

Breve aproximación a las implicaciones jurídicas y operativas del tratamiento de datos de salud

Isabel Davara Fernández de Marcos*

Davara Abogados, S.C., México, D.F.

Resumen

La regulación de la protección de datos personales es un tema novedoso y de actualidad en México. La regulación del tratamiento y uso de los datos personales relativos a la salud aún necesitará de reglamentación específica en el futuro próximo. Es indispensable que los profesionales e instituciones de salud se preparen para adecuar sus procedimientos habituales de modo que no caigan en incumplimientos que pueden acarrear multas de más de 35 millones de pesos y hasta 10 años de cárcel. Este artículo pretende ser una breve aproximación práctica a las implicaciones jurídicas y operativas de lo anterior.

PALABRAS CLAVE: Protección de datos. Salud. Privacidad. Información.

Abstract

Data protection regulation is a new and appealing issue in Mexico. The processing of health personal data will require even more specific regulation in the near future. Health care professionals and institutions need to adequate their usual proceedings to comply with the actual regulation in order to protect their patients and customers and avoid fines up to 35 million Mexican pesos and 10 years of prison. The aim of this article is to present a practical approach to the legal and managerial implications of this regulation.

KEY WORDS: Data Protection, Health, Privacy, Information.

Planteamiento

Si la protección de datos personales es una materia especializada, la protección de datos personales relativos a la salud es una submateria con multitud de aristas y ramificaciones, que, además, involucra diversas áreas y especialidades científicas que tienen que cooperar y trabajar en conjunto.

Sin embargo, dejando aparte la multitud de conceptos y cuestiones interrelacionadas, la legislación concuerda en que el centro de todo es y debe ser la persona y el respeto a su dignidad e identidad, así como la protección de su salud.

La lícita y legal utilización de los datos personales relativos a la salud necesita contar con una regulación especializada, aún más que la general relativa a la protección de datos personales¹, que atienda puntualmente a las cuestiones que surgen como consecuencia de este manejo, de manera que sea posible, en primer lugar, proteger al titular de estos datos, la persona física, el individuo, frente a abusos indebidos y al mismo tiempo, en su caso, que la sociedad en su conjunto pueda beneficiarse de los buenos usos de dicha información.

Por un lado, ningún derecho es absoluto. El derecho a la protección de datos personales, cuya finalidad es proteger a la persona frente al tratamiento ilícito de sus

Correspondencia:

*Isabel Davara Fernández de Marcos

Despacho Davara Abogados, S.C.

Blvd. Adolfo Ruiz Cortines, 3642-1502

Col. Jardines del Pedregal, C.P. 01900, México, D.F.

E-mail: idavara@davara.com.mx

Fecha de recepción en versión modificada: 21-09-2012

Fecha de aceptación: 24-09-2012

datos, también tiene límites debido a la necesidad de proteger el interés general, bien sea por los intereses legítimos de terceros o por el interés público concretado en la seguridad del Estado u otros bienes jurídicos similares, como la seguridad nacional, el orden y la seguridad públicas o la salud pública y la investigación pertinente².

Tal y como señala el artículo primero de la Constitución Política de los Estados Unidos Mexicanos, debe prevenirse «toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas».

En este sentido, prevenir la no discriminación y garantizar el uso adecuado de los datos de salud, tratados conforme a finalidades específicas, pasa por garantizar, como veremos después, el cumplimiento de los principios relativos al tratamiento de datos personales, con particular atención a las peculiaridades de los datos sensibles³.

En particular, se plantea la necesidad a nivel federal de tratar tanto con leyes estatales como con la necesidad de regular específicamente esta materia con la finalidad de evitar intromisiones ilegítimas en la intimidad, la privacidad y la vida privada de la persona.

Algunos conceptos

Privacidad

El concepto de privacidad (*privacy*) según la doctrina ha surgido en EE.UU.⁴. Sin embargo, este concepto es distinto al de «protección de datos», a pesar de que ambos mantienen una relación cercana. La privacidad, como concepto, no tiene una definición, ya que es en gran medida subjetiva, puesto que la evolución de la sociedad y los factores, como la cultura, el ambiente tecnológico, el político y el económico⁵ ocasionarán una variación en el concepto. Asimismo, podemos encontrar en el centro del significado de privacidad los datos pertinentes a la salud. De esta forma, podemos asegurar que la privacidad protege a los individuos de los excesos que pudieran cometerse como consecuencia de un tratamiento ilícito de estos datos personales⁶.

Vida privada

El Tribunal Europeo de Derechos Humanos ha afirmado, en el caso *S. and Marper v. The United Kingdom*,

que el concepto de vida privada (*private life*) es amplio y, por lo tanto, no se le puede ligar una definición exclusiva. Este tribunal ha interpretado que los diferentes aspectos relacionados con la integridad física y psicológica del individuo, su identidad física y social, o inclusive elementos relacionados con el derecho a la imagen, entran dentro del concepto de vida privada. De esta manera, podemos afirmar que existen obvias diferencias entre estos conceptos de privacidad y vida privada. En este sentido, mientras en Europa hay avances en cuanto al estudio y regulación de la vida privada, en EE.UU. hay un avance similar en cuanto al tema de privacidad. En el caso de Europa, estos avances llegan al punto de que es posible distinguir entre privacidad y derecho a la protección de datos personales.

Protección de datos personales

Finalmente, en el ámbito europeo se ha desarrollado recientemente el concepto de protección de datos personales. De acuerdo con S. Rodotà, «para comprender enteramente la manera en que se desarrolla hoy la relación entre democracia y datos personales no es posible limitarse a este tipo de consideraciones, sustancialmente basadas en una idea de privacidad como «derecho a ser dejado solo». De tal forma, se puede llegar a la clasificación del derecho a la protección de datos personales como un derecho subjetivo, fundamental, de tercera generación y colectivo. Se clasifica como subjetivo debido a que quien es titular de los datos, es decir, quien lo ostenta, es la figura que se encuentra bajo protección.

La característica de fundamental se le atribuye a través del reconocimiento como tal por el derecho internacional. Este es un derecho cuya naturaleza se encuentra ampliamente arraigada en la naturaleza humana.

Se habla de él como un derecho de tercera generación. Los derechos civiles y políticos integran lo que se denomina la primera generación, los derechos sociales y culturales forman la segunda generación, la tercera generación se caracteriza por los derechos de los pueblos o la solidaridad.

Es un derecho colectivo, cuyo marco de aplicación se extiende a todos; por lo mismo, cada uno debe luchar por él, pero al mismo tiempo podemos exigirle al Estado que lo resguarde. Son ejemplos de derechos colectivos o comunitarios⁷: el derecho a la autodeterminación, a la paz, al desarrollo, a la democracia, a la integración, a recibir y producir información equitativamente, al medio ambiente sano y ecológicamente equilibrado y a beneficiarse del patrimonio común de

la Humanidad. Cada uno de estos derechos se encuentra en un estado de desarrollo y reconocimiento internacional distinto.

Asimismo, es importante recalcar que son derechos que al mismo tiempo pueden exigir defensa ante el Estado y demandar al mismo de incumplimiento. Se requiere la participación de todos los actores sociales para lograr su cumplimiento, se encuentra en el ámbito de aplicación tanto nacional como internacional y se considera dentro del concepto de «calidad de vida».

La expresión «protección de datos personales» es algo ambigua y confusa, por lo que requiere de mayor explicación. El dato como elemento aislado no necesita ser reguardado. Sin embargo, cuando se encuentra vinculado a una persona la situación es distinta. Por lo tanto, no se protege el dato como tal, sino que se protege al titular; aún más, cuando el dato se une a la persona se convierte en información personal.

Además, las normas que se refieren a la protección de datos buscan proteger al titular ante un tratamiento ilícito de su información; esto quiere decir que el titular del derecho es el individuo. Este es un derecho subjetivo que no se basa en proteger la información como tal, sino que busca resguardar los intereses del individuo cuya información se está tratando.

En concreto, el objeto de protección es novedoso (los datos personales, siempre que estén unidos a un titular), pero el objetivo fundamental de la normatividad es resguardar la privacidad, como se puede ver reflejado en la Resolución de Madrid⁸. En el escenario actual, en el que se utiliza la tecnología en el tratamiento de información personal, ha resultado en una intrusión grande y agresiva al espacio personal de las personas⁹.

Aunque es cierto que en algunos casos la injerencia no es negativa ni ilícita, por la incertidumbre siempre se percibe como una amenaza potencial. Asimismo, se debe resaltar la importancia del tratamiento por los diferentes medios tecnológicos; anteriormente las fronteras de tiempo y espacio representaban un modo de protección a la intimidad, sin embargo, estas han desaparecido o han cambiado considerablemente, lo que ha resultado en una vulneración para la información; esta se puede tratar, comunicar, conservar, manipular en muy distintos modos y de muy diferentes maneras.

Derecho a la intimidad

La intimidad es un derecho que el sujeto controla en grado suficiente, que ya se ha asentado históricamente. Asimismo, cada individuo, en lo particular, define

qué considera como íntimo (además de los mínimos establecidos por la legislación), y, de igual forma, es bastante fácil y exacto saber cuándo esta esfera ha sido vulnerada, pero el derecho al cual se está haciendo alusión es diferente; se habla de la protección de este perfil que el individuo inclusive llega a ignorar, pero, sobre todo, que no controla. El derecho a la intimidad pasa, así, de una concepción cerrada y estática (libertad negativa) a una abierta y dinámica (libertad positiva), lo cual implica el reconocimiento de mecanismos de control sobre el tratamiento de datos personales, ligados a este mismo derecho.

Más allá de hablar del derecho a ser dejado solo (*the right to be left alone*), se habla del derecho a saber quién, cuándo, cómo y para qué un tercero trata los datos personales de los que el individuo es titular. El poder controlar la información personal y el flujo de la misma son elementos que la privacidad conlleva. De este modo, se puede afirmar que la privacidad es un término que se utiliza para referirnos al perfil que se puede obtener de una persona con el tratamiento.

Los datos de salud como datos personales

Tanto la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), conforme a la modificación introducida por la Ley Federal para la Protección de Datos Personales en Posesión de Particulares (LFPDPPP), como esta última, definen los datos personales como: «Cualquier información concerniente a una persona física identificada o identificable».

Se trata de una definición amplia, pero tampoco es un concepto ilimitado.

- La información: existen una serie de datos personales que todo el mundo identifica como tales, pero queda un gran espectro de información personal sobre la que no se tiene demasiado interés a menudo y que ni tan siquiera se considera como propia.
- Persona física: en la normativa mexicana solo tiene sentido la protección de datos sobre los datos de las personas físicas. Acerca de la información sobre personas morales hablaríamos de otras protecciones jurídicas, pero no de aplicación de la normativa en protección de datos personales.
- Identificada o identificable: incluso cuando esa persona física solo pueda ser identificable, es decir, aunque no la tengamos identificada actualmente, su información personal sigue siendo protegible.

En conclusión, cualquier información, en cuanto asociada a un titular, es información personal, no por la información en sí, sino por su asociación con la persona física a la que se protege. Así, no se puede hablar de datos personales en sentido neutro, sino que tan solo adquieren este carácter en cuanto se asocian a un titular.

En este sentido, los datos relativos a la salud serán datos personales en tanto permitan identificar o hagan identificable a la persona a la que se refieren. Pero además, los datos de salud quedan incluidos entre los datos personales sensibles¹⁰, pues el artículo 3 fracción VI de la LFPDPPP los define como: «Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual», y, consecuentemente, será necesario cumplir con los principios y obligaciones de la protección de datos, así como garantizar a su titular el ejercicio de los derechos en protección de datos (especialmente los conocidos como acceso, rectificación, cancelación y oposición)¹¹.

En definitiva, los datos relativos a la salud de las personas afectan a la vida privada de las mismas (e incluso de sus familiares) de manera particularmente importante, puesto que permiten obtener información sobre la salud, presente y futura, del individuo al que se refieren, así como cualquier otra información sensible.

Por otro lado, los datos de salud pueden ser utilizados con muy diferentes finalidades¹², como pruebas clínicas o de diagnóstico, de investigación médica y de experimentación científica, en el ámbito laboral, en el comercial (especialmente en el sector asegurador¹³), con fines de identificación, etc. En todos estos casos, además, la anonimización¹⁴ de los datos, entre otros, resulta crucial¹⁵.

Brevemente, en cuanto a la regulación actual en México¹⁶, podemos decir que:

- A nivel federal no existe ninguna regulación específica sobre el tratamiento de datos de salud¹⁷.
- Como hemos mencionado, sí existe legislación federal específica en materia de protección de datos, tanto para el sector público como para la iniciativa privada, así como diversas regulaciones estatales en la materia aplicables al sector público únicamente. Asimismo, entendemos que deben

ser aplicables las disposiciones del Código Penal Federal¹⁸.

- Sí existe normatividad relativa a la obligación de solicitar el consentimiento informado para llevar a cabo cualquier actuación o investigación que afecte a la salud de una persona y que pueda involucrar la recolección, almacenamiento o difusión de datos de salud, aunque dispersa y no estructurada de manera coherente y comprensiva en un cuerpo legal *ad hoc*.

Principios y derechos en el tratamiento de datos de salud

Como ya hemos adelantado, los datos relativos a la salud, como datos personales sensibles, tendrán que cumplir con los principios y derechos relativos a la protección de datos, buscando el equilibrio entre la necesidad de tratar estos datos y la protección de la persona para evitar discriminaciones o tratamientos ilícitos ya que como se ha mencionado, en todo tratamiento de datos personales se debe garantizar el cumplimiento de los principios de la protección de datos¹⁹:

- Consentimiento: debiendo tener en consideración, entre otras cosas, como la forma y modo de prestación del mismo. Sin embargo, este principio no es absoluto y, por tanto, cuenta con excepciones que tienen que estar previstas expresamente en la Ley.
- Licitud y calidad: atendiendo tanto al tratamiento y uso que se hace de los datos como la forma en la que estos fueron recabados.
- Finalidad y proporcionalidad: en los términos que ya fueron señalados anteriormente. En cualquier caso, la finalidad puede plantear cuestiones específicas relativas a quién y para qué se tratan los datos personales, de manera que será necesario atender en cada caso concreto a esta cuestión a efectos de determinar el cumplimiento de otros principios tales como el consentimiento o la calidad de los datos.
- Información: como garantía para que el titular de los datos personales pueda conocer y/o consentir, si fuera necesario, el tratamiento.
- Responsabilidad: el responsable debe velar por el cumplimiento de los principios y rendir cuentas al titular, a través del procedimiento incoado por el Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales (IFAI), en caso de incumplimiento. El responsable debe asegurarse de que el tratamiento por terceros

(nacional e internacionalmente), y en particular el encargado del tratamiento, cumple la normativa sobre protección de datos.

Además de los principios, los responsables del tratamiento deben cumplir con dos obligaciones o deberes añadidos:

- Seguridad de la información: teniendo en consideración que se trata de datos sensibles y, por tanto, su tratamiento requiere de medidas de seguridad específicas.
- Confidencialidad de la información: que tendrá que cumplir cualquier persona que tenga acceso a los datos sin perjuicio de que existan otras obligaciones de confidencialidad específicas en atención a la profesión de la persona o a las funciones que desempeñe.

En cuanto a los derechos, podemos brevemente resumir que, en general, se le reconocen al titular de los datos personales –aunque también podrán ser ejercidos por su representante legal– los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO). Así, el titular de los datos tendrá derecho a: a) obtener sus datos personales que obran en poder del responsable; b) tener acceso al aviso de privacidad al que está sujeto el tratamiento de los datos; c) rectificar los datos cuando sean inexactos o incompletos; d) cancelarlos, y e) oponerse al tratamiento de los datos cuando no los hubiere proporcionado al responsable.

Implicaciones en la práctica para los profesionales de la salud

Después de haber pasado brevemente por la explicación teórica sobre este nuevo derecho reconocido en nuestro país, no podemos dejar de preguntarnos sobre lo que esta normativa va a suponer para los profesionales de la salud y, en su caso, las instituciones a las que pertenecen, en su labor diaria.

Todo lo que hemos explicado antes a nivel general tiene que ser cumplido por el profesional y/o la institución responsables del tratamiento de los datos. Es decir, desde el profesional independiente que atiende en su consulta particular, hasta las grandes instituciones, tanto en el entorno de atención clínica como en el de investigación. Así, tanto procedimientos como obligaciones van a cambiar en el día a día.

Desde la manera en la que se recaba el conocido «consentimiento informado», que ahora se ve aumentado por este «consentimiento informado para el tratamiento de los datos personales», en comparación al anterior sobre las cuestiones clínicas y médicas,

pasando por el establecimiento de estrictas medidas de seguridad que vendrán en gran parte determinadas por el perfil de acceso a los datos de salud, y todo ello teniendo en cuenta los principios antes mencionados, entre los que destaca no tratar más datos de los que se pueda y deba conforme a la legalidad y lealtad en el tratamiento.

Los datos de salud, como datos personales pertenecientes a esta categoría de datos sensibles, deben ser tratados con aún más cuidado que los datos personales generales. Respecto a lo anterior, como decíamos, el consentimiento se convierte en el eje central de la normativa, si bien es cierto que también encuentra en este caso excepciones claras a la necesidad de su obtención, específicamente en situaciones de urgencia en que el interés del titular de los datos, de su vida y salud está por encima de la exigencia de dicho consentimiento. Del mismo modo, como decíamos en relación con el acceso, otra de las grandes particularidades del tratamiento de datos de salud reside en quién o quiénes pueden acceder y tratarlos. Por las particularidades mencionadas, es especialmente relevante que solo aquellos facultados para tratarlos, ya sea en un servicio médico en una empresa o en un centro sanitario, tengan acceso a los mismos.

Como un claro ejemplo de lo anterior, podemos ver que el IFAI ha establecido diversos criterios fortaleciendo las disposiciones de la Ley.

Por un lado, se reitera que el consentimiento para el tratamiento de datos personales no es absoluto, como ya se ha mencionado anteriormente, sino que tiene limitaciones. Por ejemplo, en el ámbito farmacéutico, además de las leyes antes citadas, el IFAI²⁰ ha definido que los requerimientos establecidos por instancias como la Comisión Permanente de la Farmacopea de los Estados Unidos Mexicanos son válidos para exceptuar el consentimiento para el tratamiento de datos personales.

Asimismo, el IFAI ha establecido que en el caso de que una farmacéutica deba recabar datos de identificación –nombre y domicilio– de un comprador de cierto tipo de medicamentos, se pueden actualizar dos hipótesis. Por un lado, si el comprador es distinto al paciente al cual le fue prescrito el medicamento, no se estará frente a datos de carácter sensible, por lo que no será necesario recabar el consentimiento expreso del titular. Sin embargo, si el comprador es el mismo sujeto al que se le prescribió el medicamento, sí se estará frente a un dato sensible, requiriendo así que se recabe el consentimiento expreso y que los datos sean resguardados con un nivel especial de seguridad.

En concreto, podríamos plantear, entre otras, las siguientes líneas de acción que el profesional y/o la institución sanitaria debería seguir para aproximarnos a la adecuación integral a la normativa:

- Identificar y describir las bases de datos y tratamientos, en función del flujo lógico de la información, desde el punto de vista jurídico, es decir, desde la finalidad –además de los datos contenidos– a la que se dirigen los tratamientos.
- Emitir los avisos de privacidad –con el consentimiento informado en su caso requerido– en función de los tratamientos identificados.
- Analizar y adecuar las relaciones jurídicas con terceros que accedan a los datos de los que se es responsable.
- Nombrar un responsable, comité o departamento de privacidad.
- Establecer las medidas de seguridad pertinentes en función de los datos tratados.
- Elaborar un procedimiento y formularios de atención al ejercicio de los derechos por parte de los titulares.
- Concienciar a todos los que tratan datos personales, mediante la elaboración y seguimiento a mejores prácticas en la institución.
- Capacitar y dar seguimiento continuo a la privacidad como un elemento más en la toma de decisiones.

Finalmente, como decíamos, surgirán muchas cuestiones particulares que con mucha probabilidad requerirán de desarrollo normativo específico posterior, como la propiedad del expediente clínico o la posible propiedad intelectual que acompaña a los comentarios y opiniones del profesional sanitario, la necesidad en casos específicos de evitar que el mismo paciente conozca sobre su información (como en casos de enfermedad mental o similares), entre otros, que requerirán de la colaboración multidisciplinaria para su elaboración.

Conclusiones

Resulta indiscutible que nos encontramos ante un escenario complejo. Por un lado, como decíamos, el centro de la protección jurídica es el individuo y la salvaguardia de su salud. Por otro lado, esta necesidad de proteger al ser humano no debe suponer un obstáculo o impedimento al desarrollo de la ciencia cuando es utilizada en beneficio de la persona.

Asimismo, como ya decíamos, cabe recordar que ningún derecho es absoluto en un Estado de Derecho.

Habrà entonces que buscar el equilibrio entre este y otros derechos, aplicando leyes y criterios interpretativos como la prueba del daño o la del interés público.

Sin embargo, no podemos desconocer que precisamente estos mismos avances han dado lugar a la posibilidad de dejar a la persona, y a terceros, casi sin secretos, sin privacidad.

Asimismo, existen multitud de finalidades respecto al tratamiento y uso de los datos de salud, que tienen relevantes implicaciones éticas, jurídicas y sociales, con particular énfasis en la salvaguardia de los derechos humanos involucrados, reiterando de nuevo que el centro de la protección debe ser la persona.

Pero, además, desde el punto de vista del impacto a profesionistas y/o instituciones de salud, habrá que tener en cuenta que se presentan grandes cambios y adecuaciones en la manera de trabajar, teniendo en cuenta que la especialidad de los datos tratados, y sobre todo la necesidad de proteger al titular de los mismos en cuanto a su privacidad, es particularmente relevante en este ámbito.

Y, si bien es cierto que lo anterior impactará en la manera de trabajar hasta el momento, podrá también verse como una ventaja competitiva o como una oportunidad de crecimiento, y, en todo caso, como una necesidad en el respeto al derecho fundamental del titular de los datos personales.

En definitiva, es evidente que el tratamiento de los datos relativos a la salud es necesario en muchas ocasiones, y beneficioso en muchas otras, debiendo ser en todo caso un tratamiento lícito y legítimo, leal y legal, de manera que sea posible beneficiarse de los buenos usos de dicha información y al mismo tiempo proteger a la persona frente a abusos indebidos, siguiendo las normas legales existentes o, en su caso, promoviendo la modificación de las ya existentes o la redacción de las nuevas que sean pertinentes.

A la vista de lo expuesto, parece que la realidad, en México e internacionalmente, presenta un largo camino por recorrer en la regulación de los datos personales, y específicamente en la de los datos relativos a la salud, donde el equilibrio entre los principios y derechos a respetar, con especial consideración a lo sensible del tratamiento en cuestión, y el progreso científico y social, debe ser el objetivo principal a lograr.

Bibliografía

1. La regulación en protección de datos personales en México actualmente está como sigue:
Para el sector privado:
– El artículo 6, párrafo 2.º, fracción II, y el artículo 16, párrafo 2.º de la Constitución Política de los Estados Unidos Mexicanos.

- Ley Federal para la Protección de Datos Personales en Posesión de Particulares (LFPDPPP) (DOF 5/07/2010).
 - Reglamento de la LFPDPPP (DOF 21/12/2012).
- Para el sector público:
- A nivel federal:
 - LFTAIPG.
 - Reglamento de la LFTAIPG (DOF 11/06/2003).
 - Lineamientos de Protección de Datos Personales (DOF 30/09/2005).
 - Recomendaciones del IFAI de Seguridad para la Protección de Datos Personales.
- A nivel estatal tendremos que atender a lo dispuesto por la regulación de los organismos estatales de transparencia y acceso a la información pública.
2. Davara Fernández de Marcos I. Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual. Protección de datos personales: compendio de lecturas y legislación. Instituto Federal de Acceso a la Información Pública. México, D.F.: Tiro Corto; 2010.
 3. Los datos de salud se consideran internacionalmente como datos sensibles y, específicamente, en México, la LFPDPPP (DOF 5/07/2010) así lo señala en su artículo 3. En este sentido, se tendrá que adecuar su tratamiento para garantizar su protección mediante reglas específicas relativas especialmente al consentimiento y las medidas de seguridad aplicables, entre otros. Un aspecto importante es la distinción en el régimen de protección de datos en el sector público y en el privado. Si bien en ambos casos existe una Ley Federal, en el primer caso no existe una previsión constitucional igual al artículo 73 XXIX-O que atribuye al Congreso la facultad de legislar en materia de protección de datos para el sector público. Ello podría suponer que en el caso del sector público surjan leyes estatales. Por tanto, se hace también necesario abordar la regulación de los datos de salud desde el punto de vista competencial con la finalidad de garantizar una protección efectiva de la persona y evitar discriminaciones en el sentido del artículo 1 constitucional. En lo general, *vid.* Cossío Díaz JR. La controversia constitucional. México: Porrúa; 2009. p. 3 y ss.
 4. Es posible señalar que el «derecho a la privacidad» ha evolucionado principalmente en el Derecho americano desde la Sentencia del Tribunal Supremo de EE.UU. en el caso *Griswold v. Connecticut*, 381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed. 2d 510, hasta llegar a la concepción moderna del «derecho a ser dejado solo», tal y como fue enunciado también por el Tribunal Supremo en el caso *Weathon v. Peters*, 33 U.S. 591, 634 (1834).
 5. La privacidad, tal y como señalaba en España la exposición de motivos de la antigua y derogada Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, al distinguirla de la intimidad: «constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado».
 6. Al respecto, siguiendo a S. Rodotà, al hacer referencia al «hombre de vidrio»: «si una persona quiere preservar una esfera, aunque mínima, de privacidad e intimidad, y desea que nadie conozca ciertas informaciones sobre sí mismo, se convierte, según el Estado, en "alguien que tiene algo que esconder" y, automáticamente, en sospechoso, en "enemigo del pueblo". Se trata de una lógica, típica de los regímenes totalitarios, y, por tanto, contraria a la democracia». De esta manera, el tratamiento de datos personales puede llevarse a cabo con las garantías necesarias, ya que: «Los regímenes democráticos actúan (o tendrían que actuar) según lógicas profundamente distintas, basando las posibles limitaciones a la privacidad en el principio democrático». Rodotà S. Democracia y protección de datos. https://www.agpd.es/portaleswebAGPD/canal/documentacion/conferencias/common/pdfs/DemocraciaMadrid_mayo_05.pdf.
 7. «Los derechos y las libertades de la tercera generación se presentan como una respuesta al fenómeno de lo que se ha denominado "contaminación de las libertades" -*pollution des libertés*-, término con el que algunos sectores de la teoría social anglosajona hacen alusión a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías». *Vid.* García González A. La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. Boletín Mexicano de Derecho Comparado, n.º 120, septiembre-diciembre 2007, Instituto de Investigaciones Jurídicas de la UNAM.
 8. Resolución emitida por 31 autoridades de protección de datos personales y privacidad en noviembre de 2009 consensuando un estándar internacional sobre la materia.
 9. La Resolución R (73) del Comité de Ministros del Consejo de Europa pone un ejemplo de la capacidad de tratamiento, evidentemente, en la fecha (1973) de dicha Resolución, en concreto su considerando 21.
 10. A este respecto hubo mucha discusión parlamentaria, ya que la definición de un dato como sensible tiene importantes consecuencias, como la exigencia de consentimiento expreso o la inmediata elevación de las sanciones cometidas sobre un dato de estas características. En todo caso, no podrán crearse bases de datos con información que directa o indirectamente contenga datos personales sensibles, sin que se justifique la creación de dichas bases para finalidades legítimas y concretas o se trate de un mandato legal o sea necesario en virtud de los límites establecidos en el artículo 4 de la LFPDPPP, según el artículo 56 del Reglamento a la LFPDPPP.
 11. De nuevo, debe insistirse en que, cuando hablamos de datos sensibles, se incide primordialmente en el cumplimiento de los referidos principios y la adopción de medidas de seguridad. Dichas garantías se refieren, en particular, al consentimiento, que tendrá que ser expreso y por escrito por tratarse de datos personales sensibles (art. 9), salvo que concurra alguna de las excepciones legalmente previstas y a las medidas de seguridad. Y, además, el resto de principios tendrá que aplicarse atendiendo a la especial protección conferida por la Ley.
 12. Gómez Sánchez Y. La protección de los datos genéticos: el derecho a la autodeterminación informativa. En: <http://www.ajs.es/downloads/vol1604.pdf>.
 13. Álvarez González S. La utilización de datos genéticos por las compañías aseguradoras. Instituto de Ciencias del Seguro. Madrid. Fundación MAPFRE; 2006. En: <http://www.mapfre.com/ccm/content/documentos/fundacion/cs-seguro/libros/la-utilizacion-de-datos-geneticos-por-las-companias-aseguradoras-106.pdf>.
 14. Es importante considerar la anonimización de los datos en los casos en que la persona no requiera ser identificada. Dicha anonimización es la clave en cuanto al tratamiento de estos datos, siendo necesario analizar específicamente el concepto y distinguirlo de otros como el enmascaramiento de los datos que sí podría permitir la identificación de a quién se refieren.
 15. *Vid.*, en general, Rubí Navarrete J. Protección de datos clínicos. En: Protección de datos personales. Compendio de lecturas y legislación. México, D.F.: Tiro Corto; 2010. p. 115.
 16. López Ayllón S. La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo. Memorias del II Congreso Mexicano de Derecho Procesal Constitucional. México, D.F.: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México; 2007.
 17. No obstante, sí existen diferentes disposiciones que tienen relevancia en la materia, como por ejemplo el Reglamento de la Ley General de Salud, o la Norma Oficial Mexicana NOM-168-SSA1-1998, relativa al expediente clínico, entre otras, especialmente en lo relativo a la confidencialidad en el tratamiento de esta información. Y, en este sentido, el IFAI ya ha ido haciendo estudios sobre impacto a la privacidad en el expediente clínico electrónico. *Vid.* Peschard J. El IFAI como órgano garante en protección de datos personales. Compendio de lecturas y legislación. México, D.F.: Tiro Corto; 2010. p. 115. *Vid.*, también, Rodán Xopa J. Acceso al expediente médico. En: Fox J. Derecho a saber. Balance y perspectivas cívicas. México, D.F.: Fundar; 2007.
 18. Además de la normativa en protección de datos personales en el sector público y privado citada en la primera nota al pie de este artículo, destacaremos brevemente:
 - Ley General de Salud (DOF de 7 de febrero de 1984).
 - Norma Oficial Mexicana NOM-168-SSA1-1998, del Expediente Clínico (DOF de 30 de septiembre de 1999).
 19. Davara Fernández de Marcos I. Tratamiento de datos relativos a la salud. Seminario Protección de datos personales en materia de salud; CONAMED; 11 de noviembre de 2008. En: http://www.conamed.gob.mx/prensa/pdf/datos_salud.pdf.
 20. Resolución IFAI: RES/VER/06/06/2012.01.