CONCLUSIONES

El derecho a la protección de datos personales corresponde al derecho derivado de la vida privada y la intimidad de las personas que se vio amenazado con la aparición de las nuevas tecnologías porque modificaron la forma de almacenar y distribuir la información que debía ser resguardada. En la búsqueda del bien común, el derecho y la comunicación operan como herramientas indispensables para la creación de leyes y políticas públicas que establezcan límites a la libertad humana dentro de un orden y armonía, como principios básicos de toda sociedad. Por todo esto, es posible concluir que:

1. Los derechos humanos han tenido que evolucionar al paso de las circunstancias y las épocas. Es así como ahora se habla de una tercera generación de derechos relacionados con el uso de las nuevas tecnologías en una cultura posmaterialista que vislumbra la necesidad de reconocer los derechos y libertades mediante leyes específicas.

1.2 Es necesario entender que todo sistema constitucional de derechos fundamentales debe proteger la libertad siempre y cuando no afecte a terceros. De esta manera, el tema de la protección de datos personales se confronta ante ciertas libertades y derechos establecidos, tal es el caso de la libertad de expresión, necesaria para la creación de la opinión pública; el derecho a la información como un derecho fundamental, indispensable para la toma de decisiones como parte del proceso de la comunicación; el derecho de acceso a la información pública que otorga a los ciudadanos la garantía de acceder a la información que está en manos del gobierno para conocer su forma de trabajo, el manejo de recursos públicos, sus resultados y desempeño; el derecho a la vida privada que otorga libertad de creencias, libertad ideológica, derecho a la inviolabilidad del domicilio, etc., o el derecho a la intimidad, ámbito que no puede ser invadido por la difusión de mensajes informativos.

1.3 El avance tecnológico acentuó el peligro que corre la intimidad de las personas porque facilita la intromisión de terceros en la información que se desea resguardar, tal como domicilio, registros privados, conversaciones telefónicas, datos financieros, ideología, historia clínica, etc. Por esta razón era necesario crear leyes y políticas que protegieran la información

personal aunque surgiera cierta tensión entre derechos, pero su regulación se ha convertido en un elemento indispensable para las democracias modernas.

1.4 Es difícil resguardar la información de la vida privada de personas públicas debido a que por su profesión o condición social pueden estar más al alcance de la vida pública, aunque conservan su derecho a la intimidad que les es innato.

1.5 Vivimos en una era la conocida como "sociedad de la información" que continuamente intercambia datos, una mercancía muy valiosa para el desarrollo de diferentes actividades. Los teóricos comparan el impacto de las tecnologías con una nueva revolución industrial que podría ser mejor denominada: revolución tecnológica. No importa la ubicación geográfica ni el tiempo para la realización de distintas operaciones. Esta posibilidad tecnológica es creadora de ciudadanos todopoderosos virtuales dentro de la sociedad de la información.

1.6 De la misma manera en la que el derecho se ha relacionado con la comunicación y la información para garantizar el acceso a ésta, le corresponde también crear medidas legislativas que protejan su seguridad en el intercambio de datos para garantizar la libertad informática. La protección de datos personales proviene del concepto de vida privada, sin embargo, a pesar de que surgió a partir de éste, es un derecho que goza de identidad propia. Se trata de una información de mucho valor que debe ser protegida en el proceso de transmisión porque hace identificable a una persona.

2. El derecho comparado aporta la experiencia de cada país en la materia, los convenios y tratados internacionales son una fuente de colaboración entre Estados para establecer estándares internacionales que faciliten el intercambio de información a la vez que garanticen su protección, y los foros internacionales sirven como espacios en los que los países miembros pueden exponer las particularidades de sus legislaciones y enriquecerse con sus aportaciones en beneficio común, así como evidenciar casos de mal manejo de la información.

2.1 De esto se deduce que todos los lineamientos más específicos sobre la protección de datos personales contienen en general los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) para los titulares, dictan obligaciones para los responsables, tienen principios básicos con estándares internacionales y dejan las sanciones a cargo de los

organismos y legislaciones de cada país, entre los que proponen cooperación mutua en el tratamiento de la información.

2.2 Era importante estudiar el caso de España porque se trata de un país promotor de la protección de datos personales. A pesar de que, a consideración propia de autores españoles, la primera Ley Orgánica de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD) llegó tarde y con errores, la nueva ley, sus reformas legislativas y la actividad de la Agencia Española de Protección de Datos Personales han logrado resultados con impacto a nivel internacional y sirven de ejemplo para otros países.

2.3 Argentina es uno de los países que han seguido el modelo español. Inició su camino por la protección de los datos personales a partir del *habeas data* y del derecho al olvido, y cuenta con un órgano encargado que es la Dirección Nacional de Protección de Datos Personales, aunque no aplica en toda la República Argentina, únicamente su Ley de Protección de Datos no. 25.326. Haber obtenido la acreditación ante la Unión Europea le proporcionó ventajas económicas a las empresas argentinas dentro del comercio internacional porque las hizo confiables con referencia al tratamiento de datos en las transferencias. México carecía de esta protección y este hecho le restaba competitividad al exterior. También es importante observar que la relación cercana que Argentina estableció con otras agencias de protección de datos, tales como la española, canadiense, francesa e inglesa fortaleció el derecho y facilitó el intercambio de información.

2.4 Estados Unidos es un caso muy particular. Por una parte no establece normas estrictas de protección de datos ni cumple con los estándares internacionales, pero por otra busca que se le facilite el acceso a las bases de datos con distintos fines, como es la investigación o prevención de ataques terroristas, a raíz de los atentados de los que fue víctima en 2000, sin ofrecer la misma seguridad a esa información. Bajo el concepto desarrollado por el país norteamericano, *privacy*, Estados Unidos protege los datos personales de manera sectorial. A pesar que el concepto *privacy* surgió a finales del siglo XIX en este país como un producto moderno y optó por proteger la privacidad desde la ley mediante la *Privacy Act* que contiene el *privacy right* para limitar los alcances del Estado, da la impresión de que actualmente Estados Unidos lo percibe como un obstáculo para el desarrollo de sus actividades, tanto que estuvo en contra de la regulación argentina.

2.5 Era importante mencionar la regulación que hay en Estados Unidos en materia de datos personales por la relación comercial que México tiene con este país que incluye el Tratado de Libre Comercio. Esto sin considerar otros sectores como la investigación entre los sectores policíacos que también constituye un riesgo porque adquieren información que fue recopilada con otro fin para otras actividades.

2.6 El hecho de que México no tuviera normas y políticas establecidas que velaran por la seguridad de la información limitaba su desempeño en el mercado internacional que cada vez es más exigente en cuanto al resguardo en el intercambio de bases de datos.

2.7 Las reformas realizadas a los artículos 6 y 16 de la Constitución fueron un paso sumamente importante para la regulación de estos derechos de tercera generación que forman parte de las democracias modernas. En específico estos dos artículos reconocieron únicamente la protección de datos personales en archivos públicos y lo dotaron de autonomía como un derecho fundamental independiente. Mayor fue el avance con la reforma al artículo 73 que dotó al Congreso con la facultad para legislar en materia de protección de datos en posesión de particulares.

2.8 El derecho a la protección de datos personales en México tiene ciertos puntos que destacar:

2.8.1 El hecho de que su reconocimiento como un derecho fundamental en la Constitución llegara de forma tardía ocasionó que su regulación fuera de manera sectorial. En la práctica, esto podrá complicar la aplicación del derecho puesto que los ciudadanos deben buscar su cobertura bajo distintas leyes, su operación se hace más complicada y genera mayor burocracia.

2.8.2 Empezando por el ámbito de aplicación, existen dos leyes que regulan el mismo derecho desde dos ámbitos, el público y el privado, con una ley distinta para cada uno. Si bien es cierto que la ley pública contiene únicamente unos cuantos artículos que protegen la información personal cuyos vacíos se fueron llenando con los lineamientos, es indispensable mencionar que hasta su aparición este derecho no había sido reconocido constitucionalmente como un derecho fundamental. Sin embargo, para la llegada de la ley de particulares ya existía el reconocimiento constitucional que le permitió surgir. Habría sido conveniente, por tanto, a la par de la nueva ley, proponer la reforma a la ley pública pero no en la manera en que está

proyectada ahora, que la deja como parte de la Ley de Acceso a la Información Pública –y plantea que sea llamada Ley de Acceso a la Información Pública y Protección de Datos Personales-, sino que fuera una sola ley con la de particulares. Es incongruente que una ley pública que protege la información personal conforme una misma ley con otra que por otra parte abre el acceso a la información puesto que se trata de derechos de naturaleza opuesta.

2.8.3 A pesar de que efectivamente ya existía una parte que regulaba en el sector público cuando llegó la ley de particulares, la primera carece de muchos elementos, tanto es así que ahora está en proceso de reforma, pero esta reforma pudo haber sido prevista con anterioridad a la vez que se creaba la nueva ley para buscar su integración como una misma, y más todavía cuando este planteamiento de reforma es una adaptación de la ley de particulares al sector público. A pesar del proceso histórico que explica el surgimiento y desarrollo de este derecho en nuestro país, cabe preguntar por qué es necesaria la existencia de dos leyes para defender un mismo derecho en México que, además, excluyen a las Sociedades de Información Crediticia.

2.8.4 Considero, por tanto, que habría sido más conveniente unir estas dos leyes, pública y privada, en una misma, puesto que no es el carácter público ni privado de las bases de datos lo que ponen en peligro la privacidad de las personas sino el uso que se hace de ellos y porque en teoría, México busca estar a la vanguardia en esta materia y cumplir con los principios más recientes que contiene la Resolución de Madrid, que no distingue entre público o privado y opta por la protección igualitaria de la información.

2.8.5 Ahora bien, no es que esté mal que sean dos leyes, o que fuera una misma ley sectorial, aunque las agresiones hechas por uno u otro sector no son mayores unas que otras sin importar su procedencia, pero el hecho está en que para este momento México ya contaba con la experiencia proporcionada por otros países en el derecho comparado para generar una ley más eficaz que facilitara la aplicación del derecho. Tal pareciera que la decisión de hacerla sectorial fue por la urgencia de contar con una ley inmediatamente sin considerar su parte operativa o la naturaleza del derecho, principios a los que debería ajustarse una ley durante su creación, y no obedecer a presiones o intereses políticos. Entre las principales diferencias marcadas por ambas leyes cabe destacar:

- Los Lineamientos de Datos Personales aprobados en 2005 sirvieron para llenar el vacío que tenía la LAI porque delimitan el objeto y ámbito de aplicación, los elementos de datos personales, definiciones, principios, establecen cómo debe ser el tratamiento, transmisión, seguridad, el sistema "persona" y las obligaciones del Instituto. Sin embargo, tampoco contienen todos los derechos de ARCO ni todos los principios más importantes, así como definiciones básicas para el tratamiento de los datos personales.
- En lo que se refiere a las definiciones, también existen muchas desigualdades entre ambas leyes. Las definiciones de la ley pública fueron complementadas con las escritas en los Lineamientos de Protección de Datos Personales, sin embargo, no abarcan todas las de la ley de particulares.

  Por ejemplo, la ley pública no incluye el concepto de Terceros. Los Lineamientos de Datos Personales únicamente se refieren a la transmisión y la definen como la entrega total o parcial de sistemas de datos a cualquier persona distinta al Titular, mas no aclara a quién es el receptor de la información.

  Por su parte, la ley de particulares excluye la definición de Destinatario, que es la persona que recibe la comunicación de datos, independientemente de que sea un tercero o no, mencionado por los Lineamientos de Datos Personales.

  Otra definición muy importante que no contiene la LAI es el Consentimiento, mediante el cual el titular manifiesta su voluntad para el tratamiento de sus datos, tampoco distingue los Datos sensibles, ni menciona el procedimiento de Disociación gracias al cual los datos no pueden asociarse con su titular, a pesar de que estos aspectos los incluyó en los Lineamientos de Datos Personales.
- En cuanto a los plazos, la ley de particulares da 72 meses (6 años) para eliminarlos una vez cumplida su finalidad, pero este lapso de tiempo puede ser exagerado puesto que la información podría ser alterada y caer en uso incorrecto. Por su parte, la ley pública menciona como lapso de tiempo el establecido en el formato físico o electrónico por el cual se recabaron, el establecido por las disposiciones aplicables, por los convenios formalizados entre una persona y la dependencia y el señalado en los casos de transmisión, mas en ninguno de estos casos da alguna guía para saber cómo deben definirse estos lapsos de tiempo o qué condiciones deben cumplir, así lo deja al aire y a la libre decisión de las dependencias para que estas definan cuál es el plazo conveniente de acuerdo con sus

intereses. Una vez que los datos cumplieron con su finalidad, deben tener un límite para su eliminación.

- Un principio muy importante que no tiene la LAI es el de la finalidad. Este principio es indispensable porque limita al responsable a cumplir con las finalidades determinadas y lo obliga a abstenerse de realizar tratamientos que no son compatibles con los fines para los que se recabaron los datos, a menos de que cuente con el consentimiento del titular. Llama la atención que menciona que los datos deben ser adecuados, pertinentes y no excesivos en relación con los propósitos (fines) para los cuales se obtuvo la información, como características del principio de proporcionalidad, mas no menciona el principio de finalidad en sí. Un principio nuevo que contiene la ley de particulares es el de responsabilidad, contenido por la Resolución de Madrid, según la cual el responsable debe adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en la legislación y dotarse de mecanismos necesarios para evidenciar ese cumplimiento, tanto ante los interesados como ante las autoridades que supervisan su ejercicio. Cabe recordar que esta ley es la primera en el mundo en incluir este principio.
- De los derechos de ARCO, la LAI únicamente reconoce dos de ellos en el artículo 24: el acceso y la modificación o rectificación. No es posible para las personas pedir la cancelación u oponerse al manejo de sus datos cuando lo considere pertinente, a pesar de que son derechos básicos de la protección de datos personales.
- Las dos leyes prevén la transferencia a terceros, a pesar de que la LAI no incluye su enunciación dentro de su apartado de definiciones. En ambos casos el requisito para la transferencia es el consentimiento del titular, sin embargo, establecen excepciones para cuando no es necesario. Es evidente que en ocasiones debe ponderarse si el derecho de protección de datos aplica o no cuando. Sin embargo, las razones expuestas por la LAI no son lo suficientemente claras cuando se refiere de manera simple y abierta a "los casos que establezcan las leyes".
- La LAI contiene menos causas de infracción que la ley de particulares, como si las infracciones cometidas por el sector público fueran menores que aquellas que realiza el sector privado. Por ejemplo, no menciona como infracción el hecho de incumplir con el deber de confidencialidad, la transferencia a terceros sin ningún aviso al titular, vulnerar la seguridad de las bases de datos, transferir datos fuera de los casos permitidos por la ley,

etc. Es necesario recordar que no es el carácter de público o privado lo que pone en riesgo a los datos personales sino el uso que se hace de ellos.

- En cuanto a las sanciones, el derecho comparado muestra que sirven como un mecanismo vital para el cumplimiento de la ley, tal es el caso de España, y México ha adoptado esta misma medida. La ley de particulares establece sanciones que clasifica con base en la naturaleza del dato, la improcedencia del responsable, el carácter intencional, la capacidad económica del responsable y la reincidencia. Por su parte, las sanciones indicadas por la LAI son realizadas en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos. Desafortunadamente, estas sanciones pueden caer en la impunidad por la burocracia del sistema público, tal como lo evidencian algunos casos de robos de bases de datos.

  No obstante, para el IFAI las sanciones son el último recurso necesario para hacer cumplir la ley y esperan que funcione más como un incentivo para respetar el derecho. Por lo tanto, no tener que aplicar sanciones sería señal de que el IFAI va por buen camino pero, como mencionaba, sería gravoso que la falta de sanciones se deba más bien a la impunidad y no al respeto de este derecho.

2.9 Por otra parte, cabe destacar que desde el nacimiento de las leyes que protegen los datos personales en nuestro país existe un gran vacío. Explícitamente, la ley de particulares establece en su artículo dos la excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables. Según la experiencia española, este es uno de los sectores de los que más quejas recibe la Agencia y definitivamente México no sería la excepción. Tal parece que esta decisión del legislador obedece más a presiones políticas de otros sectores que a la cuestión técnica porque la Ley de las Sociedades de Información Crediticia no otorga los mismos derechos o garantías, ni está elaborada bajo los mismos principios que operan para proteger la información personal en la ley de particulares, por lo que resulta lamentable que el resultado sea una legislación de aproximación sucesiva. Aunque cabría la posibilidad de que en un futuro el legislador decida modificar la ley de particulares e incluir a este sector para ampliar su marco jurídico, es un procedimiento que pudo preverse desde un inicio porque la información que poseen estas bases de datos es muy delicada y necesita mayor cobertura.

2.10 El tema del órgano garante también es otra cuestión que debo mencionar en esta parte de las conclusiones. El reto que tiene por delante el IFAI es muy grande. Por un lado debe seguir garantizando el acceso a la información pública y por el otro proteger los datos personales. Por tratarse de derechos opuestos también habría sido conveniente la creación de un organismo encargado únicamente de la protección de datos personales que abarque ambos sectores, tanto público como privado, como lo muestra el derecho comparado en la mayoría de los casos, aunque esto requeriría una reconfiguración del IFAI y de la ley pública para quitarle las atribuciones en el ámbito público, ya que, el hecho de que se especialice en dos cuestiones distintas posiblemente repercutirá en un detrimento para alguno de los dos derechos por tratarse de opuestos.

2.11 El IFAI deberá ser un organismo dinámico con la capacidad de diferenciar, sobre todo en el sector público, qué información es pública y cuál es privada, con el fin de evitar que la protección de datos sea un pretexto para entregar la información y que esto no se convierta en un problema orgánico por realizar dos tareas distintas.

2.12 Por otra parte, el IFAI debe dar a conocer de qué se trata este derecho que tiene poco de haber nacido en México, darle difusión y hacerlo cumplir. Lo ideal en este tema es lograr que las instituciones y empresas tomen las medidas preventivas necesarias y establecidas por las leyes y reglamentos para no tener que aplicar sanciones, puesto que su empleo representaría algún abuso o mal uso de la información personal.

2.13 Las leyes públicas estatales son otra cuestión pendiente para la protección de datos personales. Estas leyes comenzaron a aparecer cuando el derecho apenas surgía en México y son muestra del desconocimiento que había sobre el tema puesto que no fueron elaboradas bajo los mismos principios ni procedimientos. Es posible afirmar que son leyes meramente contemplativas ya que carecen de muchos elementos para aplicar el derecho eficazmente y pareciera que únicamente fueron elaboradas con el fin de contar con una ley sin importar si operaba adecuadamente o no. Las legislaciones estatales son leyes no uniformes y dispersas debido a que cada estado ha elaborado su propia articulación de acuerdo con sus necesidades o intereses políticos, pero no en la búsqueda de la aplicación del derecho, que todavía está en una zona de profundo desconocimiento.

3.1 La protección de datos personales es un tema vital en la actualidad y es una garantía para el desarrollo de cualquier actividad. De los casos particulares expuestos sobre algunos sectores expuestos, es posible concluir que:

- Como he comentado con anterioridad, las sociedades de información crediticia son la excepción de la ley que no tiene una explicación técnica sino de intereses y presiones políticas y sectoriales. La información que éstas manejan es alimentada por toda clase de instituciones financieras, compañías de tarjetas de crédito, telecomunicaciones, arrendadoras, autos, tiendas departamentales y demás empresas comerciales. Son datos de millones de usuarios que deberían tener toda la protección que ofrece la nueva ley de particulares y no sólo la cobertura de su ley sectorial.

  Si esta información no recibe el tratamiento adecuado puede representar un serio riesgo para sus titulares porque el cruce de datos fácilmente permite realizar perfiles completos que den a conocer los hábitos de consumo de las personas y, como consecuencia, podrían ser víctimas de secuestro o fraude, en el mayor de los casos, o ser discriminados para acceder a algún servicio o producto por no haber tenido una situación financiera sana con anterioridad, o de recibir propaganda de productos o servicios no deseados mediante llamadas telefónicas, correo electrónico o correspondencia a domicilio, en el menor de los casos.

  Por esta razón, esta tesis insiste en la conveniencia de que la nueva ley de particulares considere la derogación de la parte referente a estas sociedades contenida en su artículo segundo, para que su ámbito de aplicación también sea sobre ellas y que conserve a la Ley de Sociedades de Información Crediticia como una norma supletoria.
- La falta de protección de las bases de datos en poder de órganos públicos es un tema delicado debido a que, en teoría, los organismos de gobierno velan por nuestra seguridad. Sin embargo, desde este ámbito han existido graves fugas de bases de datos nacionales que deberían ser debidamente protegidas, tal es el caso de Choice Point, que fue un detonante muy fuerte que puso en evidencia la necesidad urgente que existía de resguardar la información personal que está en manos del sector público.

  El IFE, por ejemplo, además de los datos personales que identifican al titular, tiene la fotografía que los hace más identificables y, todavía más sensible, la huella digital y firma.

Una sola base de datos contiene información muy valiosa de millones de mexicanos. Toda esta información fue la que adquirió Estados Unidos mediante la empresa Choice Point, que aseguró haber comprado la base de datos dentro del marco legal. La mayoría de las ocasiones quien compra esta información es el Departamento de Seguridad Doméstica de Estados Unidos y el Servicio de Inmigración y Naturalización. Vale la pena aquí recordar que las políticas de protección de datos personales en Estados Unidos son mínimas y aunque supuestamente las destruyeron no hay una verdadera garantía de que realmente así sucedió.

Tal como lo muestra la investigación en torno a este caso, no era la primera vez que Estados Unidos realizaba una compra ilícita de información de otros países. Por esta razón, es cuestionable cómo toda esa información se fugó del IFE, por qué no tenía los candados necesarios y por qué no hubo sanciones ni responsables. La respuesta es sencilla e indignante. Se debía a la falta de ética de quienes operaban la información y ante la inexistencia de una ley protectora y sancionadora. Bajo el argumento de que las leyes mexicanas únicamente protegían y castigaban el mal uso de los documentos públicos electorales y que el padrón no era un documento sino una base de datos, no podía tipificarse el delito porque, hasta ese momento, el derecho a la protección de datos personales no había sido reconocido.

Lo lamentable en México es que este no es el único caso de robo y venta de bases de datos. Por ejemplo, la investigación realizada por la periodista Luz González dio a conocer que en Tepito están al alcance del crimen organizado más bases de datos que supuestamente están bajo el resguardo de organismos públicos, y que toda esta actividad ilícita todavía está en la impunidad, aún cuando ahora sí hay una ley que la sanciona.

- La información del sector salud también contiene datos sensibles que poseen ambos sectores, tanto público como privado. Como lo mostró el derecho comparado, México ha establecido normas que le llevan ventaja a otros países, como Argentina, al establecer un marco legal de protección en torno a la información contenida en los archivos médicos, además de la nueva norma que realiza referente al expediente clínico electrónico avalada por el IFAI para la creación de la Plataforma Nacional de Interoperatividad.

El reto, en este caso, es cumplir con la normatividad para hacer un uso apropiado de toda esta información que, desasociada del particular, puede servir para la investigación o para la academia. Está muy ligado con la ética profesional del médico, aún para determinar los casos en los que debe optar por denunciar alguna situación que pudiera poner en riesgo la salud pública para establecer cercos sanitarios.

- Otro sector muy vulnerable es el educativo. Contiene información de alrededor 25 millones de estudiantes en México además del registro oficial de documentos académicos y de certificación. Se trata de una tercera parte de la población mexicana cuyas bases de datos están inscritos en el Sistema Persona del IFAI. Ahora, con la nueva ley de particulares se espera mayor garantía de la información depositada en las escuelas privadas para evitar que no sea utilizada con otros fines más que los establecidos.
- En el sector de las telecomunicaciones, bajo el pretexto de que la Ley Federal de Telecomunicaciones sólo establece la confidencialidad de la información transmitida mediante las redes y servicios de telecomunicaciones, salvo las excepciones indicadas, algunas empresas del sector privado han incurrido en mal uso de la información de sus clientes sin recibir ninguna sanción. Tal es el caso expuesto de Nextel en el ámbito privado y en el público cabe recordar el caso de Renaut.

  Es lamentable cómo las mismas empresas violan sus propias condiciones de seguridad por cumplir con otros intereses, en detrimento de la confianza que los usuarios depositan en ellas, aprovechando que no existía una ley que sancionara y defendiera los derechos de las personas para que su privacidad no fuera invadida por terceros sin su consentimiento ni para fines no autorizados. De igual forma es asombroso que aún cuando ya existe una ley pública que protege las bases de datos en propiedad de entes de gobierno, con todo y sus deficiencias, ocurran casos como el de Renaut.
- El comercio electrónico requiere la confianza de los usuarios de Internet para que utilicen este medio. La información personal es lo más valioso que las compañías tienen en su poder, por esto es necesario garantizar su seguridad en la red. Cuando las personas saben que sus datos son debidamente resguardados confían más en hacer uso de Internet para realizar sus operaciones. Por esto es importante que las nuevas tecnologías apliquen la autorregulación como un mecanismo que dé confiabilidad a las empresas, además de cumplir lo dispuesto por la ley, lo que se reflejará en el incremento de sus ingresos.

- El tema que está muy de moda actualmente es el de las redes sociales. El dilema de la seguridad en ellas en parte consiste en establecer mecanismos de prevención mediante la educación de los usuarios para que aprendan a autoproteger su información que suben a la red, pero también corresponde a las leyes velar por que estos espacios ofrezcan políticas de privacidad que garanticen el uso adecuado de la información para salvaguardar la integridad física y moral de las personas.
- La autorregulación es indispensable porque si las empresas implementan voluntariamente mecanismos que garanticen cumplir con la ley, además de evitar el riesgo de la sanción, adquieren el beneficio de la confianza de sus clientes.
- El derecho comparado ha servido para esclarecer la relación que existe entre los medios de información y el derecho a la protección de datos personales. Al igual que el acceso a la información, existe también el derecho que tienen los medios de comunicación de informar, cuya actividad está amparada constitucionalmente.

  Se trata de derechos opuestos, aunque también es cuestión de ética del periodista que en ocasiones debe guardar la confidencialidad de su fuente para evitar algún peligro sobre su persona o que sea expuesto de forma injusta. No obstante, el derecho a la protección de datos personales no debe ser pretexto para negar información que la ciudadanía debe conocer cuando el periodista considera su obligación difundirla, y resulta más difícil todavía intentar proteger datos privados cuando se trata de personas que por su actividad son figuras públicas, como lo menciona la jurisprudencia.

Para que la aplicación del derecho a la protección de datos personales en México sea lo más exitosa posible deben intervenir diferentes factores: una ley eficaz, preventiva y sancionadora; un órgano garante; mecanismos de autorregulación de las empresas e instituciones; ética profesional de quienes trabajan directamente con los datos; enseñanza para que las personas conozcan el derecho, lo apliquen y hagan uso consciente de su información personal; cooperación entre naciones para seguir realizando foros y espacios que abran nuevas vertientes y den nuevas aportaciones al derecho que puedan ser llevadas a la práctica con el fin de que no se queden meramente en la teoría y, finalmente, corresponsabilidad de todos los actores involucrados. De esta manera podrá lograrse la armonía necesaria para que los diversos sectores realicen sus actividades dentro del marco de la protección del derecho a la protección de datos personales.

4.1 La Comunicación es una herramienta clave del derecho para la elaboración de políticas públicas. La comunicación pública no pertenece únicamente a las instituciones de gobierno sino también a las instituciones privadas. Es importante que exista un espacio público que dé cabida al desarrollo de asuntos de interés general como ocurría en la plaza pública para la construcción de la democracia. Es la apertura a estos nuevos derechos, como el de la protección de datos personales, los que permiten la evolución de las generaciones de los derechos y las democracias. Parte de este avance ha ocurrido gracias a la participación de la sociedad civil en el espacio público.

4.2 Los medios de comunicación desempeñan un papel fundamental en la creación de políticas públicas por el poder de alcance que tienen y su capacidad para establecer agendas políticas de acuerdo con sus intereses o con la coyuntura. Sin embargo, es lamentable cuando sirven a intereses privados antes de servir al interés público para fortalecer las democracias. Es difícil apuntar si deberían establecer políticas públicas más estrictas para los medios de comunicación cuando se trata de los datos personales puesto que este derecho se topa con la libertad de expresión, sin embargo, la ética es un buen elemento del que debe disponer para decidir cuándo un tema es de interés general y cuándo no, aunque no es suficiente.

4.3 Las políticas públicas creadas en México en torno a la protección de datos personales son el fruto de la participación ciudadana en el espacio público, con la participación de expertos, académicos, profesionistas y medios, que llevaron el tema al ámbito gubernamental. Este movimiento es destaca porque es claro ejemplo en nuestro país de cómo puede llegar a influenciar una colectividad organizada cuando busca un interés común.

1.1 En términos generales, esta tesis propone:

- La creación de un organismo especializado únicamente en la protección de datos personales, independiente del IFAI, que cuente con estructura propia y un presupuesto adecuado para su funcionamiento. Podría llamarse Instituto de Protección de Datos Personales.
- Unir la ley pública y la ley privada en una misma para facilitar la labor del órgano garante y el cumplimiento del derecho.
- Entretanto la legislación siga como está actualmente, con su segmentación de público y privado, eliminar el artículo segundo de la Ley de Particulares referente a las Sociedades

de Información Crediticia y establecer principios mínimos que deben cumplir las leyes estatales.

- Fomentar mecanismos de autoprotección por parte de los titulares de los datos y autorregulación de las empresas que manejan información personal.
- Continuar en la participación de foros internacionales y nacionales abiertos a todas las comunidades para fomentar la cultura de la protección.
- Dar capacitación a los funcionarios de los organismos públicos sobre la protección de datos personales para que conozcan el propósito del derecho.