FUSADES
Fundación Salvadoreña para el Desarrollo Económico y Social

Octubre de 2019 • No. 200

DEL Estudios Legales

Análisis legal e institucional

Observaciones a los proyectos de Ley de Protección de Datos Personales

Parte II: Jurisprudencia constitucional, consideraciones sobre los 2 proyectos de ley y conclusiones

Preámbulo:

En la parte I de este estudio sobre los proyectos de la "Ley de Protección de Datos Personales y Hábeas Data" presentado por ARENA y la "Ley General de Protección de Datos Personales", propuesta por el FMLN, se desarrollaron las observaciones de FUSADES relacionadas con el marco legal nacional y con el derecho comparado como antecedentes, complementados con el estudio de la jurisprudencia que se aborda en esta segunda parte, para luego dar paso al análisis central de este estudio, el cual se enfoca en los elementos de los proyectos en referencia.

1. Jurisprudencia constitucional aplicable a la protección de los datos personales

Existen pocas sentencias de la Sala de lo Constitucional que han hecho referencia a este derecho y que han ido evolucionando, por lo que, si bien se enumerarán todas, solo se tomará como referencia la 142-2012, por ser la más reciente y más completa sobre el tema.

Jurisprudencia constitucional sobre protección de datos personales: Amparos: 142-2012 del 20.10.2014; 118-2002 del 2.03.2004; y 934-2007 del 4.03.2011. Inconstitucionalidades: 36-2004 del 2.09.2005 y 58-2007 del 8.03.2013.

En primer lugar, hay que señalar que la doctrina ha debatido mucho sobre la denominación que deba darse a este derecho-acción: protección de datos personales, hábeas data o autodeterminación informativa, por nombrar los más comunes, así como sobre su naturaleza autónoma o derivada del derecho a la privacidad o a la intimidad[1]. **En la jurisprudencia reciente de la Sala de lo Constitucional, el derecho a la autodeterminación informativa se considera como un derecho fundamental, autónomo, de carácter constitucional y protegible por vía del amparo en sede constitucional (Amparo 142-2012).** En esta misma jurisprudencia se establece que el objeto de este derecho es garantizar

1 Bazán, V. (2005). El hábeas data y el derecho a la autodeterminación informativa en perspectiva del derecho comparado, en Estudios Constitucionales, Año 3, N. 2, Universidad de Talca, pp. 87 y ss. y Murillo de la Cueva, P. (1990). El derecho a la autodeterminación informativa, Tecnos, Madrid.

que las personas podamos tener control sobre nuestra propia información y, por lo consiguiente, la preservación de información de las personas, que se encuentra contenida en registros públicos o privados frente a su utilización arbitraria, especialmente ante los retos que la tecnología impone.

Por otra parte, se establece que se trata de un derecho con una doble dimensión: una material, relativa al contenido del derecho relacionada con la autonomía de las personas en relación con su información personal, y otra instrumental, que se refiere a la posibilidad de controlar la información sistematizada o contenida en bancos de datos informáticos o ficheros. En ambos casos, se activa la posibilidad de ejercer una serie de acciones para conocer, acceder, corregir y suprimir datos para defenderse de cualquier utilización abusiva, incluida la transferencia a terceros y de oponerse a dicha transferencia, con toda la protección reforzada de la que gozan en el país los derechos fundamentales.

En virtud de su calidad de derecho fundamental, el legislador tiene la obligación de crear las instituciones y procedimientos que permitan la protección de este derecho, así como el control de las entidades públicas y privadas que manejen registros o ficheros de datos personales. El amparo 142-2012 también establece que el legislador tiene cierta libertad de configuración del derecho a la autodeterminación informativa, para garantizar la delimitación de las esferas individuales requeridas por la faceta instrumental, de protección y reparación.

La Sala de lo Constitucional también reitera que asociados a este derecho existen ciertos principios que el legislador deberá tomar en cuenta al momento de regular la recolección y resguardo de los datos personales:

1) Finalidad: los datos solo pueden recolectarse para alcanzar un objetivo lícito y específico que debe ser informado al titular.
2) Pertinencia: los datos recolectados deben ser adecuados para alcanzar el fin que se persigue, para evitar la recolección de datos excesivos o innecesarios.
3) Transparencia: El responsable del almacenamiento o tratamiento de los datos debe explicar al titular el fin, el uso, y las posibles transferencias a terceros de su información.
4) Sujeción al fin: Los datos solo pueden usarse para los fines autorizados por el titular.
5) Prohibición de procesamiento para facilitar datos cuyo tratamiento no ha sido autorizado y prohibición de construcción de perfiles.
6) Principio de olvido o temporalidad: Después de un tiempo determinado, los datos deben borrarse, una vez se cumpla el fin para el cual fueron requeridos.
7) Reglas de anonimización: Deben establecerse mecanismos para la anonimidad de los datos recolectados, para proteger al individuo y facilitar el procesamiento de los datos.

2. Consideraciones sobre los proyectos de protección de datos personales presentados por los partidos ARENA y FMLN

2.1 Principios

En la enumeración de los principios, ambos proyectos incluyen:

a) legalidad
b) consentimiento
c) transparencia
d) seguridad de los datos
e) finalidad
f) calidad
g) confidencialidad, que debe incluir el de anonimización

Sin embargo, el proyecto de ARENA incluye otros principios como el de prohibición de almacenar los datos o darles un tratamiento distinto para el que fueron autorizados. También incluye el principio de privacidad, el cual se refiere a la información que deberá darse al titular de los datos, previo a que autorice su recolección y uso, como por ejemplo, la identidad y domicilio de quien los recaba, las finalidades de la recolección y el tratamiento que se les dará.

En las prohibiciones habría que agregar el hacer uso de los datos para construir perfiles para inferir y divulgar datos sensibles de los usuarios, a partir de algoritmos o programas de automatización que pueden recolectar grandes cantidades de datos, agregarlos y relacionarlos, tal como prohíbe la jurisprudencia constitucional en el amparo 142-2012 y tal como apunta la tendencia internacional, ya que sin esa prohibición ninguno de nuestros datos sensibles estará al resguardo[2].

La tecnología nos convierte en seres de cristal o transparentes, tal como menciona el experto Alfredo Chirino en varias de sus obras: **"***Los objetivos de la autodeterminación informativa pueden resumirse en dos: por una parte, convertirse en salvaguarda de la persona frente al creciente uso de las tecnologías para el tratamiento de datos personales y, en un segundo plano, crear posibilidades reales y efectivas de evitar la construcción de personalidades de cristal, transparentes a cualquier uso y abuso, sin el conocimiento ni la voluntad del afectado o sin atender a algún interés general preponderante***"[3].**

El proyecto del FMLN incluye, por su parte, principios adicionales como el de lealtad, que se refiere a la buena fe con la que el responsable de las bases de datos debe usarlos, evitando fraudes o engaños al usuario, así como el principio de responsabilidad que se refiere a la obligación de implementar los mecanismos necesarios para dar cumplimiento a los principios y obligaciones establecidos en la ley, así como también al deber de rendir cuentas al ente rector. La protección de datos personales no debe quedarse en simples declaraciones, sino que debe incluir los mecanismos que permitan hacer efectiva su protección. Para ello, el principio de responsabilidad se vuelve indispensable.

Cabe considerar que sería beneficioso que los principios de lealtad y responsabilidad fueran agregados a la versión que se apruebe, así como el de no discriminación, por el cual aboga la ONU. Por otra parte, en lo referente al principio de seguridad de los datos, la redacción del proyecto de ARENA parece más adecuada, siendo esta uno de los grandes retos que se enfrentan actualmente ante los avances de la tecnología, los cuales se abordarán en el apartado correspondiente.

Por otra parte, para ser congruente con la jurisprudencia constitucional citada y la tendencia internacional en materia de protección de datos personales, habrá que agregar el principio de temporalidad, conforme con el cual, después de un tiempo determinado, los datos deben borrarse de forma segura, una vez se cumpla el fin para el cual fueron requeridos, tanto de

2 Agencia de la Unión Europea por los Derechos Fundamentales del Consejo de Europa (2018). *Handbook on European Data protection law*, p. 233, disponible en https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf [Consultado el 31.07.2019].

3 Chirino, A. (2012). Ley de Protección de Datos de Costa Rica, en Revista Internacional de Datos Personales, Universidad de los Andes, N.1 julio-diciembre, Bogotá, Colombia.

forma digital como de forma física**. Por ejemplo, los expedientes médicos, laborales, académicos u otros que contengan datos personales -y, sobre todo, datos sensibles- que consten en forma física deberán ser destruidos de tal forma que sea imposible recuperar o conocer la información que contienen.**

2.2 Derechos de los titulares

En ambos proyectos (arts. 5-9 FMLN y arts. 16-20 ARENA) puede advertirse que hay muchas similitudes en la enumeración y descripción de los derechos de los titulares de los datos. Ambos contienen un artículo bastante detallado sobre los derechos que deben garantizarse a las personas al momento de solicitar o recopilar sus datos personales, lo cual se considera bastante positivo. También enumeran y describen los derechos de acceso a los datos en poder de un registro en forma muy similar, estableciendo la gratuidad de la solicitud y la obligación de brindar una respuesta en términos claros y fácilmente comprensibles. Los derechos de actualización y rectificación también son regulados en forma adecuada y muy similar.

Donde se detectan diferencias entre ambos proyectos es en materia de supresión de los datos. El proyecto del FMLN lo regula de forma genérica, sin mucho detalle, como parte de los derechos ARCO del titular de datos, mientras que el proyecto de ARENA enumera las situaciones concretas en las cuales se podrá solicitar la supresión de los datos, así como las excepciones o condiciones en las cuales no procederá la supresión. En esta parte, este proyecto parece dar un tratamiento más acorde con los estándares y con la doctrina internacional, salvo la de la Corte Europea de Justicia que defiende un derecho al olvido total en algunos casos[4]. El proyecto del FMLN establece excepciones al ejercicio de todos los derechos ARCO.

El art. 20 del proyecto de ARENA contiene una prohibición que también se encuentra en la Ley de Protección de Datos Personales de Estonia y es la de oponerse a que sus datos sean objeto de un tratamiento exclusivamente automatizado o a través de programas de inteligencia artificial que evalúen y saquen conclusiones sobre la personalidad de los titulares de los datos. Las personas pueden oponerse a que sus datos sean registrados en bases de datos totalmente automatizadas destinadas a determinar características de la persona o de los titulares, a predecirlas o a tomar decisiones que afecten su vida personal.

En ese sentido, es sumamente importante que, al momento de recopilar los datos, las empresas o instituciones públicas sean muy claras e informen con transparencia a los usuarios el tipo de tratamiento que se dará a sus datos, ya sea que se haga en físico o por vía de formularios electrónicos. Las personas deben saber que sus datos serán analizados por una combinación de procesos automatizados y decisiones humanas o únicamente por medio de mecanismos de inteligencia artificial u otros.

La experiencia en otros países ha demostrado que los algoritmos mal diseñados pueden incorporar los sesgos de las personas que los diseñaron aun de forma involuntaria o resultar en conclusiones erróneas, por lo que debe ponerse mucho cuidado en el diseño de los programas que a partir de la recopilación de datos de las personas pretendan predecir; por ejemplo, su capacidad para desempeñar un cargo de liderazgo, su nivel de peligrosidad o tendencia a la reincidencia en materia de delitos, o conclusiones similares. Hay experiencias realizadas en otros países que muestran el daño que se ha cometido al usar programas de este

4 Agencia de la Unión Europea por los Derechos Fundamentales del Consejo de Europa (2018). *Handbook on European Data protection law,* p. 221, disponible en *https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf* [Consultado el 31.07.2019].

tipo mal diseñados[5], y por tanto, en la UE, por ejemplo, está prohibido el tratamiento o análisis de datos personales exclusivamente de forma automatizada o por mecanismos de inteligencia artificial, sin participación humana[6].

2.3 Medidas de seguridad

El proyecto del FMLN contiene 2 disposiciones sobre la seguridad de los datos personales (arts. 15 y 16), pero en realidad el primero se refiere a las medidas adoptadas para mantener el anonimato de los usuarios, lo cual también es de suma importancia en el tratamiento de datos personales. El art. 16 establece la aplicación de notificar a la autoridad garante sobre las violaciones a las medidas de seguridad ocurridas, naturaleza del incidente, datos comprometidos, medidas correctivas adoptadas, etc. En el proyecto de ARENA los aspectos sobre la seguridad de los datos son abordados en 6 artículos (arts. 47 a 52) y su desarrollo es definitivamente más completo y más acorde con los estándares internacionales en cuanto a prevención, detección, información y corrección de las medidas de seguridad.

Sin embargo, las medidas de seguridad son un aspecto primordial en el diseño de una ley de protección de datos en la era digital, y, en ese sentido, ambos proyectos fallan en crear las obligaciones legales necesarias para que los responsables de los registros aseguren un tratamiento y custodia adecuados de los datos personales de los usuarios que se los han confiado, comenzando con medidas preventivas.

La ley de Estonia establece ciertos estándares que deben cumplirse. En primer lugar, antes de ser autorizadas para el tratamiento de datos personales, las empresas e instituciones públicas deben hacer una evaluación de riesgos y de las medidas que tomarán para superarlas. Ambos aspectos deben ser comunicados a la autoridad garante. En segundo lugar, la ley de Estonia también exige que se lleven una serie de bitácoras que permitan día a día conocer quién tuvo acceso a los datos, qué cambios se produjeron, qué datos se borraron, entre otros.

En materia de manejo automatizado de datos, los programas que se utilicen deben estar diseñados para evitar infiltraciones de terceros y para alertar cuando ha habido un acceso no autorizado o un error del mismo programa informático. La tecnología digital trae consigo grandes ventajas para el tratamiento de datos, pero también trae una cantidad enorme de riesgos, ya que los datos se han convertido en el recurso más valioso de comercialización en el siglo XXI. Asimismo, en caso de fallas de seguridad, infiltraciones en las bases, accesos no autorizados a los ficheros o registros, en Estonia los mismos deben ser informados al ente garante, a las personas afectadas, así como las medidas adoptadas para corregir la falla, lo cual da lugar a una investigación para determinar responsabilidades. Sería recomendable adoptar esta última obligación en la Ley de Protección de Datos Personales que se apruebe en El Salvador.

Por otra parte, también en materia de seguridad, cabe considerar que, si bien es cierto que las pequeñas y microempresas no tienen los recursos ni infraestructura como las grandes empresas o las multinacionales, no es conveniente flexibilizar excesivamente los requisitos en materia de seguridad, ya que por esa vía podrían filtrarse muchos datos personales, causando un perjuicio muy grande a las personas afectadas. En este caso, habría

5 Bozdag, E. (2013). Bias in algorithmic filtering and personalization, Ethics Inf. Technol.15:209–227 disponible en https://www.academia.edu/3853590/Bias_in_algorithmic_filtering_and_personalization [Consultado el 31.07.2019].

6 Agencia de la Unión Europea por los Derechos Fundamentales del Consejo de Europa (2018). *Handbook on European Data protection law,* p. 233, disponible en https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf [Consultado el 31.07.2019].

que hacer una ponderación de derechos y considerar que aquellas empresas, grandes, pequeñas o micro que no puedan garantizar un mínimo de estándares de protección y de medidas de seguridad de los datos, no podrán ser autorizadas para recolectar y tratar datos personales, por lo que la propuesta que consta en el art. 9 del proyecto de ARENA, no se considera adecuada.

Finalmente, **las medidas de seguridad deben garantizar que las medidas adoptadas para anonimizar a los titulares de los datos en los casos en que esto sea necesario o requerido por ley, sean suficientemente garantistas desde una perspectiva práctica y tecnológica, manteniendo la confidencialidad, evitando al mínimo los accesos a la identidad del usuario y diseñando o contando con los programas automatizados adecuados, sobre todo cuando se manejen datos sensibles de las personas** como su fe religiosa, ideología política, o pertenencia a grupos étnicos determinados, entre otros. En este caso, las medidas de seguridad y las que garanticen la anonimización deben reforzarse.

También debe evitarse el uso de algoritmos que permiten inferir los datos sensibles a partir de la recopilación de grandes cantidades de información sobre los titulares de los datos. Tal como se recomendó anteriormente, las fallas de seguridad que den lugar a infiltraciones, fugas o accesos no autorizados a datos personales, deberán ser informadas al ente garante y a las personas afectadas; en primer lugar, porque es un derecho de los titulares de la información saber que su información personal ha sido infiltrada de forma no autorizada y, en segundo lugar, porque la autoridad garante debe abrir una investigación para determinar responsabilidades y asegurarse que los responsables de ficheros y registros tengan al día las medidas de seguridad necesarias y suficientes. Cuando el ente garante detecte que las conductas informadas trascienden el ámbito administrativo sancionatorio deberá informar a la Fiscalía General de la República para que determine si las acciones son constitutivas de algún delito contemplado en la Ley Especial contra los Delitos Informáticos Conexos.

2.4 Entes garantes

Tal como se ha podido apreciar en el análisis del derecho comparado, abordado en estas consideraciones, **se recomienda que la protección de los datos personales sea confiada a un ente autónomo y especializado en la materia, con capacidades de regulación, supervisión, control y sanción.** Sobre este punto, se considera que, dada la naturaleza e importancia de la protección de los datos personales, la autoridad garante no debe ser la Defensoría del Consumidor, sino una de dos opciones:

Por el nivel de importancia que tienen los derechos fundamentales que se protegen o que se ponen en riesgo al filtrar o usar en forma indebida los datos personales, se considera que la opción más adecuada sería la creación de una Agencia de Protección de Datos Personales, sobre todo, porque dados los avances tecnológicos galopantes que la humanidad enfrenta y los riesgos que estos suponen para la protección de los datos personales, es necesario contar con el presupuesto y personal necesarios y suficientemente especializados para protegerlos.

En caso de no tener fondos o de no estimarse oportuna la creación de una entidad especializada, se considera que, dada la naturaleza y experiencia que en la materia ha adquirido el Instituto de Acceso a la Información Pública y dado que la Ley de Acceso a la Información Pública le da facultades de ente garante en materia de datos personales en registros públicos, el IAIP y no la Defensoría del Consumidor debería de ser el encargado

de la protección de datos personales, tanto en registros privados como públicos, previas reformas necesarias a la Ley de Acceso a la Información Pública y previo fortalecimiento presupuestario para el IAIP. En este caso, pueden tomarse algunas buenas prácticas del modelo mexicano que, a través del INAI, combina la protección de ambos derechos o del modelo chileno, que en la actualidad está discutiendo en el Senado una reforma a la Ley de Transparencia para otorgar al Consejo de la Transparencia las potestades para proteger los datos personales en manos de entes privados, puesto que ya tenía, al igual que el IAIP de El Salvador, la potestad para garantizar este derecho en el caso de registros o ficheros públicos, aunque durante la discusión que se sostuvo en Chile previa al proyecto actualmente analizado por el Senado de ese país, también se consideró que el modelo ideal es una agencia especializada únicamente en la protección de los datos personales, por su relevancia[7].

No obstante ello, se recomienda que esta sea una medida provisional, ya que la doctrina más autorizada en la materia también recomienda que los entes garantes del acceso a la información pública sean entes especializados que se enfoquen únicamente en la protección de este derecho[8]. En ese orden de ideas, mientras se aprueba la creación de una entidad para la protección de datos personales con su correspondiente partida presupuestaria, se recomienda que en las mismas reformas a la Ley de Acceso a la Información Pública que otorguen potestades al IAIP para proteger datos personales en poder de registros privados, se incluyan reformas orgánicas para crear 2 unidades separadas dentro del IAIP: una que se siga ocupando de la protección del derecho de acceso a la información y otra que se especialice en la protección de datos personales.

En cualquiera de los casos en los que el IAIP o la agencia especializada estén conociendo, llegaren a detectar que las conductas examinadas pueden ser constitutivas de alguno de los delitos regulados por la Ley Especial contra los Delitos Informáticos y Conexos, deberá informar a la Fiscalía General de la República en un plazo no mayor a 3 días hábiles.

Las defensorías del consumidor están diseñadas para defender derechos esencialmente económicos o patrimoniales de la colectividad, en su dimensión de consumidora frente a sujetos particulares encargados de brindarles algún servicio o bien, mientras que la protección de datos personales es de otra naturaleza por completo. Se busca proteger el derecho de las personas a disponer de su propia información o autodeterminación informativa, a preservar su derecho a la intimidad y a la privacidad. El ente garante debe ser una institución especializada en la protección de lo segundo.

2.5 Procedimientos

Por tratarse de información que pertenece a los titulares de los datos, los procedimientos para acceder a ellos, corregirlos, actualizarlos o suprimirlos deben ser ágiles y gratuitos. **Por otra parte, dado que se trata de un derecho fundamental protegido constitucionalmente en nuestro país, cabe precisar que, además de la solicitud directa que se haga al responsable de la base de datos, de los reclamos que puedan presentarse ante el ente garante, de los procesos contencioso administrativos que puedan incoarse en contra de resoluciones del ente garante, el titular de los datos también puede acceder al amparo constitucional, aun contra particulares, como última vía de protección, siempre y cuando**

7 Vollier, P. (2019). Avanza la tramitación de la ley de datos: lo bueno, lo malo y lo feo, en Derechos Digitales en línea del 19.07.2019, disponible en https://www.derechosdigitales.org/12316/avanza-la-tramitacion-de-la-ley-de-datos-lo-bueno-lo-malo-y-lo-feo/ [Consultado el 9.08.2019].

8 Mendel, T. (2017). Right to Information Oversight Bodies: Design Considerations, September, pp. 12-15.

haya alegado la vulneración constitucional en todas las instancias y vías anteriores[9].

En ambos proyectos estudiados se prevé la gratuidad de los procedimientos que comienzan en ambos casos con una solicitud ante el responsable del fichero, registro o base de datos. En el proyecto del FMLN, el procedimiento está regulado en los arts. 10 al 14 e incluye requisitos de la solicitud, plazos de respuesta, gratuidad del procedimiento y recursos en caso de denegatoria. En el proyecto de ARENA, el procedimiento está regulado del art. 21 al art. 27 e incluye requisitos de la solicitud, obligación de designar a un encargado para tramitar las solicitudes en el marco de esta ley, plazos de respuesta, entrega de la información, referencias al ejercicio de los derechos ARCO y gratuidad.

Ambos proyectos tienen aspectos positivos, pero también algunos vacíos. Es importante que cada institución designe claramente a la persona encargada de dar trámite a estas solicitudes y que en el sitio web exista un botón o pestaña claramente identificado en la página de inicio, para que el interesado pueda acceder fácilmente a través de una solicitud sencilla a un proceso que le permita el acceso a sus datos, su corrección, actualización o supresión. También debe existir una ventanilla o persona encargada de tramitar las solicitudes presentadas en persona por los titulares afectados para quienes no tengan acceso a internet o prefieran esta vía. El nombre y dirección del encargado deberá estar fácilmente identificable en el sitio web del responsable (público o privado) y en el directorio de la entidad.

También es importante que la ley establezca que las decisiones de las empresas y/o instituciones públicas, así como las del ente garante deben entregarse en un plazo determinado, estar redactadas en un lenguaje sencillo y que la data que se brinde al interesado esté completa y fácilmente comprensible. También es necesario que en el sitio web del responsable del registro, fichero o base de datos o en la resolución que deniegue toda o alguna información, esté claramente explicado que el titular de los datos puede recurrir de esa decisión y conste en dicho documento el nombre de la entidad garante ante la cual puede presentar su reclamo, tal y como consta en el proyecto del FMLN (art. 14).

Finalmente, debe establecerse un régimen de sanciones administrativas suficientemente duras que motiven un adecuado cumplimiento de la ley y tratamiento de los datos personales, que incluyan, por ejemplo, casos de negligencia o incumplimiento de las medidas de seguridad, de las reglas de anonimización, así como por falta de acceso o respuesta ante las solicitudes de los titulares de los datos.

En algunos sistemas, como en la ley de Estonia, cualquier uso ilegal o la filtración ilegítima de datos que se custodian bajo reglas de confidencialidad, por ejemplo, también están sujetas al Código Penal. En nuestro país, la Ley Especial contra los Delitos Informáticos y Conexos prohíbe una variedad de conductas relacionadas con la protección de los datos personales. No obstante ello, sería adecuado analizarla para determinar si la misma requiere una actualización, ya que la tecnología y los delitos informáticos evolucionan a un ritmo exponencial y debemos asegurarnos que nuestra legislación pueda seguirles el paso, sobre todo por el valor comercial que el tráfico de datos personales tiene en la actualidad y lo gravemente afectadas que pueden resultar algunas personas por el uso indebido o ilegal de sus datos.

9 Sentencia de Amparo 622-2006 del 28.09.2006.

3. Conclusiones

- La protección de los datos personales se ha vuelto una preocupación global, en función de todos los retos apuntados anteriormente en este estudio. Nuestro país se encuentra atrasado respecto de este tema, por lo que urge aprobar una ley que cumpla con la finalidad de proteger de forma efectiva la información de las personas.

- Luego de analizar ambos proyectos de ley, se considera que lo más idóneo sería fusionarlos en un solo proyecto, tomando lo mejor que cada uno incorpora, sobre todo, porque tienen muchos más elementos comunes que diferencias.

- **En materia de ente garante, la tendencia internacional observada es hacia la creación de autoridades especializadas, dada la importancia de este derecho y el volumen de reclamos que en algunos países se presentan; sin embargo, si bajo las actuales condiciones no resulta viable, se recomienda otorgar de manera provisional la potestad de proteger los datos personales en registros públicos y privados al IAIP (Instituto de Acceso a la Información Pública)**, previa aprobación de las reformas legales que correspondan y de la dotación presupuestaria adecuada, para que dicha entidad pueda asumir las nuevas funciones.

- Existe en el país el desafío normativo e institucional en el marco de los sistemas de protección de datos personales, y con el fin de asegurar que se apruebe la mejor ley y se garantice la mejor institucionalidad, es necesario generar canales y mecanismos dinámicos y participativos que incorporen a una diversidad de actores; funcionarios, sector privado y técnico, academia y sociedad civil, que permitan la adecuada identificación, comprensión, y conciliación de los distintos elementos para la defensa de las garantías asociadas a la protección de datos de las personas y los desafíos tecnológicos y económicos de la actualidad.

FUSADES
Fundación Salvadoreña para el Desarrollo Económico y Social

Edificio FUSADES, Bulevar y Urb. Santa Elena,
Antiguo Cuscatlán, La Libertad, El Salvador
Tel.: (503) 2248-5600
www.fusades.org