente, no podemos dejar de mencionar la Opinión Conjunta 03/2022 que el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos Personales, de 12 de julio de 2022, han emitido a propósito de este tema. En lo medular, expresan preocupación acerca de incluir en el Espacio Europeo de Datos Sanitarios a los que se producen por el uso de las llamadas aplicaciones de salud digital, que no solamente recaban datos de esta índole sino también de otros tipos, que también se consideran sensibles. Dada su delicadeza, deberían excluirse de la disponibilidad para el uso secundario de datos, pues de lo contrario se requiere el consentimiento previo del titular como base legitimadora para su tratamiento.

3.4.8.2 La historia clínica electrónica (ePA) de Alemania.

Este sistema fue implementado el 01 de enero de 2021 y está disponible para toda persona con un seguro obligatorio. Ahí deberán archivarse los hallazgos médicos y la información de exámenes y tratamientos anteriores (BMG, 2021),

[92] Uno de ellos, Noruega, como pudo ser comprobado a través de una consulta a su Autoridad de Protección de datos (Datatylsinet) mediante un correo electrónico de enero del año pasado. En él. Sussane Lie, Asesora legal senior, comparte que además de no contar con casos resueltos en materia de portabilidad de datos, su país, al ser uno pequeño, tampoco tiene un sistema de historia clínica, aunque no especifica si se trata de la electrónica o ni siquiera cuenta con un sistema tradicional en soporte físico, como México. (Lie, S. (27 de enero de 2021) R.E. S.V Health data resolutions. (Correo electrónico) Oslo, Noruega).

con el objetivo de optimizar el tiempo de atención y evitar exámenes múltiples de laboratorio o gabinete, reduciendo las molestias para el usuario de los servicios de salud.

Los documentos que la integran pueden ser, incluso escaneados con un teléfono inteligente o una tableta. Quienes determinan los datos y su contexto de tratamiento, así como cuáles deben eliminarse son los pacientes. Los médicos, por lo tanto, no tienen acceso automáticamente, sino que requieren de la aprobación del interesado para el ingreso y modificación de los datos que ahí se contienen. (BMG, 2021). Para tal efecto, el paciente podrá ingresar con ayuda de su tarjeta sanitaria electrónico y un número de identificación personal. Para el ingreso del personal sanitario, éste deberá contar con su tarjeta que lo avale como profesional sanitario y un número de identificación personal. Esta aplicación supone una auténtica novedad en el mundo de la salud ya que permite al paciente ejercer su derecho de autodeterminación informativa al decidir cuáles aplicaciones médicas desean utilizar y quien puede acceder a su información personal. (BMG, 2021).

Sin embargo, los pacientes pueden permitir el ingreso a la aplicación a los proveedores de servicios sanitarios por el periodo de tiempo que les resulte necesario para terminar un tratamiento, destacando que sin el consentimiento del interesado no se puede guardar o leer datos de la plataforma, que se encuentra en una infraestructura telemática, segura y autónoma (BMG, 2021). En cuanto a los menores de edad, se debe estar siempre a su interés superior, pero debería poder utilizar la plataforma de manera independiente a los quince años; sin embargo, deberá tomarse en cuenta en todos los casos su capacidad de comprensión para decidir y así asentarlo en la plataforma. (BMG, 2021).

Finalmente, es importante mencionar que el Ministerio Federal de Salud Alemán espera que para finales de 2025 el 80% de usuarios de la plataforma puedan contar con una descripción general de sus medicamentos y para finales de 2026, deberían poder implementarse por lo menos trescientos proyectos de investigación con datos de salud. (BMG, 2023). Para lograr este fin, se publicará

una Ley de Utilización de Datos de Salud, que contemplará, al menos (BMG, 2023).:

- Una oficina central de coordinación y acceso a datos, con fuentes vinculadas a través de pseudónimos de investigación y el almacenamiento descentralizado de la información.
- Se ampliarán las capacidades de la autoridad supervisora de protección de datos para proyectos de investigación trasnacionales.
- El sistema de atención de la salud será estará a cargo de un oficial de datos estatal.
- Se creará un Centro de Datos de Investigación en Salud en el Instituto Federal de Productos Farmacéuticos y Médicos. Los datos seudonimizados deberían ser accesibles de forma automática con fines de investigación.

Cuarta parte. Análisis, discusión y propuesta.

4.1 Análisis comparado de la normativa que garantiza el derecho de portabilidad de datos personales.

4.1.1 Ámbito subjetivo y de validez.

Como pudo observarse en apartados anteriores, los sujetos del derecho son los titulares de los datos personales o interesados, este último, término que utilizan las legislaciones europeas consultadas. Ellos pueden ejercer su derecho por sí mismos o a través de un representante legal en caso de que así lo determinen o bien, si se trata de personas incapaces por cuestión de minoría de edad o estado de interdicción.

Según autores como Somaini (2018, p. 181), Vanberg (2018, pp. 13-14), Vanberg & Ünver (2017, p. 14), que la garantía del derecho a la portabilidad de los datos personales se imponga como obligatoria, supone cargas desproporcionadas para responsables de tratamiento de pequeñas organizaciones, ya que pueden suponerles costos elevados al no contar con los recursos suficientes que les permitan implementar en su totalidad la tecnología necesaria para este efecto.

Sin embargo, nosotros no concordamos con la idea, ya que un derecho humano ya positivizado como tal, no puede ser limitado en su ejercicio por no perjudicar económicamente a los responsables del tratamiento; en su lugar deberían buscarse soluciones conciliatorias entre el usuario y el prestador del servicio, en el que el primero pueda ejercer responsablemente su derecho porque lo conoce y el segundo, garantiza el derecho sin poner en riesgo su patrimonio. El ejercicio del derecho y su garantía, entonces, deberían impulsar el desarrollo de la ciencia y la tecnología en un marco de respeto a los derechos humanos.

Recuérdese que según se ha expuesto, el derecho a la portabilidad de datos personales se puede ejercer en dos vías. Los autores consultados privilegian, por la novedad de la construcción tecnológica, a la forma horizontal que describió Chassang, es decir, la transmisión automática entre responsables. Sin embargo, consideramos que puede darse entre responsables con menos capacidades

tecnológicas, la forma vertical del ejercicio del derecho, es decir, transmitir directamente al interesado los datos en un formato abierto, interoperable y legible por la máquina.

Ahora bien, esto podría interpretarse como que se está limitando el ejercicio del derecho a uno de acceso, en el que el titular o usuario solicita que le sean entregados los datos que son objeto de portabilidad, en un formato electrónico, pero esta modalidad, -que cumple con lo que la legislación que hemos consultado y comparado-, conceptualiza como ejercicio del derecho a la portabilidad con un universo limitadísimo de datos personales.

En el ámbito que nos ocupa, esto puede suponer un auténtico obstáculo para acceder a la garantía del derecho a la protección de la salud. Si únicamente nos son proporcionados los datos que hemos dado al principio de la consulta con el facultativo, el ejercer el derecho a la portabilidad, de manera vertical u horizontal, únicamente nos facilitará información que bien podemos volver a comunicarle a otro profesional de la salud en nuestra siguiente visita, evitándonos el trámite que conlleva el ejercicio del derecho, que en una situación como esta bien puede verse como una carga innecesaria al usuario del sistema, para restablecer su salud.

Otro inconveniente que también se presenta es la falta de digitalización de los datos personales y el acceso a las plataformas tecnológicas de la población en general. Este factor limita el ejercicio de su derecho a la salud, pero también el de la protección de sus datos personales en medios digitales, incluyendo el derecho a la portabilidad, ya que sin este tipo de tecnologías el derecho que se estudia pierde todo sentido desde su garantía, sin el andamiaje digital que permita su debido ejercicio.

De esta suerte, coincidimos con Somaini (2018, p. 189) al afirmar que el impacto del ejercicio del derecho es directamente proporcional al grado de control y de capacidad para ejercerlo del titular de los datos, quien es el único que sabe el grado de utilidad que tiene la información que solicita. Al mismo tiempo, es muy importante que los sistemas que permitan ejercerlo estén diseñados para la rendición de cuentas y con transparencia para que los responsables de

tratamiento demuestren con claridad que su práctica se apega a la legislación vigente.

4.1.2 Requisitos de ejercicio del derecho.

Somaini (2018, p. 183) argumenta que limitar el ejercicio del derecho por violaciones a derechos de terceros, podría desincentivar a los titulares o usuarios de ejercer el derecho a la portabilidad. Los riesgos potenciales a los modelos de negocios no puede ser una razón para negar el ejercicio del derecho, por ello los responsables de tratamiento deben procurar esta acción de tal suerte que no se comparta información protegida por leyes de secreto industrial o de propiedad intelectual, ya que, de hacerse puede ser un obstáculo importante para incluso, la creación de esta información (Vanberg, 2018, sin página). El ejercicio del derecho sería también inoperante en el ámbito público mexicano con base en el consentimiento ya que el tratamiento de los datos personales se da en su gran mayoría, en el ejercicio de facultades y atribuciones.

Por otra parte, si bien es cierto que el Estado mexicano ofrece algunos servicios que deben ser contratados, como el suministro de energía eléctrica o agua potable, también lo es que estos van en contra de uno de los objetivos del reconocimiento del derecho, es decir, incentivar la competencia entre el sector ya que, al ofrecer un servicio de calidad, se prevendrían las solicitudes de portabilidad de datos, ya que no existe competencia real. En ese orden de ideas, el ejercicio del derecho resulta en un sinsentido, al menos en el país americano. Particularmente, no se requiere el consentimiento para tratar los datos de salud por parte de instituciones públicas, ya que su tratamiento se encuentra previsto como una base legitimadora, pues al hacerlo dan cumplimiento a sus facultades y atribuciones.

Así, resulta útil retomar a Sánchez-Caro y Abellán (2016, p. 11), pues señalan que cuando el médico acepta atender a un paciente, adquiere el compromiso de asegurar la continuidad de sus servicios con la excepción de que este pierda la confianza en su labor. Si la situación se presentara, deberá comentarlo con el paciente o sus familiares y hacer lo posible por favorecer que un colega continúe

con la atención, al que le transmitirá la información necesaria para tal efecto, con el consentimiento de quien deba otorgarlo, según sea el caso particular.

Uno de los pasos imprescindibles para alcanzarla es definir, por acuerdo, el conjunto de datos que, por su relevancia, deben estar contenidos en los diferentes informes clínicos que describen los procesos de atención sanitaria realizados a ciudadanos concretos en cualquier centro o servicio del Sistema Nacional de Salud mexicano o español. Esta homogeneidad es uno de los elementos de normalización que facilitan el intercambio entre sistemas diferentes al servicio de los ciudadanos.

Además de lo anterior, la instauración de modelos básicos contrastados por expertos, como instrumento para recoger y presentar la información clínica de manera estandarizada, permite garantizar una homogeneidad en los contenidos de los documentos clínicos en el sistema sanitario, que facilita su comprensión y la más rápida localización de la información, tanto a los pacientes como a los profesionales sanitarios, con independencia del territorio donde deban ser atendidos o donde se haya generado la información, dando de esta forma cumplimiento al mandato de la Legislación de salud de cohesión y calidad del Sistema Nacional de Salud, hablando en específicamente del caso mexicano. Con ello incluso podríamos hablar de su unificación al menos en materia de información, más allá de los sectores que lo conforman.
En este punto cabe preguntarnos si el derecho a la portabilidad de los datos personales es uno de las élites, por las condiciones tan específicas en que debe ejercerse y considerando que, en México, no existen las óptimas de conectividad para portar los datos, así como para establecer un sistema que pueda alimentarse en tiempo real, con las condiciones de seguridad adecuadas para el mantenimiento de la información con apego a la legislación en materia de salud y de datos personales, independientemente del argumento de inviabilidad del ejercicio del derecho expuesto en párrafos anteriores.

Tampoco se cuenta con la infraestructura suficiente para contestar las solicitudes de manera automatizada, lo que no se exige en el marco legal revisado, ni europeo ni mexicano, porque los sujetos obligados y los responsables, en su

gran mayoría, carecen de los avances tecnológicos necesarios para eficientar las respuestas a las solicitudes de ejercicio de los derechos relacionados con la protección de datos personales, cuyo primer problema es la comprobación de la identidad del solicitante.

Recordemos además que este derecho únicamente puede ser ejercido respecto a los datos proporcionados por su titular. Cabe sugerir entonces dos alternativas: la primera, que no se limite el rango de datos que pueden ser objeto de portabilidad ya que como hemos visto, al menos en materia de salud desvirtuaría la utilidad que tiene el ejercicio del derecho, volviéndose más una carga para el usuario de los servicios de salud al únicamente poder ejercerlo en torno a datos que puede proporcionar con cada visita al facultativo, pero no al resto de información que pueden considerarse como inferidos o derivados del diagnóstico que le realizan y que serán a todas luces de gran utilidad por dar a conocer el estado de salud actual del interesado.

La segunda, que los proveedores del servicio, como responsables de tratamiento de los datos personales, en cumplimiento estricto a los principios de minimización, proporcionalidad y calidad limiten la recolección de datos personales a aquellos que son estrictamente necesarios para brindar el servicio, renunciando a los que satisfacen finalidades secundarias. En el caso del expediente o historia clínica, los datos inferidos se traducen en el diagnóstico, pronóstico y dan lugar a un tratamiento, por lo que deben ser accesibles ya que tienen la categoría de personales, a hacer referencia al titular de ellos, y que en el supuesto que hablamos, no han sido disociados o anonimizados, y por lo tanto, pueden hacer al titular identificado o identificable.

En ese sentido, si las normas positivas que hemos analizado a lo largo de este trabajo y que regulan el derecho a la portabilidad se interpretan de forma estricta, no pueden ser portados ya que no fueron otorgados por el titular; sin embargo, están disponibles a través de otros mecanismos, como el ejercicio del derecho de acceso o bien, si se hace una solicitud de referencia-contrarreferencia a otra unidad de salud. En este caso, el derecho a la portabilidad como se encuentra

positivizado es inútil o por lo menos limitado, como instrumento de garantía del derecho a la salud.

Reiteramos que los datos inferidos también deben ser objeto del derecho a la portabilidad, toda vez que estos también hacen referencia a características de los interesados, por lo que se consideran datos personales, aunque conscientemente no los haya proveído: en el caso de los datos de salud, son resultado de la observación que hace el facultativo porque cuenta con los conocimientos necesarios para identificarlos y el usuario no, lo que motiva la consulta. Además, se solicita ejercer el derecho de portabilidad sobre los datos personales, es decir, los resultados de la inferencia, no el mecanismo o metodología con la que se obtuvieron. Al hacerse esa diferenciación, pueden evitarse controversias en materia de derecho de autor o competencia, impidiendo así la limitación de su ejercicio por considerar preponderante el de propiedad intelectual.

Otra característica significativa en torno al ejercicio del derecho es que los responsables no están obligados a contar con la infraestructura que permita garantizar el derecho; sin embargo, a diferencia de la norma mexicana, la europea sugiere al responsable de tratamiento procurar implementar la tecnología necesaria para la garantía paulatina de este derecho. Resulta lógico no imponer esta carga a los responsables por el poco acceso a internet y a la infraestructura tecnológica que tienen, lo que prácticamente les impide garantizar este derecho, al carecer de las garantías mínimas para llevarlo a cabo. No obstante, aunado al rango de datos que pueden ser objeto de portabilidad, las circunstancias descritas limitan aún más su ejercicio.

La falta de obligatoriedad de la garantía del derecho resulta paradójica. Si bien es cierto que no todos los responsables cuentan con los recursos económicos para hacer frente a la garantía de este derecho, también es cierto que ya se encuentra positivizado y a ojos de los interesados como sujetos del derecho, será difícil comprender esta disposición contradictoria. También lo es, estimamos, la falta de obligación que la legislación prevé para no aceptar los datos transferidos (considerando 68, 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).

Así, pensamos que la falta de posibilidad de cumplimiento de estándares mínimos en su mayoría tecnológicos es la razón de que no haya sido elevado a rango constitucional en México, lo que lo pone en desventaja con el resto de los derechos en materia de datos personales: acceso, rectificación, cancelación y oposición. ¿Sería entonces una opción viable, establecer en la legislación la obligatoriedad de la garantía de este derecho? Creemos que sí, ya que se eliminarían algunas de las barreras legales para su ejercicio y podría incluso socializarse para su correcto aprovechamiento como instrumento para garantizar el derecho a la salud, al poder comunicarse todos los datos del expediente clínico, facilitando además el ejercicio y garantía de otros derechos como el de obtener opiniones adicionales acerca de su diagnóstico, o disponiendo de sus datos con mayor facilidad, garantizando además su derecho a la autodeterminación informativa y promoviendo la competencia entre proveedores de servicios de salud, lo que a su vez les forzaría a ofrecer servicios de mejor calidad. Además, la brecha entre el responsable el tratamiento y el interesado se reduciría considerablemente, por el empoderamiento de este último, reduciéndose la asimetría en la relación.

Al volver obligatoria la garantía de este derecho, deberán también tomarse las medidas de seguridad necesarias para la conservación y tratamiento de los datos personales, lo que reducirá el riesgo de pérdida de información si el responsable de tratamiento decide dejar de prestar el servicio según Kive & Grasis (2020, p. 120) y facilitaría el acceso de los titulares a su información reduciendo la posibilidad del extravío o eliminación de los archivos.

Para establecer la obligatoriedad, primero el Estado debería garantizar el acceso universal a Internet de la población. En este sentido, cuentan con ventaja los prestadores de servicios de salud de áreas urbanas, y en sentido contrario se encuentra la población en general por el desconocimiento, pero aún más, los de áreas rurales que además deben lidiar con la falta de cobertura del servicio,

cuyas unidades de salud carecen además de los insumos más elementales, lo que les impedirían llevar a cabo el almacenamiento e intercambio de información.

En este orden de ideas, el ejercicio de este derecho no es de aplicación general de acuerdo con Kive & Grasis (2020, p. 124), y antes de solicitar el ejercicio de los datos, el interesado debe asegurarse de cumplir con los requisitos impuestos por la legislación. Por lo que, tal y como se positiviza actualmente en la norma secundaria, resulta prácticamente imposible plasmarlo en la norma constitucional ya que esto lo volvería fundamental dándole otro rango de obligatoriedad a su garantía, lo que en este momento se vislumbra complicado por los obstáculos de conectividad y accesibilidad tecnológica que ya hemos analizado. Sin embargo, sí consideramos indispensable positivizarlo en la norma mexicana en materia de datos personales en el ámbito de particulares, lo que volvería a este derecho un instrumento importante en la garantía del derecho a la salud en México.

4.1.3 Procedimiento de ejercicio del derecho.

Con el plazo específico dado por las legislaciones estudiadas, resulta un obstáculo el ejercicio del derecho en caso de una emergencia médica, ya que esperar la resolución de la autoridad administrativa o judicial, en su caso, puede resultar incluso en consecuencias catastróficas. Un derecho no puede ser limitado en su ejercicio por ser a su vez, restringida la elección del proveedor de sus servicios como en el caso mexicano que no podrían portarse los datos de un responsable del ámbito privado hacia otro del ámbito público.

Para que el ejercicio del derecho a la portabilidad tenga utilidad, deberá positivizarse también en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, de 5 de julio de 2010, toda vez que como ya hemos constatado, el Sistema Nacional de Salud Mexicano consta de los sectores público, privado y social, por lo que el intercambio de información no debería limitarse por la falta de actualización de la legislación.

Sin embargo, estamos conscientes de que la propuesta de un sistema de expediente clínico electrónico, el ejercicio de este derecho en el ámbito sanitario pierde todo sentido, al menos en una misma jurisdicción, toda vez que ya no sería necesario al contar con una plataforma única que se actualiza en tiempo real y a la que tiene acceso todo el tiempo el titular de los datos y, cuando sea necesario a la sección correspondiente, el profesional de la salud.

Solo sería lógico y útil su ejercicio entre jurisdicciones distintas, aunque para ello haya que positivizar y firmar tratados internacionales en esta materia para que los países que así lo deseen, contraigan estas obligaciones. O bien, que se ejerza entre proveedores de distintos sectores, por ejemplo, si un titular requiere que cierta información de su expediente clínico deba ser transmitida a su proveedor de seguros. No obstante, lo que debería fortalecerse es la interoperabilidad, para facilitar el intercambio de información, así como las medidas de seguridad para su resguardo y acceso. Por ello, consideramos que lo ideal es diseñar la normativa adecuadamente, con la finalidad de evitar molestias innecesarias al interesado y que puedan acceder y portar sus datos en tiempo real. Es decir, retomamos la portabilidad continuada propuesta por Krämer *et al.* (2020, p. 9)

Una buena práctica es la aplicación de sistemas automatizados como las interfaces de programación de aplicaciones (API), que facilitarán el intercambio de información con el interesado para la reducción de carga que puede imponer las solicitudes repetitivas y, en consecuencia, la negativa al ejercicio del derecho.

4.2 Análisis comparado del Sistema Nacional de Salud.

Cabe señalar algunas diferencias que resultan evidentes entre ambos sistemas de salud, que, no obstante, detallan la forma que tienen de garantizar el contenido del derecho de protección a la salud en ambas jurisdicciones.

Para comenzar, quiénes son sujetos de este derecho y quiénes pueden exigir su garantía, resultando en el caso mexicano más amplio en ambos sentidos por ser un derecho para toda persona que se encuentre en territorio nacional y no solo

limitado a quienes cuenten con la ciudadanía de este país o los extranjeros que tengan su residencia en él, como en el caso español. A la par, es evidente la diferencia de quienes integran el Sistema Nacional de Salud, que en la legislación mexicana se establece que son todos los actores sanitarios de los sectores público, privado y social, sin diferencia de si están vinculados con el primero de ellos.

También resulta importante que, aunque a lo largo de la legislación general española se destaca que el acceso al sistema de salud se hará alineado a principios de no discriminación y de corregir las desigualdades sanitarias para garantizar la igualdad a su acceso, debemos recordar que los primeros artículos de la legislación condicionan las características que las personas deben reunir para exigir la garantía del derecho; a contraposición de la legislación mexicana que, en esa garantía primaria de la que habla Bovero establece la universalidad en el acceso que ya ha sido ampliamente comentada.

Finalmente, consideramos los argumentos de Ruiz (1985, pp. 8, 9) por lo que hace la integración de la política de salud a la de desarrollo, pues discurre acerca de que las acciones sanitarias deben vincularse íntimamente a las públicas y sociales con las que se encuentra relacionada, tiene plena vigencia casi treinta años después, independientemente del ejercicio de derecho comparado que se ha realizado "darle efectividad creciente al derecho a la protección de la salud significa llevara delante el programa de justicia social; cambiar la Nación; reducir la desigualdad social; generar empleo: elevar los niveles de nutrición; ampliar los niveles de educación: racionalizar los patrones de consumo; modificar una valorativa social que propicia la enfermedad; mejorar, no ampliar, el control sanitario de la producción; modernizar la Secretaría de Salubridad y Asistencia y el Sector; abatir el mercantilismo de una sociedad capitalista; y hacer más racional el proceso de desarrollo. Será necesario introducir el ingrediente sanitario en las grandes decisiones de la Nación."

Continuando con el razonamiento primigenio, coincidimos con la afirmación acerca de que "la salud es uno de los principales objetivos del desarrollo. Constituye un bien preciado en sí mismo y una condición indispensable para la

igualdad de oportunidades" que Frenk y Gómez (2015, p. 17) realizan, ya que como se aprecia, en los párrafos precedentes, cualquiera de las normativas referidas se destaca la importancia de brindar acceso efectivo a la información, hablando de material educativo, estadísticas o información considerada pública.

4.3 Análisis comparado del expediente clínico y el electrónico.

Autores como Kurczyn (2019, pp. 896, 897), sugieren que la debida gestión documental del expediente clínico proveerá de una razonable fuente de conocimiento de la situación del paciente, no dejando de lado el principio de complementariedad, por lo que para su redacción e integración no puede limitarse a que ésta sea confeccionada acorde a las reglas de la *lex artis ad hoc* del ejercicio médico, sino que debe ineludiblemente acoplarse también a las normas que garanticen plenamente el derecho a la privacidad, intimidad y protección de datos personales.

Como se ha mencionado, el expediente clínico, en los dos ámbitos territoriales cuya normativa se estudia, está integrado por documentación diversa, como las notas médicas y reportes, que al menos deben contener nombre completo del paciente, edad, sexo y número de cama o expediente de ser el caso; las notas también deberán contener nombre de quien la elabora, así como su firma autógrafa, electrónica o digital, según sea el caso y de acuerdo con la normativa aplicable. Deben expresarse en lenguaje técnico-médico, sin abreviaturas, con letra legible, sin enmendaduras ni tachaduras y conservarse en buen estado.

En este sentido y a diferencia del caso mexicano, es destacable la facultad del Ministerio de Sanidad y Consumo para que cumpla con lo dispuesto en la ley citada, para promover la implantación de un sistema de compatibilidad que atienda la evolución y disponibilidad de los recursos técnicos y la diversidad de sistemas y tipos de historias clínicas, para que los diferentes centros asistenciales de España que atiendan al mismo paciente, eviten someter a exploraciones y procedimientos de innecesaria repetición a los pacientes que acudan en solicitud de servicios de salud.

Un expediente clínico electrónico único estandarizado para todo el Sistema Nacional de Salud promovería el ejercicio del derecho de acceso a los datos personales. Para ello, el software tendría que ser brindado por el Estado como ente regulador a través de la legislación general en materia de salud y no consideramos que anularía la competencia entre responsables del tratamiento que son los prestadores del servicio de salud, más bien, lo haría entre los proveedores del software, figuras que no necesariamente coinciden como prestadores de ambos servicios.

Esto último sería una solución plausible a la aplicación de la portabilidad como característica pues uno de los problemas más importantes que enfrenta es la multiplicidad de formatos en los que se almacena la información, lo que impide que sea comunicada efectivamente, por lo que el expediente clínico electrónico único podría ser una solución plausible en un país en el que el Estado de Derecho debe ser fortalecido, para que los titulares de los datos confíen en que el tratamiento de los mismos se dará en el marco de la legislación aplicable.

Aunado a lo anterior, también se fortalecen los mecanismos de rendición de cuentas que permitan que la ley sea correctamente aplicada sobre todo en seguridad de la información, para que se cumpla el objetivo del ejercicio del derecho a la portabilidad, es decir, que se comunique la información y se fomente la autodeterminación informativa del titular de los datos, pero en un marco de legalidad en el que se dote de verdadero sentido y utilidad al ejercicio de este derecho.

El monopolio público puede ser la respuesta para brindar seguridad jurídica a la población al establecer un modelo único de expediente clínico electrónico con estándares de tratamiento brindados por la legislación que se vean expresados en un software único a utilizar por todos los prestadores de servicio de salud, independientemente del sector al que pertenezcan. Es decir, que no podrán generarse expedientes clínicos electrónicos distintos al que provee el Estado, con el objetivo de facilitar la portabilidad e interoperabilidad de la información entre distintos proveedores, pero también para maximizar y facilitar el acceso a los datos personales de los titulares, que ven anulada su capacidad de elección

del proveedor de los servicios de salud para favorecer la garantía del derecho a los datos personales de salud.

Sin embargo, este monopolio rivaliza directamente con la prohibición constitucional de su establecimiento, pero también con uno de los objetivos doctrinales de la garantía del derecho a la portabilidad, cuyo espíritu reside en fomentar la competencia entre responsables de tratamiento para que los titulares elijan los servicios que sean más convenientes y ahí lleven su información y por ende, no se monopolice ni se centralice pues entre mayor variedad de esta, mayor posibilidad de desarrollo de aplicaciones y de inteligencia artificial se tiene, ya que hay más variables de entrenamiento y programación y los resultados son más acertados y apegados a cubrir las necesidades de la población, alrededor de la que debería ser construida la garantía del derecho.

De esta suerte, Lenard (2020, p. 6) explica que las normas antimonopolio exigen establecer que el proveedor tiene poder en el mercado que domina, practica actos anticompetitivos y que los consumidores han sido dañados de manera inequívoca, afirmando que hasta el momento de su publicación, no existían hallazgos al respecto, pero que sí este tipo de normas es positivizada acertadamente, podría ser una mejor opción frente a la propia portabilidad e interoperabilidad para el fomento de la competencia entre proveedores.

Sin embargo, consideramos que la positivización de la norma en materia de protección de datos personales, específicamente la de portabilidad, debería girar en torno al titular de los datos para su ejercicio y aprovechamiento, y no para facilitar el modelo de negocio de los proveedores de servicio, sin que esto signifique la obstaculización del avance científico y tecnológico que supone el intercambio de la información de salud, pero sí que se construya un modelo en el que el eje rector sea la garantía de los derechos humanos y su objetivo, la salvaguardia de la dignidad de los titulares de los datos personales. La respuesta al dilema podría ser modernizar y adecuar la Norma Oficial Mexicana NOM-024-SSA3-2012, pero, además, establecer mayores controles de cumplimiento para que los responsables se vean obligados a cumplir con la garantía del derecho.

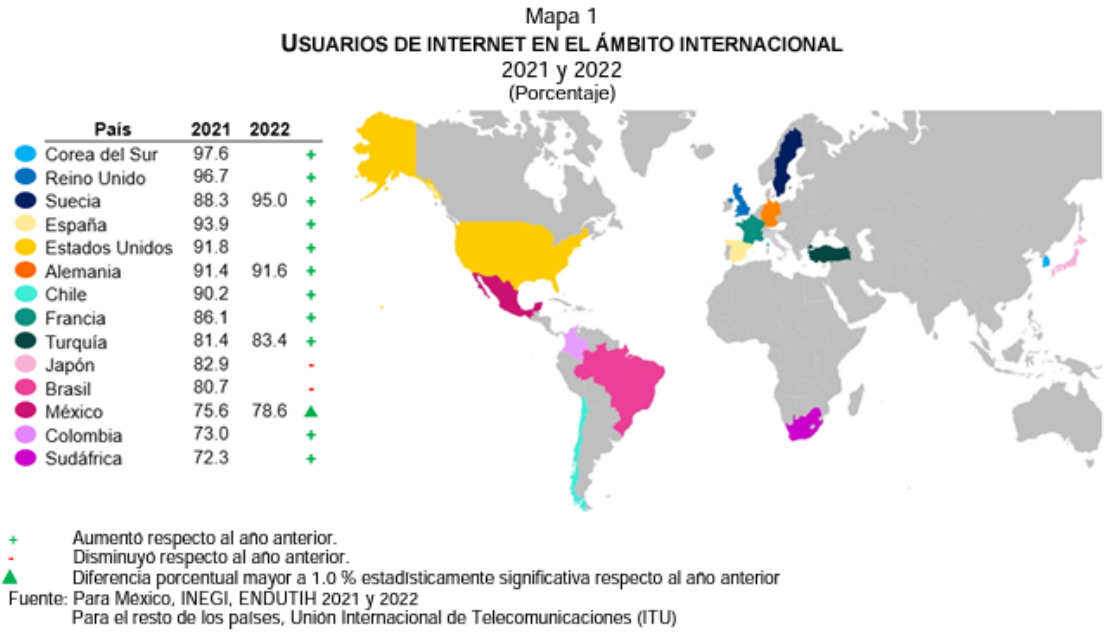
4.4. Análisis comparado del estado de digitalización y conexión universal.

Como muestran las estadísticas analizadas en apartados anteriores, México y España se encuentran en momentos distintos de su digitalización. Más allá de la diferencia en que se sitúan los países, con una clara ventaja del europeo en diversos ámbitos como el nivel de acceso a medios digitales o hasta de adquisición de los conocimientos para el aprovechamiento de estas herramientas, nos parece de particular interés señalar las acciones que se llevan a cabo para lograr las metas establecidas en los respectivos planes sectoriales en materia de salud.

En este sentido, es imperante mencionar la omisión del gobierno mexicano de plasmar líneas de acción específicas para implementar la modernización del sistema de información y comunicación en materia de salud, razón por la cual estimamos que las acciones de cumplimiento del Programa Sectorial de Salud 2022-2024 se limitan a capacitaciones y visitas. También consideramos importante que se recopilen datos de unidades médicas privadas para integrarlas al Informe de Recursos de Salud Sectorial de la Dirección de Información en Salud. Resulta importante poder comparar la información de los sectores público y privado para acortar las brechas de accesibilidad que puedan existir y así establecer estrategias de unificación del Sistema Nacional de Salud.

Resulta muy preocupante además el bajo porcentaje de implementación de tecnologías de la información en unidades de salud públicas. De interés particular para esta investigación son los rubros de expediente clínico electrónico y conectividad de internet, que contrastan de manera evidente con el alto índice de digitalización de la administración pública española. De esta suerte, podemos apreciar que, mientras en México se mide el nivel de acceso a tecnologías de la información y de cobertura a internet, en España se proyecta como meta a mediano plazo que la totalidad de su población cuente con las habilidades digitales necesarias para aprovechar los servicios digitalizados que el gobierno ya ofrece.

Ilustración 17. Usuarios de internet en el ámbito internacional.



Fuente: ENDUTIH, 2022, p. 9.

4.5 Propuesta *de lege ferenda*: la portabilidad por diseño y por defecto.

Teniendo en cuenta antecedentes jurisprudenciales tales como Airey c. Irlanda (Tribunal Europeo de Derechos Humanos, TEDH, 1979), o Hokkanen c. Finlandia (TEDH, 1994) en el que el Tribunal establece que "las obligaciones positivas […] obligan a las autoridades nacionales a adoptar las medidas necesarias y razonables para salvaguardar un derecho" pues "El Convenio [108] tiene por objeto garantizar no derechos teóricos o ilusorios, sino derechos prácticos y efectivos"; es que se realiza la propuesta que a continuación se detalla.

Y es que, el TEDH (2002) ha consolidado como doctrina que "la disuasión efectiva frente a actos graves, cuando están en juego valores fundamentales y aspectos esenciales de la vida privada, requiere disposiciones penales eficientes y su aplicación a través de una investigación y un enjuiciamiento efectivos"; doctrina que extendemos a cualquier rama del derecho que corresponda, y cuya interpretación abrimos a los medios de rendición de cuentas que nos permitan la aplicación oportuna de la legislación y si no, el establecimiento de garantías

secundarias para el debido ejercicio del derecho de portabilidad de los datos personales. Además, en Z. c. Finlandia (TEDH, 1997) se estableció que "la protección de los datos médicos es esencial para el disfrute del derecho al respeto de la vida privada y familiar de una persona", lo que resulta indispensable "no solo para respetar el sentido de la intimidad de una persona, sino también para preservar su confianza en la profesión médica y en los servicios sanitarios en general" y si esa protección falla, los usuarios de los servicios de salud podrían no tener voluntad de aportar la información suficiente al facultativo, o bien, ni siquiera buscar atención médica, por no contar con esa protección.

Así y dado el evidente atraso del Estado mexicano en materia de protección de datos personales y de expediente clínico, la propuesta solo se realizará para esta jurisdicción territorial. Para tal efecto, podrá observarse una tabla comparativa realizada por normativa a modificar, con tres columnas:

Nombre del cuerpo normativo vigente		
Artículo vigente	Propuesta de reforma	Justificación
Se incluye el artículo vigente.	Contempla el texto que se propone como vigente, derivado de la investigación.	Se incluyen argumentos complementarios a lo ya expuesto en secciones anteriores de este trabajo.

No realizaremos una propuesta para la Ley Federal de Protección de Datos Personales en Posesión de Particulares en específico ya que es anacrónica y nunca ha sufrido una reforma, por lo que debería estudiarse en profundidad su actualización, lo que excede el objetivo de esta investigación. No obstante, la reforma que se propone la consideramos válida para los dos ámbitos, toda vez que se centra en el titular de los datos o interesado, desde el diseño y por defecto, para incentivar la circulación de sus datos y su derecho de autodeterminación informativa por encima de los intereses económicos de los responsables del tratamiento.

Además, las propuestas serán realizadas dando cumplimiento a la Ley General de Mejora Regulatoria, de 18 de mayo de 2018. En ella se establecen en su artículo 7, fracción V, el principio de simplificación, mejora y no duplicidad en la emisión de regulaciones, trámites y servicios; y en el similar 8, fracción XI, el

objetivo de facilitar a las personas el ejercicio de los derechos y el cumplimiento de sus obligaciones, y en el mismo numeral, pero en la fracción XIII, facilitar el conocimiento y el entendimiento por parte de la sociedad, de la Regulación, mediante la accesibilidad y el uso de lenguaje claro.

4.5.1 En materia de portabilidad de datos personales.

Constitución Política de los Estados Unidos Mexicanos		
Artículo vigente	**Propuesta de reforma**	**Justificación**
Artículo 16 Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo. **Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.** No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión. La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculpado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal. Cualquier persona puede detener al indiciado en el momento en que esté cometiendo un delito o inmediatamente después de haberlo cometido, poniéndolo sin demora a disposición de la autoridad civil más cercana y ésta con la misma prontitud,	**Artículo 16** **Primer párrafo: sin reforma.** Segundo párrafo: Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición **a las finalidades de su tratamiento y a solicitar su portabilidad** en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. **Párrafos del tres al dieciocho, sin reforma.**	Se considera adecuado especificar a qué se oponen las personas respecto a sus datos, para mayor coherencia de la redacción. Se eleva a rango constitucional el derecho a la portabilidad de los datos, sin especificar sus tipos, para que se desarrolle en las leyes reglamentarias de la materia. Consideramos de importancia establecerlo como un derecho humano, garantizado desde el texto constitucional, para equipararlo al resto de derechos ARCO, pero también para impulsar la conexión digital y alfabetización de la población en esta materia. Al encontrarse el derecho a la portabilidad de los datos personales reconocido como un derecho humano, el titular de los datos puede, incluso, recurrir a medios de garantía secundarios, tales como el Juicio de Amparo o los recursos de impugnación en materia de datos personales, para exigir el cumplimiento del texto constitucional. Estamos conscientes de que los responsables de tratamiento cuentan con pocos medios para garantizar este derecho que se ejerce, por su naturaleza, en el entorno digital. Sin embargo, con las resoluciones del Poder Judicial, puede obligarse al Poder Legislativo a destinar el

a la del Ministerio Público. Existirá un registro inmediato de la detención. Sólo en casos urgentes, cuando se trate de delito grave así calificado por la ley y ante el riesgo fundado de que el indiciado pueda sustraerse a la acción de la justicia, siempre y cuando no se pueda ocurrir ante la autoridad judicial por razón de la hora, lugar o circunstancia, el Ministerio Público podrá, bajo su responsabilidad, ordenar su detención, fundando y expresando los indicios que motiven su proceder. En casos de urgencia o flagrancia, el juez que reciba la consignación del detenido deberá inmediatamente ratificar la detención o decretar la libertad con las reservas de ley. La autoridad judicial, a petición del Ministerio Público y tratándose de delitos de delincuencia organizada, podrá decretar el arraigo de una persona, con las modalidades de lugar y tiempo que la ley señale, sin que pueda exceder de cuarenta días, siempre que sea necesario para el éxito de la investigación, la protección de personas o bienes jurídicos, o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia. Este plazo podrá prorrogarse, siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen. En todo caso, la duración total del arraigo no podrá exceder los ochenta días. Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia. Ningún indiciado podrá ser retenido por el Ministerio Público por más de cuarenta y ocho horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial; este plazo podrá duplicarse en aquellos casos que la ley prevea como delincuencia organizada. Todo abuso a lo anteriormente dispuesto será sancionado por la ley penal.		presupuesto necesario y al Poder Ejecutivo, a que lleve a cabo las acciones necesarias para paulatinamente, impulsar la creación y el cumplimiento de políticas públicas de digitalización, acceso a nuevas tecnologías e intercambio de la información. Como vimos en apartados anteriores, este tipo de acciones ya se han plasmado en programas derivados del Plan Nacional de Desarrollo, sin embargo, hasta la fecha poco se ha realizado para dar cumplimiento a esas líneas de acción. Finalmente, consideramos adecuado que sigan existiendo dos leyes en materia de protección de datos personales. Es decir, una para regular el tratamiento de los datos personales en posesión de particulares; y otra para los que se encuentran en posesión de los sujetos obligados, es decir, autoridades de los niveles federal, local y municipal, por tener ámbitos de actuación bien diferenciados y bases legitimadoras distintas y correspondientes a lo que de acuerdo con las disposiciones legales que les rigen, pueden llevar a cabo.

En toda orden de cateo, que sólo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia. Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.		

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio. La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos. La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley. En tiempo de paz ningún miembro del Ejército podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento, bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.		
Sin artículo correlativo.	**Transitorios** Primero. El presente Decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación. Segundo. Dentro de los 365 días naturales a la publicación de este Decreto, el Congreso de la Unión deberá reformar la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento, para la inclusión del derecho de portabilidad de los datos personales. Tercero. Los Congresos de las Entidades Federativas contaran con un término de 180 días naturales para garantizar en el texto de las Constituciones locales, el derecho a la portabilidad de los datos personales.	Se concede un año natural para la reforma de la legislación citada y su reglamento, toda vez que se trata de normas jurídicas que, desde los años en que fueron publicadas -2010 y 2011-, no han sido objeto de reforma, por lo que puede ser una oportunidad de actualizarlas y no solamente incluir el derecho a la portabilidad, aunque ese sea el único mandato establecido en el transitorio. Se conceden 180 días para reformar las Constituciones locales para que garanticen el derecho a la portabilidad en el texto de las Constituciones de las Entidades Federativas.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados		
Artículo vigente	**Propuesta de reforma**	**Justificación**
Artículo 28. El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, al que refiere la fracción V del artículo anterior deberá contener, al menos, la siguiente información: I. El domicilio del responsable; II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles; III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento; IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular; **V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;** VI. El domicilio de la Unidad de Transparencia, y VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.	**Artículo 28.** Primer párrafo, sin reforma. Fracciones I a la V, sin reforma. **<u>V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad. Acerca de este último, el responsable deberá ser claro acerca de si cuenta con los medios para dar tratamiento y transmitir los datos personales en consonancia a lo establecido por el capítulo II de la Ley.</u>** Fracciones VI y VII, sin reforma.	Como comprobamos en apartados anteriores, la brecha digital en México es aún amplia y acortarla será una meta a mediano plazo que requiere de voluntad gubernamental para diseñar y cumplir con políticas públicas que para tal efecto se publiquen. En ese sentido, consideramos que una buena medida que le obligue es la de considerar al derecho a la portabilidad como derecho humano, por las consideraciones vertidas en el cuadro anterior. Sin embargo, hasta que pueda garantizarse en su totalidad, estimamos conveniente que el responsable, abonando al cumplimiento del principio de información, sea claro acerca de sus capacidades de garantía de este derecho, para no crear falsas expectativas en el titular de los datos personales. De esta suerte y si bien es cierto que los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, establecen la obligación del responsable de dar aviso al titular de su capacidad para garantizar este derecho, también lo es que se trata de un instrumento de menor jerarquía y también, menos difundido, por lo que estimamos conveniente la inclusión en este apartado, para concientizar sobre la existencia y utilidad de este derecho y también, para que queden consolidados en una misma legislación, los requisitos mínimos que debe contener el aviso de privacidad.
TÍTULO TERCERO DERECHOS DE LOS TITULARES Y SU EJERCICIO Capítulo I	**TÍTULO TERCERO DERECHOS DE LOS TITULARES Y SU EJERCICIO Capítulo I**	Se estima conveniente agregar el derecho a la portabilidad de los datos personales toda vez la propuesta realizada para elevarlo a rango constitucional, como derecho humano, junto con los de acceso, rectificación, cancelación y oposición.

De los Derechos de Acceso, Rectificación, Cancelación y Oposición Artículo 43. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro. Artículo 44. El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento. Artículo 45. El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados. Artículo 46. El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último. Artículo 47. El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando: I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos	**De los Derechos de Acceso, Rectificación, Cancelación y Oposición** Artículos del 43 al 47, sin reforma. **Artículo 47 bis.** La persona titular de los datos personales tendrá derecho a solicitar la portabilidad de sus datos personales si estos son tratados por vía electrónica, en un formato estructurado y comúnmente utilizado. Su objetivo será propiciar el intercambio de la información y fortalecer el derecho a la autodeterminación informativa de la persona titular de los datos personales. **Artículo 47 ter.** El derecho a la portabilidad de los datos personales podrá ser: I. Directo u horizontal, cuando la transmisión de los datos personales se haga de un responsable de tratamiento a otro, previa solicitud de la persona titular de los datos personales y sin que lo impida el responsable que facilite la información. II. Indirecto o vertical, cuando la transmisión se efectúe del responsable del tratamiento al titular de los datos personales, mediante la obtención de una copia de esa información.	Se agregan conceptos doctrinales de los revisados a lo largo de la investigación para dar mayor certeza del objetivo y modalidades de ejercicio de este derecho.

o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.		
Capítulo II **Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición** **Artículo 48.** La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los responsables, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia. **Artículo 49.** Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial. En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación. Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre que el	**Capítulo II** **Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación, Oposición <u>y Portabilidad</u>.** **Artículo 48.** La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO **<u>y de portabilidad</u>** que se formulen a los responsables, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia. **Artículo 49.** Para el ejercicio de los derechos ARCO **<u>y de portabilidad</u>**, será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante. El ejercicio de los derechos ARCO **<u>y de portabilidad</u>** por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial. En el ejercicio de los derechos ARCO **<u>y de portabilidad</u>** de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.	Consideramos viable agregar el procedimiento de ejercicio del derecho de portabilidad de los datos personales a este capítulo, ya que el artículo 14 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, “para el ejercicio de la portabilidad de datos personales, el responsable deberá observar los requisitos, plazos, condiciones, términos y procedimientos establecidos en el Título Tercero, Capítulo II de la Ley General o los que correspondan en las legislaciones estatales en la materia y demás disposiciones que resulten aplicables en la materia, así como lo dispuesto en el presente Capítulo.” Igualmente se incentiva a los responsables a adoptar mecanismos que permitan el intercambio de datos en formatos estructurados de uso común, lectura mecánica e interoperable.

titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto. **Artículo 50.** El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable. Para efectos de acceso a datos personales, las leyes que establezcan los costos de reproducción y certificación deberán considerar en su determinación que los montos permitan o faciliten el ejercicio de este derecho. Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste. La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular. El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular. **Artículo 51.** El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.	Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto. **Artículo 50.** El ejercicio de los derechos ARCO **y de portabilidad** deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable. Para efectos de acceso a datos personales, las leyes que establezcan los costos de reproducción y certificación deberán considerar en su determinación que los montos permitan o faciliten el ejercicio de este derecho. Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste. La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular. El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de	

El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta. En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular. **Artículo 52.** En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes: I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones; II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante; III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud; IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso; V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso. Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable deberá atender la solicitud en la modalidad requerida por el titular,	los derechos ARCO **y de portabilidad,** algún servicio o medio que implique un costo al titular. **Artículo 51.** El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO **y de portabilidad**, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud. El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta. **En el caso que el ejercicio del derecho de portabilidad se situara en el contexto de una emergencia, el plazo para su ejercicio será de 48 horas, siempre que sea técnicamente posible.** En caso de resultar procedente el ejercicio de los derechos **de este capítulo**, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular. **Artículo 52.** En la solicitud para el ejercicio de los derechos ARCO **y de portabilidad** no podrán imponerse mayores requisitos que los siguientes: I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones; II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;	

salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación. En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere este artículo, y el Instituto o los organismos garantes no cuenten con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto, o en su caso, los organismos garantes, para resolver la solicitud de ejercicio de los derechos ARCO. Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable. En el caso de la solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades	III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud; IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos **de este capítulo**, salvo que se trate del derecho de acceso; V. La descripción del derecho ~~ARCO~~ que se pretende ejercer, o bien, lo que solicita el titular, y VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso. Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación. En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere este artículo, y el Instituto o los organismos garantes no cuenten con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO **y de portabilidad**, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.	

específicas respecto de las cuales requiere ejercer el derecho de oposición. Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias. El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda. El Instituto y los Organismos garantes, según corresponda, podrán establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO. Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable. **Artículo 53**. Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente. En caso de que el responsable declare inexistencia de los datos personales en sus	Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO **y de portabilidad**. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto, o en su caso, los organismos garantes, para resolver la solicitud de ejercicio de los derechos ARCO **y de portabilidad**. Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable. En el caso de la solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición. Las solicitudes para el ejercicio de los derechos ARCO **y de portabilidad** deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias. El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO **y de portabilidad** y entregar el acuse de recibo que corresponda.	

archivos, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales. En caso de que el responsable advierta que la solicitud para el ejercicio de los derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento al titular. **Artículo 54.** Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO conforme a las disposiciones establecidas en este Capítulo. **Artículo 55.** Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son: I. Cuando el titular o su representante no estén debidamente acreditados para ello; II. Cuando los datos personales no se encuentren en posesión del responsable; III. Cuando exista un impedimento legal; IV. Cuando se lesionen los derechos de un tercero; V. Cuando se obstaculicen actuaciones judiciales o administrativas;	El Instituto y los Organismos garantes, según corresponda, podrán establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO **y de portabilidad.** Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable. **Artículo 52 bis. Será objeto de ejercicio del derecho a la portabilidad de los datos personales:** **I. La información que se considere como dato personal, de acuerdo con la definición que esta Ley haga, sin importar la forma en que se haya obtenido, ya sea directa, observada o inferida. Para tal efecto, se comunicarán únicamente los datos personales y no el mecanismo o razonamiento que se aplicó para su obtención y,** **II. La información cuyo el tratamiento sea realizado a través de medios automatizados.** **Artículo 52 ter. El ejercicio del derecho a la portabilidad será técnicamente posible como consecuencia de que el tratamiento de los datos personales se lleve a cabo a través de medios automatizados y, por lo tanto, la información pueda ser transmitida mediante un formato electrónico estructurado y comúnmente utilizado.**	

VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos; VII. Cuando la cancelación u oposición haya sido previamente realizada; VIII. Cuando el responsable no sea competente; IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular; X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular; XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o XII. Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades. En todos los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 51 de la presente Ley y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes. **Artículo 56.** Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la presente Ley.	Los responsables del tratamiento procurarán crear y utilizar formatos interoperables que permitan la portabilidad de datos. **Artículo 53**. Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos **a que se refiere este capítulo**, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente. En caso de que el responsable declare inexistencia de los datos personales en sus archivos, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales. En caso de que el responsable advierta que la solicitud para el ejercicio de los derechos ARCO **y de portabilidad** corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento al titular. **Artículo 54.** Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos **de este capítulo**, el responsable deberá informar al titular sobre **su** existencia, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO **y de portabilidad**, a efecto de que decida si los ejerce a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la	

	atención de este tipo de solicitudes, conforme a las disposiciones establecidas en este Capítulo. **Artículo 55.** Las únicas causas en las que el ejercicio de los derechos ARCO **y de portabilidad** no será procedente son: I. Cuando el titular o su representante no estén debidamente acreditados para ello; II. Cuando los datos personales no se encuentren en posesión del responsable; III. Cuando exista un impedimento legal; IV. Cuando se lesionen los derechos de un tercero; V. Cuando se obstaculicen actuaciones judiciales o administrativas; VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos; VII. Cuando la cancelación u oposición haya sido previamente realizada; VIII. Cuando el responsable no sea competente; IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular; X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular; XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o XII. Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan	

	proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades. **XIII. <u>En el caso del ejercicio del derecho a la portabilidad, si el tratamiento de los datos personales no se lleva a cabo a través de medios automatizados y, por lo tanto, la información no puede ser transmitida mediante un formato electrónico estructurado y comúnmente utilizado.</u>** En todos los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 51 de la presente Ley y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes, **<u>salvo si se tratara de una urgencia, en cuyo caso se apegará a lo establecido en el penúltimo párrafo de artículo 51 de esta Ley.</u>** **Artículo 56.** Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO **<u>y de portabilidad</u>** o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la presente Ley.	
Capítulo III **De la Portabilidad de los Datos** Artículo 57. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.	**Capítulo III** **De la Portabilidad de los Datos** **Se deroga**	Consideramos viable derogar este capítulo ya que su contenido y el de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales, de 12 de febrero de 2018, han sido agregados y armonizados al cuerpo de la ley en esta propuesta, dando cumplimiento a los principios y objetivos en materia de mejora regulatoria, detallados en las notas introductorias de este apartado.

Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales. El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.		En ese orden de ideas, los Lineamientos deberán ser abrogados.
	Transitorios **Primero.** El presente Decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación. Segundo. Los Congresos de las Entidades Federativas contaran con un término de 180 días naturales para armonizar las normas jurídicas en materia de protección de datos personales en posesión de sujetos obligados.	Se concede un año natural para la reforma de la legislación citada y su reglamento, toda vez que se trata de normas jurídicas que, desde los años en que fueron publicadas -2010 y 2011-, no han sido objeto de reforma, por lo que puede ser una oportunidad de actualizarlas y no solamente incluir el derecho a la portabilidad, aunque ese sea el único mandato establecido en el transitorio. Se conceden 180 días para reformar las Constituciones locales para que garanticen el derecho a la portabilidad en el texto de las Constituciones de las Entidades Federativas.

4.5.2 En materia de expediente clínico y expediente clínico electrónico

Ley General de Salud		
Artículo vigente	Propuesta de reforma	Justificación
Artículo 3o.- En los términos de esta Ley, es materia de salubridad general: **<u>Fracción sin correlativo</u>**	Artículo 3o.- En los términos de esta Ley, es materia de salubridad general: Fracciones I a XVI bis: sin reforma. **<u>Fracción sin correlativo: XVI Ter. El diseño, la organización, coordinación, vigilancia e implementación del Expediente Clínico Único.</u>** Fracciones XVII a XXVIII: sin reforma.	Se considera que, para abonar en la unificación de hecho del Sistema Nacional de Salud, es imperativa la existencia de un expediente clínico único diseñado, organizado, coordinado, vigilado e implementado por la cabeza del sector a nivel nacional, es decir, por la Secretaría de Salud del Poder Ejecutivo Federal. Con la palabra único nos referimos a un documento por persona, pero también al único modelo de expediente clínico. Toda vez el atraso digital en México que se hizo patente a lo largo de la investigación, se deja abierto a que el expediente pueda ser físico o digital, aunque lo ideal sería cumplir con el Programa Sectorial de Salud a través de su estrategia prioritaria "3.4.5 Implementar progresivamente tecnologías de información y comunicación tendientes a garantizar el funcionamiento de los sistemas de información, digitalización de expedientes e interoperabilidad interinstitucional, entre los diferentes niveles de atención en las instituciones que conforman el Sistema Nacional de Salud." Aunque la reforma es similar en términos para los tres artículos, el tercero hace referencia a la salubridad general, es decir, aquellos tópicos que
Artículo 7o.- La coordinación del Sistema Nacional de Salud estará a cargo de la Secretaría de Salud, correspondiéndole a ésta: **<u>Fracción sin correlativo.</u>**	Artículo 7o.- La coordinación del Sistema Nacional de Salud estará a cargo de la Secretaría de Salud, correspondiéndole a ésta: Fracciones I a X bis, sin reforma. **<u>X ter: El diseño, la organización, coordinación, vigilancia e implementación del Expediente Clínico Único.</u>** Fracciones XI a XV, sin reforma.	
CAPITULO II Distribución de Competencias Artículo 13. La competencia entre la Federación y las entidades federativas	Artículo 13. La competencia entre la Federación y las entidades federativas en materia de salubridad general quedará distribuida conforme a lo siguiente:	

en materia de salubridad general quedará distribuida conforme a lo siguiente: A. Corresponde al Ejecutivo Federal, por conducto de la Secretaría de Salud: **Fracción sin correlativo**	A. Corresponde al Ejecutivo Federal, por conducto de la Secretaría de Salud: Fracciones I a VII bis, sin reforma. VII ter. **El diseño, la organización, coordinación, vigilancia, archivo e implementación del Expediente Clínico Único.** Fracción VIII a X, sin reforma	solamente son competencia de la federación para su legislación. A su vez, el artículo séptimo especifica las facultades exclusivas de la Secretaría de Salud del Poder Ejecutivo Federal, por lo que las Secretarías de Salud y Servicios de Salud de las Entidades Federativas, solo aplicarían el modelo de expediente clínico unificado, físico o electrónico de la Federación, lo que permitirá el intercambio de la información de salud en formatos únicos e interoperables en el caso electrónico, pero también evitará las discrepancias en el formato físico. A este último respecto, si bien es cierto que la Norma Oficial Mexicana NOM-004-SSA3-2012 establece los parámetros mínimos para evitar diferencias en los registros, la reforma es innovadora en tanto unifica el sistema de archivo para que se centralice en la Federación y esto facilite la comunicación de la información al estar almacenada en una sola base de datos. Esto último facilitará incluso, el trabajo de vigilancia epidemiológica, la elaboración de estadísticas e investigaciones y esto a su vez, podrá utilizarse para realizar políticas públicas más eficientes y útiles para la garantía del derecho a la protección de la salud.
Sin correlativo	Transitorio. Se elaborará y expedirá el Reglamento de la Ley General de salud en materia de expediente clínico único a más tardar un año de la entrada en vigor de la presente disposición.	Como hemos comprobado a lo largo de la investigación, en México subsiste una confusión respecto a la percepción de que el Sistema Nacional de Salud se encuentra fragmentado, cuando la Ley General de Salud es clara respecto a que se trata uno con sectores bien diferenciados,

		pero que se rigen por las mismas normas jurídicas en el fondo, aunque no en la forma. Aunque los parámetros del expediente clínico se encuentran establecidos en la Norma Oficial Mexicana NOM-004-SSA3-2012, del expediente clínico electrónico, de 29 de junio de 2012, y para los Sistemas de Información de Registro Electrónico para la Salud se contemplan en la Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud, de 30 de noviembre de 2011, consideramos que establecerlos en una norma jurídica como lo es el Reglamento de una Legislación General, le dará mayor relevancia y difusión a su existencia, pero también es una oportunidad para dotar a este instrumento indispensable para el tratamiento médico de mayor seguridad jurídica al plasmarse en una norma de mayor rango. En este sentido, se propone en líneas generales normar lo conducente al expediente clínico físico y electrónico por la brecha digital existente en México, pero siempre proyectando a corto plazo la evolución de este sistema a uno netamente electrónico que facilite el intercambio de datos personales y no personales. Con ello se beneficiará a la población mexicana en tanto titulares de los datos personales, pero también por lo que hace a la garantía de su derecho a la protección de su salud al facilitar la elaboración de investigaciones y políticas públicas gracias al acceso a información disociada y por supuesto, como usuarios de los servicios de salud al verse mejorada su atención médica.

		Este expediente deberá estar diseñado por defecto con el usuario del sistema de salud como centro, con el objetivo de equilibrar la relación entre el profesional de la salud y el usuario al dotar a este último de los recursos necesarios para conocer su información de salud, al ejercer su derecho de protección de datos personales en cualquiera de sus modalidades.

Quinta parte. Conclusiones y futuras líneas de investigación.

5.1 Conclusiones

1. Tanto en España como en México, existen corrientes doctrinarias que consideran al expediente clínico como un documento público en el caso de que sea creado en instituciones de salud de este sector y, por tanto, obligadas en términos de la legislación de transparencia y acceso a la información; y como documento privado por su naturaleza brindada por los datos que en él se recoge. Lo anterior no quiere decir que en el primer supuesto sea de acceso público, más bien se clasificaría como confidencial por contener datos personales, únicamente accesible para el facultativo que brinda la atención y por supuesto, para el interesado o titular de los datos que ahí se contienen, con las excepciones que se explicaron a lo largo de este trabajo.

2. Las normas jurídicas que contienen lineamientos generales en materia de seguridad y protección de la información hacen referencia clara de complementarse con lo dispuesto en la legislación específica de protección de datos personales y salud.

3. Se distinguen dos objetivos generales para recabar, tratar y transmitir datos personales de salud: el primero, es para brindar la atención médica solicitada y para lograrlo se estipulan diversos mecanismos que abonan a dar certeza a su titular de que está siendo resguardada y utilizada de forma responsable, pertinente y únicamente por quienes tienen legítimo acceso a ella, es decir, quienes le prestan ese servicio. El segundo, va orientado a generar las estadísticas necesarias para generar políticas públicas que modifiquen los servicios que se ofrecen a la población, siempre en su beneficio.

4. Para lograr el segundo objetivo descrito en el punto tres, los datos personales deberán pasar por un proceso de disociación, para lo cual el personal

involucrado deberá ser capacitado y las medidas de seguridad y control establecidas.

5. Dada la complejidad del Sistema Nacional de Salud mexicano, se aprecia la ventaja de contar con un esquema único de interoperabilidad que facilite el flujo de información entre sus diversos actores, y que sea además de obligatorio cumplimiento.

6. El profesional de la salud encargado de brindar la atención médica, únicamente deberá pedir los datos que necesita para brindar la atención y ejecutar el acto médico, y tratarlos solamente para los fines estrictamente necesarios. Periódicamente deberá actualizar los datos del paciente, necesidad de la que se dará cuenta al interactuar con éste de manera sucesiva.

7. El acceso a la propia información es uno de los pilares fundamentales que ayudarán tanto a los facultativos como a los pacientes a tomar las mejores decisiones, con el único propósito del restablecimiento del estado de bienestar que debe reinar en los seres humanos y a que hace referencia la legislación y la doctrina.

8. En el ámbito médico, respetar en todo momento la expectativa razonable de privacidad del titular resulta fundamental por el tipo de información con la que se trabaja. En consecuencia, los facultativos deberán tener cuidado al momento de transmitir esos datos a terceros que no estén autorizados expresamente por el paciente para conocer su situación de salud. Así, el profesional de salud no puede tener acceso al historial clínico del usuario si no cuenta con facultades o atribuciones expresas o bien, si no existe algún tratamiento que así lo justifique.

9. No debe confundirse la obtención del consentimiento informado para la realización de algún procedimiento sanitario, con el que deberá obtenerse para el tratamiento de los datos personales del paciente. Esta información, así como la que surja derivada de la atención médica brindada, servirá para la integración del expediente clínico.

10. El tratamiento de los datos personales deberá ser realizado por una persona sujeta al secreto profesional, si se trata de datos indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, en los términos que ya hemos revisado a lo largo de la investigación y que prescribe la legislación sanitaria.

11. La portabilidad de datos, como cualquier otro derecho que para ser garantizado, externalizado o ejecutado requiere de la tecnología (expresada por ejemplo en sistemas interoperables), viene a resignificar la característica de la universalidad de los derechos humanos por su carácter instrumental para a su vez, garantizar otros derechos como lo es el de la protección de la salud, materia de esta investigación.

12. Es indispensable diferenciar entre la portabilidad como característica y como derecho fundamental. Si bien es cierto que ambos tienen como objetivo la reutilización de los datos personales, para que pueda ser considerado derecho deberá tener aparejada la finalidad de incentivar la autodeterminación del sujeto que lo ejerce. Es decir, que se busca que el individuo pueda decidir a quién y para qué transfiere su información.

13. El objetivo de reconocer a la portabilidad como otro derecho del espectro de la protección de datos, no es otro que el de reforzar la autodeterminación del titular de los datos, respecto de que quiere hacer con éstos.

14. La portabilidad es un derecho distinto al de acceso de los datos personales, ya que fue concebido para coadyuvar en el empoderamiento del titular de los datos personales al reafirmar el ejercicio de su derecho de autodeterminación informativa. En este sentido y para que pueda ejercer su derecho con la mínima participación del responsable, éste debería cumplir con los principios del tratamiento para que los datos se encuentren exactos, pertinentes y actualizados en todo momento, lo que a su vez quitará cargas innecesarias al responsable que retrasen la transmisión de los datos.

15. Otra diferencia importante entre los derechos de portabilidad y acceso, que ayuda a definir al primero, es que éste únicamente nos permite conocer los datos que se proporcionaron al inicio de la relación jurídica basada en un contrato o al brindar su consentimiento para el tratamiento de esa información. Su objetivo además será el de proporcionarlos a otro responsable directamente o a través del titular de los datos como intermediario, para brindarle un servicio similar que el del responsable original.

16. Los datos inferidos también deben ser reconocidos como datos personales, toda vez que, aunque son producto del análisis llevado a cabo por los responsables, igualmente hacen referencia a características que pueden identificar o volver identificable a las personas a las que se describen.

17. A través de los datos inferidos se descubrirán otros datos que incluso pueden llegar a ser sensibles pues darán cuenta de características de las personas tales como conductas, costumbres o el estado de salud, por concepto y determinación legal.

18. Tal y como se encuentra regulado el ejercicio del derecho a la portabilidad, los datos personales sensibles o especialmente protegidos no pueden ser compartidos por cuestiones económicas y de competencia principalmente, por la propia naturaleza de los datos. Esto evidencia que, en el campo sanitario, el ejercicio del derecho de portabilidad de datos puede representar una carga para el titular de los datos o interesado, en vez de una herramienta que le permita acceder a los servicios de salud de forma pronta y eficiente.

19. El derecho a la portabilidad de datos puede representar una verdadera innovación para la garantía de otros derechos fundamentales, como el de protección a la salud, así como del empoderamiento del titular de los datos, siempre y cuando se le dote de contenido, sobre todo tratándose del técnico indispensable para que se cumpla el objeto de su positivización.

20. El responsable del tratamiento deberá tener en cuenta siempre la clasificación de los datos que se traten y al mismo tiempo implementará las mejores prácticas para garantizar la seguridad de los datos, pero también para la agilización del ejercicio del derecho a la portabilidad. Para ello se observará la implementación de incentivos, la regulación específica en la materia e incluso, la educación a la población para el mejor aprovechamiento y garantía de este derecho. En consecuencia, se incentivaría la autodeterminación informativa del interesado o titular de los datos, facilitando su transferencia y promoviendo la innovación basada en los datos.

21. El responsable del tratamiento, sin importar si es un ente público o privado, debería procurar la modernización de sus sistemas para que paulatinamente, los datos se traten en formatos interoperables comunes y estructurados de forma que además de concebirlos privados por diseño y por defecto, también sean portables desde su origen, lo que sin duda beneficiaría a los usuarios de los servicios de salud pues entre otras ventajas, verían agilizada su

atención por no tener que estar sometidos a los tiempos de respuesta que marca la legislación.

22. Al mismo tiempo, la medida descrita coadyuvaría como mecanismo de auditoría o rendición de cuentas al trabajo de los profesionales de la salud. Aunque no es un motivo de incentivar la medicina defensiva, consideramos que resultaría un incentivo para elaborar con pulcritud y apego a la legislación vigente una fuente documental tan importante como lo es el expediente clínico.

23. A su vez, esta acción estimularía el ejercicio y garantía de otros derechos asociados como es el de protección de la salud, al proveer de los medios para tener una atención oportuna y de calidad; así como el acceso a las opiniones de tantos facultativos como se considere conveniente. También se incentivaría el ejercicio de otros derechos que tienen estrecha relación con el de protección de la salud, tal como el de protección de datos personales, al ser capaces de recibir información exacta y oportuna y que los registros se conserven con la confidencialidad necesaria, lo que a su vez se enlaza con el deber de secreto profesional, cuya violación puede derivar en responsabilidades de orden administrativo, civil o penal.

24. La hipótesis propuesta para esta investigación, no se ha comprobado por las siguientes razones:

    a. Se partió de la idea, ampliamente difundida en México por las Autoridades de protección de datos, de que el derecho de portabilidad de datos personales sería la herramienta necesaria para comunicar los expedientes clínicos completos.

b. Derivado del análisis documental y de derecho comparado realizado, se ha comprobado que esto resulta incorrecto, pues únicamente son objeto de portabilidad los datos proporcionados por el titular al principio de la relación jurídica siempre que el tratamiento tenga como base una relación contractual o bien, el consentimiento para el tratamiento de los datos personales. En ese sentido y para cumplir el objetivo descrito, sería adecuado el ejercicio del derecho de acceso a los datos personales, mediante el cual podría obtenerse la información completa y relativa al estado de salud del titular.

c. Sin embargo, aunque en apariencia el derecho a la portabilidad de datos personales podría tener aplicación en México al facilitar la apertura de expedientes con diversos prestadores de servicio de salud de la elección del titular, consideramos que esta estrategia no resulta útil en la práctica pues aunque favorece el ejercicio del derecho de tener cuantas opiniones médicas se requieran o necesiten antes de tomar una decisión concerniente al estado de salud, continuaría sin cumplirse el principio de unicidad del expediente clínico propuesto por los diversos teóricos analizados y mandatado por la legislación sanitaria vigente. Esto, a su vez derivaría en que el usuario seguiría sin contar con acceso efectivo a su información, y por lo tanto, se encontraría en franca desventaja en cuanto a la toma de decisiones se refiere.

d. El derecho a la portabilidad, tal como está previsto actualmente en la norma, no coadyuva en el ejercicio o la garantía del derecho a la salud, antes bien, impone una carga al titular de los datos pues su ejercicio no resulta útil al solo poder obtener aquellos que se hayan entregado al inicio de la relación jurídica, que bien podrían ser los que se brinden en el interrogatorio inicial, pero que no incluyen a los relativos al

diagnóstico, pronóstico y tratamiento pues se considerarían datos inferidos, independientemente de que ha sido ampliamente desestimada la propiedad intelectual del médico tratante respecto a esta información.

e. Toda vez que en materia de salud los responsables del orden público basan el tratamiento de los datos personales en el ejercicio de sus facultades y atribuciones, situación que se halla prevista en la legislación mexicana como una excepción a la obtención del consentimiento para el tratamiento de datos personales sensibles o de categoría especial, vuelve en la teoría inviable el ejercicio de este derecho a no tener como fundamento ni el consentimiento del interesado o titular o una relación contractual como base del tratamiento de la información, lo que se desprende del estudio de la legislación en la materia.

f. Los datos personales recabados reflejan el estado de salud del usuario de los servicios y no creemos que fuera el ánimo del legislador ni el objetivo de la positivización del derecho a la portabilidad que su ejercicio derivara en la obtención de todos estos datos por parte del usuario en su calidad de titular o interesado, sino que se enfoca en el estudio de los clientes mediante la creación de perfiles que les permitan entender sus necesidades para mejorar los servicios que les ofrecen.

g. Sin embargo, se limitaría la utilidad del derecho a la portabilidad de los datos personales, a la transmisión de datos que se obtienen en la primera entrevista con el médico tratante y que resultarían útiles en el supuesto de que este cumpla con su obligación de mantenerlos permanentemente actualizados y pertinentes. De lo contrario, el

profesional de la salud receptor se haría de datos que reflejarían la realidad del usuario de los servicios al solicitar en esa ocasión los servicios de salud de que se trate.

h. Así, resultaría una carga para el titular de los datos ejercer ese derecho para obtener una copia de los datos que puede proporcionar en una primera visita, por lo que consideramos que en el área de la atención a la salud el ejercicio de este derecho no es de interés o utilidad para la finalidad planteada, tal y como se encuentra previsto actualmente en la Ley.

i. En ese sentido, consideramos que la portabilidad como característica podría ser aprovechada en el ámbito de la salud en la investigación, para intercambiar los datos del sujeto involucrado en ella entre diversos responsables de llevarlas a cabo, de acuerdo con el contexto que se proponga en cada oportunidad, o bien, para llevar a cabo dictámenes periciales de una situación determinada, finalidades que resultan secundarias a la principal por la que se recaban los datos personales, es decir, a brindar asistencia sanitaria.

25. Tanto la Secretaría de Salud del gobierno federal mexicano como el INAI, deberán tomar la iniciativa, en congruencia con el principio de responsabilidad proactiva, para que dentro del Sistema Nacional de Salud se contemple la creación de un expediente clínico electrónico único de cada persona y que sea de uso obligatorio para los sectores público y privado, adoptando una estrategia que envuelva a la privacidad desde el diseño, de tal suerte que el titular de los datos pueda ejercer plenamente sus derechos a la salud y los relativos a la protección de sus datos. A su vez el prestador de servicios médicos puede ejercer su profesión con un enfoque cercano al paciente, sin mediar estrategias tales como la medicina defensiva. Con ello

estimamos que se facilitará la portabilidad de los datos y su transferencia en un entorno seguro, asegurando que se tratan en estricto apego a los principios y deberes que la norma establece para tal efecto.

26. Por el contrario, el cumplimiento irrestricto de principios y deberes de tratamiento de los datos personales permitiría contar con la oportunidad de ampliar la calidad de la atención proporcionada a los usuarios de servicios sanitarios, no importa la instancia a la que acudan, y reduciría las quejas de éstos ante organismos especializados en medios alternos de solución de conflictos como la Comisiones de Arbitraje Médico, o bien, la autoridad judicial.

27. La planeación de políticas públicas en materia de datos personales debe ser diseñada con privacidad por diseño y defecto, alrededor del titular de los datos personales, con el objetivo de empoderarlo para que lo ejerza. En este último punto, una estrategia efectiva de socialización será indispensable para que se difunda su existencia y utilidad.

28. Si resulta indispensable el tratamiento masivo de datos personales, debe realizarse una Evaluación de Impacto para la Protección de Datos.

29. No coincidimos con la opinión de la Federación Bancaria Europea (2017, p. 9), acerca de que la legislación debería especificar la temporalidad para el ejercicio del derecho de portabilidad, ya que consideramos que es una cuestión que depende directamente del tiempo de conservación que tengan los datos dependiendo de la materia que se trate, por lo que, mientras se tenga el deber de conservarlos, aunque haya cesado la relación jurídica entre el responsable y su titular o incluso se encuentren bloqueados para su tratamiento, no debe impedirse el ejercicio de los derechos que se le

relacionen, como se establece en las legislaciones en materia de datos personales que hemos revisado.

30. Sin embargo, la interoperabilidad, característica exigida por las normas consultadas como básica para facilitar la portabilidad de los datos, resultará crucial en beneficio del ejercicio del derecho a la salud. Así, al pensar en la interoperabilidad debemos entenderla a partir del concepto de portabilidad, pero no del derecho a la portabilidad de datos personales que se encuentra tan limitado por la norma vigente.

31. La interoperabilidad como característica también resulta indispensable si en México finalmente se implementara un expediente clínico electrónico único, siguiendo el ejemplo del Espacio Europeo de Datos Personales, ya que permitiría el acceso a ese archivo único a nombre del interesado o titular de los datos, en el que podrían reflejarse las diversas opiniones de los profesionales de la salud que emitan en el área de su especialidad acerca de su estado de salud.

32. Igualmente, deben establecerse medidas de seguridad suficientes que permitan el acceso seguro tanto del médico como del paciente, lo que sin duda sí coadyuvaría a cumplir el objetivo planteado para la positivización del derecho a la portabilidad, es decir, empoderar al titular de los datos al tener verdadero control acerca del conocimiento de su estado de salud y de quién puede acceder a esa información, estableciendo para ello los controles suficientes que permitan saber quiénes y bajo qué circunstancias han tenido acceso a esos datos.

33. Para que la portabilidad pueda ser integrada por diseño debe trabajarse en la redacción de estándares específicos para el sector salud, ya que los Lineamientos que establecen los parámetros, modalidades y procedimientos

para la portabilidad de datos personales, emitidos por el Sistema Nacional de Transparencia Mexicano, de 12 de febrero de 2018, por su propia naturaleza, fueron redactados de forma tan abierta que naturalmente no responden a las necesidades particulares de los diferentes sectores a los que pertenecen los responsables del tratamiento de los datos personales.

34. Estos estándares deberían incluir los especializados en materia de archivo para el sector salud, específicamente del caso que abordamos en la investigación, es decir, la conservación del expediente clínico para dar cumplimiento a la finalidad primordial de su creación, es decir, la atención del usuario del sistema de salud.

35. La falta de capacitación y especialización de los profesionales de la salud constituye un obstáculo para el tratamiento adecuado de los datos personales y la garantía del derecho de portabilidad.

5.2 Futuras líneas de investigación.

1. La concurrencia en materia de derecho a la protección de datos personales, entre Federación y Estados, con el objetivo de comprobar la viabilidad de unificar la legislación en la materia y que no se cuente con dos diferenciadas para responsables de los ámbitos públicos y privados.

   Como se revisó en materia de salud, consideramos viable establecer concurrencia en materia de protección de datos personales para determinar con claridad las esferas competenciales, facultades y atribuciones de la federación y las entidades federativas. Con ello se evitará la mala práctica de reproducir la Ley General para cumplir con la obligación de armonizar las leyes locales en materia de protección de datos personales, pues únicamente

se podrá legislar en los Congresos de las Entidades Federativas de temas específicos.

2. El proyecto del expediente clínico electrónico

Aunque la investigación estuvo limitada por la escasa literatura y resoluciones de casos prácticos en torno al derecho de portabilidad que existen, y a su vez el estudio de caso por las condiciones que se nos brindaron para su desarrollo y consolidación, creemos que una línea de investigación viable sería el desarrollo de un modelo único de expediente clínico electrónico para el Estado mexicano, que se vea beneficiado de las experiencias en otras latitudes, por ejemplo, la Unión Europea, para que se consolide al grado que pueda ser implementada.

Este deberá contar con un marco jurídico lo suficientemente flexible para permitir el aprovechamiento de los datos seudonimizados o anonimizados. Para ello, deberá diseñarse un software capaz de anonimizar o seudonimizar los datos *por diseño y por defecto*, para enviarlos a un repositorio general que sea responsabilidad en el caso de México, de la Dirección General de Información en Salud y puedan ser reutilizados; o bien, para utilizarlos con distintos fines.

Lo anterior puede ser aprovechado para realizar investigación en seres humanos pues al contar con el software diseñado desde la privacidad y anonimización o seudonimización por diseño y por defecto, los datos pueden ser tratados para este fin brindando mayores garantías de seguridad a los interesados o titulares de esta información.

3. Reputación del usuario o el prestador del servicio:

a. ¿El ejercicio del derecho de portabilidad puede afectar la reputación del prestador del servicio, por el número de veces que el usuario de los servicios de salud decide ejercer su derecho y/o dejar su servicio?

   i. Los datos de profesionales de la salud en instituciones públicas, ¿serían información de interés público, publicable o exigible a través del ejercicio de derecho de acceso a la información pública por tratarse del desempeño profesional de un servidor público? ¿O serían información confidencial por tratarse de una evaluación al ejercicio profesional del prestador de servicios y, por lo tanto, datos personales de índole laboral?

   ii. ¿Cómo afectan su reputación profesional este tipo de datos, si son recolectados?

   iii. Partiendo de lo dispuesto en las legislaciones ya estudiadas, de que el derecho a la portabilidad no puede ser ejercido si se afectan derechos de terceros, si se hacen públicas la cantidad y causas del ejercicio del derecho a la portabilidad y están resultan ser en su mayoría negativas, ¿podría impedirse el ejercicio del derecho en un futuro a otros usuarios, para evitar afectar la reputación del prestador de servicios de salud?

   iv. Los datos, ¿podrían ser solicitados por autoridades judiciales o administrativas para allegarse de medios de prueba o valoración de prueba en un procedimiento relacionado con el desempeño del ejercicio profesional?

b. ¿La reputación del usuario también está en riesgo si se puede acceder al número de veces que decide ejercer su derecho?

c. ¿Sería plausible añadir en la plataforma o la solicitud la causa que motiva el ejercicio del derecho a la portabilidad? Esto no como requisito para el ejercicio, sino como estadística para la mejora del servicio prestado.

4. Socialización del derecho a la portabilidad de datos personales y el cumplimiento de su garantía:

    a. ¿Los titulares de los datos personales conocen que tienen el derecho a la portabilidad de los datos personales?
    b. El estudio de las razones esgrimidas por los responsables de tratamiento de los datos personales para garantizar o no el derecho de portabilidad.
    c. ¿Se contestan las solicitudes de los titulares?
    d. ¿Cuáles son las razones en cada caso?
    e. Identificación de las áreas de oportunidad para la búsqueda de soluciones que permitan dar garantía al derecho (tipo de impedimento: tecnológico, jurídico).

5. Estrategia de digitalización que vaya de la mano con la socialización del derecho, para que todas las personas, no importando el lugar donde residan, puedan entender y ejercer los derechos relacionados con la protección de sus datos personales.

Fuentes de consulta y referencia

Bibliografía

Acosta, V. (1990). *De la responsabilidad civil médica*. Jurídica de Chile.

Adame Goddard, J. (2017). Ética, legislación y derecho. En J. Saldaña Serrano (coord.). *Problemas actuales sobre derechos humanos*. Una respuesta filosófica. (p. 27-38). Universidad Nacional Autónoma de México.

Aguayo Cruz, E. (2017). Una nueva propuesta iusnaturalista en la filosofía mexicana para fundamentar los derechos humanos. En J. Saldaña Serrano (coord.). *Problemas actuales sobre derechos humanos*. Una propuesta filosófica (p. 39-50). Universidad Nacional Autónoma de México.

Alkorta Idiakez, I. (2022). *El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*. Aranzadi.

Andreu Martínez, M. (2018). Los menores y sus derechos en la sociedad digital. En De la Quadra, S. T., y Piñar Mañas, J. L., (coords.) *Sociedad digital y derecho* (p. 417-438). Ministerio de Industria, Comercio y Turismo, Red. es y Boletín Oficial del Estado.

Atienza, M., & Ferrajoli, L. (2017). *Jurisdicción y argumentación en el Estado Constitucional de Derecho*. UNAM; Instituto de Investigaciones Jurídicas.

Barak, A. (2017). *Proporcionalidad. Los derechos fundamentales y sus restricciones*. Palestra Editores.

Barco Vega, G., Cervantes Padilla, A., y Dávara Fernández de Marcos, I. (2019). Dato personal. En Dávara, I., (coord.), *Diccionario de protección de datos personales. Conceptos fundamentales*. (p. 211-215). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Barco Vega, G., Cervantes Padilla, A., y Dávara Fernández de Marcos, I. (2019). Tercero. En Dávara, I., (coord.), *Diccionario de protección de datos personales. Conceptos fundamentales*. (p. 850-851). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Barco Vega, G., Cervantes Padilla, A., y Dávara Fernández de Marcos, I. (2019). Titular de los datos personales. En Dávara, I., (coord.), *Diccionario de*

protección de datos personales. Conceptos fundamentales. (p. 850-852). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Barth, M. (2021). A Case Study on Data Portability. Measuring the Maturity on Data Portability Exports in IoT Platforms. *Datenschutz und Detensicherheit*. 3:190-197.

Basterra, M. (2008). *Protección de datos personales. Ley 25.326 y Dto. 1558/01 Comentados, Derecho Constitucional Provincial, Iberoamérica y México*. Ediar.

Beauchamp, T. L., y Childress, J. F. (2013). *Principles of Biomedical Ethics*. Oxford University Press.

Beauchot, M. (1999). *Derechos humanos. Historia y filosofía*. Fontamara.

Beauchot, M. (2017). Los derechos humanos y el fundamento de su universalidad. En Saldaña Serrano, J., (coord.), *Una nueva propuesta iusnaturalista en la filosofía mexicana para fundamentar los derechos humanos*, (p. 51-60). Universidad Nacional Autónoma de México.

Bedate, A., y Torre, J. (2010). *Dignidad humana y bioética*. Universidad Pontificia Comillas.

Bernier, C. (2016). El futuro ha llegado. *Revista uruguaya de protección de datos personales*, 4-10. Recuperado en abril de 2019 de https://tinyurl.com/y3vyppxg

Bistolfi, C., Scudiero, L. (2016). *Bringing your data everywhere in the Internet of (every)Thing: a legal reading of the new right to portability*. Istituto Italiano per la Privacy. DOI 10.1109/WAINA.2016.106

Bobbio, N. (1991). *El tiempo de los derechos*. Sistema.

Bordes Solana, M. (2006). Investigación médica y genética y protección de datos. En Bacaria Martrus, J., y Ripol Carulla, S. (eds.), *Estudios de protección de datos de carácter personal en el ámbito de la salud* (p. 213-258). Marcial Pons; Agencia Catalana de Protección de Datos.

Bovero, M. (2002). Globalización, democracia, derechos ¿siete globalizaciones? *Justicia electoral*, 17. 51-58. Recuperado en agosto de 2021 de https://revistas-colaboracion.juridicas.unam.mx/index.php/justicia-electoral/article/view/11960/10775

Bovero, M. (2013). *La protección supranacional de los derechos fundamentales y la ciudadanía*. Tribunal Electoral del Poder Judicial de la Federación.

Bozdag, E. (2018). Data Portability Under GDPR: Technical Challenges. Recuperado en agosto de 2021 de http://dx.doi.org/10.2139/ssrn.3111866

Brena Sesma, I. (2004). *El derecho y la salud. Temas a reflexionar*. Universidad Nacional Autónoma de México.

Brena, I. (2020). Presentación. En Brena, I., (coord.), *Derecho y salud* (pp. XV-XVII). Universidad Nacional Autónoma de México.

Briebich, C., & Spíndola, A. (2014). *Diccionario de la Constitución Mexicana (Vol. I Jerarquía y vinculación de sus conceptos)*. México: Miguel Ángel Porrúa, Senado de la República.

Burgoa, I. (2008). *Las garantías individuales*. México: Porrúa.

Buttarelli, G. (2016). Prólogo. En Piñar Mañas, J. L. (coord.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Reus.

Bygrave, L. (2022). Security by Design: Aspirations and Realities in a Regulatory Context. *Oslo Law Review, 8* (3), 126-177. Recuperado en aosto de 2021 https://doi.org/10.18261/olr.8.3.2

Canales Gil, A. (2013). La protección de datos en el sector sanitario. En Ornelas Núñez, L. y Piñar Mañas, J. L. (coords.), *La protección de datos personales en México* (p. 423-464). Tirant lo Blanch.

Cano Valle, F. (2016). *Derecho a la protección a la salud en América Latina*. UNAM, Instituto de Investigaciones Jurídicas.

Cantoral, K. (2012). *Derecho de protección de datos personales de la salud*. Liber Iuris Novum.

Carbonell, J., y Carbonell, M. (2013). *El derecho a la salud: una propuesta para México*. UNAM.

Carbonell, M. (2013). *Derechos fundamentales y democracia*. Instituto Federal Electoral.

Carcar Benito, J. (2012). Criterios de valoración del derecho a la salud en relación a las (TIC). Especial referencia a la integridad y calidad de vida. En Marcos del Cano, A. (coord.), *Bioética y derechos humanos* (p. 319-344). UNED.

Carnicero, J., y Fernández, A. (2012). *Manual de Salud Electrónica para directivos de servicios y sistemas de salud*. Organización de las Naciones Unidas.

Carpintero, M. (2017). Igualdad y simetría: la selección de los derechos. En Saldaña Serrano, J. (coord.), *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (p. 61-90). Universidad Nacional Autónoma de México.

Carrancá y Rivas, R., y Carrancá y Trujillo, R. (2001). *Código Penal Anotado*. Porrúa.

Casa Madrid Mata, O., y Tarasco Michel, M. (1997). El derecho sanitario mexicano. La enfermería en México. Sistemática jurídica y legitimación del acto biomédico. En Pastor García, L. M. y León Correa, F. J. (coords.), *Manual de ética y legislación en enfermería. Bioética de enfermería*. (p. 231-239). Mosby.

Casa-Madrid, O. (2012). *El juramento de Hipócrates y los fines del derecho*. FUNDAP.

Casa-Madrid, O. (2013). *La responsabilidad jurídica en psiquiatría*. Alfil.

Castro, M., Díaz, G., Mur, F., Peire, J., y Sancristóbal, E. (2012). *Seguridad en las comunicaciones y en la información*. Universidad Nacional de Educación a Distancia.

Chassang, G., Southerington, T., Tzortzatou, O., Boeckhout, M., & Slockenberga, S. (2018). Data portability in health research and biobanking: legal benchmarks for appropriate implementation. *European Data Protection Law Review, 4*, 296-307. Recuperado en agosto de 2021 de https://doi.org/10.21552/edpl/2018/3/8

CIDH. (2020). *Cuadernillo de Jurisprudencia de la Corte Interamericana de Derecho Humanos No. 28: Derecho a la salud*. Corte Interamericana de Derechos Humanos y Cooperación Alemana (GIZ).

Comandé, G., & Schneider, G. (2018). Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of 'Health Data'. *European Journal of Health Law, 25* (3), 284-307. Recuperado en agosto de 2021 de https://doi.org/10.1163/15718093-12520368

Comandè, G., & Schneider, G. (2021). Can the GDPR make data flow for research easier? Yes it can, by differentiating! A careful reading of the GDPR shows how EU data protection law leaves open some significant flexibilities for data protection-sound research activities. *Computer Law & Security Review, 41*, 105539, Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2021.105539

Comandé, G., Nocco, L., & Peigné, V. (2015). An empirical study of healthcare providers and patients' perceptions of electronic health records. *Computers in Biology and Medicine,* 59, 194-201. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.compbiomed.2014.01.011

Commitee on Boethics. (1 de febrero de 1995). Informed Consent, Parental Permission, an Assent in Pediatric Practice. *Pediatrics*, 95 (2) 314-317. Recuperado en abril de 2021 de https://pediatrics.aappublications.org/content/pediatrics/95/2/314.full.pdf

CONBIOÉTICA. (2010). *Guía nacional para la integración y el funcionamiento de los comités hospitalarios de bioética*. CONBIOÉTICA.

Congreso de la Unión (2010). *Cuadernos de apoyo. Terminología Legislativa*. Congreso de la Unión de los Estados Unidos Mexicanos. Recuperado en abril de 2023 de https://www.diputados.gob.mx/sedia/biblio/doclegis/cuaderno_terminolegis.pdf

Consejo y Chapela, C. (2017). Elementos esenciales del consentimiento informado. En Martínez Bullé Goyri, V. M., (coord.), *Consentimiento informado.*

Fundamentos de su aplicación práctica (p. 51-66). Universidad Nacional Autónoma de México.

Cotino Hueso, L. (2014). El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: <<un falso derecho, a juzgar por un falso tribunal>>. En Bel Mallén, J. I., y Correidora y Alfonso, L. (dirs.), *Derecho de la información: el ejercicio del derecho a la información y su jurisprudencia*, (p. 387-430). Centro de Estudios Políticos y Constitucionales.

Cotino Hueso, L. (2015). Algunas cuestiones clave de protección de datos en la nube. Hacia una <<regulación nebulosa>>. *Revista catalana de drete públic* (51), 85-103. Recuperado en octubre de 2022 de doi: http://dx.doi.org/10.2436/20.8030.01.55

Cotino Hueso, L. (2017). Big data e inteligencia artifical. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata*. Año 9, no. 24, 131-150. Recuperado en octubre de 2022 https://dialnet.unirioja.es/descarga/articulo/6066829.pdf

Cotino Hueso, L. (2018). La necesaria actualización de los derechos fundamentales como derechos digitales ante el desarrollo de internet y las nuevas tecnologías. En Pendás, B. (Dir.), *España constitucional (1978-2018). Trayectorias y perspectivas III*. (p. 2347-2362). Centro de Estudios Políticos y Constitucionales.

Cotino Hueso, L. (2019). Ética en el diseño para el desarrollo de una inteligencia artifical, robótica y big data confiables y su utilidad desde el derecho. *Revista Catalana de Dret Públic* (58), 29-48. Recuperado en octubre de 2022 de https://doi-org.bibliotecauned.idm.oclc.org/10.i58.2019.3303

Cotino Hueso, L. (2020). Datos Personales. En Pendás, B. (ed.), *Enciclopedia de las Ciencias Morales y Políticas para el Siglo XXI. Ciencias Políticas y Jurídicas*. (p. 665-668). Real Academia de Ciencias Morales y Políticas. Boletín Oficial del Estado.

Cotino Hueso, L. (2020). El alcance interactuación del régimen jurídico de los datos personales y big data relacionado con salud y la investigación biomédica. *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicna Avanzada* (52), 57-138. Recuperado en octubre de 2022 de https://www.uv.es/cotino/publicaciones/Revista%20Genoma%2052COTINO.pdf

Cotino Hueso, L., García, R., Murillo, P., Medina, M., Rallo, A., Rebollo, L., Troncoso, A., Vidal, C. (2020). Encuesta sobre la protección de datos personales. *Teoría y Realidad Constitucional* (46), 15-118. Recuperado en octubre de 2022 https://doi.org/10.5944/trc.46.2020.29105

Cotino Hueso, L. (2022). Ciberseguridad, privacidad y gobernanza para la explotación de datos por la ciudad inteligente. En Cotino Hueso, L. y Todolí Signes, A. (coords.), *Explotación y regulación del uso del big data e inteligencia artificial para los servicios públicos y la ciudad inteligente* (p. 81-124). Tirant Lo Blanch.

D'Agostino, F. (2017). Los derechos y deberes del hombre. En Saldaña Serrano, J., (coord.), *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (p. 91-106). Universidad Nacional Autónoma de México.

D'Imperio, A., Ienca, M., Maiese, A., Fazio, V., & La Russa, R. (2021). Uninformed consent: Who knows what Ivan Ilych would have thought? *Clinica Terapeutica, 172*(4), 264-267. Recuperado en agosto de 2021 de https://doi.org/10.7417/CT.2021.2328

Daniolou, S., Rapp, A., Haase, C., Ruppert, A., Wittwer, M., Scoccia, A., Pandis, N., Kressing, R., y Ienca, M. (2021). Digital Predictors of Morbidity, Hospitalization, and Mortality Among Older Adults: A Systematic Review and Meta-Analysis. *Frontiers in Digital Health*. Recuperado en agosto de 2021 de https://doi.org/10.3389/fdgth.2020.602093

De Hert, P. , & Lazcoz, G. (2022). When GDPR-Principles Blind Each Other: Accountability, Not Transparency, at the Heart of Algorithmic Governance.

European Data Protection Law Review. Volume 8, Issue 1 (2022) pp. 31 – 40 Recuperado en agosto de 2021 de https://doi.org/10.21552/edpl/2022/1/7

De Hert, P., & Papakonstantinou, V. (2020). Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer law & Security Review, 40*. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2020.105496

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., y Sánchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, 193-203. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2017.10.003

De Montalvo Jääskeläinen, F. (2019). *Menores de edad y consentimiento informado*. Tirant lo Blanch.

Del Conde Ugarte, A., y Martínez Rojas, E. (2013). Sujetos que intervienen en la relación jurídica que se genera derivado del tratamiento de datos personales. En Ornelas Núñez, L. y Piñar Mañas, J. L., (coords.), *La protección de datos personales en México* (p. 143-180). Tirant lo Blanch.

Delgado, J. (2004). Ética counnicativa y bioética. *Aldaba, 32*, 279-295. Recuperado en agosto de 2021 de https://doi.org/10.5944/aldaba.32.2004.20488

Deng, Z. (2021). Preliminary study on the right to data portability. *Journal of legal studies and research*. Vol. 7, Isssue 4 – ISSN 24552437

Díaz López de Falcó, R. M., y Figueroa Bello, A. (2020). *El ombudsman de la salud en México*. Universidad Nacional Autónoma de México.

Díaz Orueta, G. (2004). *Seguridad en las comunicaciones y en la información*. UNED.

Diéz Rodríguez, J. (2012). El derecho del paciente a conocer y decidir: ¿quién decide? En Marcos del Cano, A. (coord.), *Bioética y derechos humanos* (p. 269-318). UNED.

Diccionario de la Real Academia Española.

Dutta, S. & Lanvin, B. (eds.) (2022). *The Network Readiness Index 2022*. Portulans Institute.

Edenberg, E., & Jones, M. L. (2019). Analyzing the legal roots and moral core of digital consent. *New Media & Society, 21*(8), 1804-1823. Recuperado en agosto de 2021 de https://doi.org/10.1177/1461444819831321

Elfering, S. (2019). *Unlocking the Right to Data Portability. An analisis of the Interface with the Sui Generis Database Right.* Nomos. The Max Planck Society. Universität Augsburg University. The George Washington University. Technisque Universitat München.

Emaldi Cirión, A. (2021). Protección de datos personales en el ámbito sanitario y de investigación biomédica: una visión europea. *Actualidad Jurídica Iberoamericana*, 718-747. Recuperado en octubre de 2022 https://idibe.org/wp-content/uploads/2021/03/20._Aitziber_Emaldi_pp._718-747.pdf

Engels, F. (2006). *El origen de la familia, la propiedad privada y el Estado*. Editores Mexicanos Unidos.

Engels, B. (11 de junio de 2016). Data portability among online platforms. *Internet Policy Review, 5*(2). Recuperado en agosto de 2021 de https://doi.org/10.14763/2016.2.408

Ermakova, T., Fabian, B., Kelkel, S., Wolff, T., & Zarnekow, R. (2015). Antecedents of Health Information Privacy Concerns. *Procedia Computer Science, 63*, 376-383. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.procs.2015.08.356

Fajardo Dolci, G. (2011). La protección de los datos personales en el sector salud. En Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (coord.), *Retos de la protección de datos personales en el sector público* (p. 211-316). Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Fernández Domínguez, J. J. (2021). El derecho a la protección de datos personales: configuración y relación con otros derechos de la persona. *Revista del Ministerio de Trabajo y Economía Social*, 65-95.

Fernández, M. (2015). La protección del paciente frente a los deberes de información y secreto profesional médico. *Prolegómenos. Derechos y Valores*, 153-168.

Ferrajoli, L. (2004). *Epistemología jurídica y garantismo*. Fontamara.

Ferrajoli, L. (2013). *Principia iuris. Teoría del derecho y de la democracia* (Vol. 1-3). Trotta.

Flaumenhaft, Y., & Ben-Assuli, O. (2018). Personal health records, global policy and regulation review. *Health Policy, 122*(8), 815-826. Recuperado en agosto de 2021 dehttps://doi.org/10.1016/j.healthpol.2018.05.002

Flores Ávalos, E. L. (2017). Asentimiento informado de menores e incapaces. En Martínez Bullé Goyri, V. M., *Consentimiento informado. Fundamentos y problemas de su aplicación práctica* (p. 97-118). Universidad Nacional Autónoma de México.

Florez Ramos, E., & Blind, K. (2020). Data portability effects on data-driven innovation of online platforms: Analyzing Spotify. *Telecommunications Policy, 44*(9). Recuperado en agosto de 2021 de https://doi.org/10.1016/j.telpol.2020.102026

Frenk, J. y Gómez, O. (2015). *El sistema de salud en México (Colección Para Entender)*. Nostra Ediciones.

Fundación Telefónica Movistar & Taurus (2021). *Sociedad Digital en Latinoamérica 2020-2021*. Penguin Random House, Grupo Editorial.

Fundación Telefónica Movistar & Taurus (2023). *Sociedad Digital en España 2023*. Penguin Random House, Grupo Editorial.

Galán Cortés, J. C., & Roda García, L. (1997). Las historias clínicas y su incorporación a los expedientes judiciales. *Actualidad del Derecho Sanitario*(33), 599-606.

Galán, J. C. (1999). La responsabilidad médica y el consentimiento informado. *Revista Médica del Uruguay*, 5-12. Recuperado en febrero de 2019 de http://www.smu.org.uy/publicaciones/rmu/1999v1/art2.htm

Galán Cortés, J. C. (2020). *Responsabilidad civil médica*. Thomson Reuters.

García Mexía, P. (2020). Derecho al olvido. En Pendás B., (editor), *Enciclopedia de las Ciencias Morales y Políticas para el Siglo XXI. Ciencias Políticas y Jurídicas*, (p. 962-964). Real Academia de Ciencias Morales y Políticas. Boletín Oficial del Estado.

García-Huidobro, J. (2017). Derecho y derechos humanos. Introducción a un problema. En Saldaña Serrano, J. (coord.), *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (p. 107-118). Universidad Nacional Autónoma de México.

Geiregat, S. (2022). Copyright Meets Consumer Data Portability Rights: Inevitable Friction between IP and the Remedies in the Digital Content Directive. *GRUR International*. 71(6), 495-515. Recuperado en febrero de 2023 https://doi.org/10.1093/grurint/ikac042

Gert, B., Culver, C., & Clouser, K. (2006). *Bioethics: a systematic approach*. Oxford University Press.

Gianella Malca, G. (2011). El sentido y la importancia del secreto profesional desde la medicina. En Gamarra Herrera, R., Uceda Pérez, R., y Gianella Malca, G. (coords.), *Secreto profesional: Análisis y perspectiva desde la medicina, el periodismo y el derecho*, (p. 69-99). Promsex.

Gil González, E., & De Hert, P. (2019). Understanding the legal provisions that allow processing and profiling of personal data - an analysis of GDPR provisions and principles. *ERA Forum*(19), 597-621. Recuperado en agosto de 2021 de https://doi.org/10.1007/s12027-018-0546-z

Gill, D. & Metzger, J. (2022). Data Access through Data Portability – Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars. *European Data Protection*

Law, 3/2022. Recuperado en febrero de 2023 *https://ssrn.com/abstract=4107677*

Gille, F., Jobin, A., & Ienca, M. (2020). What we talk about when we talk about trust: Theory of trust for AI in healthcare. *Intelligence-Based Medicine, 1-2*, 100001. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.ibmed.2020.100001

Gkotsopolou, O., Charalambous, E., Limniotis, K., Quinn, P., Kavallieros, D., Sargsyan, G., Shiaeles, S., Kolokotronis, N. (2019). Data Protection by Design for cybersecurity systems in a Smart Home environment. *IEEE Conference on Network Softwarization (NetSoft)*, 101-109. Recuperado en agosto de 2021 de https://doi.org/10.1109/NETSOFT.2019.8806694

Gómez Robledo Verduzco, A. (julio-septiembre de 2006). La propiedad del expediente clínico. *Revista CONAMED, 11*(7), 11-12.

Gracia, D. (1998). *Bioética clínica*. El Búho.

Guastini, R. (2001). *Estudios de teoría constitucional*. Fontamara, Universidad Nacional Autónoma de México.

Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the Gap Between AI and Explainability in the GDPR: Towards Trustworthiness-by-Design in Automated Decision-Making. *IEEE Computational Intelligence Magazine, 17*(1), 72-85. Recuperado en agosto de 2021 de https://doi.org/10.1109/MCI.2021.3129960

Hamui Sutton, L., Paulo Maya, A., & Hernández Torres, I. (2018). *La comunicación dialógica como competencia médica esencial*. UNAM; Manual Moderno.

Heredero Higueras, M. (1983). La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población. *Documentación administrativa*(198), 139-159. Recuperado en abril de 2019 de https://dialnet.unirioja.es/servlet/articulo?codigo=220507&orden=1&info=link

Hernandez, R., *et al* (2006). *Metodología de la investigación*. McGraw Hill.

Hernández Corchete, J. A. (2018). Expectativas de privacidad, tutela de la intimidad y protección de datos. En De la Quadra, S. T., y Piñar Mañas, J. L., (coords.), *Sociedad digital y derecho* (p. 279-300). Ministerio de Industria, Comercio y Turismo, Red. es y Boletín Oficial del Estado.

Herrero, M. (2017). Los derechos humanos en la lucha política. En Saldaña Serrano, J. (coord.), *Problemas actuales sobre derechos humanos. Una propuesta filosófica* (p. 119-132). Universidad Nacional Autónoma de México.

Hesse, M. & Teubner, T. (2020). Reputation potability – quo vadis? *Electronic Markets* 30:331-349. Recuperado en febrero de 2023 https://doi.org/10.1007/s12525-019-00367-6

Hipócrates. (1983). *Tratados Hipocráticos*. Madrid: Gredos.

Hoyos Castañeda, I. M. (2017). Los derechos humanos en una época de crisis. En Saldaña Serrano, J., *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (p. 133-154). Universidad Nacional Autónoma de México.

Ienca, M. (2021). Neuroderechos: ¿Por qué debemos actuar antes de que sea demasiado tarde? *Anuario Internacional CIDOB*, 42-43.

Ishii, K. (2018). Discussions on the Right to Data Portability from Legal Perspectives. In: Kreps, D., Ess, C., Leenen, L., Kimppa, K. (eds) *This Changes Everything – ICT and Climate Change: What Can We Do?*. HCC13 2018. IFIP Advances in Information and Communication Technology, vol 537. Springer, Cham. Recuperado en febrero de 2023 de https://doi.org/10.1007/978-3-319-99605-9_26

Indarte, S. (2012). Interoperabilidad. En Carnicero, J., y Fernández, A., (coords.), *Manual de salud electrónica para directivos de servicios y sistemas de salud* (p. 317-330). Organización de las Naciones Unidas, CEPAL, Sociedad Española de Informática de la Salud, Alianza para la sociedad de la información en América Latina y el Caribe.

Indarte, S., y Pazos Gutiérrez, P. (2011). *Estándares e interoperabilidad en salud electrónica: requisitos para una gestión sanitaria efectiva y eficiente.* Comisión Económica para América Latina y el Caribe.

Izquierdo Blanco, P. (2019). Respecto de la historia clínica como objeto de prueba: ¿puede solicitarse como medio de pruba el acceso a las notas reservadas del médico y demás profesionales de la salud? *Revista jurídica sobre consumidores y usuarios* (4), 43-52.

Jasmontaite, L., & De Hert, P. (2015). The EU, children undeer 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law, 5*(1), 20-33. Recuperado en agosto de 2021 de https://doi.org/10.1093/idpl/ipu029

Kathuria, V. & Lai, Jessica C. (2018). User review portability: Why and how? *Computer Law & Security Review* 34, 1291-1299.

Karin, G., McLoughlin, I., Dalley, A., Wilson, R., & Yu, P. (2016). National electronic health record systems as `wicked projects': The Australian experience. *Information Polity, 21*(4), 367-381. Recuperado en agosto de 2021 de https://doi.org/10.3233/IP-160389

Kelsen, H. (1991). *¿Qué es la teoría pura del derecho?* (Trad. E. G. Valdez) Fontamara.

Kelsen, H. (2001). *Introducción a la teoría pura del derecho.* Instituto de investigaciones jurídicas de la UNAM; Asociación peruana de derecho constitucional.

Kiseleva, A., & De Hert, P. (2021). Creating a European Health Data Space: Obstacles in Four Key Legal Areas. *European Pharmaceutical Law Review, 5*(1), 21-36. Recuperado en agosto de 2021 de https://doi.org/10.21552/eplr/2021/1/5

Kive, M., Grasis, J. (2020). Problems of application of the right to data portability. *Acta Prosperatis*. doi 10.37804/1691-6077-2020-11-116-127

Kolkowska, E., y Kristofferson, A. (2016). Privacy by Design Principles in Design of New Generation Cognitive. En Hoepman, J.-H., Katzenbeisser, S., (eds), *ICT Systems Security and Privacy Protection* (p. 384-397). Springer.

Krämer, J., Senellart, P., & de Street, A. (2020). *Making Data Portability More Effective for the Digital Economy. Economic Implications and Regulatory Challenges*. Centre of regulation in Europe.

Krämer, J., & Stüdlein, N. (2019). Data portability, data disclosure and data-induced switching costs: Some unintended consequences of the General Data Protection Regulation. *Economics Letters, 181*, 99-103. Recuperado en febrero de 2023 de https://doi.org/10.1016/j.econlet.2019.05.015

Kuebler-Wachendorff, S., Luzsa, R., Kranz, J., Mager, S., Syrmoudis, E., Mayr, S., & Grossklags, J. (2021). The Right to Data Portability: conception, status quo, and future directions. *Informatik Spektrum, 44*, 264-272. Recuperado en febrero de 2023 de https://doi.org/10.1007/s00287-021-01372-w

Kurczyn Villalobos, P. (enero-abril de 2019). Contenido e importancia del expediente clínico. Acceso y confidencialidad. *Revista de la Facultad de Derecho de México, LXIX*(273), 893-915.

Lara, J., Pincheira, C., y Vera, F. (2014). *La privacidad en el sistema legal chileno*. ONG Derechos Digitales.

Lenard, Thomas M. (2020). *If Data Potability is the Solutions, What´s the Problem?* Technology Policy Institute.

Linares, J. (2018). El consentimiento informado como regla básica de la bioética. En Ruiz de Chávez, M. (coord.), *Bioética y derechos humanos. XXV años de reflexiones* (p. 153-164). Fontamara.

López Ayllón, S. (2009). *El acceso a la información como un derecho fundamental: la reforma al artículo 6° de la Constitución mexicana*. Instituto Federal de Acceso a la Información.

López Mesa, *et. al*. (2007). *Tratado de responsabilidad médica: responsabilidad civil, penal y hospitalaria*. Legis Argentina.

López Mesa, M. (2007). Teoría general de la responsabilidad civil médica en el derecho argentino y comparado. En López Mesa, M., (coord.), *Tratado de responsabilidad Medica: responsabilidad civil, penal y hospitalaria* (p. 1-387). Legis, Ubijus.

López Ruiz, M. (2022). *Redacción Legislativa.* Senado de la República. Recuperado en febrero de 2023 de https://archivos.juridicas.unam.mx/www/bjv/libros/6/2926/1.pdf

Lynskey, O. (2020). Article 20 Right to data portability. Kuner, C., Bygrave, L. A., & Docksey, C. (cords.), *The EU General Data Protection Regulation (GDPR). A Commentary*. (p. 497-507). Oxford University Press.

Maihofer, W. (2008). *Estudio de derecho y dignidad humana*. IBdeF.

Malgieri, G. (2020). Data protection and research: A vital challenge in the era of COVID-19 pandemic. *Computer Law & Security Review, 37*, 105431. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2020.105431

Malgieri, G. (2021). In/acceptable marketing and consumers' privacy expectations: four tests from EU data protection law. *Journal of Consumer Marketing*. Recuperado en agosto de 2021 de https://doi.org/10.1108/JCM-03-2021-4571

Malgieri, G., y Comandé, G. (2017). Sensitive-by-distance: quasi-health data in the algorithmic era. *Information & Communications Technology Law, 26*(3), 229-249. Recuperado en agosto de 2021 de https://doi.org/10.1080/13600834.2017.1335468

Malgieri, G., y Custers, B. (2018). Pricing privacy - the right to know the value of your personal data. *Computer Law & Security Review, 34*(2), 289-303. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2017.08.006

Malgieri, G., y Niklas, J. (2020). Vulnerable data subjects. *Computer Law & Security Review, 37*, 105415. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2020.105415

Mantovani, E., y Quinn, P. (2013). mHealth and data protection – the letter and the spirit of consent legal requirements. *International Review of Law, Computers*

& Tecnology, 28(2), 222-236. Recuperado en agosto de 2021 de https://doi.org/10.1080/13600869.2013.801581

Maqueo, M. (2018). Capítulo I. Del objeto de la ley (comentario). En Maqueo, M. (coord.), *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de 26 de enero de 2017, comentada* (p. 33-52). Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

Marco Cuenca, G., y Salvador Oliván, J. (2017). Representación del conocimiento en historia clínica electrónica: el caso de la Historia Clínica Digital del Sistema Nacional de Salud de España. *Scire*, 25-38.

Markopoulou, D., y Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer & Law Security Review, 41*, 105502. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2020.105502

Marqués Fernández, F. (2003). El Sistema Nacional de Salud después de las transferencias sanitarias. En *Revista de Administración Sanitaria Siglo XXI*. Vol. 1, núm. 4, p.p. 543-554., consultado en septiembre de 2023 https://www.elsevier.es/es-revista-revista-administracion-sanitaria-siglo-xxi-261-articulo-el-sistema-nacional-salud-despues-13055234

Martínez Bullé Goyri, V. M. (2017). Elementos esenciales del consentimiento informado. En Martínez Bullé Goyri, V. M. (coord.), *Consentimiento informado. Fundamentos y problemas de su aplicación práctica* (p. 23-50). Universidad Nacional Autónoma de México.

Martínez Calcerrada, L. (1998). <<Lex artis ad hoc>> y la responsabilidad médico profesional. *Anales de la Real Academia de Doctores*, 155-166. Recuperado en abril de 2019 de https://www.radoctores.es/doc/1v2n1-martinez%20calcerrada-lexartis.pdf

Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas. *Revista de Internet, Derecho y Política*. Recuperado en agosto de 2021 de https://raco.cat/index.php/IDP/article/view/82905/107891

Massini Correas, C. (1994). *Filosofía del derecho*. Abeledo-Perrot.

Massini Correas, C. I. (2017). El derecho a la vida en la sistemática de los derechos humanos. En Saldaña Serrano, J. (coord.), *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (p. 153-179). Universidad Nacional Autónoma de México.

Medina Arellano, M., (2016). *Decisiones relevantes de la Suprema Corte de Justicia de la Nación, núm 84. Derecho a la salud*. Suprema Corte de Justicia de la Nación. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.

Micheli, J., Valle, J. (2018). La brecha digital y la importancia de las tecnologías de la información y la comunicación en las economías regionales de México. *Realidad, datos y espacio. Revista Internacional de Estadística y Geografía.* Vol. 9, Núm. 2. pp. 38-53. Recuperado en febrero de 2023 http://internet.contenidos.inegi.org.mx/contenidos/sitios/rdebeta/rde_26/RDE25_art04.pdf

Moctezuma Barragán, G. (2000). *Derechos de los usuarios de los servicios de salud. Cámara de Diputados.* Universidad Nacional Autónoma de México.

Montes de Oca Arboleya, R. (2016). Un modelo jurídico para la medicina preventiva (primaria). En Pérez Tamayo, R., Cossío Díaz, J. R., (coord.), *Modelos médicos y modelos jurídicos* (pp. 117-140). Tirant lo Blanch.

Moro, T. (2016). *Utopía*. Grupo editorial Tomo.

Muñoz Conde, F. (1996). Falsedad documental y secreto profesional en el ámbito sanitario. *DS: Derecho y salud, 4*(1), 147-155.

Murillo de la Cueva, P. (1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos (Nueva Época)* (104), 35-60. Recuperado en octubre de 2022 https://www.cepc.gob.es/sites/default/files/2021-12/17224repne104037.pdf

Murillo de la Cueva, P. (2007). Perspectivas del derecho a la autodeterminación informativa. *Revista de Internet, Derecho y Política*, 18-32. Recuperado en octubre de 2022 de https://raco.cat/index.php/IDP/article/view/82903/107889

Nakashima, M. (2022). Comparison of legal Systems for Data Portability in the EU, the US and Japan and the Direction of Legislation in Japan. *Srpinger Nature Switzerland*. 656, 159-169. Recuperado en febrero de 2023 de https://doi.org.10.1007/978-3-031-15688-5_14

Nanni, M., Andrienko, G., Barabási, A.-L., Boldrini, C., Bonchi, F., Cattuto, C., Chiaromonte, F., Comandé., Conti, M., Coté, M., Dignum. F., Dignum, V., Domingo-Ferrer, J., Ferragina, P., Giannotti, F., Guidotti, R., Helbing, D., Kaski, K., Kertesz, J., … Vespignani, A. (2021). Give more data, awareness and control to individual citizens, and they will help COVID-19 containment. *Ethics and Information Technology, 23* (1), 1-6. Recuperado en febrero de 2023 de https://doi.org/10.1007/s10676-020-09572-w

Office for Civil Rights (2003). *Summary of the HIPAA Privacy Rule.* United States Department of Health and Human Services. Recuperado en febrero de 2023.

ONU (2022). *United Nations E-gobernment durvey 2022- The future of Digital Government*. Department of Economic and Social Affairs, United Nations. Recuperado en febrero de 2023 de https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf

Ornelas Núñez, L., & Piñar Mañas, J. (2013). Los principios de la protección de datos personales. En Ornelas Núñez, L. y Piñar Mañas, J. L., (coord.), *La protección de datos personales en México* (p. 39-96). Tirant lo Blanch.

Osuna Carrillo de Albornoz, E. (2013). Relación sanitaria e información. En Salcedo Hernández, J. R., *Derecho y Salud, Estudios de Bioderecho (Comentarios a la Ley 3/2009, de Derechos y Deberes de los Usuarios del Sistema Sanitario de la Región de Murcia)*, (p. 83-103). Tirant lo Blanch.

Oxford Advanced Learner's Dictionaries.

Pacheco, A. (2011). *Legitimación del Acto Biomédico*. México: Alfil.

Pardo López, M. M. (2007). Intimidad personal, protección de datos sanitarios e intromisiones legítimas: una proyección hipotética de la Doctrina Tarasoff sobre el ordenamiento jurídico español. *Anales de Derecho* (25), 181-214.

Parejo Guzmán, M. J. (2018). *Consentimiento informado y autonomía del paciente: su aplicación en el ocaso de la vida en la España y Europa del siglo XXI.* Universidad Nacional Autónoma de México.

Parziale, A., Comandé, G., y Amram, D. (2021). How Covid-19 unveils the blurred borderlines between research and clinical practice monitoring:the use case of data protection and consent. *BioLaw Journal - Rivista di BioDiritto, Special Issue* (2), 139-155. Recuperado en agosto de 2021 de https://doi.org/10.15168/2284-4503-852

Perces-Barba Martínez, G. (1994). La universalidad de los derechos humanos. *Doxa*, 613-633. Recuperado en agosto de 2021 de https://doi.org/10.14198/DOXA1994.15-16.30

Peces-Barba Martínez, G., Fernández, E., & De Asís, R. (2000). *Curso de teoría del derecho*. Marcial Pons.

Pérez Luño, A. (2012). Bioética e intimidad, la tutela de los datos personales biomédicos. En Marcos del Cano A. (coord.), *Bioética y derechos humanos*, (p. 77-104). UNED.

Pérez Miranda, R. J. (2020). *Exigibilidad del derecho de acceso a la salud y licencias obligatorias en materia de medicamentos*. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.

Peschard Mariscal, J. (2013). El derecho fundamental a la protección de datos personales en México. En Ornelas Núñez, L., y Piñar Mañas, J. L., (coord..) *La protección de datos personales en México* (p. 19-38). Tirant lo Blanch.

Pinto Bustamante, B. J., y Gulfo Díaz, R. (2013). Asentimiento y consentimiento informado en pediatría: aspectos bioéticos y jurídicos en el contexto colombiano. *Revista Colombiana de Bioétoca*, 144-165.

Piñar Mañas, J. L. (2018). Sociedad digital y derecho. En De la Quadra, S. T. y Piñar Mañas, J. L., (coords.) *Sociedad digital y derecho*, (p. 95-112). Ministerio de Industria, Comercio y Turismo, Red. es y Boletín Oficial del Estado.

Porfirio Cervantes, Á. (julio-septiembre de 2006). Registro de la conducta médica en el expediente clínico. *Revista CONAMED, 7*, 35-36.

Price, M., Bellwood, P., Kitson, N., Davies, I., Weber, J., & Lau, F. (2015). Conditions potentially sensitive to a Personal Health Record (PHR) intervention, a systematic review. *BMC Medical Informatics and Decision Making*, 15-32. Recuperado en febrero de 2023 https://doi.org/10.1186/s12911-015-0159-1

Puccinelli, O. (2017). El derecho a la portabilidad de los datos personales. Orígenes, sentido y límites. *Pensamiento constitucional, 22*. Recuperado en abril de 2019 de https://2019.vlex.com/#vid/derecho-portabilidad-datos-personales-736214789

Quinn, P. (2017). The anonymisation of Research Data - A Pyric Victory for Privacy that Should Not Be Pushed Too Hard by the EU Data Protection Framework? *European Journal of Health Law, 24* (4), 347-367. Recuperado en agosto de 2021 de https://doi.org/10.1163/15718093-12341416

Quinn, P. (2018). Is the GDPR and Its Right to Data Portability a Major Enabler of Citizen Science? *Global Jurist, 18* (2), 20180021. https://doi.org/10.1515/gj-2018-0021

Quinn, P. (2021). Research under the GDPR – a level playing field for public and private sector research? *Life, Sciences, Society and Policy, 17* (4). Recuperado en agosto de 2021 de https://doi.org/10.1186/s40504-021-00111-z

Quinn, P., y De Hert, P. (2012). The European Patients' Rights Directive: A clarification and codification of individual rights relating to cross border healthcare and novel initiatives aimed at improving pan-European healthcare co-operation. *Medical Law International, 12* (1), 28-69. Recuperado en agosto de 2021 de https://doi.org/10.1177/0968533212439573

Quinn, P., y Malgieri, G. (2021). The difficulty of defining sensitive data - the concept of sensitive data in the EU Data Protection Framework. *German Law Journal*, 1583-1612. Recuperado en agosto de 2021 de https://doi.org/10.1017/glj.2021.79

Quinn, P., y Quinn, L. (2018). Big genetic data and its big data protection challenges. *Computer Law & Security Review, 34* (5), 1000-1018. Recuperado en agosto de 2021 de https://doi.org/10.1016/j.clsr.2018.05.028

Rawls, J. (1995). *Teoría de la justicia*. Fondo de Cultura Económica.

Rebollo Delgado, L. (1998). Derechos de la personalidad y datos personales. *Revista de Derecho Político* (44), 143-206. Recuperado en octubre de 2022 de https://revistas.uned.es/index.php/derechopolitico/article/view/8725/8319

Rebollo Delgado, L. (2000). El secreto de las comunicaciones: problemas actuales. *Revista de Derecho Político*, 351-382. Recuperado en octubre de 2022 de http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:Derechopolitico-2000-48-49-129603AD&dsID=PDF

Rebollo Delgado, L. (2003). Veinticinco años de relación entre la informática y los derechos al honor y a la intimidad personal y familiar. *Revista de Derecho Político* (58-59), 215-239. Recuperado en octubre de 2022 de http://e-spacio.uned.es/fez/eserv.php?pid=bibliuned:Derechopolitico-2003-2004-58-59-6A1E5F72&dsID=pdf

Rebollo Delgado, L. (2008). *Biomedicina y protección de datos*. Dykinson, S.L.

Rebollo Delgado, L. (2009). *Vida privada y protección de datos en la Unión Europea*. Dykinson, S.L.

Rebollo Delgado, L. (2009). La imagen como dato. *Anuario de la Facultad de Derecho de la Universidad de Alcalá* (2), 177-201.

Rebollo Delgado, L. (2018). La protección de datos del menor en la investigación biomédica. En Gómez, Y. (coord.), *Menores e investigación biomédica* (p. 231-260). Dykinson, S.L.

Recio Gayo, M. (2013). La transferencia nacional e internacional de datos personales. En Ornelas Núñez, L., y Piñar Mañas, J. L. (coords.), *La protección de datos personales en México* (p. 207-236). Tirant lo Blanch.

Recio Gayo, M., y Vega Gómez, J. C. (2013). La protección de datos en el ámbito de las telecomunicaciones e Internet. En Ornelas Núñez, L., y Piñar Mañas, J. L. (coord..), *La protección de datos personales en México* (p. 395-422). Tirant lo Blanch.

Remolina Angarita, N. (2013). Los derechos de acceso, rectificación, cancelación y oposición en la ley de datos personales y su reglamento. En Ornelas Núñez, L., y Piñar Mañas, J. L. (coords.), *La protección de datos personales en México* (p. 181-206). Tirant lo Blanch.

Reyes Krafft, A. (2013). La legislación mexicana en materia de protección de datos personales; autorregulación y sellos de confianza. En Ornelas Núñez, L., y Piñar Mañas, J. L. (coords.), *La protección de datos personales en México* (p. 363-394). Tirant lo Blanch.

Rodotà, S. (2014). *El derecho a tener derechos*. Madrid: Trotta.

Rodotà, S. (2018). Del ser humano al posthumano. En De la Quadra, T., y Piñar Mañas, J. L., (coords.), *Sociedad digital y derecho* (p. 87-94). Ministerio de Industria, Comercio y Turismo, Red. es y Boletín Oficial del Estado.

Rodríguez Gaona, R. (2013). *Lecciones sobre derechos fundamentales*. Universidad Autónoma del Estado de Hidalgo.

Romeo Casabona, C. M. (1981). *El Médico y el derecho penal (Vol. I. La actividad curativa (licitud y responsabilidad penal)*. Bosch, Casa Editorial.

Romeo Casabona, C., y Castellano Arroyo, M. (1993). La intimidad del paciente desde la perspectiva del secreto médico y el acceso a la historia clínica. *Derecho Sanitario, 1* (1), 4-19.

Ruiz Massieu, J. F. (1985). El derecho a la protección de la salud y la responsabilidad del Estado. *Salud Pública*, 3-9.

Sánchez Caro, J., y Abellán, F. (2006). *Derechos del médico en la relación clínica*. Comares.

Santos Ballesteros, J. (2007). La responsabilidad civil médica en el derecho colombiano. En López Mesa, M. (coord.), *Tratado de responsabilidad médica. Responsabilidad civil, penal y hospitalaria*, (p. 457-535). Legis, Ubijus.

Sardinero García, C. (2016). *Responsabilidad administrativa, civil y penal por falta de información en el ámbito clínico. Criterios indemnizatorios*. Tirant lo blanch.

Sass, H. (1990). La bioética: fundamentos filosóficos y aplicación. *Boletín de la Oficina Sanitaria Panamericana*, 391-398. Recuperado en abril de 2019 de https://tinyurl.com/y6lnxy4e

Schaub, A., Bazin, R., Hasan, O., y Brunie, L. (2016). A Trustless Privacy-Preserving Reputation System. En Hoepman, J.-H. y Katzenbeisser, S., (eds), *ICT Systems Security and Privacy Protection* (p. 398-412). Springer.

Scheibner, J., Ienca, M., y Vayena, E. (2021). Whose health record? A comparison of patient rights under national electronic health record (NEHR) regulations in Europe and Asia-Pacific jurisdictions. *Singapore Journal of Legal Studies, 2021*, 56.75.

Scheibner, J., Ienca, M., Kechagia, S., Troncoso-Pastoriza, J. R., Raisaro, J. L., Hubaux, J.-P., Fellay, J. y Vayena, E. (2020). Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences, 7* (1), lsaa010. Recuperado en agosto de 2021 de https://doi.org/10.1093/jlb/lsaa010

Scheibner, J., Raisaro, J. L., Troncoso-Pastoriza, J., Ienca, M., Fellay, J., Vayena, E., y Hubaux, J.-P. (2021). Revolutionizing Medical Data Sharing Using Advanced Privacy-Enhancing Technologies: Technical, Legal, and Ethical Synthesis. *Journal of Medical Internet Research, 23* (2), e25120. Recuperado en agosto de 2021 de https://doi.org/10.2196/25120

Scheibner, J., Sleigh, J., Ienca, M., y Vayena, E. (2021). Benefits, Challenges and Contributors to Success for National eHealth Systems Implementation: A Scoping Review. *ournal of the American Medical Informatics Association, 28*

(9), 2039-2049. Recuperado en agosto de 2021 de https://doi.org/10.1093/jamia/ocab096

Scheibner, J., Sleigh, J., Ienca, M., y Vayena, E. (2021). Benefits, challenges, and contributors to success for national eHealth systems implementation: a scooping review. *Journal of the american Medical Informatics Association, 28* (9), 2039-2049. Recuperado en agosto de 2021 de https://doi.org/10.1093/jamia/ocab096

Schwabe, J. (2009). *Jurisprudencia del tribunal constitucional federal alemán*. Konrad-Adenauer-Stiftung Programa Estado de Derecho para Latinoamérica.

Serrano, S., & Vázquez, D. (2011). *Programa de capacitación y formación profesional en derechos humanos (Vol. Curso IV. Fundamentos Teóricos de los derechos humanos)*. Comisión de Derechos Humanos del Distrito Federal.

Smith, H. W. (1946). Legal privilege on therapeutic grounds, to withhold specific diagnosis from patient sick with serious or fatal illness. *Tennesse Law Review, 19* (3). Recuperado en agosto de 2021 de https://doi.org/10.7326/0003-4819-24-6-960

Solove, D. (2002). Conceptualizing Privacy. *California Law Review, 90*, 1087-1155.

Solove, D. (2008). *Understanding Privacy*. Harvard University Press.

Solove, D. J. (2008). "I´ve Got Nothing to Hide" and Other Misunderstandings of Privacy. *San Diego Law Review*, 745-772.

Solove, Daniel J. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security.* Yale University Press.

Somaini, L. (2018). The right to data portability and user control: ambitions and limitations. *Media Laws, Rivista di Diritto dei Media*, 3/2018 164-190.

Sotomayor, J. (2007). *El secreto profesional*. Porrúa.

Suprema Corte de Justicia de la Nación, (2004). *Donación de órganos. Inconstitucionalidad del artículo 333, fracción VI, de la Ley General de Salud.* Suprema Corte de Justicia de la Nación.

Suprema Corte de Justicia de la Nación, (2014). *Modelo social de discapacidad. Directrices para la interpretación del estado de interdicción en el Distrito Federal, México*. Suprema Corte de Justicia de la Nación.

Stenn, F. (2000). El caduceo y la vara de Esculapio. *Cuaderno de Historia, 87*. Recuperado en abril de 2019 de http://bvs.sld.cu/revistas/his/cua_87/cua0487.pdf

Swire, P., & Lagos, Y. (31 de mayo de 2013). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review. Ohio State Public Law Working Paper*. Recuperado en febrero de 2023 de http://dx.doi.org/10.2139/ssrn.2159157

Tapia Conyer, R., y Motta Murguía, M., (2005). El derecho a la protección de la salud pública. En Brena Sesma, I., (coord.), *Salud y derecho. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados* (p. 149-183). Universidad Nacional Autónoma de México.

Tenorio Cueto, G., y Rivero del Paso, M. (2012). Análisis crítico de la protección de datos en México. En Tenorio Cueto, G. (coord.), *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares.* (p. 51-69). Porrúa, Universidad Panamericana.

Torregrosa Vázquez, J. (2018). Privacidad e intercambio de información en el mundo digital. En De la Quadra, S. T., y Piñar Mañas, J. L., (coords.), *Sociedad digital y derecho* (p. 339-398). Ministerio de Industria, Comercio y Turismo, Red. es y Boletín Oficial del Estado.

Troncoso Reigada, A. (2003). La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional. *Cuadernos de Derecho Público* (19-20), 231-334.

Troncoso Reigada, A. (2006). La confidencialidad de la historia clínica. *Cuadernos de Derecho Público* (27).

Troncoso Reigada, A. (2007). Historia clínica y privacidad. *I+S: Revista de la Sociedad Española de Informática y Salud* (66), 14-20.

Troncoso Reigada, A. (2010). El principio de calidad de los datos. Título II. Principios de la protección de datos. Artículo 4. En Troncoso Reigada, A., (coord.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (p. 340-394). Aranzadi.

Troncoso Reigada, A. (2010). La comunicación de datos personales. Título II. Principios de la Protección de los Datos. Artículo 11. En Troncoso Reigada, A., (coord.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal* (p. 950-1006). Aranzadi.

Troncoso Reigada, A. (2013). La historia del derecho a la protección de datos personales. En Ansuátegui Roig, F., Rodríguez Uribes, J., Peces-Barba Martínez, G. y Fernández García, E., (coord.), *Historia de los derechos fundamentales (Vols. 4, Tomo 5)*, (p. 431-492). Cultura de la Paz y Grupos vulnerables.

Troncoso Reigada, A. (2015). El derecho al olvido digital de los médicos a la luz de la Sentencia del Tribunal Supremo, de 15 de octubre. *I+S: Revista de la Sociedad Española de Informática y Salud* (114), 67-68. Recuperado en octubre de 2022 de https://seis.es/revista-n-114/

Troncoso Reigada, A. (2016). Los límites al acceso a la información: la protección de datos personales. *Informática y Derecho* (1). Recuperado en octubre de 2022 de https://docs.wixstatic.com/ugd/fe8db5_2cd97adf3d4544039f87f7c206b450c3.pdf

Troncoso Reigada, A. (2017). La protección de datos personales como límite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 "Protección de datos personales". En Troncoso Reigada, A. (director), *Comentario a la ley de transparencia, acceso a la información pública y buen gobierno* (p. 958-1078). Civitas, Thomson Reuters.

Troncoso Reigada, A. (2018). Del principio de seguridad de los datos al derecho a la seguridad digital. *Economía industrial* (410), 127-151. Recuperado en

octubre de 2022 de https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/410/ANTONIO%20TRONCOSO%20REIGADA.pdf

Troncoso Reigada, A. (2018). Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley orgánica de protección de datos personales y garantía de los derechos digitales. *Revista de derecho y genoma humano. Genética, biotecnología y medicina avanzada*, 187-266.

Troncoso Reigada, A. (2019). La seguridad en el Reglamento General de Protección de Datos de la Unión Europea. *Actualidad administrativa*, 1.

Troncoso Reigada, A. (2020). Los tratamientos de datos personales para fines de salud pública y el derecho a la protección de datos personales en tiempos del COVID-19. En Rodríguez Ayuso, J. y Atienza Macías, E. (directores), *Retos jurídicos antes la crisis del COVID-19*, (p. 553-601). Dykinson.

Troncoso Reigada, A. (2021). Los principios relativos al tratamiento (Comentario al artículo 5 del 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 al artículo 4 Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales de 06 de diciembre de 2018). En Troncoso Reigada, A., (coord.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, (Vol. 1, pp. 847-907)*. Aranzadi.

Troncoso Reigada, A. (2021). El marco jurídico de la protección de datos personales: Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de 06 de diciembre de 2018, de 5 de diciembre. *Revista del Ministerio de Trabajo y Economía Social*, 23-64.

Turner, S., Galindo Quintero, J., Turner, S., Lis, J., & Tanczer, L. (2020). The exercisability of the right to data portability in the emerging Internet of Things (IoT) enviroment. *New Media & Society*, 1-21.

Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of Things. *Pers Ubiquit Comput.* 22:317-322. Recuperado en febrero de 2023 de https://doi.org/10.1007/s00779-017-1069-2

Ursic, H. (2018). Unfolding the Newborn Right to Data Portability: Four Gatewaus to Data Subject Control. *Scripted*, 42-69. Recuperado en agosto de 2021 de https://doi.org/10.2966/scrip.150118.42

Valadés, D. (2020). Consideraciones en torno al pensamiento jurídico contemporáneo. En Brena, I. (coord.), *Derecho y salud*, (p. IX-XIV). Universidad Nacional Autónoma de México.

Valadez Martínez, H. (2012). La protección de datos personales en posesión de particulares: una aproximación a la protección de los derechos humanos entre privados. En Tenorio Cueto, G., (coord.), *Los datos personales en México (perspectivas y retos de su manejo en posesión de los particulares)*, (p. 69-86). Porrúa, Universidad Panamericana.

Vanberg, A. (2018). The Right to Data Potability in the GDPR: What Lessons Can Be Learned from the EU Experience? *Journal of Internet Law* 21 (7) 13-14.

Vanberg, A., & Ünver, B. (2017). The right to data portability in the DGPR and EU competition law: odd couple or dynamic duo? *European Journal of Law and Technology*. Vol 8, no. 1 -22.

Van der Auwermeulen, B. (2017). How to attribute the right to data portability in Europe: A comparative analysis of legislations. *ScienceDirect, 33*, 57-72. Recuperado en agosto de 2021 de http://dx.doi.org/10.1016/j.clsr.2016.11.012

Véliz, C. (2020). *Privacy is power*. Penguin Random House UK.

Vera Vallejo, L. (2013). La protección de datos en el ámbito de la mercadotecnia. En Ornelas Núñez, L., y Piñar Mañas, J. L. (coords.), *La protección de datos personales en México* (p. 465-498). Tirant lo Blanch.

Velarde Queipo de Llano, C. (2017). La evolución del concepto de derechos humanos y sus modernas críticas. En Saldaña Serrano, J. (coord.), *Problemas actuales sobre derechos humanos. Una propuesta filosófica*. (p. 217-243). Universidad Nacional Autónoma de México.

Viesca T., (2017). Paternalismo médico y consentimiento informado. En Martínez Bullé Goyri, V. M. (coord.), *Consentimiento informado. Fundamentos y problemas de su aplicación práctica* (pp. 1-22). Universidad Nacional Autónoma de México.

Villaronga, E., Chokoshvili, D., Vallevik, V., Ienca, M., & Pierce, R. (2021). Implementing AI in healthcare: An ethical and legal analysis based on case studies. En D. Hallinan, R. Leenes, & P. De Hert, *Data Protection and Privacy. Data Protection and Artificial Intelligence* (pp. 187-216). Hart Publishing. Recuperado en agosto de 2021 de https://doi.org/10.5040/9781509941780.ch-007

Wang, Y., y Shah, A. (2017). *Supponting Data Portability in the Cloud Under the GDPR.* Carnegie Mellon University.

Warren, S., y Brandeis, L. (15 de diciembre de 1890). The right to privacy. *Harvard Law Review, 4* (5), 193-220.

Wynne Lam, W., y Liu, X. (2020). Does data portability facilitate entry? *International Journal of Industrial Organization, 69*, 102564. Recuperado en febrero de 2023 de https://doi.org/10.1016/j.ijindorg.2019.102564

Zanfir, G. (2012). The right to Data portability in the context of the EU data protection reform. *International Data Privacy Law*, 1-14. Recuperado en agosto de 2021 de https://doi.org/10.1093/idpl/ips009

Zomignani Barboza, J., y De Hert, P. (2021). Data Protection Impact Assessment: A Protection Tool for Migrants Using ICT Solutions. *Social Sciences, 10*(12),

466. Recuperado en febrero de 2023 de https://doi.org/10.3390/socsci10120466

Zuboff, S. (2019). *La era del capitalismo de la vigilancia*. Planeta.

Legislación y documentos legales

Actualización del Plan Estatal de Desarrollo Hidalgo 2016-2022: Visión Prospectiva para un estado Resiliente ante COVID-19.

Acuerdo CONAIP/SNT/ACUERDO/ORD01-15-/12/2017-06 que contiene las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales. [Sistema Nacional de Transparencia]. 23 de enero de 2018. Diario Oficial de la Federación.

Acuerdo mediante el cual se aprueban los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales [Sistema Nacional de Transparencia]. 12 de febrero de 2018. Diario Oficial de la Federación.

Acuerdo por el que se da a conocer el Programa de Conectividad en Sitios Públicos 2020-2021 [Secretaría de Comunicaciones y Transportes]. 16 de abril de 2021. Diario Oficial de la Federación.

Acuerdo por el que se delegan facultades para conocer, tramitar, evaluar y emitir la determinación correspondiente de las solicitudes de autorización de medidas compensatorias previstas en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, de 05 de julio de 2010, de 05 de julio de 2010 y su Reglamento en favor de los servidores públicos que se indican. 01 de enero de 2012. Diario Oficial de la Federación.

Banco de México (2018). Circular 03/2012 Disposiciones aplicables a las operaciones de las instituciones de crédito, las sociedades financieras de objeto múltiple reguladas que mantengan vínculos patrimoniales con instituciones 29 de octubre de 2018. Diario Oficial de la Federación.

Carta de los Derechos Fundamentales de la Unión Europea. 07 de diciembre de 2000.

Código internacional de ética médica. Asociación Médica Mundial. Octubre de 1983.

Código Internacional de Ética Médica. Asociación Médica Mundial. Septiembre de 1994.

Código Penal Federal. 12 de abril de 2019. Diario Oficial de la Federación.

Constitución Española. 29 de diciembre de 1978. Boletín Oficial del Estado.

Constitución Política de los Estados Unidos Mexicanos. 05 de febrero de 1917. Diario Oficial de la Federación.

Constitución Política del Estado de Hidalgo. 01 de octubre de 1920. Periódico Oficial del Estado.

Convención Americana sobre Derechos Humanos (Pacto de San José). 22 de noviembre de 1969.

Convención sobre los derechos del niño. 20 de noviembre de 1989.

Convenio del Consejo de Europa para la protección de los derechos humanos y la dignidad del ser humano respecto de las aplicaciones de la biología y la medicina (Convenio de Oviedo), de 04 de abril de 1997.

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo, Francia, el 28 de enero de 1981 del Consejo de Europa. 28 de enero de 1981.

Convenio para la protección de los derechos y las libertades fundamentales. 01 de junio de 2010.

Criterios Generales para la instrumentación de medidas compensatorias en el sector público del orden federal, estatal y municipal. 23 de enero de 2018. Diario Oficial de la Federación.

Criterios generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos. 18 de abril de 2012. Diario Oficial de la Federación.

Declaración de Ginebra. Asociación Médica Mundial. Septiembre de 1948.

Declaración de la Asociación Médica Mundial sobre la defensa del paciente. Abril de 2016.

Declaración de Lisboa sobre los derechos del paciente. Asociación Médica Mundial. Octubre de 1981, reafirmada en Oslo en abril de 2015.

Declaración Internacional de Datos Genéticos Humanos. UNESCO. 16 de octubre de 2003.

Declaración Universal de Derechos Humanos. 10 de diciembre de 1948.

Decreto de creación de la Comisión Nacional de Arbitraje Médico. 06 de marzo de 1996. Diario Oficial de la Federación.

Decreto n° 396/003. [Presidencia de la República Oriental del Uruguay]. Historia clínica electrónica única de cada persona. 30 de septiembre de 2003.

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. [Parlamento Europeo y Consejo Europeo]. 19 de julio de 2016.

Directiva 95/46/CE del Parlamento Europeo y del Consejo. [Parlamento Europeo y Consejo Europeo] de 24 de octubre de 1995.

Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado 1, letra b), del 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 en el contexto de la prestación de servicios en línea a los interesados. 08 de octubre de 2019. Comité Europeo de Protección de Datos.

Gobierno de México. (2019). *Plan Nacional de Desarrollo 2019-2014.* 12 de julio de 2019. Diario Oficial de la Federación.

Estatuto Orgánico de Servicios de Salud de Hidalgo. [Junta de Gobierno de los Servicios de Salud de Hidalgo]. 03 de agosto de 2020. Periódico Oficial del Estado de Hidalgo.

Gobierno de España (2021). *Plan Nacional de Competencias Digitales*. Recuperado en febrero de 2023 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_nacional_de_competencias_digitales.pdf

Instructivo Normativo para la asignación de la Clave Única de Registro de Población. Publicado en el Diario Oficial de la Federación el 18 de junio de 2018.

Ley 14/1986 de 25 de abril, General de Sanidad. Boletín Oficial del Estado.

Ley 14/2007, de 3 de julio, de Investigación biomédica. Boletín Oficial del Estado.

Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud llevada a cabo a través del Real Decreto-ley 7/2018, de 27 de julio. Boletín Oficial del Estado.

Ley 33/2011, de 4 de octubre, General de Salud Pública. 05 de octubre de 2011. Boletín Oficial del Estado.

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. 15 de noviembre de 2002. Boletín Oficial del Estado núm. 274.

Ley de Salud del Estado de Hidalgo. 30 de agosto de 2004. Periódico Oficial del Estado de Hidalgo.

Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo. 04 de mayo de 2016. Periódico Oficial del Estado de Hidalgo.

Ley Federal de Comunicaciones y Transportes. 20 de mayo de 2021. Diario Oficial de la Federación.

Ley Federal de Protección de Datos Personales en Posesión de Particulares. 05 de julio de 2010. Diario Oficial de la Federación.

Ley Federal de Protección al Consumidor el Registro Público de Consumidores. 24 de diciembre de 1992. Diario Oficial de la Federación.

Ley Federal de Telecomunicaciones y Radiodifusión. 14 de julio de 2014. Diario Oficial de la Federación.

Ley de Protección y Defensa al Usuario de Servicios Financieros. 09 de marzo de 2018. Diario Oficial de la Federación.

Ley de Protección de datos personales en posesión de sujetos obligados para el Estado de Hidalgo. 24 de julio de 2017. Periódico Oficial del Estado de Hidalgo.

Ley General de los Derechos de Niñas, Niños y Adolescentes. 04 de diciembre de 2014. Diario Oficial de la Federación.

Ley General de Mejora Regulatoria. 18 de mayo de 2018. Diario Oficial de la Federación.

Ley General de Población. 07 de enero de 1974. Diario Oficial de la Federación.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. Diario Oficial de la Federación.

Ley General de Salud. 07 de febrero de 1984. Diario Oficial de la Federación.

Ley General de Transparencia y Acceso a la Información Pública. 04 de mayo de 2015. Diario Oficial de la Federación.

Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes. 04 de diciembre de 2014. Diario Oficial de la Federación.

Ley para la transparencia y ordenamiento de los servicios financieros. 15 de junio de 2007. Diario Oficial de la Federación.

Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, de modificación parcial del Código Civil y de la Ley de Enjuiciamiento Civil. 15 de enero de 1996. Boletín Oficial del Estado.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales de 06 de diciembre de 2018. Boletín Oficial del Estado núm. 294.

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Boletín Oficial del Estado.

Ley Orgánica 14/1983, de 12 de diciembre, por la que se desarrolla el artículo 17.3 de la Constitución, en materia de asistencia letrada al detenido y al preso, y modificación de los artículos 520 y 527 de la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado.

Ley Orgánica de la Administración Pública para el Estado de Hidalgo. 04 de mayo de 2016. Periódico Oficial del Estado.

Lineamientos del aviso de privacidad [Secretaría de Economía]. 17 de enero de 2013. Diario Oficial de la Federación.

Lineamientos generales de protección de datos personales para el sector público. 19 de diciembre de 2017. Diario Oficial de la Federación.

Lineamientos para el uso de hiperenlaces o hipervínculos en una página de Internet del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para dar a conocer avisos de privacidad a través de medidas compensatorias. 18 de enero de 2016. Diario Oficial de la Federación.

Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. 12 de febrero de 2018. Diario Oficial de la Federación.

Manual del expediente clínico electrónico. [Dirección General de Información en Salud de la Secretaría de Salud]. 2011.

Marco de privacidad del foro de cooperación económica Asia Pacífico, de 2015.

Norma Oficial Mexicana NOM-004-SSA2-2012, del expediente clínico. 29 de junio de 2012. Diario Oficial de la Federación.

Norma Oficial Mexicana NOM-017-SSA2-2012, Para la vigilancia epidemiológica. 19 de febrero de 2013. Diario Oficial de la Federación.

Norma Oficial Mexicana NOM-024-SSA3-2012, Sistemas de información de registro electrónico para la salud. Intercambio de información en salud. 30 de noviembre de 2011. Diario Oficial de la Federación.

Norma Oficial Mexicana NOM-035-SSA3-2012, En materia de información en salud. 30 de noviembre de 2011. Diario Oficial de la Federación.

Oficina Nacional de Prospectiva y Estrategia del Gobierno de España (coord). (2021). *España* 2050: Fundamentos y propuestas para una Estrategia Nacional de Largo Plazo. Ministerio de la Presidencia. Recuperado en julio de 2023.

https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/200521-Estrategia_Espana_2050.pdf

Pacto Internacional de Derechos Civiles y Políticos. 23 de marzo de 1976.

Pacto Internacional de Derecho Económicos, Sociales y Culturales. 3 de enero de 1976.

Programa Especial de Ciencia, Tecnología e Innovación de Hidalgo 2016-2022.

Programa Sectorial de Salud 2016-2022 del Estado de Hidalgo.

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos). 25 de noviembre de 2020.

Protocolo adicional a la convención americana sobre derechos humanos en materia de derechos económicos, sociales y culturales "Protocolo de San Salvador". San Salvador, 1988.

Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hecho en Estrasburgo, Francia el 08 de noviembre de 2001.

Protocolo de enmienda del convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal hecho en Estrasburgo el 10 de octubre de 2018. [Consejo de Europa]. 29 de mayo de 2020.

Real Decreto 81/2014, de 7 de febrero, por el que se establecen normas para garantizar la asistencia sanitaria transfronteriza, y por el que se modifica el Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación. Boletín Oficial del Estado.

Real Decreto 1093/2010, de 3 de septiembre, por el que se aprueba el conjunto mínimo de datos de los informes clínicos en el Sistema Nacional de Salud. Boletín Oficial del Estado.

Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Boletín Oficial del Estado.

Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal. Boletín Oficial del Estado.

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. [Parlamento Europeo y Consejo de Europa]. 04 de mayo de 2016. Diario Oficial de la Unión Europea.

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión no. 1247/2002/CE. Diario Oficial de la Unión Europea. 23 de octubre de 2018.

Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea. Diario Oficial de la Unión Europea. 28 de noviembre de 2018.

Reglamento (UE) No 182/2011 del Parlamento Europeo y del Consejo de 16 de febrero de 2011 por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competen. 16 de febrero de 2011. Diario Oficial de la Unión Europea.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. 21 de diciembre de 2011. Diario Oficial de la Federación.

Reglamento de la Ley General de Salud en materia de investigación para la salud. 06 de enero de 1987. Diario Oficial de la Federación.

Reglamento de la Ley General de Salud en materia de prestación de servicios de atención médica. 14 de mayo de 1986. Diario Oficial de la Federación.

Reglamento de la Ley General de Salud en Materia de Protección Social en Salud. 05 de abril de 2004. Diario Oficial de la Federación.

Reglamento de la Ley General de Salud en materia de trasplantes. 26 de marzo de 2014. Diario Oficial de la Federación.

Reglamento de procedimientos para la atención de quejas médicas y gestión pericial de la Comisión Nacional de Arbitraje Médico. 25 de julio de 2006. Diario Oficial de la Federación.

Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos y por el que se modifica el reglamento (UE) 2018/1724 (Reglamento de gobernanza de datos). 04 de mayo de 2022. 2020/0340 (COD). Diario Oficial de la Unión Europea.

Reglamento Interior de la Secretaría de Salud. 27 de julio de 2017. Periódico Oficial del Estado de Hidalgo.

UNE-EN ISO 13606-1:2020. Informática sanitaria. Comunicación de la historia clínica electrónica. Parte 1: Modelo de referencia.

Secretaría de Salud. (2020). Programa Sectorial Derivado del Plan Nacional de Desarrollo 2019-2024. 17 de agosto de 2020. Diario Oficial de la Federación.

Secretaría de Salud (2022). Programa Sectorial de Salud 2020-2024: Avance y resultados 2022.

Casos, resoluciones o recomendaciones

‘LS’ and ‘LT’ (Privacy) [2017] AICmr 60. CP14/04346. Australian Privacy Commissioner. (26 de junio de 2017).

18 de enero de 2016. [Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales]. Acuerdo mediante el cual se aprueba el proyecto de Lineamientos para el uso de hiperenlaces o hipervínculos en una

página de Internet del INAI, para dar a conocer avisos de privacidad a través de medidas compensatorias.

Asunto V.C. c. Eslovaquia. 18968/07. Corte Europea de Derechos Humanos. (08 de febrero de 2012).

Asunto Aire c. Irlanda no. 6289/73, de 09 de octubre de 1979. Sentencia del Tribunal Europeo de Derechos Humanos.

Asunto Hokkanen c. Finlandia, no. 19823/92, de 24 de agosto de 1994. Sentencia del Tribunal Europeo de Derechos Humanos.

Asunto Y.G. c. Rusia, no. 8647/12, de 20 de agosto de 2022. Sentencia del Tribunal Europeo de Derechos Humanos.

Asunto Z. c. Finlandia, no. 22009/93, de 25 de febrero de 1997. Sentencia del Tribunal Europeo de Derechos Humanos

Circular 1/2012, de 3 de octubre, sobre el tratamiento sustantivo y procesal de los conflictos ante transfusiones de sangre y otras intervenciones médicas sobre menores de edad en caso de riesgo grave. [Fiscalía General del Estado]. 03 de octubre de 2012.

Circular 2/2017, de 6 de julio, sobre el ingreso no voluntario urgente por razón de trastorno psíquico en centros residenciales para personas mayores. [Fiscalía General del Estado]. 06 de julio de 2017.

Consulta 3/1985, de 30 de abril, en torno a la capacidad de los oligofrénicos para prestar el consentimiento justificante previsto en el artículo 428, párrafo segundo, del Código Penal. [Fiscalía General del Estado]. 30 de abril de 1985.

Consulta 0098/2020, si es conforme al 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos 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 (RGPD) y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección

de Datos Personales y garantía de los derechos digitales de 06 de diciembre de 2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales de 06 de diciembre de 2018), desde su condición de responsable de un hospital privado (el Hospital en lo sucesivo), el permitir el acceso a la historia clínica de los pacientes en distintos supuestos, en aplicación de lo dispuesto en el artículo 9.2 f) 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.

Corte Europea de Derechos Humanos. Caso Hristozov y otros vs. Bulgaria, 47039/11 y 358/12. 29 de abril de 2013.

Dictamen N° D19-008 Acceso a la historia clínica de personas fallecidas por parte de familiares, Exp. CN10-003. [Agencia Vasca de Protección de Datos]. 30 de mayo de 2019.

Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data. [Committee of Ministers Steering Committee on Media and Information Society]. 27 de marzo de 2019.

Instituto Federal de Acceso a la Información Pública. PS.0011/13. 25 de septiembre de 2013.

Instituto Federal de Acceso a la Información Pública. 0551/09. 01 de julio de 2009.

Instituto Federal de Acceso a la Información Pública. 285/05, 11 de mayo de 2005.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Criterio 03/2018.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. RRA 4278/18. 26 de septiembre de 2018.

Instructivo Normativo para la asignación de la Clave Única de Registro de Población. 18 de junio de 2018. Diario Oficial de la Federación.

Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space [European Data Protection Board – European Data Protection Supervisor]. 12 de julio de 2022.

Observación general Nº 14 (2000) El derecho al disfrute del más alto nivel posible de salud (artículo 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales). [Organización de las Naciones Unidas]. 11 de agosto de 2000.

Ordinanza ingiunzione - 28 ottobre 2021, 9716887. [Garante per la protezione dei dati personali] 28 de octubre de 2021.

R/00106/2021, TD/00267/2020 [Agencia Española de Protección de Datos]. 09 de marzo de 2021.

R/00211/2021, Expediente Nº: TD/00033/2021 [Agencia Española de Protección de Datos]. 04 de mayo de 2022.

R/02909/2015, AP/00029/2015. [Agencia Española de Protección de Datos]. 29 de diciembre de 2015.

Recomendación 01/2019 sobre el proyecto de lista del Supervisor Europeo de Protección de Datos en relación con las operaciones de tratamiento supeditadas al requisito de una evaluación de impacto relativa a la protección de datos del artículo 39, apartado 4 del Reglamento (UE) 2018/1725. [Comité Europeo de Protección de Datos]. 2019.

Recomendación General N° 29/2017, sobre el expediente clínico como parte del derecho a la información en servicios de salud. [Comisión Nacional de los Derechos Humanos]. 2017. Diario Oficial de la Federación.

Recomendación CM7Rec (2019) 2 del Comité de Ministros a los Estados Miembros sobre la protección de datos relacionados con la salud. [Consejo de Europa]. 2019.

Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data. [Committee of Ministers, Council of Europe]. 27 de marzo de 2019.

Resolución 45/95 acerca de los principios rectores sobre la reglamentación de los ficheros computarizados de datos personales. [Organización de las Naciones Unidas]. De 14 de diciembre de 1990.

Resolución de Procedimiento Especial Sancionador, PS/00250/2021 [Agencia Española de Protección de Datos]. 01 de julio de 2021.

Resolución N°. R/00552/2019, Expediente Nº: TD/00195/2019. [Agencia Española de Protección de Datos]. 03 de diciembre de 2019.

Resolución Nº: R/00186/2021, Expediente Nº: TD/00250/2020. [Agencia Española de Protección de Datos]. 30 de abril de 2021.

Resolución Nº: R/00679/2021, Expediente Nº: TD/00205/2021. [Agencia Española de Protección de Datos]. 24 de septiembre de 2021.

Schrems II, C-311/18. [Tribunal de Justicia de la Unión Europea]. 2018.

Sobre la solicitud de información efectuada por un parlamentario de la Junta General del Principado de Asturias, calificada y admitida a trámite por la Mesa de la Cámara, sobre la relación de altos cargos y cargos directivos del Principado de Asturias, 2021-0025 [Agencia Española de Protección de Datos]. 22 de marzo de 2021.

Sobre la utilización de la historia clínica al amparo del artículo 9.2 f) 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, 2020-0098. [Agencia Española de Protección de Datos]. 12 de mayo de 2021.

Sobre los tratamientos de datos derivados de la pandemia por COVID-19, 2020-0017. [Agencia Española de Protección de Datos]. 12 de marzo de 2020.

Sobre si el derecho de acceso a la historia clínica comprende conocer quién ha accedido, 2021-0003. [Agencia Española de Protección de Datos]. 08 de febrero de 2021.

Sobre si la comunicación de la Oficina de Prevención y Lucha contra la Corrupción los datos personales de todos los ciudadanos vacunados sin que éstos estuvieran anonimizados o si bien, y atendiendo a la normativa, sería

coherente y suficiente proporciona, 2021-0032. [Agencia Española de Protección de Datos]. 04 de mayo de 2021.

Suprema Corte de Justicia de la Nación. Primera Sala. Tesis de Jurisprudencia 8/2019 (10ª.). 13 de febrero de 2019.

Suprema Corte de Justicia de la Nación. Segunda Sala. Amparo en revisión, 632/2014. 19 de noviembre de 2014.

The People, Plaintiff and Respondent, v. Prosenjit Poddar, Defendant and Appellant., 10 Cal.3d 750 (1974) 518 P.2d 342 111 Cal. Rptr. 910. [Supreme Court of California]. 7 de febrero de 1974.

Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito. Tesis aislada I.4º. 86 A. 03 de octubre de 2013.

Vitaly Tarasoff et al., Plaintiffs and Appellants, v. The Regents of the University of California et al., Defendants and Respondents., 551 P.2d 334, 17 Cal. 3d 425, 131 Cal. Rptr. 14. [Supreme Court of California]. 1 de julio de 1976.

Guías y documentos de agencias especializadas en protección de datos personales

Agencia de Gobierno Electrónico y Sociedad de la Información. (2017). *Guía de disociación y anonimización de datos personales en el ámbito de la salud.* Recuperado en abril de 2019 de https://centrodeconocimiento.agesic.gub.uy/documents/207224/425682/Gu%C3%ADa+de+disociaci%C3%B3n+y+anonimizaci%C3%B3n+de+datos+personales+en+el+%C3%A1mbito+de+salud.pdf/18a17107-fbcf-cbeb-38b8-387eb6eab119?download=true

Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales.* Recuperado en abril de 2019 de https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf

Agencia Española de Protección de Datos. (2022). *Guía para profesionales del sector sanitario.* Recuperado en febrero de 2023 https://www.aepd.es/es/documento/guia-profesionales-sector-sanitario.pdf

Agencia Española de Protección de Datos. (s./f.). *Listado de cumplimiento normativo.* AEPD. Recuperado en abril de 2019 de https://tinyurl.com/2ckkjjyz

Agencia Española de Protección de Datos. (2017). *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD.* Recuperado en abril de 2019 de https://tinyurl.com/pk29cuzx

Agencia Española de Protección de Datos. (2017). *Plan de inspección sectorial de oficio Hospitales Públicos.* Recuperado en abril de 2019 de https://www.aepd.es/sites/default/files/2019-10/plan-de-inspeccion-hospitales-publicos.pdf

Agencia Española de Protección de Datos. (2019). *Guía de Privacidad desde el Diseño.* Recuperado en abril de 2019 de https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

Agencia Española de Protección de Datos. (2019). *Guía para pacientes y usuarios de la sanidad.* Recuperado en marzo de 2021 de https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

Agencia Española de Protección de Datos Personales. (2019). *Modelo de informe de evaluación de impacto en la protección de datos (EIPD) para administraciones públicas.* Recuperado en marzo de 2021 de https://tinyurl.com/4fjbf4bm

Competition and Cosumen Commision of Singapore (2019). *Dicussion paper on Data Portability.* Recuperado en agosto de 2021 de https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf

Comité Europeo de Protección de Datos (2019). *Recomendación 01/2019 sobre el proyecto de lista del Supervisor Europeo de Protección de Datos en relación*

con las operaciones de tratamiento supeditadas al requisito de una evaluación de impacto relativa a la protección de datos [artículo 39, apartado 4 del Reglamento (UE) 2018/1725]. Recuperado en agosto de 2021 de https://tinyurl.com/4skthh7m

Comité Europeo de Protección de Datos (2020). *Declaración sobre las restricciones de los derechos de los sujetos de datos en el marco del estado de alarma en los Estados miembros*. Recuperado en marzo de 2021 de https://tinyurl.com/y5tkb2bc

Comité Europeo de Protección de Datos (2020). *Declaración sobre el tratamiento de datos personales en el contexto de la reapertura de las fronteras tras el brote de la COVID-19*. Recuperado en marzo de 2021 de https://tinyurl.com/y5tkb2bc

European Data Protection Supervisor. (2018). *Opinion 5/2018 Preliminary Opinion on privacy by design.* Recuperado en abril de 2019 de https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf

European Data Protection Board. (2019). *Directrices 2/2019 sobre el tratamiento de datos personales en virtud del artículo 6, apartado1, letra b), del 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 en el contexto de la prestación de servicios en línea a los interesados.* Recuperado en marzo de 2021 de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_es.pdf

European Data Protection Board. (2020). *Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19.* Recuperado en marzo de 2021 de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_es.pdf

European Data Protection Board. (2020). *Directrices 2/2020 relativas a la aplicación del artículo 46, apartado 2, letra a), y del artículo 46, apartado 3, letra b),del 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 los que respecta al tratamiento de datos personales y a la libre circulación de estos datos con respecto a las transferencias de datos personales entre autoridades y organismos públicos del EEE y de fuera de este*. Recuperado en marzo de 2021 de https://edpb.europa.eu/system/files/2021-06/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_es.pdf

European Data Protection Board. (2020) *Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19 adoptadas en 21 de abril de 2020*. Recuperado en marzo de 2021 de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf

European Data Protection Board. (2020). *Directrices 4/2019 relativas al artículo 25, Protección de datos desde el diseño y por defecto, versión 2.0. Adoptadas el 20 de octubre de 2020.* Recuperado en marzo de 2021 de https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_es.pdf

European Data Protection Board. (2020). *Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del Reglamento (UE) 2016/679 (1.ª parte).* Recuperado en marzo de 2021 de https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_es.pdf

European Data Protection Board. (2020). *Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679.* Recuperado en agosto de 2021 de

https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

European Data Protection Board. (2021). *Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el 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.* Recuperado en octubre de 2022 https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_es.pdf

European Data Protection Board. (2021). *Guidelines 01/2021 on Examples regarding Personal Data Breach Notification.* Recuperado en octubre de 2022 de https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_pdbnotification_adopted_en.pdf

European Data Protection Board. (2021). *Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE.* Recuperado en octubre de 2022 de https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_es.pdf

European Data Protection Board. (2022). *Guidelines 01/2022 on data subject rights - Right of access.* Recuperado en octubre de 2022 de https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012022_right-of-access_0.pdf

European Data Protection Board. (2022). *Guidelines 02/2022 on the aplication of the Article 60 GDPR.* Recuperado en octubre de 2022 de https://edpb.europa.eu/system/files/2022-03/guidelines_202202_on_the_application_of_article_60_gdpr_en.pdf

European Data Protection Board. (2022). *Guidelines 04/2021 on Codes of Conduct as tools for transfers.* Recuperado en octubre de 2022 de https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

European Data Protection Board. (2022). *Guidelines 9/2022 on personal data breach notification under GDPR*. Recuperado en octubre de 2022 de https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf

European Union Agency for Network and Information Security. (2014). *Privacy and Data Protection by Design -from policy to engineering.* Recuperado en marzo de 2021 de https://doi.org/10.2824/38623

European Union Agency for Network and Information Security. (2022). *Deploying pseudonymisation techniques. The case of the Healh Sector.* European Union Agency for Cybersecurity. Recuperado en febrero de 2023 https://doi.org/10.2824/092874

Grupo de Trabajo del Artículo 29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales.* Comisión Europea. Recuperado en marzo de 2021 de https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Grupo de Trabajo del Artículo 29. (2007). *Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME).* Recuperado en marzo de 2021 de https://metgesdecatalunya.cat/uploaded/File/Documentacio/Informes/General/proteccion%20datos%20historia%20medica.pdf

Grupo de Trabajo del Artículo 29. (2014). *Dictamen 05/2014 sobre técnicas de anonimización.* Agencia Española de Protección de Datos. Recuperado en abril de 2019 de https://www.aepd.es/sites/default/files/2019-12/wp216-es.pdf

Grupo de Trabajo del Artículo 29. (2017). *Directrices sobre el derecho a la portabilidad de datos.* Agencia Española de Protección de Datos. Recuperado en abril de 2019 de https://www.aepd.es/sites/default/files/2019-09/wp242rev01-es.pdf

Grupo de Trabajo del Artículo 29. (2017). *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento <<entraña probablemente un alto riesgo>> a efectos del Reglamento (UE) 2016/679.* Recuperado en marzo de 2021 de https://tinyurl.com/5fr52auk

Instituto de Información Sanitaria (2010). *El sistema de historia clínica digital del Sistema Nacional de Salud.* Agencia de Calidad del Sistema Nacional de Salud. Recuperado en abril de 2019 de https://www.sanidad.gob.es/organizacion/SistemaNacionaldeSalud/planCalidadSISTEMA_NACIONAL_DE_SALUD/docs/HCDSISTEMANACIONAL DE SALUD_Castellano.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2015). *Guía para implementar un sistema de gestión seguridad de datos personales.* Recuperado en marzo de 2021 de https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2015). *Metodología de análisis de riesgo.* Recuperado en marzo de 2021 de http://corpusiurispdp.inai.org.mx/iberoamericano/OtrosDocumentos/MetodologiaAnalisisRiesgos.pdf#search=disociaci%C3%B3n

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (2016). *Guía para cumplir con los principios y deberes de la Ley federal de protección de datos personales en protección de particulares.* Recuperado en marzo de 2021 de https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_Ley

Federal de Protección de Datos Personales en Posesión de Particulares, de 05 de julio de 2010, de 05 de julio de 2010_junio2016.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2020). *Guía para la elaboración de evaluaciones de impacto a la privacidad. Documento orientador en el marco de la Protección de Datos Personales en Posesión de Particulares.* Recuperado en marzo de 2021 de https://tinyurl.com/8t4ratj4

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (s.f.). *El ABC del Aviso de Privacidad*. Recuperado en marzo de 2021 de https://tinyurl.com/8brm969s

Ministerio de sanidad (2022). *Estrategia de salud pública 2022 ESP 2022. Mejorando la salud y el bienestar de la población.* Recuperado en abril de 2019 de https://www.sanidad.gob.es/ciudadanos/pdf/Estrategia_de_Salud_Publica_2022___Pendiente_de_NIPO.pdf

Montaña, C., & Rodríguez, B. (2017). *Criterios de disociación de datos personales.* Unidad Reguladora y de Control de Datos Personales; Agencia de Gobierno Electrónico y Sociedad de la Información. Recuperado en abril de 2019 de https://www.gub.uy/unidad-reguladora-control-datos-personales/sites/unidad-reguladora-control-datos-personales/files/documentos/publicaciones/Criterios%2Bde%2Bdisociacion%2Bde%2Bdatos%2Bpersonales.pdf

Personal Data Protection Commision of Singapore. (2020). *Response to feedback on the public consultation on proposed data portability and data innovation provisions.* Recuperado en agosto de 2021 de https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/Response-to-Feedback-for-3rd-Public-Consultation-on-Data-Portability-Innovation-200120.pdf

Secretaría General de Salud Digital, Información en Innovación para el SISTEMA NACIONAL DE SALUD (2021). Estrategia de salud digital. Ministerio de

Sanidad. Recuperado en abril de 2019 de https://www.sanidad.gob.es/ciudadanos/pdf/Estrategia_de_Salud_Digital_del_SISTEMA NACIONAL DE SALUD.pdf

Páginas de internet

Agencia de Calidad del Sistema Nacional de Salud. Ministerio de Sanidad y Política Social. (2021). *El sistema de Historia Clínica Digital del SISTEMA NACIONAL DE SALUD*. Recuperado en octubre de 2022 de https://www.mscbs.gob.es/organizacion/SistemaNacionaldeSalud/planCalidadSISTEMA_NACIONAL_DE_SALUD/docs/HCDSISTEMANACIONAL DE SALUD_Castellano.pdf

Agencia de Gobierno Electrónico y Sociedad de la Información (2019). *Novedades del programa Salud.uy*. Recuperado en abril de 2019 de https://tinyurl.com/yy3rk585

Agencia Española de Protección de Datos. (2020). *Consulta sobre el uso de la HC cuando el médico ha cesado en su actividad 2020-0079*. Recuperado en marzo de 2021 de https://www.aepd.es/es/documento/2020-0079.pdf

Agencia Española de Protección de Datos. (2022). *Los centros sanitarios y hospitales que prestan servicios a aseguradoras y Mutuas, ¿son encargados de tratamientos o responsables?* Recuperado en octubre de 2022 de https://www.aepd.es/es/preguntas-frecuentes/16-salud-y-coronavirus/FAQ-1617-centros-sanitarios-y-hospitales-que-prestan-servicios-a-aseguradoras-y-mutuas-son-encargados-de-tratamientos-o-responsables

Agencia Española de Protección de Datos. (2022). *En una clínica que presta asistencia psicológica a trabajadores y alumnos de una Universidad, ¿los servicios de prevención pueden acceder a estos informes?* Recuperado en octubre de 2022 de https://www.aepd.es/es/preguntas-frecuentes/16-salud-y-coronavirus/FAQ-1618-clinica-presta-asistencia-psicologica-a-

trabajadores-y-alumnos-universidad-servicios-de-prevencion-pueden-acceder-a-estos-informes

Agencia Española de Protección de Datos. (16 de diciembre de 2018). *¿Qué es el derecho a la portabilidad?* Recuperado en abril de 2019 de https://www.aepd.es/es/prensa-y-comunicacion/blog/que-es-el-derecho-la-portabilidad

Agencia Española de Protección de Datos. (2022). *Salud*. Recuperado en octubre de 2022 https://www.aepd.es/es/areas-de-actuacion/salud

Arévalo, D. (2022, 29 septiembre). *Impulsan creación de Carta de Derechos de la Persona Digital*. Consumotic. Recuperado en octubre de 2022 de https://consumotic.mx/tecnologia/impulsan-creacion-de-carta-de-derechos-de-la-persona-digital/

Asia-Pacific Economic Cooperation. (septiembre de 2021). *What if the Cross-Border Privacy Rules System*. Recuperado en octubre de 2022 de https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

Asociación Médica de Noruega. (2015). *Curso Fundamentos de ética Médica*. Recuperado en agosto de 2021 de http://nettjurs.legeforeningen.no/enrol/index.php?id=37

BMG (05 de noviembre de 2021). *La historia clínica electrónica (ePA)*. Bundesministerium für Gesundheit. Recuperado en febrero de 2023 de https://www-bundesgesundheitsministerium-de.translate.goog/elektronische-patientenakte.html?_x_tr_sl=de&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=nui,sc)

Blutitude, Funsalud & Revista Expansión. *Ranking "Los mejores hospitales privados de Mexico".* Recuperado en febrero de 2023 de *https://www.blutitude.com/proyectos/ranking-mejores-hospitales-privados/*

Calavia, M. (2022). *La digitalización de la sanidad, un cambio de modelo en marcha pero con mucho camino por recorrer*. Cinco días, El País. Recuperado en febrero de 2023 de

https://cincodias.elpais.com/cincodias/2022/12/02/companias/1669978729_411163.html

Cantero Rivas, R. (s.f.). *Historia clínica.* Enciclopedia de bioderecho y bioética. Recuperado en agosto de 2021 de https://enciclopedia-bioderecho.com/voces/173

Cavoukian, A. (agosto de 2009). *Privacy by Design. The 7 Foundational Principles.* Privacy by Design. Recuperado en agosto de 2021 de www.privacybydesign.ca

Cavoukian, A. (2010). *Privacy by design: the definitive workshop. A foreword.* Privacy by Design. Recuperado en agosto de 2021 de https://link.springer.com/article/10.1007/s12394-010-0062-y

Centers for Disease Control and Prevention. (14 de semptiembre de 2018). *Health Insurance Portability and Accountability Act od 1996 (HIPPA)*. Recuperado en febrero de 2023 de https://www.cdc.gov/phlp/publications/topic/hipaa.html

Centre for Information Policy Leadership. (2017). *Comments by the Centre for Information Policy Leadership on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability" adopted on 13 December 2016.* Recuperado en agosto de 2021 de https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf

Comisión Europea. (16 de diciembre de 2018). *¿Qué es el derecho a la portabilidad?* Agencia Española de Protección de Datos. Recuperado en agosto de 2021 de https://www.aepd.es/es/documento/wp242rev01-annex-es.pdf

Comisión Europea. (03 de mayo de 2022). *Preguntas y respuestas. Salud en la UE. Espacio Europeo de Datos Sanitarios (EEDS)*. Recuperado en octubre de 2022 https://ec.europa.eu/commission/presscorner/detail/es/qanda_22_2712

Comisión Europea. (03 de mayo de 2022). *Proposal for a regulation of the european parliament and of the council on the European Health Data Space*. EUR-Lex.

Recuperado en octubre de 2022 de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

Comisión Europea. (03 de mayo de 2022). *Public Health. Espacio europeo de datos sanitarios.* Recuperado en octubre de 2022 de https://ec.europa.eu/health/ehealth-digital-health-and-care/european-health-data-space_es

Comisión Europea. (03 de mayo de 2022). *Servicios electrónicos sanitarios transfroterizos*. Recuperado en octubre de 2022 de https://ec.europa.eu/health/ehealth-digital-health-and-care/electronic-cross-border-health-services_es

Comisión Europea. (03 de mayo de 2022). *Unión Europea de la Salud: Un espacio europeo de datos sanitarios para las personas y la ciencia*. Recuperado en octubre de 2022 de https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2711

Comité Europeo de Protección de Datos. (2020). *Declaración sobre el tratamiento de datos personales en el contexto de la reapertura de las fronteras tras el brote de la COVID-19.* Recuperado en marzo de 2021 de https://tinyurl.com/y5tkb2bc

Comité Europeo de Protección de Datos. (2020). *Declaración sobre las restricciones de los derechos de los sujetos de datos en el marco del estado de alarma en los Estados miembros.* Recuperado en marzo de 2021 de https://tinyurl.com/y5tkb2bc

Comisión Nacional del Sistema de Ahorro para el Retiro (20 de julio de 2023). *La Consar y los Instituto de Seguridad Social formalizan la operatividad del convenio sobre portabilidad de derechos*. Recuperado en febrero de 2023 de https://www.gob.mx/consar/articulos/la-consar-y-los-institutos-de-seguridad-social-formalizan-la-operatividad-del-convenio-sobre-portabilidad-de-derechos

Comisión Nacional para la protección y Defensa de Usuarios de Servicios Financieros. (julio de 2023) *¿Sabes que puedes cambiar tu cuenta de nómina*

al Banco de tu preferencia? Recuperado en febrero de 2023 de https://www.condusef.gob.mx/?p=contenido&idc=937&idcat=1

Future. (julio de 2019). *Data portability: what is at stake?* Recuperado en agosto de 2021 de https://www.datumfuture.org/wp-content/uploads/2019/07/Datum-Future-Data-Portability-July-2019.pdf

De Lorenzo, R. (03 de abril de 2019). *El acto médico y su trascendencia jurídica*. *Redacción Médica*. Recuperado en abril de 2019 de https://www.redaccionmedica.com/opinion/el-acto-medico-y-su-trascendencia-juridica-6725

De Lorenzo, R. (2012). *Regulación de datos biométricos*. *Ecos y comentarios*. Recuperado en abril de 2019 de https://www.delorenzoabogados.es/articulos/2012/20120531_regulacion_datos_biometricos.pdf

El país. (07 de noviembre de 2022) *"Podrías darles un puñetazo en la garganta": el consejo de Alexa a una madre para calmar a sus hijos".* Recuperado en febrero de 2023 de https://elpais.com/tecnologia/2022-11-07/podrias-darles-un-punetazo-en-la-garganta-el-consejo-de-alexa-a-una-madre-para-calmar-a-sus-hijos.html?ssm=TW_CM_AME#Echobox=1667865446

Egan, E. (2019). *Data portability and privacy.* Facebook. Recuperado en agosto de 2021 de https://about.fb.com/ltam/wp-content/uploads/sites/14/2019/09/data-portability-privacy-white-paper.pdf

Fundación Avedis Donabedian – Profesor Avedis Donabedian. (s. f.). *Profesor Avedis Donabedian (1919-2000).* https://www.fadq.org/nosotros-2/profesor-avedis-donabedian/

Galende Domínguez, I. (2020). *Derecho a la información sanitaria. Enciclopedia de Bioderecho y Bioética.* Recuperado en agosto de 2021 de https://enciclopedia-bioderecho.com/voces/94

Garante per la protezione dei dati personali. (10 de noviembre de 2021). *Newsletter 10/11/21 Ricette mediche appese fuori dalla finestra, il Garante privacy sanziona un medico - Pa: ok del Garante privacy alla piattaforma digitale per*

la notifica degli atti - Carta europea della disabilità, via libera del Garante privacy. Recuperado en octubre de 2022 de https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9716908

Gematik (2023). *EPA, datos personales, elecciones personales.* Recuperado en febrero de 2023 *https://www-gematik-de.translate.goog/anwendungen/e-patientenakte/?_x_tr_sl=de&_x_tr_tl=es&_x_tr_hl=es*

Gobierno de España (2021). *Poítica de privacidad de la aplicación Radar COVID*. Recuperado en octubre de 2022 https://radarcovid.gob.es/politica-de-privacidad?s=35

Gómez Sánchez, Y. (2020). *Derecho a no saber*. *Enciclopedia de Bioderecho y Bioética*. Recuperado en marzo de 2021 de https://enciclopedia-bioderecho.com/voces/102

IAPP (07 de octubre de 2022). *The EU-US Data Privacy Framework: A new era for data transfers?* Recuperado en febrero de 2023 de https://iapp.org/news/a/the-eu-u-s-data-privacy-framework-a-new-era-for-data-transfers/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (24 de septiembre de 2017). *Comunicado INAI-317-17 EXPEDIENTE CLÍNICO.* Recuperado en agosto de 2021 de https://tinyurl.com/5fca5h5f

INEGI (2023). *Directorio Nacional Estadístico de Unidades Económicas.* Recuperado en febrero de 2023 *https://www.inegi.org.mx/app/mapa/denue/default.aspx*

INEGI, IFT (2023). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2022*. Recuperado en febrero de 2023 de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf

ISO (2023). *ISO 31700-1:2023 (en)*. Online Browsing Platform._Recuperado en febrero de 2023 https://www.iso.org/obp/ui/#iso:std:iso:31700:-1:ed-1:v1:en

Lois, E. (18 de febrero de 2019). *La fiscalía pide cuatro años a una empleada del Sergas por acceder al historial clínico de su hija.* El País. Recuperado en agosto de 2021 de https://elpais.com/ccaa/2019/02/18/galicia/1550519832_648229.html

MacGillivray, A., & Shambaugh, J. (30 de septiembre de 2016). *Exploring data portability*. The White House (President Barack Obama). Recuperado en febrero de 2023 de https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability

Data Protability Project. (s.f.). *Data Portability Project (About and Implement).* Recuperado en febrero de 2023 de http://dataportability.org/

Lueders, H. (2004). *El marco europeo de interoperabilidad. Recomendaciones de la industria de las tecnologías de la información y comunicación*. Recuperado en febrero de 2023 de https://administracionelectronica.gob.es/pae_Home/en/dam/jcr:f6a61cb2-0764-4f36-aa43-1ffe3ca4df06/3_026.pdf

Organización Mundial de la Salud, (2003). *Adherence to long-term therapies: evidence for action (edited by Eduardo Sabaté).* Recuperado en agosto de 2021 de https://apps.who.int/iris/handle/10665/42682

Organización Mundial de la Salud. (2017). *Preguntas más frecuentes*. Recuperado en abril de 2019 de http://www.who.int/suggestions/faq/es/

Programa de las Naciones Unidas para el Desarrollo (s.f). *¿Qué son los Objetivos de Desarrollo Sostenible?* Recuperado en febrero de 2023 de https://www.undp.org/es/sustainable-development-goals

Secretaría de Economía. (08 de febrero de 2013). *México se une al Sistema Transfronterizo de datos personales de APEC*. Recuperado en agosto de 2021 de Gobierno de México https://www.gob.mx/se/prensa/mexico-se-une-al-sistema-transfronterizo-de-datos-personales-de-apec

Sollano, S. S. (15 de diciembre de 2020). *Iniciativa con proyecto de decreto por el que se reforma el artículo 77 bis 9 de la Ley General de Salud para la implementación de un registro de pacientes individual, así como la creación de un archivo electrónico de historias clínicas*. Gaceta del Senado. Recuperado en agosto de 2021 de https://www.senado.gob.mx/64/gaceta_del_senado/documento/114707

The White House (07 de octubre de 2022). *Fact sheet: President Biden Signs Executive Orden to Implement the European Union-U.S. Data Privacy Framework.* Recuperado en febrero de 2023 de https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/

TRENDTIC Tendencias tecnológicas & negocios (28 de enero de 2022). *"Chile Digital" La propuesta para la nueva Constitución que aborda los Derechos Digitales*. Recuperado en octubre de 2022 https://www.trendtic.cl/2022/01/chile-digital-la-propuesta-para-la-nueva-constitucion-que-aborda-los-derechos-digitales/#:~:text=Derecho%20a%20la%20privacidad%2C%20protecci%C3%B3n,identidad%20en%20el%20mundo%20digital

Xataka (10 de octubre de 2022). *EEUU y Europa tienen nuevo acuerdo de protección de datos. Nia la tercera parece que irá la vencida.* Recuperado en octubre de 2022 de https://www.xataka.com/legislacion-y-derechos/eeuu-europa-tienen-su-nuevo-acuerdo-proteccion-datos-no-esta-claro-que-a-tercera-vaya-vencida

Informes

Agencia Española de Protección de Datos (2017). *Interés legítimo, portabilidad y blanqueo, Informe 0195/2017*. Recuperado en agosto de 2021 de

https://asociaciondpd.com/wp-content/uploads/2018/12/2017-0195-interes-legitimo-portabilidad-y-blanqueo.pdf

Comisión de Arbitraje Médico del Estado de Hidalgo. (2021). *Informe anual de actividades 2020.* Recuperado en marzo de 2021 de https://cameh.gob.mx/joomla30/documentos/CAMEH_2020.pdf

Comisión Europea. (2020). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité eEonómico y Social Europeo y al Comité de las Regiones. Una Estrategia Europea de Datos.* Bruselas. Recuperado en marzo de 2021 de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0066&from=ES

Dirección General de Información en Salud (2021). *Recursos en salud Sectorial, 2021*. Secretaría de Salud del Gobierno de México. Recuperado en marzo de 2021 de http://www.dgis.salud.gob.mx/descargas/datosabiertos/recursosSalud/Recursos_Salud_Sectorial_2021.zip?V=2022.08.11

Ethics Advisory Group. (2018). *Towards a digital ethics.* EDPS Ethics Advisory Group. Recuperado en octubre de 2022 https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

European Banking Federation. (2017). *European Banking Federation's comments to the Working Party 29 guidelines on the right to data portability.* Recuperado en abril de 2019 de https://www.ebf.eu/wp-content/uploads/2017/04/EBF_025448E-EBF-Comments-to-the-WP-29-Guidelines_Right-of-data-portabi.._.pdf

Gans, J. (2018). *Enhancing Competition with Data and Identity Portability. Policy proposal.* Brookings. Recuperado en agosto de 2021 de https://www.hamiltonproject.org/assets/files/Gans_20180611.pdf

Actas de conferencia

Atkinson, W. (1976). *Introduction*. [Sesión de conferencia]. 10 policy issues in data protection and privacy. Concepts and perspectives. (pp. 144-146). París: OECD.

Braibant, G. (24-26 de junio de 1976). *The citizen's right of access to his personal file* [Sesión de conferencia]. 10 policy issues in data protection and privacy. (pp. 147-158). OECD.

Hamon, R., Junklewitz, H., Malgieri, G., De Hert, P., Beslay, L., & Sanchez, I. (2021). *Impossible Explanations?: Beyond explainable AI in the GDPR from a COVID-19 use case scenario*. FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, (pp. 549-559). Recuperado en agosto de 2021 de https://doi.org/10.1145/3442188.3445917

Rodatà, S. (24-26 de junio de 1976). *Privacy and Data Suveillance: Growing Public Concern* [Sesión de conferencia]. 10 policy issues in data protection and privacy. Concepts and perspectives. (pp. 130-143). OECD.

Romeo Casabona, C. (2005). *Utilización de muestras biológicas y bancos para la investigación biomédica*. En Brena Sesma, I. (coord.), Salud y derecho. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados (pp. 31-62). UNAM.

Videos

Canal INAI. (25 de octubre de 2019). *Módulo 5. Portabilidad de Datos Personales.* [Archivo de Video].recuperado el 19 de octubre de 2021, de https://www.youtube.com/watch?v=3rVKwvIQrzU

Agradecimientos

No se puede nadar hacia nuevos horizontes hasta no tener el coraje de perder de vista la costa.
William Faulkner

Culminar mis estudios doctorales fue uno de los retos más interesantes que hasta la fecha he enfrentado. Aunque siempre tuve claro que quería alcanzar este grado académico, nunca imaginé el impacto que tendría en todos los aspectos de mi vida. Estoy segura de que este proceso me ha transformado en una mejor persona y siempre estaré agradecida por haberlo experimentado tal como sucedió.

Así, primero quiero agradecer a mis padres, Crescencio Olvera y Rosalva Arellano, así como a mi hermana Rosalba quienes con su infinita confianza, paciencia y amor son los pilares indiscutibles de mi vida.

A Melissa, porque su llegada me recordó lo importante que es luchar por alcanzar y mantener aquello que nos hace felices, pero también que debo disfrutar el tiempo presente.

A mis compañeros perrunos de escritura, Chispa, Chiquitín y Negrito, que se fueron antes de terminar este proyecto, pero sin cuya compañía y amor hubiera sido imposible trabajar largas jornadas.

A mis queridos David Gutiérrez, Aida Carabantes, Germán Jiménez, Carlos Castro, y Javier Lozano quienes siempre han tenido una palabra de aliento cuando más la he necesitado y que han creído en mí y en esta investigación, sobre todo en aquellas veces en las que me costaba tanto hacerlo.

A la Universidad de Guadalajara en México, en especial a la Maestría en Transparencia y Protección de Datos Personales y a Rigoberto Silva, que me dieron

la oportunidad de crecer como su alumna y ahora como docente de su claustro académico.

A mis alumnos quienes, en los momentos más retadores de mi formación y ejercicio profesional, se vuelven mi principal motivación para seguir aprendiendo.

A la Secretaría de Salud de Hidalgo y a Alejandro Pacheco; así como al Congreso del Estado de Hidalgo, a Vanesa Escalante y a Tania Guzmán por las facilidades brindadas para la realización de esta investigación y culminación de mis estudios de posgrado.

A la UNED, mi nueva casa de estudios, que especialmente al inicio, a través de la Dra. Dña. Fernanda Moretón, me brindó todo el acompañamiento y facilidades necesarias para comenzar mis estudios de tercer ciclo, además de por la atinada selección de mis directores.

Finalmente, a mis muy queridos directores, los Dres. Dn. Luis Miguel González de la Garza y Dña. Carmen Muñoz Delgado. Su guía para con mi formación ha sido decisiva para que este trabajo llegara a manos de los lectores. Sobre todo, agradezco profundamente su paciencia para recordarme que puedo lograr cosas increíbles siempre que crea en mí, tal como ustedes permanentemente lo hicieron, a pesar de conocernos solo en el mundo virtual. Gracias por recordarme que el límite está solo en mi mente y por sostenerme cuando me sentí tan cuesta arriba. Ojalá un día pueda retribuirles su trabajo, cariño y dedicación. Mientras, trato de homenajear sus tantas enseñanzas, aplicándolas con mis propios alumnos.