CAPÍTULO II

DERECHO COMPARADO Y MÉXICO

2.1 La protección de los datos personales en el mundo y la historia

Suñé, en su Tratado de Derecho Informático, citado por Castro (2005), habla sobre el debilitamiento de la privacidad de una persona dentro de la sociedad de la información: "Al entrar en la era de la informática, cosa que sucederá inmediatamente después de la Segunda Guerra Mundial, el ser humano se vuelve más y más de cristal, a partir del tratamiento masivo de los más diversos datos de las múltiples acciones de su vida cotidiana, que son susceptibles de quedar, y de hecho quedan registrados en un ordenador". Esta sociedad de la información que se menciona anteriormente pone al descubierto la vida privada de las personas gracias a las herramientas tecnológicas con las que cuenta.

En 1967 se constituyó en Europa una Comisión Consultiva para estudiar las tecnologías de la información y las posibles consecuencias que podrían traer sobre los derechos de la persona. Años después, el Comité de Ministros del Consejo dictó resoluciones a los Estados Miembros en las que les recomendaba que tomaran medidas preventivas para evitar el abuso o mal uso de la informática con la creciente aparición de bancos de datos tanto a nivel privado como público (Campuzano, 2000). De esta Comisión surgió la Resolución 509 de la Asamblea del Consejo de Europa con el que inició la legislación en materia de protección de datos en Europa que después se extendería a países de otros continentes, así como los tratados y convenios internacionales.

Entre los pioneros de la protección de datos se encuentra un Estado integrado en la antigua República Federal de Alemania, Hesse, que promulgó su ley en 1970. Alemania se trató de un caso especial porque el pasado de este país hacía a los alemanes especialmente sensibles con respecto a la información que podía ser usada por la policía. En la década de los cuarenta los nazis controlaron la información de la población con los datos del censo y los archivos del gobierno, con los que identificaron a los judíos y a otros grupos. Este hecho propició que la

Constitución alemana incluyera el derecho a la privacidad. A pesar de esto, en 1970 la policía alemana usó perfiles contenidos en bases de datos para capturar a los miembros de la organización terrorista *Rote Armee Fraktion*, pero debido a que esta investigación suscitó muchas inconformidades, en ese mismo año el estado de Hesse aprobó la primera Ley de Protección de Datos (*Datenschutz*), y en 1977 el Parlamento Federal alemán aprobó la Ley Federal *Bundesdatenschutzgesetz* que, a la fecha, es de las más estrictas (Gregorio, 2004).

En 1973 Suecia se convirtió en el primer Estado soberano que estableció las Leyes de Protección de Datos (Castro, 2005).

Fue a partir de entonces que países de la Comunidad Europea comenzaron a elaborar iniciativas para que el manejo privado y público de los datos personales de sus ciudadanos fuera legalizado y controlado. Los países europeos vieron la necesidad de legislar la protección de datos: Portugal fue el primer país en constitucionalizarla en 1976, seguido por Austria en 1978, y posteriormente por España. Antes de 1980 Suecia, Alemania, Francia, Holanda, España, Austria y Luxemburgo ya contaban con leyes que cubrían este derecho (Castro, 2005). Los principios comunes que regían la protección de los datos personales de estas primeras normas europeas eran los siguientes (Ríos, 2005): justificación social, limitación de la recolección, calidad o fidelidad de la información, especificación del propósito o la finalidad de la recogida, tratamiento y transmisión, confidencialidad, salvaguardia de la seguridad, política de apertura, limitación en el tiempo, control público (implica la creación y funcionamiento de un organismo que vigile el cumplimiento de los principios contenidos en las legislaciones) y participación individual (consagra el derecho de acceso a los datos y los derechos inherentes).

En América, las reformas constitucionales sobre la protección de datos personales surgieron como una necesidad ante la presión de los intereses económicos que generan las bases de datos. Brasil, Paraguay, Perú, Argentina, Ecuador y México son algunos de los países que introdujeron su protección constitucional (unos de ellos bajo la forma de *habeas data*). De igual forma, Perú y Venezuela han percibido los riesgos de la informática y lo han incluido en sus legislaciones. Las Leyes Generales de Protección de Datos Personales que existen en Argentina, Chile, Panamá, Brasil, Paraguay y México son muy semejantes a la legislación

europea, mientras que países como Venezuela y Panamá tienen leyes sectoriales que protegen los datos personales (Gregorio, 2004).

Argentina fue pionero en establecer una legislación adecuada sobre el tema. Estados Unidos, a principios de los noventa, intentó detener la aprobación de esta ley porque agrumentaba que regular el avance de la información afectaba el desarrollo industrial y económico (Castro, 2005), a pesar de que desde 1970 en este país se había dictado el *Fair Credit Reporting Act* para regular el trato genérico de los datos personales que en 1974 dio origen al *Privacy Act*, y a pesar de que ahí Warren y Brandeis dieron inicio al derecho a la intimidad en su artículo *The Right to Privacy*, en el que exponían la necesidad de proteger de los medios de comunicación el derecho a la intimidad o los hechos de la vida privada de una persona que originó el derecho de exclusión (*the right to be let alone*), que velaba por la intimidad y la individualidad (Castro, 2005).

Por otra parte la Constitución Política de Nicaragua de 1987 señala que es derecho de todo ciudadano conocer la información que las autoridades registran sobre su persona, así como la razón y el fin por la que existe (Castro, 2005).

Paraguay establece la protección expresa de la intimidad en la manipulación de los datos personales en su Constitución, mientras que Chile aprobó en 1999 la Ley de Protección de Datos Personales que define los alcances de la protección de la intimidad en el manejo, archivo y disposición de los datos de los ciudadanos (Castro, 2005).

El artículo 15 de la Constitución colombiana afirma que las personas tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (Castro, 2005).

Canadá es un modelo en esta materia puesto que tiene políticas sobre privacidad y protección de datos dentro de un marco regulatorio en el que el gobierno no tiene un control excesivo pero tampoco hay una libre autorregulación de las empresas, a la vez que combina la legislación con políticas autorregulatorias. Así, protege los derechos de los consumidores y de los ciudadanos canadienses al tiempo que no constituye un obstáculo para las empresas. Este país optó por el consenso entre los interesados, que bien pueden ser empresarios, consumidores, organizaciones no gubernamentales, académicos, ciudadanos, etc., y emitió la

ley federal *The Personal Information Protection and Electronic Documents Act, PIPED Act*, que establece estándares mínimos de protección a la privacidad dentro del sector privado (Ovilla, 2005).

A nivel internacional diversas organizaciones han emitido lineamientos que no siempre tienen un carácter obligatorio, pero sus principios sirven como referencia para el trato de la protección de datos personales.

La Declaración Universal de Derechos Humanos de 1948 establece en su artículo 12 que: "Nadie será objeto de injerencias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En febrero de 1990, Naciones Unidas dictó los Principios rectores aplicables a los ficheros computarizados de datos personales en la Resolución 45/95 de 14 de diciembre, de la Asamblea General de las Naciones Unidas, que contenía los principios relativos a las garantías mínimas que debían prever las legislaciones nacionales y la aplicación de las directrices a archivos de datos personales mantenidos por organizaciones internacionales gubernamentales, que dejaba a la iniciativa de cada Estado los procedimientos para realizar las normas referentes a los archivos de datos personales informatizados. Entre los principios establecidos se encuentran: principio de legalidad y lealtad, principio de exactitud, de acceso de la persona interesada, de no discriminación, facultad para hacer excepciones, principio de seguridad, supervisión y sanciones, flujo transfronterizo de datos y campo de aplicación.

El Pacto de San José de la Convención Americana sobre Derechos Humanos, ratificada por México en 1981, delimita en su artículo 11 la protección de la honra y la dignidad y menciona el derecho a la privacidad, en el que inicialmente se resguardaron los datos personales:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. 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.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

De forma similar, la Convención sobre los Derechos del Niño de 1989 en su artículo 16 establece que:

1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.

2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

Por otro lado, la Organización para la Cooperación y el Desarrollo Económico creó desde 1969 el Grupo de Expertos sobre Bancos de Datos, dedicado a analizar y estudiar diferentes aspectos relacionados con datos personales y la privacidad. En el Simposio de Viena de 1977, recopiló principios básicos que reconocen: a) la necesidad de que la información fluyera de manera regulada entra los países; b) la legitimidad de los países para regular el flujo de información que pueda ser contraria al orden público o que atente contra la seguridad nacional; c) el valor económico del flujo de la información va unido con las economías de los países; d) los países deben contar con medidas de seguridad mínimas para proteger la información así como para regular sobre su protección, evitar su uso o aprovechamiento ilegítimos; y, e) los países deben comprometerse para adoptar principios generales para la protección de los datos (Reyes, 2006).

Para 1978, la OCDE creó el Grupo de Expertos sobre Barreras Transfronterizas de Información y Protección de Privacidad, que en 1980 desarrolló los Lineamientos sobre la Protección de la Privacidad y el Flujo Transfronterizo de datos Personales. A pesar de que no tenía carácter obligatorio, exhortó a vigilar la obtención y calidad de los datos y cuidar que los principios de finalidad, calidad, utilización, lealtad, seguridad y transparencia fueran respetados para la protección de la vida privada. Para garantizar la libre circulación de la información, los Estados deben asegurar su integridad, el respeto y el uso correcto en su flujo transfronterizo mediante la aplicación de sanciones y el reconocimiento de la responsabilidad jurídica de quienes controlan los datos y la exigencia de que haya transparencia en dicho control (Ovilla, 2005).

En este mismo giro, la Cooperación Económica de Asia-Pacífico (APEC) se centró en crear un marco de privacidad (*APEC Privacy Framework*) para proteger los derechos humanos y libertades fundamentales, con énfasis en que la falta de legislación en la materia genera

desconfianza en los consumidores y usuarios de las comunicaciones y otras tecnologías de la información, lo que entorpece el comercio y repercute en la economía de las naciones. Los principios de la APEC equilibran entre la privacidad de la información y la necesidad de los negocios comerciales. Dichos principios son: prevención de daño, obligación de dar aviso, límites a la recolección, uso de la información personal (finalidad), presentación de opciones, preservación de la integridad de los datos personales, seguridad, acceso, corrección y responsabilidad (Reyes, 2006).

Edith Ramírez (2010), comisionada de la *Federal Trade Commission*, expuso durante su participación en el VIII Encuentro Iberoamericano de Protección de Datos Personales que en 2007 APEC creó un proyecto formal para desarrollar un marco autorregulatorio empresarial para la transferencia de datos entre países de esta región, con protecciones de privacidad armonizadas y consistentes con sus principios de privacidad. Estas normas continúan en etapa de elaboración, pero en su reporte destacó los progresos y beneficios que otorgarán: "Bajo el sistema propuesto, compañías que quieren participar aplicarían a un agente de responsabilidad reconocido por APEC, el cual podría ser una organización de marca de confianza, firma de contabilidad o, en algunas economías de APEC, una entidad pública como la autoridad de protección de datos. Este agente examinaría las políticas y prácticas de privacidad considerando las normas internacionales de APEC y certificaría la compañía. Pueden pensar en esto como un sello de privacidad de APEC" (Ramírez, 2010).

De acuerdo con Ramírez (2010), el sistema posee un gran potencial para proveer un marco responsable y eficiente para transferencias dentro de la región. Todos los interesados en este sistema podrán beneficiarse si lo establecen de forma apropiada porque incrementa la uniformidad, los consumidores tendrán la garantía de estar protegidos por organizaciones responsables que optan por un régimen riguroso con procedimientos efectivos de resolución de disputas, y las autoridades se favorecerán por su eficiente sistema autorregulador.

En este orden de ideas, la Organización Internacional del Trabajo considera necesario garantizar el respeto de la vida privada de los trabajadores. En 1996 emitió un Informe para la protección de sus datos personales para favorecerlos como la parte menos privilegiada dentro de un contrato laboral. La OIT intenta limitar su control y vigilancia durante la jornada laboral

con las técnicas que se le aplican de video vigilancia, acceso a correos electrónicos de los empleados y rastreo (Ovilla, 2005).

También prohíbe al empleador tener datos personales sobre la vida sexual de los trabajadores, sus puntos de vista políticos o religiosos, etc., así como sus condenas penales en caso de que las haya tenido. En lo que se refiere a los datos sensibles, como información sobre la salud, deben estar bajo la supervisión de lo establecido por la ley del Estado y bajo el principio de confidencialidad médica. Todo esto con la finalidad de conservar el respeto de la vida privada y de la dignidad del empleado dentro de la empresa (Ovilla, 2005).

En 1981 se firmó el Convenio 108 del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal. En un inicio sólo fue ratificado por cinco Estados: Alemania, España, Francia, Noruega y Suecia, en la actualidad suma 47. Fue la primera norma que determinó las pautas a seguir para el tratamiento automatizado y protección de los datos de carácter personal. Pretendía ampliar la protección de los derechos y las libertades fundamentales, específicamente el derecho al respeto a la vida privada, a la vez que reafirmaba su compromiso con la libertad de información. Fue pionero en esta materia nueva de creciente relevancia, provino de una Organización acreditada en el ámbito de los derechos humanos, se proyectó sobre una norma que necesitaba ser regulada por las leyes y adquirió dimensión internacional sobre la protección de datos (Garzón, 1981).

Dicho Convenio, que entró en vigor hasta 1985, garantizó a toda persona física el respeto de sus derechos y libertades fundamentales, sobre todo su derecho a la vida privada respecto al uso automatizado de datos concernientes a su persona, y se constituyó en el primer texto internacional que conjuntaba leyes de Estados diferentes, lo que representó su armonización y un paso importante para la creación de un frente común en la protección de datos (Campuzano, 2000). Buscó conciliar el respeto de la vida privada de las personas con la libertad de la información para flexibilizar la cooperación en el ámbito internacional en materia de protección de datos y limitó los riesgos que pudieran aparecer en los huecos de las legislaciones nacionales.

Dada la complejidad que representa la protección de datos personales, el Consejo de Europa decidió seguir la técnica jurídica de adopción de recomendaciones de carácter sectorial en el

Convenio, dirigidas a los gobiernos sobre temas específicos que requieren protección. Estas recomendaciones giran en torno a temas de carácter médico, datos estadísticos, información policiaca, bancos electrónicos, seguridad social, etc., y una de las recomendaciones más recientes es relativa a la protección de la vida privada en Internet. Esta labor de colaboración entre los Estados miembros no tiene lugar en dos casos: cuando la protección de los datos personales no es equivalente en ambas partes y cuando su transmisión se realiza a un tercer Estado no miembro del Convenio (Pavón, s/f).

En la década de los noventa el mercado interior de la Unión Europea demandaba que se garantizara la libre circulación de los datos personales, debido al valor económico que poseen para las transacciones comerciales dentro de su economía global y transfronteriza. Dentro de este escenario aparece la Directiva 95/46/CE para la protección de las personas físicas frente al tratamiento automatizado de datos personales: su importancia para la configuración de una normativa común en la materia, que asienta en sus tres primeros considerandos el sentido de la norma. Así, la comunidad europea creó el mercado interior con base en el respeto a los derechos fundamentales, y la libre circulación de los datos con base en el respeto al derecho de la intimidad, considerado de gran importancia, finalidad de la Directiva 95/46/CE, de la que provienen las legislaciones de los países sobre protección de datos (Piñar, 2005).

La Directiva 95/46/CE cubrió el vacío que existía en la legislación comunitaria respecto de la protección de los datos personales y a su libre circulación entre Estados miembro. El objetivo principal de la misma no fue la unificación del Derecho sino la aproximación de legislaciones (Sánchez, 2001). La norma surgió para garantizar la protección de los derechos y libertades fundamentales de las personas físicas, sobre todo la de su derecho a la intimidad en lo que se refiere al tratamiento de datos personales. Como parte de sus aportaciones, el artículo 29 de la norma crea el grupo sobre protección de las personas en lo que respecta al tratamiento de datos personales, cuya obligación es facilitar al Parlamento Europeo y al Consejo un informe anual sobre la protección de datos personales en la Comunidad y en países terceros (Campuzano, 2000). Entre otros elementos, destacan de este Convenio los siguientes (Ríos, 2005):

a) Los sistemas de tratamiento de datos deben respetar los derechos fundamentales y libertades de las personas físicas, sobretodo, la intimidad;

b) La libre circulación de datos personales de un Estado miembro del Consejo y del Parlamento a otro Estado reclama, antes que otra cosa, la protección de los derechos fundamentales de las personas;

c) El objeto de las legislaciones nacionales en materia de datos personales debe ser garantizar el respeto de los derechos y libertades fundamentales, principalmente el derecho al respeto de la vida privada, resguardados en el artículo 8º del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, además de los principios generales del derecho comunitario, y

d) Los principios de la protección de los derechos y libertades, principalmente el de la intimidad, quedan establecidos en esta directiva que amplía y precisa los del Convenio de 1981 del Consejo de Europa para la protección de las personas, en lo que se refiere al trato automatizado de la información personal.

A quince años de su aprobación, la Directiva 95/46/CE constituye una base para la protección de datos puesto que sus principios son de aplicación y reconocimiento general. Es la norma comunitaria que ha extendido la actividad a la Unión Europea.

En noviembre de 2009, la Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el Tratamiento de Datos de carácter personal fue aceptada por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Estos Estándares Internacionales, también conocidos como la Resolución de Madrid, aportaron dos valores novedosos a la protección de datos: por una parte enfatizó la vocación universal de los principios y garantías de este derecho y, por otra, reafirmó la posibilidad de que se realice un documento con vinculación internacional que proteja los derechos y libertades individuales en una era globalizada, caracterizado por las transferencias internacionales, con el objeto de facilitar su flujo (Rallo, 2009).

En sus Disposiciones Generales, la Resolución de Madrid define a los datos de carácter personal como: “cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados.” La Resolución es aplicable a todo tratamiento de datos de carácter personal, total o parcialmente automatizados, bien pertenezcan al sector público o al privado, y establece que corresponde a

cada legislación nacional hacer que estas disposiciones no serán aplicadas a personas físicas que utilicen la información con uso exclusivo de su vida privada o familiar.

Asimismo contempla principios básicos para la protección de datos: 1) principio de lealtad y legalidad, con respeto a la legislación nacional aplicable y los derechos y libertades de las personas, de acuerdo con esta Resolución y con la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, en particular considerará desleales a el trato que promueva la discriminación contra los interesados; 2) principio de finalidad, el trato de los datos se limita a cumplir con los fines determinados, explícitos y legítimos del responsable, para hacer un trato no compatible con esto, el responsable deberá contar con el consentimiento del interesado; 3) principio de proporcionalidad, el trato de los datos debe ser adecuado, relevante y no excesivo con relación al fin, el responsable deberá esforzarse por limitar al mínimo necesario los datos personales que trate; 4) principio de calidad, los datos deben ser exactos, completos y actualizados, el responsable deberá conservarlos el tiempo mínimo necesario conforme a su finalidad; 5) principio de transparencia, el trato de los datos deberá ser transparente; y, 6) principio de responsabilidad, el responsable debe cumplir con los principios y obligaciones de la Resolución y de la legislación nacional.

En su tercer apartado, la Resolución de Madrid establece el principio general de legitimación con los supuestos bajo los cuales los datos personales podrán ser tratados y los mecanismos que deben habilitar los responsables para que los interesados tengan la oportunidad de revocar su consentimiento sin que les implique algún costo. Considera como datos sensibles a aquéllos que afectan la esfera más íntima del interesado, cuya utilización indebida pueda originar discriminación ilegal o arbitraria, o ponerlo en riesgo. El origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas, datos relativos a la salud o sexualidad están clasificados como sensibles.

En cuanto a las transferencias internacionales, éstas podrán efectuarse cuando el Estado al que se transfieran cuente con el nivel de protección señalado por la Resolución, o cuando el responsable garantice que el destinatario ofrece protección a la información. Las transferencias de darán cuando sea en beneficio o protección de un interés vital del interesado u otra persona, o para salvaguardar un interés público. En estos casos, la legislación aplicable podrá permitir

la transferencia internacional de datos a Estados que no cumplan con el nivel de protección establecido.

De la forma en que establece obligaciones para los responsables, también fija derechos del interesado: acceso, rectificación y cancelación, y oposición.

Los Estados deberán promover medidas que incentiven el cumplimiento de sus leyes en materia de protección de datos, así como establecer autoridades parciales e independientes que supervisen el cumplimiento de los principios establecidos y que cooperen entre sí en aras de proteger el tratamiento de los datos personales. En caso de que ocurra algún daño y/o perjuicio, tanto moral como material, causado a los interesados, que haya violado la legislación en protección de datos, la persona responsable será determinada y sancionada a menos que pueda demostrar que no se le puede atribuir el daño.

La Resolución de Madrid fue el resultado de los esfuerzos que realizan diferentes naciones para fijar pautas internacionales que beneficien a los Estados para asegurar la protección de los datos personales y asimismo facilitar su transferencia de forma segura. Entre sus principales aportaciones está el principio de responsabilidad y cabe destacar que no diferencia entre datos públicos o privados, más bien se enfoca en el carácter sensible de la información.

En general, los lineamientos en los convenios están marcados por principios internacionales de protección de datos, que son: finalidad, existencia de un derecho de información, derechos de acceso, rectificación y información a los titulares de estos datos, la creación de reglas especiales que protejan los datos sensibles y a los consumidores, un límite para la obtención de datos personales, el derecho de pedir que se borren los datos de las listas y la creación de una autoridad de protección de datos, con una política transparente, salvo los casos relacionados con la seguridad nacional, el orden público o la salud pública. Todos los acuerdos logrados a nivel internacional cobran importancia porque buscan establecer igualdad y cooperación entre los Estados para beneficio mutuo, los obligan a cumplir y crear mecanismos de regulación en sus legislaciones que contengan principios básicos, generan responsabilidad y hacen posible la transferencia necesaria para el desarrollo de distintas actividades mediante acuerdos.

Sin embargo, José Manuel de Frutos (2010) identificó dos clases de desafíos que enfrenta la protección de datos personales en su ponencia sobre la protección de datos desde el modelo europeo:

> Por un lado, los impactos de las nuevas tecnologías. Cito aquí a título de ejemplo las redes sociales, la publicidad personalizada que cada vez es más frecuente, sobre todo en los ámbitos *on line* o de comercio electrónico, en los tratamientos de datos que se hacen en la nube del *cloude computing* que están planteando cada vez mayores cuestiones, las identificaciones para radiofrecuencias o técnicas de RCAD y luego los temas de biometría, los controles de personas vía ADN, etcétera; los temas de globalización y los flujos de datos transfronterizos. Existe también una tendencia cada vez mayor a proceder a técnicas de outsourcing en su contratación para facilitar el tratamiento de datos personales, que suelen ser contrataciones a niveles internacionales y, por tanto, plantean desafíos interesantes que hay que ver cómo se pueden resolver.
>
> Y luego hay otros tipos de desafíos que no son específicos de la Unión Europea, pero en los que la Unión Europea está siendo especialmente sensible, por un lado, los fallos de seguridad y el robo de identidad plantean muchos problemas hoy en día, y hoy en día los ciudadanos son más sensibles cuando saben que sus datos han sido perdidos… Las autoridades policiales cada vez pretenden tener acceso a datos que se han recogido y recabado con fines específicamente comerciales y que pueden generar información útil y muy válida para sus investigaciones… para una finalidad totalmente distinta de la que fueron inicialmente recogidos. Además, estos datos comerciales que se recogen para finalidades específicamente comerciales… Suelen ser objeto de comunicación internacional. Con lo cual, los datos que eran en un principio puramente nacionales de un estado miembro, son recogidos por la policía de un estado para ser transferidos a otra policía de otro estado miembro para fines puramente policiales. Esto plantea problemas porque los niveles de protección de datos entre las autoridades de policía y de los Estados es diferente, y el sector policial no tiene una normatividad unificada…, contrario a lo que ocurre con la del sector comercial.

Estos dos desafíos no son únicos de la Comunidad Europea. Bajo sus propias circunstancias, cada país debe resolver de la mejor manera posible la cuestión referente a las tecnologías de la información sin caer en la excesiva regulación que impida la transferencia de datos necesaria para el desarrollo de distintas actividades. Se trata de establecer un balance y generar conciencia para la autorregulación y la autoprotección. El caso de la investigación policiaca

que menciona Frutos es algo a lo que también se enfrentan los países americanos en sus distintas vertientes dependiendo de sus casos específicos: combate de narcotráfico, lavado de dinero, crimen organizado, combate de grupos armados, etc. Por esto, corresponde también a los países americanos tomar cartas en el asunto para que la información de sus habitantes no sea expuesta.

Para concluir, Frutos (2010) identificó algunos objetivos de la Unión Europea en materia de protección de datos personales:

1. Establecer un régimen global aplicable a todo el tratamiento de datos en la Unión, que incluya al sector policial y de orden público.
2. Reforzar los derechos de los individuos en todas las operaciones de tratamiento de datos, ya sean comerciales o de autoridades de orden público.
3. Reforzar los mecanismos de protección y de garantía al cumplimiento de la protección.
4. Aclarar el contenido de algunos principios y nociones que se plantean en la directiva o en la normativa europea, como el principio de responsabilidad, la "*contability*", que es un concepto en inglés bastante desarrollado por el sistema canadiense, pero no en el europeo.

Estos objetivos planteados por Frutos no deberían ser únicos de la normativa europea sino de todos los países que intercambian información personal, o bien de un régimen global iberoamericano que refuerce los derechos de las personas bajo principios comunes.

2.5 España

España es uno de los países que más ha contribuido al desarrollo y difusión del derecho a la protección de datos personales. A pesar de que ha tenido desatinos también ha estado acompañado de aciertos que lo enriquecen por su misma experiencia.

El derecho a la intimidad en España está garantizado en el artículo 18.4 de su Constitución de 1978: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Sin embargo, el derecho a la protección de datos apareció como un derecho autónomo e independiente de la mano de las sentencias 290 y 292 del Tribunal Constitucional: la primera ratificaba la constitucionalidad de la Agencia Española de Protección de Datos, competente en todo el país, como garante del

derecho, encargada de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial respecto a los derechos de información, acceso, rectificación y cancelación. La segunda configuró el reconocimiento del derecho a la intimidad y privacidad, y el derecho a la autodeterminación informativa. Reconoce también que el derecho fundamental a la protección de datos personales proviene de la Constitución y debe ser considerado como un derecho autónomo e independiente (Piñar, 2005).

En resumidas cuentas, esta sentencia admitió el derecho a la protección de datos como autónomo e independiente del derecho a la intimidad, determinó su contenido esencial y fue relacionado con los artículos 18.4 y 10.2 de la Constitución española, a la vez que citaba instrumentos internacionales, como la Carta Europea de Derechos Fundamentales que recién había sido adoptada. Junto con la LORTAD de 1992 y la Ley Orgánica de Protección de Datos de 1999, conforman lo más representativo en protección de datos en España (Piñar, 2005).

2.5.1 LORTAD

Para la legislación española, la Ley Orgánica 5/1992 de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) llegó tarde y llena de errores. Tarde porque desde que se promulgó el artículo 18.4 de la Constitución y desde la obligación adquirida con el Convenio de 1984 con el Consejo de Europa, España debió haber establecido una norma que tutelara las libertades informáticas. Con errores porque se esperaba que el retraso otorgara el beneficio de haber aprendido de experiencias previas del Derecho comparado y no fue así. La LORTAD presenta deficiencias en su creación (Pérez, 1992).

El objetivo de la LORTAD fue garantizar los derechos y libertades de las personas físicas, especialmente su intimidad, frente al uso de la informática. Para el cumplimiento de este fin, estructuró un sistema de garantías y medidas recogidas del Derecho comparado en materia de protección de datos personales y, particularmente, optó por el modelo de las leyes de tercera generación, que se han encargado de la revolución microinformática y los bancos de datos y se extienden a la dinámica de su uso o funcionalidad (Pérez, 1992).

Esto último quiere decir que no se limita a su tutela como meros depósitos de información, sino que abarca la protección de los datos personales como una globalidad de procesos o aplicaciones de informática que pueden llevarse a cabo con los datos almacenados susceptibles

de modificar el perfil personal cuando se conectan entre sí (Pérez, 1992). El perfil se refiere a la reputación o fama expresada en el honor, puede ser valorado favorable o desfavorable para diferentes actividades públicas o privadas, la obtención de un empleo, la adquisición de un préstamo, etc. La función de la LORTAD fue tutelar la calidad de los datos pero no en sí mismos, sino en función de evitar que su informatización permita o dé lugar a ciertos actos discriminatorios (Pérez, 1992).

La LORTAD estuvo integrada por 48 artículos distribuidos en siete títulos, tres disposiciones adicionales, una transitoria, una derogatoria y cuatro finales. Pérez Luño (1992) hizo un análisis de los aspectos más polémicos de la LORTAD y la confrontó con otras legislaciones de datos personales, de acuerdo con esto:

1. La LORTAD se inclinaba por un sistema mixto que conjuga una disciplina unitaria con marco jurídico adaptado a los requerimientos de ciertos aspectos jurídicos (responsabilidad, penal, archivos públicos, etc.) o tecnológicos específicos (telecomunicaciones, transferencias electrónicas…). Sin embargo, no resuelve los problemas de concordancias, reiteraciones y contradicciones que surgen en este sector de ordenamiento jurídico. Cuando la ley entró en vigor coexistió con leyes sectoriales y dispersas (en materia civil, penal, tributaria, sanitaria, etc.) que contenían disposiciones sobre el uso de la informática y los derechos fundamentales (Pérez, 1992).

   Era conveniente que la LORTAD estableciera un orden en las reglamentaciones sectoriales y dispersas que existían en materia de protección de datos ya que ocasionaron problemas legislativos (Pérez, 1992).
2. Una técnica legislativa de cláusulas o principios generales es aconsejable para regular materias que, como la informática, ocurren en muchos cambios e innovaciones tecnológicas. Una reglamentación legal flexible evita modificar continuamente las normas, a la vez que permite a los órganos encargados de su aplicación adaptar los principios a los casos presentados (Pérez, 1992).

   Aparentemente la LORTAD tenía esa orientación puesto que se trataba de un texto de principios básicos y gran parte de su contenido es reglamentario. Desarrollar esas reglamentaciones demora la entrada en vigor de un sistema que proteja la información personal. Tampoco pueden hacerse de lado las facultades normativas generales y

facultativas que favorecen a la Agencia de Protección de Datos. De la misma manera, la independencia otorgada a los ficheros del sector privado con la posibilidad de crear códigos deontológicos facilita que los principios básicos de la LORTAD se adapten a las innovaciones de la tecnología (Pérez, 1992).

3. La LORTAD adoptó un modelo de tutela estática, basado en la "calidad" de las informaciones en función de los datos sensibles, en combinación con la tutela dinámica centrada en el control de los programas y su uso, mediante la Agencia de Protección de Datos. Con respecto a la tutela estática, la LORTAD erró en haber tipificado las informaciones especialmente sensibles en torno a la ideología, religión o creencias, tal como lo manifiesta el artículo 16 de su Constitución, cuando era más conveniente tomar como referencia el artículo 14 que previene de actividades discriminatorias por nacimiento, raza, sexo, religión, opinión o de cualquier otra índole (Pérez, 1992).

   Con respecto a la Agencia de Protección de Datos, Pérez (1992) la define como uno de los aspectos más negativos e insatisfactorios de la Ley. Primero por la destacada "absoluta independencia" de su Director. En el Derecho comparado, el Director no lo nombra el Parlamento sino el Gobierno, y el reporte anual, que en otros casos se presenta ante las Cámaras representativas, el español debía hacerlo ante el Ministerio de Justicia. Esto condicionaba la neutralidad y credibilidad de la Agencia (Pérez, 1992).
4. La LORTAD conjugaba la protección de datos personales almacenados en bases de datos públicas y privadas y establecía sistemas de garantías diferentes. La mayor objeción que podría tener la Ley en este punto recae en la debilidad del sistema de tutela de las bases de datos privadas con respecto a las públicas porque, mientras que a las segundas se les exigía una norma general sometida a la jurisdicción y al control y tutela de los órganos públicos de los que dependan, así como al Defensor del Pueblo estatal y a la Agencia de Protección de Datos, las bases privadas sólo están bajo la supervisión de la Agencia. La LORTAD prevé la posibilidad de que las garantías se extiendan a los ficheros convencionales, sin embargo, lo deja en decisión del Gobierno con previo informe del Director de la Agencia (que es un delegado gubernativo) (Pérez, 1992).
5. El ámbito de tutela puede ser para las personas físicas o ampliarse a las personas jurídicas. En el Derecho comparado se observa el primer caso en mayor medida. Esto ocurre porque esta legislación fue creada para proteger la intimidad y las libertades individuales, pero a

> medida que los procesos de datos se proyectan a las empresas, instituciones y asociaciones, se vislumbra más la necesidad de incluir a las personas jurídicas en el régimen que impida o repare daños ocasionados por el uso incorrecto de la información. En otras palabras, la defensa de la intimidad y los demás derechos fundamentales no debe ser exclusiva de los individuos, sino extenderse a las agrupaciones sociales en las que las personas se desenvuelven. De aquí proviene la exigencia de reconocer a las personas colectivas el derecho a la protección de la información que sea de su referencia. Es tendencia de los derechos de tercera generación ampliar las formas de titularidad (Pérez, 1992).
>
> La LORTAD, igual que los ficheros manuales, preveía la posibilidad de ampliar su sistema de protección para las personas físicas, a las jurídicas. Sin embargo, después del debate del Parlamento, el proyecto se suprimió y no se incluyó en su texto final (Pérez, 1992).

Pérez Luño (1992) dedica especial atención a otro punto en el que la LORTAD no cumplió con las expectativas. Se trató de los "ficheros peceras". El "síndrome de pecera" se refiere a la psicosis de las personas por saber que viven atrapados dentro de cristal, que todas sus acciones pueden ser controladas y que su perfil puede ser construido mediante el cruce de información. Por esto, con el fin de arreglar esta situación, era conveniente que las bases de datos de quienes explícitamente no querían que su intimidad fuera tutelada con respecto al tráfico de datos personales se llamaran ficheros pecera y no "ficheros Robinson", cuya diferencia radica en que éstos últimos debían inscribirse aquellos ciudadanos que no quisieran ver su privacidad invadida por propaganda no deseada y estar libres del mercado de los archivos de información. La objeción de los ficheros Robinson es que los ciudadanos tuvieran que inscribirse en un archivo adicional de datos para que sus derechos y libertades fueran respetados dentro de un sistema democrático que, en teoría, garantizaba y velaba por el derecho a la intimidad.

La propuesta de solución que ofreció la LORTAD a esta situación no fue suficiente. En su artículo 22 exceptúa a su ámbito de tutela: "A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales". También establece en el artículo 29 que las empresas que recopilan direcciones, reparten documentos, publicitarias o de venta directa únicamente utilizarían listas informatizadas de nombres y direcciones de personas físicas cuando aparezcan en documentos a los que el

público tiene acceso, que fueron facilitados por los afectados o fueron obtenidas con su consentimiento, y que podían ser dados de baja de esos ficheros mediante una solicitud (Pérez, 1992).

En cuanto a las fallas que presentadas en estos artículos de la LORTAD, Pérez Luño (1992) destaca dos que considera más importantes. Primero, la LORTAD contradice el principio fundamental en la protección de datos que es la finalidad, plasmado en el artículo 4.2 de la misma. Esto es porque la información recabada y publicada en función de intereses colectivos y sociales no puede ser almacenada ni utilizada para fines privados comerciales, ajenos a los que justificaron su creación y publicidad. Segundo, en alusión a los ficheros Robinson, la LORTAD invierte erróneamente la carga de la responsabilidad porque establece que el ciudadano sea quien sea quien salvaguarde su vida privada, cuando las empresas deberían probar que tienen el consentimiento previo de todas las personas registradas en su información comercial.

Entre los aspectos que Pérez Luño (1992) menciona como más inquietantes de la LORTAD, destacan las constantes y significativas excepciones que limitan el alcance práctico en el ejercicio de las libertades informáticas. Estudiosos de los derechos fundamentales critican la práctica que desvirtúa los textos normativos que, después de reconocer solemnemente las libertades, limitan su ejercicio con un régimen de excepciones y limitaciones. En este sentido, la LORTAD, después de proclamar garantías que protegen los datos y los derechos de las personas, establece excepciones significativas referentes a: la información de los afectados (art. 5.3), a su consentimiento (art. 6.1), a las garantías de los datos sensibles (art. 7.3), a la posibilidad de que las Fuerzas de Seguridad del Estado puedan hacer uso de los datos sensibles sin control judicial, fiscal o de la propia Agencia (art. 20.2 y 3), a las restricciones impuestas al ejercicio de los derechos de acceso, rectificación y cancelación de las bases de datos públicas, así como a los límites del derecho a la información de los ciudadanos referentes a la recopilación de sus datos por parte de Administraciones Públicas por razones tan vagas como “las funciones de control y verificación” de las mismas, así como someter la tutela a todo lo relacionado con la defensa nacional, seguridad pública, persecución de infracciones penales o administrativas, interés público o de terceros que son más dignos de protección (art. 22.1 y 22). Estas excepciones pueden afectar la esencia de la garantía que la

Constitución española reconoce en su artículo 18.4, mismo que debe ser respetado de acuerdo con lo establecido con el Convenio 108, por lo que, cualquier divergencia determina una antinomia en el ordenamiento español.

Por otro lado, no todo lo establecido en la LORTAD fueron aspectos negativos, esta Ley constituyó un logro para proteger la información de las personas. Entre lo más significativo está la definición de los principios básicos: calidad de los datos, la transparencia, el consentimiento, la tutela reforzada de los datos sensibles, la seguridad, el secreto y la cesión. Otro aspecto positivo consiste en la tutela de la libertad informática, que garantiza a los ciudadanos las facultades de información, acceso y control de sus datos contenidos en las bases de datos, referente al *habeas data* de las sociedades tecnológicas correspondiente al *habeas corpus* en los derechos de la primera generación (Pérez, 1992).

2.5.2 Ley Orgánica de Protección de Datos

La Ley Orgánica 15/1999 de protección de datos de carácter personal regula los principios, la garantía de ejercicio y la tutela del derecho fundamental a la protección de datos. Sustituyó a la Ley Orgánica 5/1992, LORTAD, considerada como compleja y de no fácil aplicación. El legislador español presenta la Ley Orgánica como un producto legislativo nuevo, sin mencionar que también fue realizada en virtud de la obligación que le impuso la Directiva 95/46/CE. De acuerdo con Sánchez Bravo (2001), esta nueva Ley Orgánica inició incumpliendo una norma comunitaria porque no hace referencia a la Directiva, según lo establecido en el artículo 32.1, segundo párrafo, que cita: "Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial". En otras palabras, la norma española, que debería introducir la Directiva, comienza, de forma no explícita, vulnerándola.

A pesar de que la nueva regulación española fue aplaudida por lo "avanzada" y "europea", Álvaro Sánchez (2001) enumeró diez cuestiones que, en común acuerdo con demás expertos sobre la materia, son prueba de algunas deficiencias que presenta la legislación:

1. En cuanto a su ámbito de aplicación, mantiene la diferenciación entre los ficheros públicos y privados. Consolida lo señalado por la Exposición de Motivos de la antigua LORTAD, que explicaba en su apartado 4, párrafo segundo, haber establecido esta clasificación "toda

vez que, con evidencia, resulta más problemático el control de los de titularidad privada que el de aquéllos de titularidad pública". Sin embargo, lo anterior no está expuesto en la Directiva 95/46 porque su fin era establecer un régimen igualitario de protección sin importar la titularidad de los ficheros, pues recae en la figura de quien es responsable del tratamiento de los datos, independientemente si se trata del sector público o del privado (Sánchez, 2001).

Por otro lado, Sánchez (2001) menciona que no es el carácter público del fichero, ni su acceso, lo que pone en peligro la intimidad de las personas, sino el uso que se hace del mismo, con quebranto al principio fundamental de la finalidad del tratamiento que contiene la norma.

Que el fichero sea público no significa que los datos que contiene sean públicos. Y en lo referente a los ficheros públicos, Álvaro Sánchez (2001) cita a Pérez Luño: "las agresiones de este sector (privado) no son menores que las que provienen del poder, por lo que la diferencia de regímenes de protección no tendría por qué traducirse en merma de los instrumentos de garantía frente a los abusos perpetrados desde la espera de los grandes interese económicos privados".

2. En las definiciones contenidas en el artículo 3 no incluye el concepto de *terceros*, que sí aparece en la Directiva en el artículo 2, punto *f)*, que los conceptúa como personas físicas o jurídicas, con excepción del interesado, del responsable del tratamiento y de las personas autorizadas para tratar la información, ya sea bajo su autoridad directa o por su cuenta.

   Al recoger la posibilidad de cesión de datos, no señalaba quiénes eran considerados como terceros, independientemente del cedente y cesionario. Sobre todo cuando la cesión de los datos generalmente la realiza el responsable del tratamiento al margen de los fines para los que el cedente (afectado) los otorgó.

   En este orden de ideas, la Directiva de 92 estableció precisiones respecto a entidades y empresas de gestión y actividades descentralizadas, que pueden ser consideradas para interpretar la nueva regulación. De esta manera, las personas que laboran en otra empresa, aunque sea parte del mismo grupo, generalmente deberían ser consideradas como terceros. Por otro lado, las sucursales de los bancos situadas bajo la autoridad directa de la sede que hacen uso de la información de su clientela, no deberían considerarse terceros. Lo mismo

ocurre con los agentes de seguros, pero en lo referente a los representantes, la situación puede ser diferente de acuerdo con el caso (Sánchez, 2001).

Sánchez (2001) argumenta que también excluye la noción de *destinatario*, mencionado por la Directiva 95 en su artículo 2, que lo define como la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, sea un tercero o no. Comparable con la figura del "cesionario" de datos personales, "útil para garantizar la transparencia de los tratamientos con respecto a las personas afectadas".

3. Sánchez (2001) también destaca como sorprendente la generosidad expuesta en el art. 3 apartado *j)* con respecto a los grupos de profesionales. Considera accesibles al público, a la vez que prácticamente excluye de la protección de la legislación española, a: "las listas que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo". La propia Ley 15/1999 establece en su artículo 15 como primer derecho de las personas no verse sometidas a apreciaciones basadas en el tratamiento de datos que evalúan determinados aspectos de su personalidad. Esta amplitud constituye un desfase legislativo que recae en un régimen no protector. La infinita información que puede tratarse de los profesionales permite la elaboración de perfiles con datos accesibles al público.
4. El derecho a la libertad informática incluye que el afectado puede decidir cuándo terceros pueden tener acceso a sus datos personales. Si su consentimiento es requisito para que se realice un tratamiento automatizado de los datos, el consentimiento debería ser libre tanto al momento de otorgarlo, como para revocarlo. Hecho contrario sería desposeerlo del contenido esencial de sus derechos y dar marcha atrás en cuanto a la disposición de su propia información (Sánchez, 2001).

   El artículo 6.3 de la Ley Orgánica no deja ver de forma clara el requisito suplementario para ejercer el derecho a la revocabilidad del consentimiento. Al igual que la Directiva 95, en su momento también fue muy criticada porque, de acuerdo con profesionales en la materia, cualquier tratamiento exigía el consentimiento previo del interesado, lo que suponía un obstáculo para sus actividades económicas o mercantiles. Ante esta situación, la Ley optó por incluir el derecho, pero le restó su valor como manifestación de la autodeterminación informativa.

5. La Ley abre, en el artículo 7.3, una puerta al tratamiento de datos sensibles que se refieren al origen racial, la salud y la vida sexual, cuando lo establezca una ley, por motivos de interés general. En este sentido, las críticas apuntan hacia lo abstracto e indeterminado del interés general que, lejos de aclarar la duda, permite el uso de esta información. Se trata de una regulación que restringe un derecho individual sin ver cuáles podrían ser los alcances de esta excepción (Sánchez, 2001).

   De acuerdo con la Comisión de las Comunidades Europeas, interés general puede englobar todas aquellas medidas que salvaguarden los valores fundamentales de una sociedad democrática, expresado en términos similares por el Consejo de Europa. Sin embargo, la concurrencia de ese interés general debe constar en una Ley, porque en la existente no se afirma cuál es su rango normativo. También sería conveniente precisar cuáles datos pueden ser tratados, quiénes serán los destinatarios, la cualificación del responsable del tratamiento, las personas autorizadas para acceder, las garantías contra los abusos y los accesos no autorizados. Todo esto con el fin de salvar las garantías de los ciudadanos establecidas por los Estados democráticos con Derecho (Sánchez, 2001).

   El apartado 6 del mismo artículo posibilita el trato de datos sensibles referentes a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, entre otros, para los servicios sanitarios. Sánchez (2001) califica esta inclusión como fuera de lugar porque estarán orientados al desempeño de funciones administrativas. Para compensar, como mecanismo corrector y protector, acude al secreto profesional y asume lo señalado por la Directiva en su artículo 8.
6. Por otro lado, el artículo 15.3 establece que el derecho de acceso sólo podrá ejercerse en plazos de doce meses, a menos que el interesado demuestre un interés legítimo. Esta regulación resulta lesiva porque en el plazo de un año los datos pueden ser modificados o alterados y su uso puede ser incorrecto, excesivo o inexacto. Sin embargo, este precepto fue resultado de las presiones de los diferentes sectores que quisieron evitar peticiones masivas de acceso y que para ellos constituye un freno a sus actividades (Sánchez, 2001).
7. La posibilidad de cesión de datos entre las Administraciones públicas y la consagración de la excepción del consentimiento de los afectados en este caso (arts. 21.1 y 22.4), fueron declaradas inconstitucionales porque están al margen de todo procedimiento de control (Sánchez, 2001).

8. Los ficheros creados por los Cuerpos y Fuerzas de Seguridad (art. 22) desprotegen especialmente a los ciudadanos porque:
   a) Los datos de las personas pueden ser recogidos y tratados sin su consentimiento. La apelación que hace al peligro real para la seguridad pública no cubre las exigencias de legalidad puesto que vigilar en secreto a los ciudadanos no es tolerable, según el Convenio, más que en la medida estrictamente necesaria.
   b) Los datos sensibles pueden ser tratados bajo el amparo de los fines de una investigación concreta, sin establecer ningún control por parte de la Agencia de Protección de datos, y tampoco existe otro requisito para establecer alguna garantía.
   c) La cancelación de los datos la determina el responsable del tratamiento, quien decidirá cuando ya no sean necesarios. Asimismo, las circunstancias "objetivas" que establece la posibilidad del trato, generalmente se tratan de fines de una investigación concreta, que debería comprender tanto la investigación del delito como su persecución. Sin embargo, aunque esto pareciera lógico para proteger la seguridad pública, desarticula el sistema de garantías de los ciudadanos. Por otro lado, los responsables del tratamiento deciden unilateralmente cuándo deben ser utilizados, así como el ámbito material y temporal de su uso.

   Finalmente, Sánchez (2001) argumenta que el problema no radica en la derogación de los derechos de los ciudadanos, sino en la consolidación de medidas arbitrarias.
9. El artículo 23.2 priva de los derechos de acceso, rectificación y cancelación ante las bases de datos de Hacienda Pública. Las obligaciones tributarias ni las inspecciones pueden ser impuestas para desproteger los derechos de los ciudadanos, pues entra en arbitrariedad. En el marco de una investigación inspectora o sancionadora, el ciudadano debería poder conocer toda la información para su defensa.
10. Los ficheros de insolvencia familiar establecidos en el artículo 29.2, deja en manos del acreedor la posibilidad de incluir en el fichero los datos del supuesto deudor, que pone en entredicho no sólo su intimidad, sino su honorabilidad. También resultan exagerados los seis años que los afectados pueden permanecer en el registro para enjuiciar su solvencia económica.

Todas estas observaciones de Pérez Luño y Sánchez enriquecen el conocimiento en materia de datos personales y contribuyen al estudio y análisis de las nuevas leyes mexicanas. La

legislación y quehacer español en materia de datos personales ha sido fuente de inspiración y ejemplo para su tratamiento en nuestro país. Es necesario recordar que, efectivamente, los derechos a la vida privada y a la protección de los datos personales forman parte de los derechos fundamentales, sin embargo, estos derechos no deben representar un bloqueo absoluto a la información personal ya que entonces, en determinados casos, se podrían violar otros derechos fundamentales y no contribuir con un interés común. Por esta razón, en la línea frágil en donde oscila el límite de lo público y lo privado, los intereses protegidos por las leyes en ocasiones obligan a decidir a favor de los titulares y su capacidad de ejercer el derecho de protección a su información, y en otras deberá optar por hacerla pública o prescindir del consentimiento de su titular.

2.5.3 Sector Salud

En España, los datos de salud son especialmente protegidos y tienen un sistema de protección reforzado en el consentimiento expreso, es decir, una habilitación legal que puede fundamentar su tratamiento, así como medidas de seguridad de máximo nivel y un régimen de infracciones y sanciones cualificado. Jesús Rubí, en su ponencia dentro del VIII Congreso Iberoamericano de Protección de Datos Personales (2010), abarcó tres temas principales en cuanto a los datos de salud: historia clínica, estudios epidemiológicos e información sanitaria.

La historia clínica tiene un conflicto de derechos puesto que, de acuerdo con la experiencia española, concurre con los titulares de los datos y con terceros. En este sentido, Rubí (2010) explica que el titular tiene derechos de autonomía, protección de datos y tutela judicial efectiva, así como los profesionales sanitarios tienen derecho de acceso a la historia clínica para garantizar asistendia adecuada al paciente y un derecho adicional que es la reserva a sus anotaciones subjetivas. Por su parte, la administración sanitaria también puede acceder legítimamente a la información clínica con distintos fines: epidemiología, investigación, docencia, inspección y evaluación de la calidad. Finalmente, hay terceras instituciones que no están dentro del sector sanitario y pueden acceder a la historia clínica, como los jueces y tribunales, la fiscalía, la defensa del pueblo y la policía judicial en investigaciones criminales. El equilibrio entre estos derechos se obtiene mediante los principios de protección de datos, que son: consentimiento, posibilidad de excepciones legales, información, concretar la finalidad, reglas de proporcionalidad y calidad de datos, y de seguridad y secreto (Rubí, 2010).

En estudios epidemiológicos no son necesarios datos personales sino disociados y hay un abanico importante de situaciones y legitimación. Uno de los principales problemas a los que la legislación española se ha enfrentado en la práctica es el ejercicio de derechos sobre la información sanitaria porque integra normas de la Ley de Protección de Datos y de la Ley de Autonomía del Paciente. El titular de la historia clínica tiene derecho de acceso, rectificación –limitado no en cuanto a los datos identificativos sino en lo referente a los diagnósticos que dependen de la práctica profesional-, cancelación y oposición –limitados también por el interés general para conservar la historia clínica con fines de epidemiología, investigación, evaluación de la calidad, etc. (Rubí, 2010).

En cuanto a la historia clínica electrónica, Rubí (2010) manifiesta la necesidad de que haya un mecanismo de identificación viable de los accesos por parte de los pacientes o de los profesionales con diferentes niveles de acceso puesto que determinada información sensible debe ser accesible para algunos profesionales. Cuando se trate de transferencias internacionales de datos, por ejemplo para pedir una segunda opinión en un centro de otro país, se requiere el consentimiento expreso y se utilizan mecanismos alternos, como el anonimato o el uso de seudónimos con las medidas de protección y seguridad adecuadas. Para esto último, la Ley de Cohesión y Calidades del Sistema Nacional de Salud prevé la posibilidad de realizar intercambios electrónicos de información para asistencia del paciente sin que sea necesario su consentimiento siempre que existan redes seguras, certificación electrónica, firma electrónica y cifrado (Rubí, 2010).

La inspección sanitaria es otro de los riesgos asociados al acceso a la historia clínica en España. Ésta debe estar limitada a las actuaciones necesarias para el objeto de la inspección, y los datos deben ser proporcionados, adecuados, pertinentes y no excesivos, tampoco puede llevarse la historia clínica, únicamente la información o una copia, y quien accede a ella debe guardar secreto y utilizar los datos con niveles de seguridad (Rubí, 2010).

Otro riesgo lo representa la jurisdicción puesto que no hay evaluación de la proporcionalidad y no se define qué partes de la historia clínica puede ser adecuada para determinado objeto y cuáles no, y la Agencia de Datos española no tiene competencia para impedir el envío de la historia clínica, sin embargo ha firmado un convenio con el Consejo General del Poder Judicial para que los jueces reflexionen sobre la proporcionalidad y qué datos pueden utilizar

(Rubí, 2010). En materia de datos genéticos existe la polémica sobre si son datos personales o no, pero la Ley de Investigación Biomédica marca criterios para definir cuándo soy datos personales y cuándo no. Si los datos son disasociables entonces no se trata de datos personales, ni siquiera las muestras, los datos genéticos o las actuacianes que se hagan de ellos (Rubí, 2010). Esta ley también prevé la existencia de biobancos.

La complejidad del sector salud enfrenta retos no únicamente en España, en México también existen dificultades similares relacionadas con el expediente clínico, los derechos del paciente y algunas limitantes, como la salud pública. Es importante conocer y aprender de las experiencias de otros países y foros como el Encuentro Iberoamericano son medios excelentes para este fin porque contribuyen a generar conocimiento a partir de las prácticas realizadas.

2.5.4 Mecanismos sancionadores

Artemi Rallo Lombarde (2010), director de la Agencia Española de Protección de Datos, explicó, durante su participación en el VIII Encuentro Iberoamericano de Protección de Datos, que: "el régimen sancionador previsto en la LOPD tiene mucho que ver con lo que nosotros consideramos y calificamos el alto crecimiento de la cultura y del cumplimiento de la Ley de Protección de Datos por parte fundamentalmente de la industria y de las empresas". Rallo lo llama la psicología de la sanción por el éxito que ha tenido como garantía del cumplimiento de la ley.

El sistema sancionador previsto por la ley española contiene tres categorías: leves, graves y muy graves, con escalas de 600 a 60 mil euros, 60 mil a 300 mil y de 300 mil a 600 mil euros, respectivamente, de acuerdo de la gravedad de las infracciones de la ley en función de la tipología. En 2009, por ejemplo, la Agencia sancionó 33 muy graves, 527 graves y 122 leves, de las cuales 621 fueron a entidades privadas y sólo 71 a administraciones públicas (Rallo, 2010).

Rallo (2010) admite que, a pesar de los resultados, las multas son un tema cuestionado en España por muchos sectores, pero únicamente se imponen a entidades privadas. Tradicionalmente la agencia nunca ha sancionado económicamente ni ha multado a las administraciones públicas que quebrantan la ley de datos, sino que declara que existe una

infracción, le formula algunas recomendaciones para que corrija las causas de la infracción y lo hace del conocimiento del defensor del pueblo.

Por otro lado Rallo (2010) comenta que cuando la Agencia percibe una cualificada disminución de antijuridiciato de culpabilidad en el infractor puede reducir su sanción y saltar al rango inferior de las sanciones potenciales. Es decir, a una infracción que podría ser grave se le impone una leve si se identifica que derivó del error y no tenía una intención declarada. La Agencia ha utilizado este mecanismo de manera significativa en los últimos años en un porcentaje de 30 a 35 de sus sanciones, por la experiencia que han tenido basados en los errores que las empresas cometen debido a las herramientas tecnológicas.

Las sanciones que impone la Agencia no están basadas únicamente en función de la ley de protección de datos, sino también de la Ley de Sociedades de Servicio de la Información por SPAM y la Ley General de Telecomunicaciones.

Los sectores de los que reciben más denuncias, muchas de las cuales no requieren sanciones sino únicamente la garantía efectiva de los derechos de ARCO, se encuentran: telecomunicaciones, entidades financieras, video vigilancia, administración pública, *spam*, marketing, etc. En los últimos años han recibido más denuncias en el ámbito de internet en demanda del derecho al olvido, relacionadas con redes sociales, videos en *youtube* y casos similares. De la misma manera, la Agencia también recibe solicitudes de tutela de los derechos de acceso, rectificación, cancelación y oposición provenientes de quejas relacionadas la publicidad y el marketing *on line*.

En este sentido la ley mexicana también optó por un sistema sancionador, será interesante saber cuáles son los sectores generadores de mayor número de consultas o denuncias puesto que eso podría sugerir posibles reformas futuras a las legislaciones. Es posible también que, con base en su propia experiencia, México aplique el mecanismo para reducir las sanciones cuando el caso lo amerite.

2.6 Argentina

Específicamente en Argentina, la reforma constitucional de 1994 que contempló el *habeas data* planteó casos que solicitaban eliminar o corregir datos personales bajo el argumento de

que con el tiempo son obsoletos. A pesar de que algunos tribunales se negaron a dar tutela mediante el habeas data debido a que la información contenida no era falsa, otros reconocieron el derecho al olvido pese a que no estaba contemplado en la Constitución, definido como: "el principio a tenor del cual ciertas informaciones deben ser eliminadas de los archivos, transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren, para evitar que el individuo quede preso de su pasado (Palazzi, 2006)".

A pesar de que la doctrina del derecho al olvido había sido aprobada, la jurisprudencia rechazó el derecho a eliminar información personal de los bancos de datos sólo por el transcurso del tiempo y no lo admitía sobre una interpretación literal del habeas data dentro de la constitución argentina. Fue hasta finales de 1999 que una sentencia de primera instancia aceptó el derecho al olvido para los datos de las personas y la justicia comercial comenzó a establecer límites temporales para tratar los datos de las personas. Como lo señala la postura del Fiscal de Cámara ante la Cámara Nacional de Apelaciones en lo Comercial en un dictamen: "Los datos acerca de la inhabilitación para operar con cuentas corrientes bancarias pueden ser conservados durante el lapso de cinco años por la entidad privada que suministra informes sobre antecedentes comerciales, pues en ausencia de norma legal que establezca un plazo debe aplicarse lo regulado por el inc. 3 del art. 51 del Cód. Penal" (Palazzi, 2006).

Poco a poco, el derecho al olvido fue reconocido no únicamente en el ámbito comercial sino también en el campo de la información administrativa, penal y tributaria. Por ejemplo, un fallo del fuero contencioso de Buenos Aires reconoció el derecho de un contribuyente a borrar información en la Dirección General de Rentas de la Ciudad de Buenos Aires. También fue reconocido en dos demandas contra un medio de prensa que publicó información sobre asuntos relacionados con la intimidad y así el derecho comenzó a adquirir aprobación en la doctrina del país (Palazzi, 2006).

La Ley de Protección de Datos Personales no. 25.326 fue aprobada en noviembre de 2000. A partir de entonces el derecho al olvido se aplicó para la información que existía en bancos de datos y, por lo tanto, la información bancaria almacenada por más de cinco años debía ser eliminada. A pesar de esto, algunos encargados de bases de datos no la aplicaron inmediatamente, como el Banco Central de la República de Argentina, que poseía bases de datos como centrales de deudores, la nueva central de cheques rechazados y la base de datos

de entidades liquidadas. La última contenía los deudores de cuentas liquidadas en los ochenta, para las que aplicaba el derecho al olvido, y el Banco Central proveía la información en forma codificada a los bancos sin identificar a la persona que accedía a los datos, pero argumentaba que la ley no estaba reglamentada y carecía de vigencia. Una vez en vigor la ley en 2001, el Defensor del Pueblo de la Nación recomendó al BCRA que eliminara todos los datos crediticios caducos al momento del dictado de la Ley de *habeas data*, en cumplimiento de la ley 25.326, puesto que el hecho de que el Ejecutivo no hubiera reglamentado todavía la norma no significaba que no fuera operativa y no tenía que castigar a las personas con datos no actuales (Palazzi, 2006).

La Ley de Protección de Datos Personales no. 25.326 asegura la protección integral de los datos personales almacenados en archivos, registros, bancos de datos y otros medios técnicos que traten datos, ya sean públicos o privados, a fin de garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información registrada sobre las mismas, de acuerdo con el artículo 43 de la constitución argentina. El organismo encargado de garantizar el cumplimiento de la ley es la Dirección Nacional de Protección de Datos Personales.

Desde su inicio, la Dirección se involucró con las conocidas DPAs (*Data Protection Agencies*) y obtuvo la acreditación ante la Unión Europea que, además del reconocimiento internacional, da ventajas económicas a empresas argentinas en el marco del comercio económico. Argentina fue el quinto país en obtener esa calificación. También comenzó relaciones institucionales con la agencia española, canadiense, francesa e inglesa a fin de establecer medios de colaboración y asistencia en protección de datos. Asimismo, la DNPDP se puso en contacto con el Grupo Internacional de Protección de Datos en Telecomunicaciones integrado por algunos protectores de datos de Europa, investigadores y empresarios, dedicado a la aplicación de políticas de protección de datos en las telecomunicaciones. Por otro lado, también proyectó la Red Iberoamericana de Protección de Datos Personales, contemplada en el Seminario Iberoamericano sobre Protección de Datos, que contó con el apoyo técnico de la Agencia de Protección de Datos del Reino de España (Travieso, 2004). Los pasos emprendidos por Argentina como representante latinoamericano deber servir como ejemplo para el resto de los países latinos. Es interesante para México conocer el proceder argentino que procuró seguir los pasos de España.

2.6.1 Marco legal argentino en protección de datos

La reforma realizada a la Constitución argentina en 1994 corresponde al ámbito de derechos personales del mundo contemporáneo donde el procesamiento de la información, la acumulación y la circulación han generado amenazas reales a la libertad y a otros derechos personales de los argentinos, en el campo de acción del amparo, *hábeas corpus* y *hábeas data*, que protegen a las personas privadas de su libertad corporal sin orden de autoridad competente.

En su artículo 43 de la Constitución, a pesar de que da a la persona el atributo de poder tener conocimiento de su información y su finalidad en registros públicos o privados, sólo permitía la supresión, rectificación, confidencialidad o actualización de los datos en caso de falsedad, mas no por el transcurso del tiempo, situación por la cual la jurisprudencia argentina hizo uso de otros recursos, como el derecho al olvido, que abrió paso a la Ley de Protección de Datos Personales en Argentina, que hasta entonces representaba un vacío en su legislación.

La Ley de Protección de Datos Personales en Argentina garantiza el derecho de acceso a la propia información, rectificación de datos erróneos o incompletos, confidencialidad frente a los datos sensibles como los relacionados con creencias religiosas, políticas y preferencias sexuales, y el derecho de actualización de la información. Es un mecanismo eficaz para que los titulares de la información puedan defender sus derechos.

En este orden de ideas también aprobó la Ley de Tarjetas de Crédito en 1998 que prohíbe a las instituciones bancarias o crediticias informar a las bases de datos de antecedentes financieros personales sobre los Titulares y beneficiarios de extensiones de Tarjetas de crédito u opciones (Castro, 2005).

La Ley 25.326 contempla características mencionadas anteriormente dentro de su capítulo II que integra los principios generales relativos a la protección de datos, entre los que se encuentran: licitud, calidad de datos, consentimiento del titular, información expresa y clara al titular de la finalidad para la que serán tratados, categoría de datos (ninguna persona puede ser obligada a dar datos sensibles), datos relativos a la salud (respetando los principios del secreto profesional), seguridad de datos, deber de confidencialidad, cesión de datos y transferencia internacional.

De la misma manera, también establece los derechos de los titulares de datos:

1. Derecho de información: toda persona puede solicitar información al organismo de control de datos, relativa a la existencia de los archivos de su persona.
2. Derecho de acceso: el titular tiene derecho a solicitar y obtener información de sus datos personales.
3. Contenido de la información: debe ser clara y sin codificaciones.
4. Derecho a la rectificación, actualización o supresión.
5. Excepciones: información que ponga en riesgo la Nación, el orden y la seguridad pública.
6. Comisiones legislativas: establece comisiones con acceso a los archivos o bancos de datos.
7. Gratuidad: la rectificación, actualización o supresión de datos personales debe realizarse sin cargo alguno para el interesado.
8. Impugnación de valoraciones personales. Los actos contrarios a las disposiciones se anularán.

Por su parte, Basterra (2001) hizo hincapié en algunas cuestiones de la ley que encontró destacables:

1. Establece que su objeto es proteger la protección integral de los datos personales almacenados en archivos, registros o bases de datos públicos o privados dirigidos a dar informes, para garantizar el derecho al honor y la intimidad de las personas. Por esta razón, no se aplica a otras bases de datos que tienen un fin distinto, como las periodísticas, culturales o científicas que se encuentran en el ámbito de la intimidad. Basterra (2001) argumenta que esto no es coherente con el bien jurídico que la ley intenta proteger (*habeas data*) y vulnera el derecho mismo a la intimidad. También que esta ley es copia de la derogada LORTAD, que limita la garantía a la protección del derecho al honor y la

intimidad de las personas, cuando se trata de una gama más amplia de derechos y no únicamente los señalados en la norma.

2. La ley dicta en su artículo primero, segundo párrafo que:

   > Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

   A éste respecto, Basterra (2001) opina que el legislador adoptó correctamente la denominación de "persona de existencia ideal" en lugar de "persona jurídica", ya que abarca todos los supuestos que pretende incluir (género) y no conlleva errores de interpretación. Para algunas doctrinas, las personas de existencia ideal pueden dividirse en personas de existencia ideal propiamente dichas (un consorcio, una asociación) y personas jurídicas (una sociedad anónima), lo que no ocurre con las personas de existencia visible, que únicamente están constituidas por las personas físicas.

   En este mismo párrafo, Puccinelli, citado por Basterra (2001) encuentra que la frase "en cuanto resulte pertinente", puede llevar amputaciones innecesarias a las facultades reconocidas por la ley cuando intenta definir los casos bajo los que se tutelan los derechos las personas de existencia ideal.

3. La norma exige el consentimiento del titular de los datos.
4. Crea un organismo de control que asesora a las personas afectadas que requieren la defensa de los derechos que esta ley garantiza, con la facultad de imponer sanciones a quienes violen sus disposiciones.
5. Con referencia a los Registros de antecedentes, el texto legal también se aplica a los registros públicos, por lo que el registro permanente y el tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las Fuerzas Armadas, fuerzas de seguridad, órganos policiacos o de inteligencia también están obligados a respetar la confidencialidad, a los límites en la cesión de datos y permiten al interesado acceder a ellos para verificar su exactitud. Esto es con el fin de que no almacenen información que no es necesaria para su función, como los datos sensibles. Por otro lado, la ley no altera el registro de antecedentes penales o contravencionales, regulados por su ley específica, que garantiza que la Justicia cuente con la información que requiere para evaluar la eventualidad.

Esto quiere decir que la ley de *habeas data* no facilita la alteración de los datos necesarios para mantener la seguridad pública que se almacenarán por los plazos y bajo las condiciones previstas por las leyes que rigen, de tal forma que quien tiene antecedentes penales pueda beneficiarse por esta ley.

Un caso especial son las empresas que brindan información crediticia, que sólo pueden guardar datos referentes a la solvencia económica. En cuanto a deudores que hayan cumplido su obligación sus datos se conservarán únicamente dos años para evitar que pueda acceder a un crédito.

También establece que las empresas deben suprimir de sus registros los datos referidos a incumplimientos de obligaciones extintas cuando apareció la ley.

6. La ley aplica en toda la República Argentina, excepto en lo que respecta al órgano de control. Corresponde a los estados federados regular los aspectos que no abarca la norma federal, que gozan de autonomía provincial de acuerdo con lo establecido en el artículo 5 de la Constitución Argentina.
7. La ley tipifica nuevos delitos, que son: insertar datos falsos en un archivo de datos y proporcionarlos a un tercero, a sabiendas de que son falsos, en perjuicio de alguna persona (la sanción a esto aumenta cuando se trata de un funcionario público en ejercicio de sus funciones, a quien se inhabilita de su ejercicio por el doble del tiempo a la condena); acceder a un banco de datos personales de forma ilegítima o violando su seguridad y confidencialidad, y revelar información contenida en un archivo protegido por la ley.

Basterra (2001) también menciona algunos errores de los que adolece la ley: no define la estructura y financiamiento de la actividad del órgano de control; en el capítulo VII incluye artículos que no van con la denominación del capítulo, como el "ámbito de aplicación de la ley", que debería ir en un inicio; no contempla un capítulo de "Disposiciones Transitorias"; nombra a la garantía como "acción de protección de los datos personales o de *habeas data*" cuando los institutos jurídicos no pueden tener dos nombres y tiene dos artículos sin epigrafía, el 45 y 47.

A pesar de esto, a juicio de Basterra (2001), la ley cumple con la regulación de los archivos de datos de personas físicas y de existencia ideal, y regula a las bases de datos privados,

destinados a dar informes, o públicos, en las condiciones que establece esta ley, con equilibrio entre el derecho a la información y el derecho a la intimidad.

Si se revisan los principios enumerados por Campuzano (2000) y por el Convenio 108, es posible destacar que esta ley pionera en América Latina tiene ciertas semejanzas con sus antecesoras, incluso, cuenta con comisiones legislativas que garantizan el acceso a las bases de datos personales.

2.6.2 Sector Salud

El sector salud en Argentina trata con elementos que Travieso identificó, durante el VIII Encuentro Iberoamericano de Protección de Datos Personales (2010), como cinco etapas: datos sensibles, historia clínica, consentimiento informado, datos genéticos y seguridad de la información.

Según Travieso (2010), la característica esencial del dato sensible es el potencial que posee para generar actitudes discriminatorias respecto de sus titulares precisamente porque tratan sobre cuestiones de origen racial o étnico, opiniones políticas, convicciones religiosas, afiliación sindical, información sobre la salud o vida sexual de la persona. Como punto de partida, la ley prohibe crear bases de datos con datos sensibles, sin embargo, fue creada bajo ciertos principios. Por ejemplo, la Ley de Protección de Datos Personales no aplica cuando se trata de investigaciones científicas o médicas en la medida en que esta información no se atribuya a una persona determinada o determinable. Travieso (2010) menciona que el problema surge cuando todos esos datos tienen identidad.

Aparece aquí la historia clínica. Travieso (2010) explicó que México le lleva ventaja en este tema porque Argentina tiene poco tiempo de haber establecido una Ley del Paciente –que a la fecha no ha sido reglamentada- que entiende a la historia clínica como: “un documento obligatorio, cronológico, foliado, con todos los detalles establecidos sobre el paciente establecido por profesionales y auxiliares de la salud”.

La protección de datos, el secreto profesional y los datos sensibles se cruzan aquí para propiciar la protección de la información en la historia clínica y Travieso (2010) menciona principios claves: la autodeterminación informativa como puerta de acceso a los datos

personales, la integridad referente al complejo de datos que debe tener esa historia clínica, la unicidad necesaria para que haya un mismo criterio incluso cuando la información se comparta por diferentes establecimientos, la inviolabilidad para que nadie pueda tener acceso y, por supuesto, la privacidad.

El consentimiento informado corresponde a la declaración de voluntad que da conocimiento a la persona sobre su estado de salud, los procedimientos propuestos y alternativos y las consecuencias. Se efectúa bajo los principios de confidencialidad, privacidad y autonomía de la voluntad, así como la obligatoriedad de informar al paciente y la instrumentación (Travieso, 2010). Esto necesario para que el paciente pueda ejercer su derecho a la autodeterminación para disponer de su propio cuerpo.

Según Travieso (2010), de manera similar a los principios de la protección de datos, la información proporcionada debe ser lícita, adecuada, pertinente y no excesiva, utilizada para los fines que motivaron su obtención, debe también ser exacta y permitir ejercer los derechos de acceso, rectificación y supresión de datos, así como ser destruida cuando deje de ser necesaria para los fines que motivaron su recolección, y revocable.

La excepción a todo esto es, a juicio de Travieso (2010), cuando se pone en peligro la seguridad pública y cita a Piñarra diciendo: “nunca hay que ser fundamentalista en los datos personales, evidente es así, cuando hay riesgo grave para la salud o la vida del paciente”. Cabe destacar que la seguridad pública es uno de los límites de todas las leyes que protegen la información personal puesto que no es posible anteponer el interés de una persona al de toda una comunidad, por esto aplica el principio de ponderación.

En cuanto a los datos genéticos de carácter personal, definidos como la información sobre las características hereditarias, Argentina cuenta con normas en el ámbito internacional. Finalmente, los datos de salud tienen unicidad y consanguineidad puesto que distinguen a una persona de las demás (Travieso, 2010).

Destaca en Argentina el caso de tres laboratorios trasnacionales que cumplen con la ley para proteger los datos personales, se trata de Sanofi Aventis, Rush y Novartis, debido a la labor que han desempeñado en la materia.

2.7 Estados Unidos

2.7.1 La privacy

En contraste con la tendencia europea en lo que se refiere a la protección de datos personales, el camino que Estados Unidos ha seguido se regula mediante el desarrollo del concepto *privacy*, que aplica en diferentes vertientes del derecho: privacidad genética, privacidad en las conversaciones profesionales, privacidad en la información médica, privacidad en las asociaciones, privacidad en el hogar, en la escuela, trabajo, etc. Los datos personales se protegen en la privacidad aplicada a los registros y las bases de datos electrónicas (Puente, 2006).

El derecho a la privacidad es un concepto relativamente nuevo, relacionado con ilícitos civiles, derecho constitucional federal, derecho constitucional estatal, derecho codificado federal y estatal, información privilegiada, derecho de la propiedad, derecho contractual y derecho penal (Puente, 2006).

El concepto de *privacy* surgió a finales del siglo XIX, cuando los medios impresos revolucionaron la circulación de la información, el tiraje de los periódicos aumentó casi mil por ciento y el periodismo sensacionalista se convertía en el modelo del periodismo amarillista. El incremento de la prensa escrita y los avances de la tecnología originaron el interés por protegerse de la invasión a la privacidad, reflejado en el artículo de Warren y Brandeis, *The right to privacy*, que revolucionó el sentido de privacidad que se tenía en aquella época y que fue retomado en muchas decisiones de la Corte Suprema de Estados Unidos (Puente, 2006).

Warren y Brandeis estuvieron influenciados por Godkin, comentarista social de la época, quien mencionaba que: "la privacidad es un producto moderno, uno de los lujos de la civilización, el cual no sólo pasaba desapercibido, sino que era desconocido en las sociedades primitivas… el principal enemigo de la privacidad en la vida moderna es el interés de la gente de conocer los asuntos personales que en días después los periódicos divulgaran como chisme…", y agrega "…mientras que ahora la comunicación acerca de la privacidad es impresa, y fabrica una víctima con todos los defectos, mismos que son conocidos cientos de

miles de millas de su lugar de origen, llevando la información con todos los detalles de una persona" (Puente, 2006).

En su artículo, Warren y Brandeis hacen mención del texto de Godkin, pero, a diferencia de éste que ve como solución al problema que la gente cambiara su actitud al respecto, Warren y Brandeis se inclinaron por proteger la privacidad mediante la ley. El derecho a la privacidad que ellos advocaban se concentraba en el interés que tenían las personas en prevenir la comercialización de los asuntos de su vida privada mediante la prensa. El artículo escrito por estos autores afirmaba que cada individuo debía estar protegido completamente en su persona y en su propiedad como un viejo principio del derecho común, pero este derecho tenía que redefinirse continuamente para fijar los límites de su protección, de acuerdo con su naturaleza, a la vez que reconocen que la línea que separa la dignidad personal y la conveniencia de la protección de los derechos personales es difícil de definir. Por esto, Warren y Brandeis mencionaron seis limitaciones al derecho a la privacidad (Puente, 2006):

1. El derecho a la privacidad no prohíbe publicar aspectos de interés público o general.
2. No prohíbe que se comunique sobre algún tema cuando la publicación se haga bajo circunstancias que representen un privilegio.
3. Posiblemente no garantice que la invasión a la privacidad por publicaciones orales sea reparada puesto que el derecho las considera insignificantes.
4. Se suspende cuando la publicación la realice el individuo o bajo su consentimiento.
5. No es defensa que el contenido sea verdadero puesto que lo que se protege es la divulgación, más no la verdad o falsedad de los hechos.
6. De la misma manera, la falta de "malicia" tampoco sirve para la defensa.

A partir de este momento, el derecho de la privacidad en los Estados Unidos fue modelado por las decisiones de la Corte Suprema corte de Justicia, y en 1974 se sancionó la *Privacy Act*. Los precedentes jurisprudenciales en los que decidía la Suprema Corte se referían a casos muy diferentes que estaban en zonas personales en las que el Estado no podía intervenir.

En Meyer contra Nebraska y Pierce contra *Society of Sisters*, la Corte Suprema declaró inconstitucionales leyes que traspasaban en el adoctrinamiento de niños. En Nebraska, el señor Meyer había sido condenado por enseñar pasajes bíblicos en alemán en una parroquia luterana

porque estaba prohibido enseñar en otro lenguaje que no fuera inglés a los niños antes de noveno grado. El objeto según la Ley de Nebraska era prevenir que los niños aprendieran ideales y lenguas extranjeras antes que la lengua e ideales americanos. La Corte Suprema anuló la sentencia y descalificó la prohibición era como la práctica que existía en Esparta de encerrar a los niños en barracas para adoctrinarlos (Gregorio, 2004).

En 1958, un dictamen unió el reconocimiento de los valores de autonomía personal y el control de la información, cuando prohibió a una organización en Alabama que pusiera al descubierto las listas de sus socios. La decisión dictaba: "el derecho de sus miembros a perseguir su interés legal a la privacidad y de asociarse libremente con otros sin que se le pretenda disuadir…" (Hendricks et al, 1990).

En 1965, la Suprema Corte de Connecticut por primera vez sostuvo que la Constitución protegía el derecho de la privacidad sexual. El caso envolvía un estatuto de Connecticut que prohibía a las parejas casadas el uso de anticonceptivos. La Corte creó las "zonas de privacidad" dentro de la "penumbra" y dijo que la Primera Enmienda otorgaba a las personas el derecho de la privacidad y un cierto grado de autonomía personal en sus decisiones, mientras que la Cuarta Enmienda afirmaba el derecho de la gente a estar segura en su persona, casas, documentos (Hendricks et al, 1990). A partir de entonces, las principales sentencias de la Suprema Corte estuvieron vinculadas a temas de sexualidad y a preservar la intimidad (Gregorio, 2004).

Para 1967, la Corte aplicó los principios de la privacidad a una nueva esfera. Determinó que la intervención de las llamadas telefónicas era inconstitucional y creo el término de "la razonable expectativa de la privacidad", que serviría de guía para los casos subsecuentes. La Corte creó cuatro criterios para determinar las zonas de privacidad protegidas constitucionalmente que no se referían únicamente a transgresiones tangibles: las comunicaciones entre las personas, la personalidad, las ideas políticas y los pensamientos (Hendricks et al, 1990).

En 1973 la Décimocuarta Enmienda otorgó a la mujer el derecho al aborto, una regla que fue simbólica dentro del derecho a la privacidad a pesar de su controversia (Hendricks et al, 1990).

Todos estos casos constituyeron el *privacy right* relacionado con la autonomía personal. Rubenfel (Gregorio, 2004) concibe al *privacy right* como "un conjunto de limitaciones a un Estado totalitario.

2.7.2 Constitución de Estados Unidos y Derecho Codificado

Requirió años para que las cortes lo abordaran de manera más amplia y se aproximaran hacia temas como la autonomía personal y el control de la información (Hendricks et al, 1990).

El derecho a la privacidad en un inicio se interpretó como la protección contra la intrusión tangible hacia una persona. A pesar de que la Constitución de Estados Unidos no se refiere explícitamente a éste, existen disposiciones que lo protegen o que las cortes y legislaturas comenzaron a aceptar como principios para describirlo como tal. Entre estas disposiciones adoptadas por la Corte Suprema se encuentran las siguientes (Puente, 2006):

- Primera enmienda Constitucional. Salvaguarda algunos aspectos de la privacidad, como "hablar en forma anónima", a la vez que protege a los individuos de ser obligar a dar a conocer los grupos a los que pertenecen o a los que contribuyen.
- Tercera enmienda Constitucional. Protege la privacidad del hogar al establecer que ningún soldado puede acuartelarse en ninguna casa en tiempo de paz, sin el consentimiento del dueño, no en tiempo de guerra, pero de acuerdo con lo prescrito por la ley.
- Cuarta enmienda Constitucional. Prevé el derecho de la persona sobre sí misma, su casa, documentos y pertenencias sobre registros excesivos y embargos. Aproximadamente cuarenta años después de que Brandeis escribiera *The Right to Privacy*, como Ministro de la Corte Suprema de Justicia, señaló que este punto de la cuarta enmienda no protegía la propiedad sino el derecho a ser dejado solo en sus bienes materiales, en los que se expresaban sus pensamientos y emociones. Por tanto, este derecho (*the right to be alone*) no justifica que el gobierno se entrometa en la privacidad de las personas porque atenta contra esta cuarta enmienda.
- Quinta enmienda. Garantiza que no puede obligarse a ninguna persona a declarar en contra de sí misma en el orden penal. Esta enmienda protege la privacidad porque establece que nadie puede ser obligado a responder por un delito a menos que sea frente un jurado, con excepción de causas derivadas de las fuerzas navales o militares. Tampoco podrá ser

juzgada por el mismo delito dos veces, ni se le podrá obligar a declarar en su contra en causas penales, ni privada de su vida, libertad ni propiedades, si no es mediante el proceso que dicte la ley.

- Decimocuarta enmienda. Establece que ningún Estado promulgará ni hará valida ninguna ley que restrinja los privilegios e inmunidades de los ciudadanos de los Estados Unidos. Tampoco podrán privar a ninguna persona de su vida, libertad o posesiones, si no es mediante lo establecido por la ley. A diferencia de la quinta enmienda, ésta se refiere a los procesos realizados en los Estados y la otra en la Federación.

A mediados de la década de los sesenta surgió en Estados Unidos un interés sobre los alcances que podía tener el crecimiento tecnológico sobre la privacidad, por esto, a pesar de no tener una ley específica que proteja los datos personales, ha creado políticas de autorregulación que protegen la privacidad de los sectores más sensibles de la sociedad: Fair Credit Reporting Act, de 1970; *PrivacyAct*, de 1974; *Family Educational Rights and Privacy Act*, de 1974; *Right to Financial Privacy Act*, de 1978; *Privacy Protection Act*, de 1980; *Cable Communications Privacy Act*, de 1986; *Computer Matching and Privacy Protection Act,* de 1988; *Employee Polygraph Protection Act*, de 1988; *Video Privacy Protection Act*, de 1988; *Telephone Consumer Protection Act*, de 1991; *Driver´s Privacy Protection Act*, de 1994; *Health Insurance Portability and Accountability Act*, de 1996; *Children's Online Privacy Protection Act*, de 1998; *Graham-Leach Bliley Act*, de 1999 (Puente, 2006).

2.7.4.1 Privacy Act de 1974

La *Privacy Act* de 1974, que podría ser lo más cercano a la protección de los datos personales contra el uso inadecuado por parte del gobierno en Estados Unidos, fue creada en respuesta a la creciente preocupación que existía por la aparición de las bases de datos computarizadas y el riesgo que podían representar para la privacidad de las personas. Mediante cuatro procedimientos que protegen los datos personales: establece el acceso a la información personal que las agencias de gobierno poseen del titular, garantiza el manejo adecuado de los datos durante y después de su recopilación con los principios de prácticas de información, fija restricciones a las agencias sobre cómo pueden compartir los datos con terceras personas y agencias, y permite que las personas protegidas, es decir ciudadanos norteamericanos y

residentes permanentes, puedan demandar en caso de que se violen sus garantías (EPIC, 2010).

Sin embargo, su alcance es limitado puesto que sólo aplica a los datos que procesa el gobierno federal y no abarca a los gobiernos estatales ni al sector privado. En la sección siete restringe su aplicación al *Social Security Number* en el ámbito federal, estatal y local, y son sujetos obligados el Departamento Ejecutivo, militar, agencias regulatorias independientes y corporaciones de control gubernamental. Por lo tanto, todo esto abarca sectores como el Servicio Postal Norteamericano, el Departamento de Educación, la FDA, el FBI, y, a pesar de que incluye la Oficina del Presidente, el Congreso no está mencionado (EPIC, 2010).

Además de esto, la *Privacy Act* contiene varias excepciones que permiten a las agencias de gobierno incumplir con las reglas que establece, por ejemplo, aunque requiere el consentimiento previo para la cesión de datos, la transmisión de información a otra agencia del gobierno está permitida dentro del concepto de "uso rutinario". Asimismo, la falta de una definición clara de "registros", "sistemas de registros" y "agencias", ocasiona que el Acta no pueda cubrir los diferentes tipos de bases de datos y sus procedimientos de recopilación (EPIC, 2010).

En cuanto a las prácticas comerciales que Estados Unidos tiene con la Unión Europea está el acuerdo "*safe harbor*", con el que las empresas estadounidenses que se comprometan y acepten sus cláusulas podrán recibir datos personales provenientes de la Unión Europea, sin embargo, este convenio no ha tenido mucho éxito (Ovilla, 2005).

Por otra parte en su lucha contra el terrorismo, la Administración estadounidense ha violado los principios de la protección de datos, principalmente después de los atentados del 11 de septiembre, con la creación de dos leyes: *Aviation and transportation security* y la *Enhanced border security and visa entry reform*. Con estas leyes no únicamente tenían acceso a la información de los pasaportes, sino que exigieron a las aerolíneas sus sistemas de reservación que contiene información confidencial de los pasajeros, como ocurrió con la *Passanger Name Record*, que les permitía conocer el lugar en donde se hizo la reservación, la forma de pago, dirección personal del pasajero, si tiene otras reservaciones, si requiere asistencia médica, etc. (Ovilla, 2005).

En este mismo sentido, su última creación fueron los nuevos pasaportes estadounidenses con un chip electrónico incluido, *radio frequency identification tag*, que tiene información con una fotografía digitalizada del titular (Ovilla, 2005). Y no está de más mencionar el caso Choice Point que será tratado más adelante.

A manera de conclusión, es posible afirmar que en Estados Unidos no hay un derecho general que proteja la vida privada, a pesar del concepto *privacy*, que más bien se refiere a la época en que las personas buscaban protegerse de la prensa estadounidense y proclamaron su derecho a estar solos (Ovilla, 2005). En general, el derecho a la privacidad en Estados Unidos se ha relacionado con la Decimocuarta Enmienda, mientras que otras decisiones judiciales lo han colocado en la penumbra cerca de la Primera, Cuarta y Novena enmiendas, y descansa parcialmente en la legislación federal que lo protege en sectores determinados.

Para recapitular, la tendencia actual en Europa apunta hacia la unificación bajo el principio de uso mínimo de los datos personales en defensa de la persona, con límites del Estado y de los particulares para su información, mientras que en Estados Unidos no hay políticas constitucionales sobre el tema, sólo normas sectoriales que operan desde la esfera de la privacidad como proceso de auto-regulación. America Latina, en específico Argentina, sigue los pasos de la tendencia europea y ha adaptado sus leyes a los lineamientos europeos.

2.8 La protección de los datos personales en México

México forma parte de diferentes disposiciones que reconocen la protección de la vida privada como un derecho, entre estas se encuentra la Convención Americana sobre los Derechos Humanos y la Organización de las Naciones Unidas. De la misma manera, está suscrito a tratados con socios comerciales que ponen en peligro la seguridad de los datos en el flujo transfronterizo si las naciones no respetan las garantías mínimas que deben guardar. El TLCAN (América del norte), el TLCUE (Unión Europea) y el APEC (Asia-Pacífico) conforman los principales tratados y socios comerciales con los que México comparte información.

Las principales actividades económicas, políticas y sociales requieren la información de las personas para funcionar, sin embargo, su regulación es necesaria dado los riesgos que el flujo

de datos representa. Era importante, entonces, que México reconociera la protección de los datos personales como un derecho fundamental para garantizar que los poseedores de las bases de datos no hicieran uso inadecuado de la información.

Hasta hace poco la Constitución Política de los Estados Unidos Mexicanos protegía el derecho a la privacidad sin hacer mención específica de los datos personales. La libertad de expresión y el derecho a la información estaban garantizados en el artículo 6º. con los daños que pudieran ocasionar a los terceros como límite, sin embargo, como se analizará más adelante, la libertad de expresión y la protección de datos personales son derechos opuestos y, salvo en ocasiones que pudieran poner en riesgo la seguridad de terceros, difícilmente la primera cederá ante la segunda.

> La manifestación de las ideas no será objeto de ninguna inquisición judicial administrativa, sino en el caso de que ataque a la moral, los derechos de terceros, provoque algún delito o perturbe el orden público, el derecho a la información será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

En su artículo 7º, la Constitución se refiere a la libertad de imprenta y de igual manera destaca como su límite la vida privada de terceros:

> Es inviolable la libertad d escribir y de publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tienen más límite que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento de delito.

Finalmente, en el artículo 16 sólo mencionaba con respecto al derecho a la intimidad:

> Art. 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.

A pesar de que los artículos constitucionales ya defendían el derecho a la privacidad, no fue hasta la puesta en vigor de la Ley Federal de Transparencia y Acceso a la Información y la creación del Instituto Federal de Acceso a la Información en 2002 que México dio un gran paso en la protección de datos. Acuña (2004) explica que a pesar de que en un inicio el IFAI decidió desaparecer la Dirección General de Datos Personales de su organismo, un tanto absorto en el tema del acceso a la información pública y la transparencia, comenzó a mostrar nuevamente interés en la protección de datos ya que la desregulación en esta materia situaba al

ciudadano en la intemperie y era totalmente vulnerable al encontrarse sin el cobijo del Estado que, se supone, debía garantizar la organización estatal para convivir en democracia. La Ley de Acceso a la Información se vinculaba con el derecho a la protección de datos personales en el apartado en que se refiere a ellos como la información que concierne a una persona física, además de que su artículo 8º está dedicado al derecho de la protección de datos personales, de los cuales el IFAI es garante. A pesar de que la LAI no constituía un modelo suficiente para la protección de datos personales en México porque únicamente conformaba lineamientos generales que son disposiciones de carácter administrativo, todas estas acciones se llevaron a cabo para que el derecho a su protección fuera reconocido como un derecho fundamental, a fin de que se garantizara la facultad de los individuos de tener acceso a la información que existe sobre ellos en las bases de datos, controlar su calidad y que tuvieran la oportunidad de modificar o eliminar datos inexactos, así como tener control sobre su transmisión (Ornelas y Martínez, 2006). Esos fueron los primeros pasos para la protección de datos personales en México, todavía insuficientes.

Ante la pobreza constitucional sobre el tema, algunas propuestas de legislación fueron promovidas sin que ninguna hubiera fructificado hasta la aprobación en abril de 2010 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares que, junto con la reforma de los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, conforma lo último en materia regulatoria para la protección de datos personales segmentados en públicos y particulares, sin excluir la propuesta de reforma a la LAI que se espera sea aprobada por el Ejecutivo en 2011.

2.8.1 La Constitución Mexicana

Desde 1917, la Carta Magna establece en las garantías individuales los derechos referentes a la libertad individual entre los que destacan la inviolabilidad de correspondencia y domicilio y, después, el secreto de las comunicaciones privadas, derechos relacionados con la privacidad y la intimidad porque protegen áreas que pertenecen a todo ser humano. Sin embargo, con el avance tecnológico se volvió necesario dar respuesta a las nuevas tendencias de la sociedad de la información. La reforma constitucional al artículo 6º, en julio de 2007, estableció la protección de los datos personales y la información referente a la vida privada, así como el

derecho de acceso y corrección de datos públicos. Fue la primera vez que de forma expresa se hizo referencia a la protección de datos en la Constitución como un derecho diferente al derecho de acceso a la información pública. Esta protección se limitó al ámbito público, es decir, a la información que poseían las autoridades, entidades, órganos y organismos de los tres órdenes de gobierno, sin incluir el ámbito privado.

Con la reforma, al artículo 6º. Constitucional se le agregó el segundo párrafo y siete fracciones:

> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
>
> IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos.
>
> V. (…)

El principio de máxima publicidad tiene como límite, además del daño ocasionado a terceros, al ámbito de la privacidad y los datos personales. El principio de ponderación, que en este caso deriva entre lo público y lo privado, sirve para determinar hacia qué lado debe inclinarse la balanza, dado que hay información de puede ser divulgada cuando conviene al interés público y hay otra clase de información que no por pertenecer al sector público debe darse a conocer. Este artículo también garantizó acceso y la rectificación de los datos personales de las bases públicas.

En 2006 se presentó un proyecto de ley para agregar párrafos al artículo 16 Constitucional. Fue en 2008 cuando la reforma reconoció el derecho de toda persona a la protección de su información como un derecho fundamental independiente. Cuando se presentó el proyecto de

ley la Constitución hacía referencia únicamente a la vida privada de las personas, pero la reforma le añadió un segundo párrafo que habla explícitamente de los datos personales, reconoce su naturaleza autónoma que lo distingue de otros derechos fundamentales y plasma los derechos de "Acceso, Rectificación, Cancelación y Oposición", denominados derechos de ARCO. Con la aprobación de la reforma, el titular de los datos puede, a diferencia de lo que ocurría anteriormente, decidir sobre el uso de los datos que le conciernen, oponerse en los casos en que sean obtenidos sin su consentimiento y cancelarlos cuando el tratamiento no sea conforme a lo dispuesto o cuando sean inexactos o incompletos. Son derechos reconocidos internacionalmente en la Directiva Europea 95/46 que dotan de poder al gobernado para disponer sobre sus datos personales (Dictámenes de Primera Lectura, 2008).

A partir de entonces, el artículo 16 de la Constitución establece que:

> 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.
>
> 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 (…)

La reforma incluye excepciones bajo ciertas condiciones, esto es cuando por su trascendencia este derecho se contrapone con otros derechos y amerita que la autoridad pondere en la búsqueda del bien común, puesto que un derecho fundamental no puede estar por encima de otro ni de intereses públicos o sociales (Gaceta no. 306, 2008). Dichas condiciones se refieren a:

- Seguridad nacional: cuando es necesario salvaguardar la integridad, estabilidad y permanencia del Estado mexicano.
- Disposiciones de orden público: esto es porque representa el núcleo íntegro de la sociedad, rebasa los intereses particulares, privados o individuales.

- Seguridad pública: comprende la prevención, investigación y persecución de los delitos, así como la sanción de infracciones administrativas.

- Salud pública: corresponde al Estado controlar o erradicar enfermedades, al igual que prevenir factores de riesgo que puedan afectar la salud de la población.

En el dictamen de la reforma al artículo 16 Constitucional se reconoce el derecho de disponer de manera libre, informada y específica para el uso de los datos personales sobre la base del consentimiento. Este consentimiento puede ser otorgado de diferentes maneras, dependiendo de la naturaleza de los datos, la fuente de la que se obtuvieron, finalidad del tratamiento, entre otros; así se distingue el consentimiento presunto, tácito, expreso y por escrito, mismos que serían complementados por los principios de información, calidad, seguridad y confidencialidad, a través de los cuales el titular tiene la posibilidad de:

1) Conocer el uso que se hará de sus datos personales;

2) Garantizar que éste será adecuado, pertinente y no excesivo en relación con el fin para que el que se obtuvieron;

3) Adoptar medidas técnicas y organizativas que garanticen su seguridad, y

4) Saber que el manejo de los datos se hará con las precauciones necesarias de acuerdo con su naturaleza.

Otra de las reformas grandes que tuvo la Constitución se encuentra en el artículo 73, al que se le añadió la fracción "O", que dice:

> Artículo 73. El Congreso tiene facultad:
>
> XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.
>
> XXX. (…)

Después de la reforma al artículo 6º constitucional, que protegía la información de las personas que poseían los entes públicos, la legislación consideró necesario tener mecanismos que también protegieran los datos personales que están en manos de particulares. Parte del argumento para realizar la reforma al artículo 73 fue que México forma parte de tratados

internacionales con países federales que cuentan con legislación en torno a la protección de datos personales, como Argentina y Canadá, lo que podía traer implicaciones para el Estado Mexicano por incumplir con los requisitos y compromisos establecidos internacionalmente al privar a la Federación la facultad de regir las relaciones jurídicas derivadas del tratamiento de datos personales en posesión de los particulares (Dictamen art. 73, 2007).

Con esta fracción "XXIX-O" quedó establecida la facultad del Congreso para expedir leyes que protejan los datos personales que estén en manos de los particulares, como bancos, hospitales, universidades, empresas, etc. Es decir, el Congreso Federal comenzó a regular a escala nacional la manera en que los particulares utilizaban y transmitían la información relativa a las personas, que normalmente tiene fines comerciales. Esta reforma le dio al legislador los elementos necesarios para elaborar una ley federal que protegiera los datos personales que plasmara los principios, derechos, procedimientos, infracciones, la existencia de una autoridad designada y un régimen de transferencias internacionales de datos, de acuerdo con estándares internacionales. Además de esto, también otorgaría seguridad jurídica a los datos de las personas que se utilizan en las transferencias internacionales (Dictamen art. 73, 2007). Esta ley fue la Ley de Protección de Datos Personales en Posesión de Particulares aprobada en 2010.

2.8.2 Ley Federal de Transparencia y Acceso a la Información (LAI)

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental tenía por objeto regular el derecho a la información a la vez que conectó este derecho con el derecho a la protección de datos como su el límite. En este caso, los límites al derecho de acceso están expresamente señalados en la LAI en los artículos 13 y 14, referentes a la información que puede ser clasificada con el carácter de reservada, y en el artículo 18, que son supuestos en los que alguna información puede clasificarse como confidencial, como son los datos personales que requieran del consentimiento de los sujetos para su difusión, distribución o comercialización en los términos señalados en la ley (Ornelas y Martínez, 2006).

El primer punto en el que la LAI regula a los datos personales es en el artículo 3, fracción II, en el que los define como:

> II. Datos personales: La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad:
>
> III. (…)

Asimismo, el capítulo IV de la LAI está dedicado a la protección de los datos personales, y establece:

> Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:
>
> I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61.
>
> II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
>
> III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61.
>
> IV. Procurar que los datos personales sean exactos y actualizados;
>
> V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y
>
> VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.
>
> Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.
>
> Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
>
> I. (Se deroga).

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.

Artículo 24. Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Artículo 25. Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

Artículo 26. Contra la negativa de entregar o corregir los datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25.

En cuanto a la tutela que esta Ley proporciona únicamente a las personas físicas y no a las morales, colectivas o jurídicas privadas, la Tesis Aislada no. 169167 (2008) argumenta que tal

distinción queda justificada en que el derecho a la protección de datos personales está encausado al respeto de un derecho personalísimo, como el de la intimidad, del cual deriva. Esto quiere decir que no hay igualdad jurídica entre las personas físicas y morales puesto que están en situaciones de derecho dispares, y la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es un derecho del que únicamente goza el individuo, entendido como la persona humana.

Los sujetos obligados a cumplir con las disposiciones de esta ley, de acuerdo con lo establecido en el artículo 3, fracción XIV de la LAI, son: el Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; el Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; el Poder Judicial de la Federación y el Consejo de la Judicatura Federal; los órganos constitucionales autónomos (IFE, CNDH, Banco de México, etc.); los tribunales administrativos federales, y cualquier otro órgano federal, bajo tres principios fundamentales mencionados por Reyes (2006):

1. La información de los poderes y organismos federales es pública y la sociedad debe poder tener acceso a ella, excepto en los casos previstos por la propia Ley.

2. El derecho de acceso a la información es universal, esto quiere decir que cualquier persona, sin distinción, puede solicitarla sin necesidad de explicar cuál es su interés o fin.

3. Los datos de las personas que contienen las instituciones públicas son confidenciales, por lo que no deben divulgarse ni usarse para fines distintos para los que fueron recabados, de tal forma que se garantiza el derecho a la intimidad y a la vida privada, a la vez que sus titulares pueden tener acceso cuando lo requieran.

Aunque de forma incipiente, en la LAI quedaron descritas las primeras disposiciones relacionadas con el derecho a la protección de datos personales y, para que las normas anteriores fueran efectivas, en los capítulos siguientes contiene otras que señalan las atribuciones del entonces Instituto Federal de Acceso a la Información (IFAI) como órgano garante del derecho a la protección de datos públicos, así como reglas de procedimientos para el recurso de revisión. Para cumplir con esta misma misión de velar por la correcta aplicación de la LAI y para complementar todos sus vacíos, el IFAI dictó la normatividad federal que

rige a los sistemas de datos personales públicos en México, constituida por Lineamientos Generales y resoluciones de carácter administrativo que dan operatividad a la LAI:

- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública. De acuerdo con su artículo 1: "Este ordenamiento tiene por objetivo reglamentar las disposiciones de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en lo relativo al Poder Ejecutivo Federal, sus dependencias y entidades y, en general, cualquier otro órgano que forme pare de la Administración Pública Federal.

  En lo referente a la protección de datos personales, el Capítulo VIII, artículo 47, establece que los procedimientos para acceder a los datos personales que poseen las dependencias y entidades deben garantizar que los derechos de los individuos serán protegidos, especialmente la vida privada y la intimidad, así como el acceso y corrección de su información, de acuerdo con los lineamientos del Instituto. En su artículo 48 obliga a las dependencias y entidades a hacer del conocimiento del Instituto y del público en general sobre los sistemas de datos con los que cuenten, así como su objeto, tipo de datos, uso, unidad administrativa y responsable.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las soluciones de corrección de datos personales que formulen los particulares. Determina las reglas que deben seguir las dependencias y entidades de la Administración Pública Federal para atender a las solicitudes de los particulares para corregir la información contenida en sus sistemas y bases.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección. Además de establecer el procedimiento que debe seguir la Administración Pública, contiene el Sistema de Solicitudes de Información o SISI, que es el sistema autorizado por el Instituto que contiene los formatos impresos o

electrónicos con los que las personas presentan sus solicitudes de acceso. Es el único sistema para registrar y capturar las solicitudes recibidas por las dependencias.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos. Establece los procedimientos que deben seguir las dependencias y entidades de la Administración Pública Federal para recibir, procesar, tramitar, solucionar y notificar los resultados de las solicitudes de acceso, con excepción de las solicitudes de corrección, que corresponden a otro lineamiento.

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales. En éste se fijan los procedimientos que las dependencias deben seguir para notificar al Instituto las listas de sistemas de datos personales que tienen en su poder.

- Lineamientos de protección de datos personales. En octubre de 2005 el Instituto Federal de Acceso a la Información emitió los Lineamientos para la Protección de Datos Personales, que garantizan el derecho del individuo a tener acceso a la información sobre sí mismo que contienen las bases de datos del gobierno federal; además, creó Sistema Persona, aplicación informática de acceso al público con la que los ciudadanos ejercen su derecho a la autodeterminación informativa, basados en el artículo 16 Constitucional, para limitar la intromisión del Estado en el ámbito de la persona, tutelar la inviolabilidad del hogar, las comunicaciones y las relaciones familiares, y consagrar la libertad del individuo a desarrollarse libremente como tal.

- Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales. Es un instrumento técnico sobre medidas de seguridad que se aplican a los sistemas de datos personales físicos y automatizados. Establece los niveles de seguridad para la protección de los datos, de acuerdo con criterios internacionales, según la naturaleza de la información que contienen los sistemas de datos personales, que va desde nivel básico (datos de identificación y laborales), intermedio (datos patrimoniales, sobre procedimientos administrativos seguidos en forma de juicio, académicos y de tránsito o

movimientos migratorios) y alto (datos ideológicos, de salud, características personales, físicas, vida sexual, origen).

Hasta este momento la Constitución todavía no reconocía el derecho a la protección de datos personales como un derecho fundamental. Por esto, de acuerdo con García (2007), la LAI únicamente dio protección a la información que para la persona era considerada como íntima. En estos términos, de acuerdo con Ornelas y Martínez (2006), la primera impresión era que México ya contaba con una regulación completa, sin embargo cuestionaron si era un modelo suficiente o si sólo se trataba de una aproximación a la protección de datos personales desde una ley de acceso a la información. No obstante, defienden que la actividad desarrollada por el IFAI sirvió para nutrir el derecho a la protección de datos en diferentes aspectos, como establecerlo como límite frente al interés público.

Otro paso importante que México dio para entrar en la protección de los datos personales fue su incorporación en la Red Iberoamericana de Protección de Datos, un foro importante donde participan tanto autoridades de protección de datos como la iniciativa privada o académicos, de la que fue sede en 2005, cuando México pugnó por una ley que diera mayores garantías a la protección de datos. La Red es el segundo de los ejes más importantes que constituyeron el derecho a la protección de datos en nuestro país, ya que su participación en la misma permitió obtener y divulgar información e intercambiar conocimientos útiles para una mejor comprensión e implementación de este derecho como un derecho fundamental. En 2010, nuevamente como sede del Encuentro, México dio a conocer su Ley Federal de Protección de Datos Personales en Posesión de Particulares que, de acuerdo con Peschard (2010), incorpora a nuestro país al selecto grupo de democracias modernas porque reconoce en su Constitución al derecho de acceso a la información y protección de datos para garantizar máxima publicidad en lo público y plena protección a la privacidad de las personas, que colocan al IFAI como órgano responsable. Todos estos hechos en conjunto dieron mayor apertura al tema en México, por eso, su participación en este tipo de foros como espacios públicos enriquece el conocimiento, la práctica del derecho y la creación de políticas públicas.

2.8.3 Ley Federal de Protección de Datos Personales en Posesión de Particulares

Además de la Ley Federal de Transparencia y Acceso a la Información Pública, que incluyó la protección de datos personales dentro del ámbito público, era necesario ampliar la protección y dar cobijo al ámbito privado. Desde 2000, en México se promovieron iniciativas de ley referentes a la protección de datos personales, sin embargo, ninguna se había consolidado puesto que no existía una disposición constitucional que le diera sustento, hasta que las reformas realizadas a la Carta Magna en 2008 otorgaron al Congreso la facultad de legislar en materia de protección de datos en posesión de particulares y reconocieron el derecho a la protección de datos personales y los derechos de ARCO de los titulares.

El 8 de abril de 2010, la Comisión Dictaminadora delimitó el objeto y el ámbito de la ley que protegería los datos personales con base en las principales propuestas presentadas que formaron su columna vertebral. De la misma manera, dictó principios, definiciones, procedimientos, autoridades reguladoras; determinó al IFAI como autoridad garante, los procedimientos de protección ante el Instituto, medidas de seguridad, así como infracciones y sanciones. Acto seguido, el 27 de abril del mismo año, el Senado de la República aprobó el proyecto de Ley, que abarcó los siguientes aspectos (Gaceta 127, 2010):

- Su objeto es proteger los datos personales que poseen los particulares con el fin de que su trato sea legítimo, controlado e informado, para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

- Los sujetos obligados son los particulares que manejan bases de datos personales, con excepción de las sociedades de información crediticia, sus usuarios y los particulares que utilizan los datos personales con fines de uso personal o doméstico. Esta Ley exceptúa a las sociedades de información crediticia dado que están bajo el ordenamiento de la Ley que Regula las Sociedades de Información Crediticia, que prevé los principios y derechos en materia de protección de datos personales, así como los mecanismos que los hacen valer.

- Las disposiciones que suplen esta Ley son el Código Federal de Procedimientos Civiles y la Ley Federal del Procedimiento Administrativo.

- Propone definiciones y términos fundamentales para la aplicación de la Ley. Incluye el principio de licitud, de consentimiento, de calidad, de finalidad, de proporcionalidad, de responsabilidad, de información, de lealtad, los datos personales sensibles y el derecho al olvido.

- Regula la sencillez, agilidad y eficacia del procedimiento ante el responsable para que los titulares puedan ejercer los derechos de acceso, rectificación, cancelación y oposición.

- Regula la "solicitud de protección de datos" que es el procedimiento de protección de derechos ante el IFAI.

- Plantea que el IFAI sea el órgano garante del derecho a la protección de los datos personales, para lo que debía cambiar su denominación a Instituto Federal de Acceso a la Información y Protección de Datos.

- Señala la obligación de la persona, autoridad responsable, encargados y terceros que obtengan, utilicen, transmitan, almacenen o/y resguarden, de establecer medidas de seguridad que impidan el acceso incorrecto a la información.

- Marca infracciones y sanciones para quien trasgreda la Ley.

Con esta ley, México se colocó entre las democracias que cuentan con un marco normativo que regula esta materia y garantiza la seguridad del flujo transfronterizo de datos. La ley incluye una doble vertiente. Por un lado impone obligaciones a los responsables de las bases de datos para que usen la información de acuerdo con lo convenido en esta ley y, por el otro, da al titular el derecho de poder controlar su información que posea cualquier particular: aseguradoras, bancos, tiendas departamentales, universidades, etc. A la vez que las personas pueden acudir ante una autoridad, que es el IFAI, que garantiza total acceso, rectificación, eliminación o borrado de su información, con pleno derecho a oponerse a que ésta sea utilizada a menos que otorgue su consentimiento (Gaceta 127, 2010).

La ley contiene sesenta y seis artículos divididos en diez capítulos. De acuerdo con los legisladores se trata de un modelo que da equilibrio a los principios de protección de datos personales internacionalmente reconocidos, el flujo de información necesario para el desarrollo económico, y las garantías de las que gozan los titulares de los datos de que su

información será tratada de forma lícita e informada, en conformidad con las recomendaciones hechas por la Organización para la Cooperación y el Desarrollo Económico (Gaceta 127, 2010).

Las excepciones mencionadas en la ley son las sociedades de información crediticia, que van en conformidad con la ley que las regula, y los particulares que utilizan los datos para uso personal o doméstico, sin que presten algún bien o servicio (Gaceta 127, 2010). Respecto a este tema, en entrevista, Antonio Troncoso (2010) manifestó que, a pesar de que en términos generales esta ley cumple con los parámetros internacionales, esta excepción le causa desconcierto: "A mí me llama la atención que hayan eliminado los ficheros de solvencia, por qué el IFAI no puede controlarlos, no lo entiendo, con mucho respeto lo voy a hablar mañana con Jacqueline Peschard (Presidenta del IFAI). El artículo dos es lo que más me inquieta. Yo creo que se debió a una razón intragubernamental, me explicaron en su momento que era por el problema de las situaciones entre ministerios. En México (los datos personales) son controlados por una comisión específica independiente en el ámbito de economía. No pasa nada con que se haga esto pero no tiene sentido que al IFAI le hayan exceptuado el tema de los ficheros de solvencia".

En este orden de ideas, Carmen Fernández (2010), Directora de Datos Personales del IFAI, explicó en entrevista que esta excepción se debió a que las sociedades de información crediticia ya contaban con una regulación, una normativa específica, por lo que el legislador mexicano pensó que por la naturaleza que tienen quedaron destituidas de esta nueva aplicación, porque ya contaban con un marco robusto y su ley prevé los derechos y principios bajo una normatividad específica. Sobre el mismo respecto, Lilia Vélez (2010) expuso que el tema es muy complejo. Desde su punto de vista los sujetos obligados que ahora tiene la ley son los más importantes y se trata de un primer avance, contempla asimismo la posibilidad de que en un futuro las facultades y atribuciones del marco jurídico puedan ampliarse porque las leyes siempre son perfectibles. Según comenta: "Este es un tema nuevo en América Latina y en nuestro país, por lo que habrá que esperar a ver cómo funciona y, si es necesario, se le podría incorporar".

Por su parte, Villanueva (2010) en entrevista opinó que "la ley tiene muchas oportunidades de mejorar, tiene que enriquecerse en distintos rubros. Esto no se hizo porque el propósito fue o

tenemos una ley mala o no tenemos nada y se optó por una ley así. Fue una decisión política. Lo deseable habría sido tener un consenso más amplio y aprobar una ley que reuniera los mayores requisitos posibles. Aquí vemos que la decisión fue mejor tengamos algo de mucho que todo de nada". Asimismo Vélez (2010) comentó que: "el problema con las leyes es que puede existir una ley excelente pero si no va con la realidad en términos institucionales y de recursos se vuelve una ley que no opera. Entonces, lo que ya opera esta ley es un trabajo inmenso, tienen que empezar por ver cómo funciona, necesitan más recursos y gente capacitada. Con el paso del tiempo se podrá evaluar su funcionamiento".

Es evidente que cada país tiene sus particularidades al momento de crear sus leyes. Efectivamente es posible mejorarlas con el paso del tiempo después de ponerlas a prueba y adaptarlas a nuevas circunstancias, tal es el caso de Colombia, en donde como medida preventiva, según explicó Puccinelli (2010), en entrevista, se aprobó una normativa regulatoria de los datos financieros de aquellos que son desaparecidos por las Fuerzas Armadas de la República de Colombia (FARC), que obliga a las entidades financieras a bloquear estos datos porque aparecen como deudores cuando en realidad están secuestrados y no es fidedigno, pero esta modificación se debió a presiones ajenas y posteriores a su creación. Sin embargo, este no es el caso de México, en donde no es concebible que desde su instauración sea considerada alguna reforma para incorporar a las Sociedades de Información Crediticia y más cuando el derecho comparado funciona como guía para su elaboración.

A pesar de esto, desde su perspectiva como periodista y después de haber realizado una investigación sobre la venta de información personal, Luz González (2010) manifestó que las bases de datos de los bancos constituyen información muy delicada que se comercializa, por lo que los bancos deben hacerse responsables de la protección de sus clientes y de sus sistemas, y ve como un problema que las sociedades de información crediticia no sean materia de la nueva ley.

Por otra parte, la Ley de Particulares resalta cuatro ejes desarrollados (Gaceta 127, 2010):

1. Principios reconocidos internacionalmente: licitud, consentimiento, finalidad, proporcionalidad, calidad, información y responsabilidad.

2. Derechos de los titulares de los datos: acceso, rectificación, cancelación y oposición (ARCO).

3. Procedimientos para exigir ante los responsables de las bases de datos los derechos de ARCO, así como el procedimiento para su tutela ante el IFAI, que es el órgano garante.

4. Infracciones y sanciones para quien realice conductas inadecuadas con relación al trato de la información.

Esta nueva ley atiende los principios recogidos en la Resolución de Madrid, aprobada en 2009, que son los *Estándares Internacionales sobre protección de datos personales y privacidad*, y hace hincapié en que la causa que hace legítimo el tratamiento de la información personal es el consentimiento del titular, caracterizado por ser libre, específico, informado e inequívoco (Gaceta 127, 2010). Entre las innovaciones que esta Ley adoptó de la Resolución de Madrid está precisamente el principio de responsabilidad, que según Ivette García (VIII EIPDP, 2010) garantiza que sin importar a quién se manden los datos dentro o fuera del país, siempre se cumplirá con el aviso de privacidad, que resulta fundamental porque la empresa que busque transferir los datos siempre deberá comunicar las finalidades para las que se recaba el dato y notificarle que va a realizar la transferencia. Sin embargo, establece también excepciones al consentimiento del titular en el caso de datos sensibles, que sólo procederán si se cumple con los principios de protección bajo dos condiciones: que el trato sea legítimo, concreto y acorde con las actividades o fin del sujeto regulado, y que se cumpla el principio de proporcionalidad (Gaceta 127, 2010).

Las operaciones bancarias están comprendidas dentro de las fracciones I y IV del artículo 10 de la ley, que permite el tratamiento de datos necesarios para realizar operaciones bancarias entre las instituciones financieras y sus clientes, sin que sea necesario el consentimiento de estos últimos cuando las operaciones sean previstas en una Ley aplicable. Sin embargo, los datos deberán conservar el principio de finalidad (Gaceta 127, 2010).

En el caso de personas menores de edad o incapaces, el consentimiento lo otorgarán sus padres o tutores, o mediante reglas del derecho civil aplicables. Asimismo considera la protección a los datos sensibles, relacionados con preferencia sexual, origen étnico o racial, o estado de salud, grupos vulnerables cuya información puede ser utilizada o mal utilizada para

discriminar o excluir a una persona (Gaceta 127, 2010). Por otro lado, prevé los mecanismos necesarios para ejercer los derechos de ARCO ante los responsables de las bases de datos y, en caso de que sean vulnerados, el titular podrá acudir ante el órgano garante, es decir, el IFAI.

Otra característica de esta nueva ley es que retoma elementos del marco de privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC), que da preeminencia a las decisiones del titular de los datos, sin imponer actividades innecesarias de cumplir a los sujetos obligados (Gaceta 127, 2010):

- No requiere un Registro de las bases de datos en posesión de los particulares.
- No prevé la obligación de solicitar al órgano garante la autorización de las transferencias internacionales, sino mecanismos que garanticen que el destinatario cumple con las mismas reglas de protección que el responsable de los datos (principio de responsabilidad).
- Regula la cooperación de las autoridades sectoriales con el IFAI.
- Equilibra la protección de la persona y el desarrollo de la tecnología y de los mercados, mediante un libre flujo de información transfronterizo, con las garantías necesarias para el uso apropiado del dato.
- Establece la posibilidad a los sujetos obligados de refutar las resoluciones del órgano garante, bajo legalidad, en la imposición de multas.
- Aclara y añade definiciones: bloqueo, transferencia de datos, encargado y tercero.
- Prevé mecanismos de autorregulación que faciliten el cumplimiento de la ley en el país y en el extranjero.

De esta manera, la ley garantiza la seguridad de los datos personales y hace flexible su transferencia necesaria para el desarrollo de las actividades en el marco internacional bajo principios comunes con la tutela de un órgano garante.

El ejercicio de los derechos contenidos en la Ley Federal de Protección de Datos en Posesión de Particulares tendrá vigencia después de 18 meses de su publicación en el Diario Oficial de la Federación ocurrida el 5 de julio de 2010, en ese tiempo el IFAI está obligado a capacitar a

las empresas o cámaras que las agrupan, para encaminarlas hacia la protección de los datos personales (IFAI/081/10). Esto es un gran reto para el IFAI puesto que, además de su nueva labor en materia de protección de datos personales, sigue siendo el órgano que garantiza el acceso a la información y deberá cumplir con ambas funciones.

2.8.4 Leyes sectoriales

Una de las principales críticas hechas a la legislación española en torno a la protección de datos, se encuentra precisamente en que regula de forma sectorial a las instituciones públicas y privadas. El mismo cuestionamiento podría hacerse a esta nueva reglamentación en México, puesto que no es el carácter de público o privado lo que pone en peligro la intimidad de las personas, sino el uso que se hace de su información. Pérez Luño (2001) señalaba que las lesiones del sector privado no son, necesariamente, menores que las que pueden realizarse en el poder de las entidades gubernamentales, por lo que no debería existir diferencia entre uno y otro frente a los posibles abusos perpetrados.

En lo que se refiere a este punto, existen diferentes opiniones de los expertos basadas en la experiencia de su propio país. Por ejemplo, Felipe Rotondo (2010), se basa en el caso de Uruguay, en donde existe una única legislación, y señala la doble tarea que esto representa para el IFAI como órgano garante del acceso a la información y la protección de datos, que puede representar un problema orgánico. Por su parte, Oscar Puccinelli (2010), de Argentina, expresó que cada país tiene sus particularidades, por ejemplo, la ley de su país es prácticamente una copia de la ley española y sigue con esa tradición, aunque no cuentan con una unidad específica de acceso a la información pública sino solamente con la Dirección Nacional de Datos. Explicó que su ley también prevé normativa general para el tratamiento de datos tanto de particulares como del Estado y establece los principios básicos y las excepciones, pero argumenta que los datos son únicos y deben ser tratados de igual manera tanto en el sector privado como en el sector público, "tampoco se ve como un escándalo que haya un número nacional único, hay un documento nacional de identidad que tiene el mismo número que se usa para la seguridad social y para la identificación tributaria, hay países que están totalmente en contra de esa idea, lo consideran como una violación fragrante a la protección de datos".

Una opinión que no favorece la doble regulación en México la dio Ballester Fernández (2010), de España, quien dijo: "Nosotros en España lo hemos unificado, las personas son únicas, entonces no distinguimos entre empresas privadas o empresas públicas. La misma reglamentación tiene que funcionar para todas las instituciones. Así, lo que se hace es que se discrimina y nosotros lo que hemos hecho es concentrado. Sólo tenemos una ley de privacidad que además también emana de las directivas europeas". Pero, a pesar de que en España poseen una misma ley, su ley es sectorial porque distingue los ficheros públicos de los privados, a lo que agregó: "Se menciona específicamente que las bases de datos públicas tienen que estar protegidas de una manera mucho más especial, por ejemplo los datos de la policía o de los contribuyentes. Los gobiernos tienen muchos más datos de carácter personal y lo que se ha hecho es que se ha modificado todo en un solo modelo: niveles de datos básicos, medios y altos. Entonces debe protegerse cada uno de esos distintos tipos de nivel. Es mucho más simple aplicar los mismos criterios independientemente de que sean públicos o privados, por ejemplo pueden existir empresas privadas del ámbito sanitario que van a aplicar las mismas medidas de seguridad que una del sector públicos". Y añadió que la discriminación se genera porque las instituciones públicas que tienen mayor poder pueden ejercer mayor abuso sobre los datos de las personas.

A esto, Emmanuel de Gibry (2010), de Francia, comentó que no encuentra discriminación como se mencionó anteriormente, pero la legislación francesa, a partir de su modificación en 2004, no se rige por el criterio de lo público o privado, aunque regula estos sectores, sino por el carácter sensible de los datos personales.

Sumado a esta desigualdad, cabe destacar que la LAI tuvo que implementar los lineamientos de protección de datos personales adicionales para llenar los vacíos que tenía en esta materia. Una de sus debilidades de la LAI es que no garantiza los derechos de ARCO, únicamente garantiza el acceso y la modificación de los datos. Por tanto, tampoco garantiza la autodeterminación informativa. Es necesario mencionar que muchos de los abusos ocurridos a la protección de los datos han sido desde el sector público, por mencionar el caso de Choice Point y la venta de bases de datos importantes que, se supone, son resguardadas por las instituciones públicas.

A todo esto, Carmen Fernández (2010), argumenta sobre la particularidad del caso de México, y explica que se trata de dos leyes porque son dos sectores: "Lo que pasa es que es un derecho que está previsto en la Constitución pero tiene dos factores que lo regulan. El artículo seis prevé el acceso a la información y uno de sus límites es el acceso a los datos en donde prevé las bases para la protección de los datos en el sector público, pero recordemos que a nivel público hay estados con la facultad para regular al margen de la LAI porque cada estado es autónomo. En el nivel privado no teníamos ninguna regulación hasta que se reformó el artículo 16 constitucional que dio contenido al derecho. Una vez que se reformó la Constitución se emitió la Ley de Protección de Datos para el sector privado. Entonces es una ley que ya estaba antes y una ley que llegó y, por lo tanto, no pudieron estar en la misma porque una es una ley nacional que es la del sector privado y la otra es federal y estatal a la vez, entonces no podíamos hacer una ley general de datos porque no podíamos decirle a los estados qué hacer con los datos cuando ya lo tenían regulado, entonces esa fue la problemática para nosotros (el IFAI).

Aclaró además que: "Los órganos estatales no tienen que hacer nada que ver con el sector privado, únicamente pueden ayudarnos a difundir el derecho. Es una responsabilidad que el IFAI va a realizar a nivel nacional, por eso estamos pensando en mecanismos que nos ayuden a llevar a cabo el trabajo. En julio (de 2011) debemos tener el reglamento, las empresas deben tener su aviso de privacidad y en enero de 2012 ya tienen que presentar sus solicitudes de derechos ARCO y en febrero sus recursos ante el Instituto (Fernández, 2010)".

A pesar de todo esto, para Villanueva (2010) lo ideal sería tener una misma ley sin distinción alguna y que no elimine a las sociedades de información crediticia, puesto que se trata del mismo objeto y bien jurídico protegido. Esto sin considerar que la Resolución de Madrid no distingue entre el sector público y privado y teóricamente la ley mexicana cumple con sus principios.

Es necesario recordar que además de que los datos personales están regulados por dos leyes sectoriales, la pública y la privada, también lo están por la Ley de las Sociedades de Información Crediticia, lo que en un futuro podrá ocasionar diferencias en el tratamiento de la información.

Las principales diferencias y similitudes de las dos legislaciones vigentes hasta el momento, se encuentran contenidas en el siguiente cuadro.

Sus principales diferencias recaen en las definiciones, derechos, principios, plazos, obligaciones, excepciones, infracciones, sanciones, delitos, etc. En general, la LAI, para suplir sus vacíos, recurre a los Lineamientos que detallan de forma más específica la forma en que procede este derecho.

	Sector Privado	Sector Público
Denominación oficial	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental / Lineamientos de Protección de Datos Personales
Fecha de publicación	5 de julio de 2010	11 de junio de 2002
Vigencia Ley a partir de	6 de julio de 2010	12 de junio de 2002
Ejercicio del derecho desde	18 meses después de su publicación	12 de junio de 2003
Artículos en ley	69	64
Artículos transitorios	8	11
Reglamento de ley	Al año siguiente después de su entrada en vigor	Sí
Aspectos que regula	Protección de datos personales	Transparencia, acceso a la información, protección de datos personales
Objeto	La protección de los datos personales en posesión de los personales, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.	Proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal. / Establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, para asegurar su tratamiento adecuado e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado (Cap. I, Primero).
Sujetos obligados	Personas físicas o morales de carácter privado, excepto sociedades de información crediticia y personas sin fines de	Poderes Ejecutivo, Legislativo y Judicial de la Federación, órganos constitucionales autónomos, tribunales

	divulgación.	administrativos federales y cualquier otro órgano federal.
Algunas definiciones	Aviso de privacidad: Documento físico, electrónico o de cualquier otro formato generado por el responsable para disposición del titular. Bases de datos: Conjunto de datos personales referentes a una persona identificada o identificable. Bloqueo: Identificación y conservación de datos personales una vez cumplida la finalidad para determinar posibles responsabilidades con su tratamiento hasta el plazo legal. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa su tratamiento. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización pueda dar origen a discriminación o conlleve un riesgo grave para éste. Días: Días hábiles Disociación: Procedimiento mediante el cual los datos personales no pueden asociarse al titular. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable. Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, en conformidad con lo señalado en el Reglamento. Instituto: Instituto Federal de Acceso a la Información y Protección de Datos. Ley: LFPDPP. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Secretaría: Secretaría de Economía. Tercero: La persona física o moral, nacional o extranjera,	LAI Datos personales: Cualquier información concerniente a una persona física, identificada o identificable. Instituto: Instituto Federal de Acceso a la Información Pública y Protección de Datos. Información: La contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título. Información reservada: Aquella información que se encuentra temporalmente sujeta a alguna excepción. Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado. Unidades administrativas: Las que de acuerdo con la normatividad de cada uno de los sujetos obligados tengan la información de conformidad con las facultades que les correspondan. LDP Destinatario: Cualquier persona física o moral pública o privada que recibe datos personales. Encargado: El servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el Responsable para llevar a cabo el tratamiento. Sistema “Persona”: Aplicación informática desarrollada por el Instituto para actualizar el listado de los sistemas de datos personales que posean las dependencias y entidades para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos. Responsable: Servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado

	distinta del titular o del responsable de los datos. Titular: La persona física a quien corresponden los datos personales. Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.	de datos personales, así como el contenido y finalidad de los sistemas de datos personales. Titular de los datos: Persona física a quien se refieren los datos personales que sean objeto de tratamiento. Transmisión: Entrega total o parcial de sistemas de datos a cualquier persona distinta al Titular. Transmisor: Dependencia o entidad que posee los datos personales objeto de la transmisión. Tratamiento: Operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar los datos personales. Usuario: Servidor público facultado por un instrumento jurídico o autorizado por el Responsable que utiliza cotidianamente los datos personales.
Principios de protección	Licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.	LAI: Adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido. LPD: Licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión
Excepciones al consentimiento	Esté previsto en una ley, los datos estén en fuentes de acceso público, los datos se sometan a un procedimiento previo de disociación, cumpla obligaciones derivadas de una relación jurídica entre el titular y el responsable, exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes, y sean indispensables para cuestiones de salud mientras el titular no esté en condiciones en términos que establece la Ley General de Salud, o cuando se dicte resolución de una autoridad competente.	Sean necesarios por razones estadísticas, científicas o de interés general previstas en la Ley, cuando se transmitan entre sujetos obligados o entre dependencias y entidades, cuando exista orden judicial, a terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos, y en los demás casos que establezcan las leyes (Art. 22).
Plazo para eliminar información una vez cumplida su finalidad	72 meses (seis años)	a) El que se haya establecido en el formato físico o electrónico por el cual se recabaron;

		b) El establecido por las disposiciones aplicables; c) El establecido en los convenios formalizados entre una persona y la dependencia o entidad, y d) El señalado en los casos de transmisión.
Obligaciones del responsable	Velar por el cumplimiento de los principios de protección de datos (Art. 14). Informar a los titulares de los datos la información que se recaba de ellos y con qué fines, mediante el aviso de privacidad (Art. 15). Las vulneraciones de seguridad ocurridas, serán informadas por el responsable al titular, a fin de que pueda tomar las medidas correspondientes (Art. 20). El responsable o terceros deberán guardar confidencialidad, aun después de finalizar su relación con el titular o con el responsable (Art. 21).	El responsable deberá hacer del conocimiento al Titular de los datos la mención de que serán protegidos en términos de lo dispuesto por la Ley, el fundamento legal y la finalidad del Sistema de datos personales (LDP).
Derechos de los Titulares	Acceso, rectificación, cancelación y oposición ante el responsable o terceros (arts. 22 y 25).	Acceso, modificación (Arts. 24 y 25 LAI).
Plazo para comunicar la determinación adoptada	20 días (art. 32)	
Plazo para proceder	15 días a partir de la notificación (art. 32)	Diez días para acceso (art. 24 LAI). 30 días para modificación (art. 25 LAI).
Excepciones a los derechos de los titulares	Cuando el solicitante no sea el titular de los datos personales, o el representante legal no está correctamente acreditado. Cuando el responsable no tiene en su base de datos al solicitante. Cuando lesionen los derechos de un tercero. Cuando haya un impedimento legal o la resolución de una autoridad competente. Cuando la rectificación, cancelación u oposición haya sido	En caso de negarse, el Comité de Información deberá fundar y motivar la improcedencia total o parcial de las modificaciones que se solicitaron, e indicar al titular.

	realizada anteriormente.	
Costos de solicitud	Gratuito (excepto cargos de envío que corren por cuenta del titular). Únicamente se cobrará un costo de no mayor a tres días de salario mínimo vigente en el Distrito Federal, cuando la persona reitera su solicitud en un periodo menor a doce meses.	Gratuito (excepto cargos de envío que corren por cuenta del titular). Si la persona reitera su solicitud en un periodo menor a doce meses el costo no deberá ser superior al costo de los materiales utilizados y el costo de envío.
Transferencia de datos	Necesita el consentimiento del titular para la transferencia a terceros nacionales o extranjeros. No será necesario el consentimiento cuando: La transferencia esté prevista en una Ley o Tratado al que México pertenezca; Sea necesaria para prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios; Se realice a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o cualquier sociedad del mismo grupo; Sea necesaria por un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; Para salvaguardar un interés público, o para la procuración o administración de justicia; Sea precisa para reconocer, ejercer o defender un derecho en un proceso judicial, y Mantenga o cumpla una relación jurídica entre el responsable y el titular.	Se realizarán cuando así lo prevea de forma expresa una disposición legal y cuando medie el consentimiento del titular (Lineamiento vigésimo segundo). No será necesario el consentimiento de acuerdo con lo convenido en el art. 22 de la LAI: Razones estadísticas, científicas o de interés previstas en la ley. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando se utilicen para el ejercicio de facultades propias de los mismos. Cuando exista orden judicial. A terceros, cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales, que no deberán utilizar los datos para propósitos distintos a aquéllos para los que se les transmitieron. En los demás casos que establezcan las leyes.
Obligaciones del Instituto	Difunde el conocimiento del derecho a la protección de datos, promover su ejercicio, vigilar su cumplimiento e imponer sanciones según corresponda (arts. 38 y 39).	Supervisar la protección de los datos y establecer las sanciones correspondientes al incumplimiento de la Ley y los lineamientos (Cap. VII Lineamientos).
Contenido de la solicitud de acceso, rectificación, cancelación u oposición	Nombre del titular, representante legal y tercero interesado (si es que lo hay). Nombre del responsable ante el cual se presentó.	Recurso de revisión (art, 54 LAI): La dependencia o entidad ante la cual se presentó la solicitud. El nombre del recurrente y del tercero interesado (si lo hay),

ante el Instituto / Recurso de revisión	Domicilio para oír y recibir notificaciones. La fecha en que se dio a conocer la respuesta del responsable. Los actos que motivan su solicitud de protección de datos. Demás elementos que considere necesarios. (Art. 46).	domicilio o medio para recibir notificaciones. Fecha en que se le notificó o tuvo conocimiento del acto reclamado. El acto que se recurre y los puntos de la petición. La copia de la resolución que se reclama y la notificación que corresponde. Los demás elementos que considere necesarios.
Infracciones	No cumplir con la solicitud del titular para los derechos de ARCO con incumplimiento a la Ley. Actuar con negligencia o dolo en el trámite y respuesta de solicitudes de ARCO. Declarar la inexistencia de datos personales, cuando existen total o parcialmente en la base de datos del responsable. Tratar los datos de forma contraria a los principios establecidos. Omitir en el aviso de privacidad, elementos del artículo 16 de esta Ley. Mantener datos inexactos, no realizar las rectificaciones o cancelaciones cuando afecten los derechos de los titulares. No cumplir con el aviso del art. 64. Incumplir el deber de confidencialidad. Cambiar sustancialmente la finalidad del tratamiento. Transferir datos a terceros sin comunicar el aviso de privacidad. Vulnerar la seguridad de bases de datos. Transferir datos fuera de los casos que permite la ley. Recabar o transferir datos sin el consentimiento del titular, cuando éste sea exigible. Impedir la verificación de la autoridad. Recabar información de forma fraudulenta. Hacer uso ilegítimo de los datos cuando el Instituto o los titulares han solicitado el cese. Impedir o afectar el ejercicio de los derechos de ARCO. Contravenir el segundo párrafo del artículo 9 de esta Ley. Incumplir con las obligaciones establecidas por lo previsto en	Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de forma indebida la información. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información. Denegar información no clasificada como reservada o no confidencial de manera intencional. Clasificar como reservada información que no cumple con las características de la Ley. Entregar información considerada como reservada o confidencial por la Ley. Entregar de manera intencional información no completa requerida en una solicitud de acceso. No proporcionar la información a que se refiere el punto anterior. (Art. 63 LAI).

	esta Ley. (Art. 63).	
Sanciones	Con base en la naturaleza del dato, la improcedencia del responsable, el carácter intencional, la capacidad económica del responsable y la reincidencia, las sanciones serán (arts. 64 y 65): Multa de 100 a 160 mil días de salario mínimo vigente en el Distrito Federal en los siete primeros casos previstos en las infracciones. Multa de 200 a 320 mil días de salario mínimo vigente en el Distrito Federal, en los casos previstas en las fracciones VIII a XVIII de las infracciones. En caso de que persistan las infracciones citadas se impondrá una multa adicional de 100 a 320 mil días de salario mínimo vigente en el Distrito Federal.	Las sanciones derivadas del incumplimiento de esta Ley, se realizarán en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores públicos (art. 63 LAI).
Delitos	De tres meses a tres años de prisión a quien tenga autorización para tratar datos personajes y vulnere su seguridad con ánimo de lucro. Prisión de seis meses a cinco años a quien trate datos personales mediante engaño, con lucro indebido, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. En el caso de datos sensibles, las penas anteriores se duplicarán.	Las responsabilidades administrativas generadas por el incumplimiento a que se refiere el artículo 63, son independientes de las del orden civil o penal que procedan (art. 64).

Tabla 2. Comparación de leyes de protección de datos personales en México

2.8.5 Proyecto de Decreto para reformar la Ley Federal de Acceso a la Información y Protección de Datos Personales

Dadas las diferencias tan marcadas entre las leyes que protegen la información personal en nuestro país, sobre todo las carencias de las que padecía la LAI en materia de datos personales al considerar que inicialmente se trató de una ley que buscaba garantizar el acceso a la información pública y la transparencia, el 29 de abril de 2010, entró a la Cámara de Diputados la minuta para reformar, adicionar y derogar algunas disposiciones de esta Ley.

Para comenzar, esta propuesta modifica su denominación y propone que se llame "Ley Federal de Acceso a la Información y Protección de Datos Personales". Este proyecto de Ley plantea su división en dos libros: el Libro Primero corresponde al "Derecho de Acceso a la Información Pública Gubernamental", y el Libro Segundo, al que llama "Derecho de Protección de Datos Personales", que garantiza la protección de datos personales de manera similar a la Ley en Propiedad de Particulares, con la diferencia de que regula al sector público. Por lo tanto, de acuerdo con esto, en la nueva Ley quedaría derogado el capítulo IV que la LAI dedica a la protección de datos personales puesto que estaría establecida en el Libro Segundo.

Con respecto al Libro Segundo, Fernández (2010) explicó que se trata de la ley de protección de datos del sector privado, reformada y adecuada para el sector público, que va a aplicar para el Ejecutivo, Legislativo y Judicial Federal y que será la base para todos los estados pero estos últimos tendrán que crear su propia normatividad. Actualmente esta propuesta únicamente está a la espera de la aprobación del Ejecutivo, aunque, como se ha estudiado anteriormente, a opinión de los expertos continúa siendo complicado que se apliquen dos leyes para un mismo derecho porque esto no responde al principio de operatividad de la ley.

2.8.6 El IFAI

A pesar de que los expertos en la materia mostraron cierta inconformidad, el IFAI se convirtió en la autoridad correspondiente para atender la protección de datos y, a la vez, garantizar el acceso a la información pública. Entre sus amplias facultades está encargado de vigilar, supervisar, investigar, inspeccionar y sancionar las conductas indebidas para garantizar el cumplimiento y observancia de la ley. Para cumplir con sus nuevas funciones, el IFAI, que conserva este acrónimo, cambió su nombre a Instituto Federal de Acceso a la Información y

Protección de Datos, tal y como lo establecen las reformas de las fracciones II, sobre los datos personales, y VII, sobre el nombre, del artículo 3, referente a las definiciones, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental:

> Artículo 3.- Para los efectos de esta Ley se entenderá por:
>
> VII. Instituto: El Instituto Federal de Acceso a la Información y Protección de Datos, establecido en el Artículo 33 de esta Ley;

El Capítulo II, del Título Segundo, cambió su nombre a únicamente "Del Instituto", y el artículo 33 contenido en el mismo, se modificó de la siguiente manera:

> Artículo 33.- El Instituto es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades.

Con respecto a la doble función del IFAI, Villanueva (2010) manifiesta su desacuerdo con que el Organismo cumpla con las dos tareas: "En el mundo en general, España y otros países, el órgano garante de protección de datos es un órgano especializado y no puede ser especializado en dos cosas, menos cuando pueden entrar en conflicto de derechos, porque de una mano va a decir abre la información y de otra va a decir ciérrala. Esto es una fórmula que se realizó en México por una razón de carácter facilitador y económico, pero no atiende al principio de especialidad que debió haber sido considerado al momento de legislar. Por esto, me parece que desde ahí debió haberse creado un organismo garante de la protección de datos personales y otro dedicado al acceso a la información pública".

Para Villanueva (2010), el principal reto del IFAI será adquirir versatilidad para abrir el acceso a la información por una parte y, por otra, restringir la información en el ámbito personal. Se trata de un problema de organización, principios y diseño. Posiblemente en nombre de la protección de datos personales aparezca un mecanismo regresivo en materia de acceso a la información pública en un mediano plazo, porque el nombre de datos personales se hace sinónimo de restricción informativa, a pesar de que no es así. Hay datos personales que son públicos y datos personales que no lo son, pero si no se diferencia claramente puede generar mayores problemas y tomar a los datos personales como pretexto para no entregar la información pública.

En este mismo sentido, Lilia Vélez (2010), comisionada de la Comisión de Acceso a la Información en Puebla, afirma que en ocasiones, durante la práctica de ambos derechos, cuando las solicitudes de información se convierten en recurso, la unidad de información de los sujetos obligados ha argumentado que se protegen los datos personales para no proporcionar la información y, al momento de realizar el estudio, la Comisión se da cuenta de que no aplica el concepto por lo que ordena que se entregue la información requerida. Este es el mismo dilema al que se enfrenta el IFAI y todas las comisiones para que la protección de datos personales no sea mal interpretada como un bloqueo al acceso a la información pública, por lo que el IFAI deberá ser muy versátil para garantizar el cumplimiento de ambos derechos.

Rotondo (2010) expone el caso de Uruguay, en donde existen dos unidades distintas: una que abre el acceso a la información pública y una unidad diferente de protección de datos personales. Considera un problema orgánico que el IFAI realice las dos tareas, pero es conveniente aclararlo porque los datos que tienen los órganos públicos en principio son públicos, pero pueden tener información que no lo es, es decir, también puede haber datos privados y confidenciales. Finalmente, Rotondo (2010) manifiesta que en cada país hay situaciones institucionales que determinan casos distintos a lo que él plantea, pero desde su punto de vista personal y de su legislación es razonable que exista una única legislación así como un solo órgano garante.

De manera similar, Puccinelli (2010) explica que Argentina tiene una ley que de alguna manera copió de la española y sigue con su tradición, con un sistema similar, no obstante, no cuentan con una unidad específica de acceso a la información pública sino que solamente controla los datos la Dirección Nacional de Datos. Asimismo opina que cada país tiene sus particularidades, con la posibilidad de decidir si el organismo de control tiene que estar en un área de gobierno o en otra, si tiene que juntar las dos funciones o separarlas, pero eso depende de cada nación.

Para Ignacio Núñez (2010), subdirector de datos personales en el Info DF, debió haberse creado una institución dedicada a garantizar específicamente la protección de datos personales. Considera que el IFAI deberá aliarse con las entidades y promover mecanismos de autorregulación para que las empresas cumplan con la ley, si no, al organismo le será muy difícil desempeñar su doble tarea, más si a ello se le suma que el incremento presupuestal

autorizado por la Secretaría de Hacienda para poner en marcha el derecho a la protección de datos personales es de quince millones de pesos, que representa el cinco por ciento, misma cantidad que fue autorizada con anterioridad cuando el IFAI únicamente se encargaba del acceso a la información.

2.8.7 Tratamiento de los datos personales y su regulación en diferentes disposiciones en México

Como se analizó en el primer capítulo, el derecho a la protección de datos personales es un derecho que ha evolucionado considerablemente a partir de la aparición de las nuevas tecnologías de la información. En este sentido, previo a la LAI y a la LPDPP, en México se generaron disposiciones legales que establecen la confidencialidad de cierta información que las personas ceden al Estado y organismos privados para el cumplimiento de determinadas funciones. El siguiente cuadro, basado en Gómez y Ornelas (2006), ejemplifica algunas leyes que ahora son complementarias y artículos que protegen desde su ámbito a la información personal.

.

2.8.6.1 Leyes

Ley	Artículo	Contenido
Código Civil Federal	58 Capítulo XI	58. Señala que los datos del acta de nacimiento son el sexo del presentado, el nombre y apellidos que le correspondan; asimismo, la razón de si se ha presentado vivo o muerto; y la impresión digital del presentado. Marca los procedimientos de rectificación, modificación y aclaración de las actas del Registro Civil. Los daños ocasionados al honor, reputación, vida privada, etc., son protegidos por los artículos 1910 y 1916 y serán sancionados dependiendo del grado de la lesión.
Ley Federal del Derecho de Autor	188	El nombre, seudónimo o imagen de alguna persona determinada, sin consentimiento expreso del interesado, no son materia de reserva de derechos de autor. De la misma manera, infracciona cuando se utilice la imagen de una persona sin su autorización o la de sus causahabientes.
Ley Federal de Telecomunicaciones	49 79	La información transmitida a través de las redes y servicios de telecomunicaciones será confidencial, salvo aquella que por su propia naturaleza sea pública, o cuando medie orden de autoridad competente. Establece una multa para quien intercepte información transmitida por las redes públicas de telecomunicaciones.
Ley de Vías Generales de Comunicación	383, 423, 576, 577 y 578	Los empleados y funcionarios de comunicaciones eléctricas dedicados al servicio están obligados a guardar secreto absoluto y riguroso en lo que respecta al contenido de los mensajes cuya transmisión o recepción haya estado a su cargo, o de los que tengan conocimiento por razón de su empleo, y a no dar ningún informe con relación a los mismos, sino a los signatarios, destinatarios o a la autoridad competente. Impone penas severas a quienes incumplan con lo establecido por estos artículos.
Ley de Información Estadística y Geográfica	5. 20, 37 y 51	Prohíben publicar, en una sola estadística, datos de una sola persona física o moral. Garantiza a los informantes de datos estadísticos la confidencialidad de los que proporcionen. La transferencia de la información sólo podrá proporcionarse a particulares, organismos o gobiernos extranjeros por conducto de la Secretaría o de unidades que formen parte de los servicios nacionales autorizados. Cabe mencionar que la ley específica que los datos deben darse desagregados, es decir, que no pueden
Reglamento de la Ley de Información	3, 77 y 79	

Estadística y Geográfica		asociarse a nadie. Además, se anota que los datos obtenidos para fines estadísticos no tienen validez legal.
Ley Federal de Responsabilidades de los Servidores Públicos	47	El servidor público tiene la obligación de custodiar y cuidad la documentación e información que por razón de su empleo, cargo o comisión, conserve bajo su cuidado o a la cual tenga acceso, impidiendo o evitando el uso, la sustracción, destrucción, ocultamiento o inutilización indebidas de aquellas. Asimismo, debe usar la información reservada a que tenga acceso exclusivamente para los fines a que están afectos.
Código Penal Federal	Título quinto Título Vigésimo Sexto 210	Delitos en materia de Vías Generales de Comunicación y de Correspondencia. Delitos en materia de Derechos de Autor. Sanciona con treinta a doscientas jornadas de trabajo a favor de la comunidad, al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto.
Ley Federal contra la Delincuencia Organizada	16-28	Prevé los supuestos y modalidades en los que la autoridad judicial podrá autorizar la interceptación de comunicaciones privadas.
Código de Comercio	43-44	La Doctrina del Derecho Mercantil reconoce los conceptos de comunicación y exhibición de la contabilidad de los comerciantes. La comunicación trata sobre la presentación de la totalidad de su contabilidad para su examen y la exhibición sobre la develación de asientos y documentos que se relacionan con una operación. El artículo 43 autoriza la comunicación únicamente en caso de sucesión universal, liquidación de compañía, dirección o gestión comercial por cuenta de otro o quiebra. El artículo 44 decreta la exhibición de los libros, registros y documentos de los comerciantes, a instancia de parte de oficio, cuando la persona a quien pertenezcan tenga interés o responsabilidad en el asunto en que proceda la exhibición.
Ley de Instituciones de Crédito	117	El artículo 117 establece el secreto bancario, esto quiere decir que la información y documentación referente a las operaciones y servicios bancarios tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o

		servicio, salvo algunas excepciones.
Ley General de Población	98, 101, 103 y 107	Se refiere a la Cédula de Identidad Ciudadana y a la verificación de identidad por parte de la Secretaría de Gobernación.
Ley Orgánica de la Administración Pública Federal	19	Se refiere a las funciones de registro, archivo e información de las dependencias y entidades de la administración pública.
Código Fiscal de la Federación	69	Obliga a los servidores públicos a guardar reserva respecto de la información proporcionada por los contribuyentes o por terceros con ellos relacionados, así como los datos obtenidos por ese personal en el ejercicio de sus facultades de comprobación.
Ley Federal de Imprenta	1, 2 y 3	Desarrolla los supuestos de ataques a la vida privada, ataques a la moral, asimismo, específica la prohibición de publicar información que puede ser considerada como reservada o confidencial.
Ley Federal de Radio y Televisión	4,6,58 y 66	Prohibición de interceptar, divulgar o aprovechar mensajes, noticias o informaciones que no estén destinados al dominio público y que se reciban por medio de aparatos de radiocomunicación.
Ley para Regular Sociedades de Información Crediticia	5, 18, 25, 28, 37, 38-51 y 56	Establece el tratamiento de la información crediticia de los usuarios del servicio de banca y crédito y los derechos que éstos tienen respecto del servicio que prestan las sociedades de información crediticia.
Código Fiscal de la Federación	69	Obliga a los servidores públicos a guardar reserva respecto de la información proporcionada por los contribuyentes o por terceros con ellos relacionados, así como los datos obtenidos por ese personal en el ejercicio de sus facultades de comprobación. Tratándose de medios electrónicos los datos que se obtengan del contribuyente para la obtención de su certificado o sello digital (como sus datos biométricos) no formarán parte del secreto fiscal.
Código Federal de Instituciones y Procedimientos Electorales	92, 135-140, 141 y 164	Señala el tratamiento que deben recibir los datos personales que constituyen el padrón electoral, así como las medidas de seguridad y los supuestos en que está permitida su transmisión a los partidos políticos.
Ley Federal de Protección al Consumidor	16, 17, 18, 18 bis, 76 bis	Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella…El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio. El

		proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor.
Reglamento de la Ley Federal de Protección al Consumidor	22	Establece los lineamientos para el cumplimiento del artículo 16 de la Ley.
Ley General de Salud	77 bis 37	Establecen ciertos derechos con respecto a la confidencialidad y a la información.
Reglamento de la Ley General de Salud en materia de Prestación de Servicios de Atención Médica	29, 32 y 35	
NOM 168-SSA1-1998 del expediente clínico		

Tabla 3. Artículos de leyes que protegen la privacidad

Existen, además de las mencionadas, otras leyes relacionadas con la protección de la información personal:

- Ley de Fiscalización Superior de la Federación (Art. 16)
- Ley de Inversión Extranjera (Art. 31)
- Ley de Policía Federal Preventiva (Art.12)
- Ley de Protección y Defensa al Usuario de Servicios Financieros (Art. 14 y 15)
- Ley del Banco de México (Art. 58)
- Ley Federal de Correduría Pública (Art. 15)
- Ley Federal del Equilibrio Ecológico y la Protección al Ambiente (Art. 190)
- Ley General que establece las bases de coordinación del Sistema Nacional de Seguridad Pública (Art. 22)
- Ley Orgánica de la Procuraduría General de la República (Art. 54)

2.8.7.2 Reglamentos

Asimismo están otras disposiciones en la legislación federal, como los reglamentos:

- Reglamento de la Ley de Pesca (Art. 45 y 111)
- Reglamento de la Ley Reglamentaria del art. 5 Constitucional relativo al ejercicio de las prestaciones en el Distrito Federal (Art. 48)
- Reglamento de operación del comité técnico de valuación de la Secretaría de la Reforma Agraria (Art. 37)
- Reglamento de Transparencia y Acceso a la Información Tribunal Federal de Conciliación y Arbitraje (Art. 17, 18, 19 y 20)
- Reglamento del Banco de México relativo a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Art. 5)

- Reglamento del Instituto Federal Electoral en materia de Transparencia y Acceso a la Información Pública Gubernamental (Art. 26 y 27)
- Reglamento General de Deberes Navales (Art. 307 y 342)
- Reglamento Interior de la Comisión Nacional Bancaria y de Valores (Art. 16, 17, 33, 34, 35, 36 y 54)
- Reglamento Interior de la Junta de Conciliación y Arbitraje (Art. 46)
- Reglamento Interior del Banco de México (Art. 30 y 31)
- Reglamento Interior del Instituto Federal de Acceso a la Información Pública (Art. 23 y 26)
- Reglamento Interno del Consejo Nacional para la Prevención y Control del Sida (Art. 19)

2.8.7.3 Jurisprudencia

En varias ocasiones la Suprema Corte de Justicia de la Nación se ha referido a los rasgos que caracterizan la noción de lo "privado". La ha relacionado con: "lo que no constituye vida pública; el ámbito reservado frente a la acción y el conocimiento de los demás; lo que se desea compartir únicamente con aquellos que uno elige; las actividades de las personas en la esfera particular, relacionadas con el hogar y la familia; o aquello que las personas no desempeñan con el carácter de servidores públicos (Tesis aislada no. 165823, 2009)".

La tesis aislada no. 165823 de la Jurisprudencia recuerda que el derecho a la vida privada está reconocido y protegido en las declaraciones y tratados de derechos humanos que forman parte del orden jurídico mexicano, tales como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y la Convención sobre los Derechos del Niño. En su interpretación, estos organismos internacionales destacan que la noción de vida privada incumbe a la esfera de la vida en la que las personas pueden desarrollar libremente su identidad, y la han extendido a múltiples derechos, como la inviolabilidad de la correspondencia y de las comunicaciones en general, la inviolabilidad del domicilio, las garantías respecto de los registros personales y corporales, las relacionadas con la recopilación y registro de información personal en bancos

de datos y otros dispositivos; el derecho a una vivienda adecuada, a la salud y a la igualdad; los derechos reproductivos, o la protección en caso de desalojos forzados.

Asimismo explica que las resoluciones nacionales e internacionales reconstruyen la imagen general que evoca la idea de privacidad, en la que las personas tienen derecho a gozar de un ámbito de proyección de su existencia reservado de la invasión de los demás, con condiciones adecuadas para el desenvolvimiento de su individualidad. En otras palabras, la idea apela al derecho que tienen las personas de mantener fuera del conocimiento de los demás determinadas manifestaciones o dimensiones de su existencia (conducta, datos, información, objetos), y a que los demás no invadan sin su consentimiento. Así el derecho a la vida privada implica el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, contra el uso abusivo de comunicaciones privadas, la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular (Tesis aislada no. 165823, 2009).

En este mismo orden de ideas, la Tesis 168944 (2008) defiende el derecho a la intimidad como una esfera que separa el ámbito público y el privado. Garantiza al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sea particulares o los Poderes del estado. Este derecho atribuye al titular el poder resguardar ese ámbito para sí y su familia y poseer la intimidad para controlar sobre la publicidad de la información que le concierne, traducido como 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 conservar en secreto, así como decidir quién y bajó qué circunstancias puede usarse. De esta manera el derecho a la intimidad asigna obligaciones a los poderes públicos y a particulares las obligaciones de: “no difundir información de carácter personal entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; asimismo, el Estado a través de sus órganos debe adoptar todas las medidas tendentes a hacer efectiva la protección de este derecho (Tesis 168944, 2008).

Otra determinación de la jurisprudencia la presenta la tesis aislada 166037 (2009) referente a la toma de fotografías a quienes no tienen calidad de detenidos o presuntos responsables. De

acuerdo con ésta, tomar fotografías a personas que no están a disposición del Ministerio Público en calidad de detenidas o presuntas responsables es un acto de molestia porque restringe los derechos de la persona, cuando hace uso de su imagen, sumado a que obtener fotografías puede trasgredir los derechos a la honra y a la dignidad que contienen los artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y el 11 de la Convención Americana Sobre Derechos Humanos, si el Estado incumple con sus obligaciones referentes a la protección de datos personales, que consisten en: a) solicitar o registrar información que contenga datos personales únicamente en los casos que la ley prevé; y, b) tratar de forma confidencial esos datos, lo que implica usarlos o revelarlos solamente con el consentimiento de la persona a la que pertenecen.

Por lo tanto, si la autoridad obtiene fotografías de cualquier persona sin importar cuál es su situación jurídica, menoscaba y deteriora sus derechos pues el acto de molestia continúa mientras el resultado del acto, es decir las fotografías, no se elimine (Tesis aislada 166037, 2009).

De igual forma, previo a la aprobación de la Ley de Protección de Datos en Posesión de Particulares, la jurisprudencia consideró de orden público e interés general los lineamientos por los que se determina la operación y funcionamiento del Registro Público de Usuarios –personas físicas- que no deseaban que su información fuera utilizada para fines mercadotécnicos o publicitarios, ya que su concesión afectaría el interés social y contravenía disposiciones de orden público, puesto que su finalidad era otorgar seguridad al limitar que la información de las personas físicas fuera utilizada para fines mercadotécnicos o publicitarios, y evitar abusos o irregularidades en su transmisión y comunicación, que generen manejo indiscriminado, ocasionando riesgo, incertidumbre y molestias frente al interés particular de quien quiere divulgarlos o usarlos con fines comerciales, propios o de terceros. Así, la jurisprudencia negó la suspensión en el juicio de garantías contra los efectos y consecuencias de estos lineamientos porque afectaría el interés social y contravendría disposiciones de orden público (Tesis aislada no. 166780, 2009).

2.8.7.4 Legislación estatal

Las legislaciones estatales en materia de transparencia y acceso a la información sumaron a su contenido la protección de datos personales. Lilia Vélez (2010) señala que estas leyes se

hicieron en promedio entre 2004 y 2005 cuando el concepto de protección de datos personales todavía no estaba bien desarrollado en México, por lo que en general son leyes que necesitan mejorarse, o bien, generar dos leyes, como han hecho algunos estados, una en materia de acceso a la información y otra en protección de datos personales.

Entre estas leyes se encuentran:

- Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila
- Ley de Protección de Protección de Datos Personales del Estado de Colima
- Ley de Protección de Datos Personales para el Distrito Federal
- Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato
- Código Civil del Estado de Jalisco (Art. 40 Bis sobre datos personales)
- Ley de Información Pública, Estadística y Protección de Datos Personales del Estado de Morelos
- Ley de Protección de Datos Personales del Estado de Oaxaca
- Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Tlaxcala

Vélez (2010) mencionó en entrevista que sería ideal que se establecieran los mínimos que deberían contener las leyes estatales en materia de protección de datos con el fin de plantear criterios homogéneos, tales como: definiciones similares, principios y derechos ARCO, porque varias de las legislaciones de los estados carecen de ellos.

Para Villanueva (2010) todas estas leyes son simbólicas puesto que hay una discusión si la protección de datos personales era un tema de orden federal, de una ley general o una normativa como la que existe hoy. Si fuera una normativa de orden general habría una misma ley con aplicaciones puntuales en cada estado, bajo un mismo procedimiento y principio, pero no ocurre así. Cada ley estatal se hace a imagen y semejanza de las necesidades políticas de cada entidad federativa, tienen algunos puntos en común pero también muchas diferencias

sustantivas que dan cuenta del profundo desconocimiento que hay en la materia y del propósito de tener una ley por cumplir con esa finalidad independientemente de que sirva o no (Villanueva, 2010).

El problema es que en realidad las leyes de datos personales estatales tienen una eficacia y cumplimiento reducidos. Sus deficiencias recaen principalmente en: los mecanismos de protección de datos personales, la definición de los alcances de la ley y los mecanismos que tienen para asegurar el cumplimiento de la norma. Hay un problema de carencia de carácter técnico jurídico porque los medios no están suficientemente bien elaborados para cumplir con el fin que es la protección de datos, y porque hay leyes parciales que, dependiendo del estado, algunas son más protectoras, semicomprensivas o reducidas que otras. Todo esto provoca que la protección de datos personales sea un tema similar al acceso a la información pública antes de la reforma al artículo 6º. Constitucional cuando las leyes no eran uniformes, porque no hay una regulación específica en el ámbito constitucional de datos personales que diga qué elementos deben incluir de forma desglosada y, como consecuencia, se genera dispersión legislativa (Villanueva, 2010).

Por su parte, Fernández (2010) explica que lo que sería la Ley Federal de Transparencia y Acceso a la Información y Protección de Datos, de aprobarse, constituirá la base de las leyes de los estados pero estos tendrían que elaborar su normatividad propia. Posiblemente esto dará mayores herramientas a las legislaciones estatales pero aún así siguen sin establecerse los mínimos que deberían contener estas leyes.

La protección de datos personales en México tiene muchos retos por delante, se trata de un tema naciente que eventualmente debe generar mayor conocimiento mediante la difusión del derecho para que su cumplimiento no quede únicamente como responsabilidad de las autoridades, sino que también exista una cultura de autoprotección generada por una masa crítica. Es interesante conocer el trato que se le ha dado en nuestro país a esta información desde diferentes sectores, que se analizan en el capítulo posterior.