FUSADES
Fundación Salvadoreña para el Desarrollo Económico y Social

Octubre de 2019 • No. 199

DEL Estudios Legales

Análisis legal e institucional

Observaciones a los proyectos de Ley de Protección de Datos Personales

Parte I: Introducción, antecedentes normativos, principios internacionales y derecho comparado

Preámbulo:

El presente estudio consigna la opinión que en septiembre del año en curso, el Departamento de Estudios Legales de FUSADES envió a la Comisión de Economía de la Asamblea Legislativa, sobre los 2 proyectos de ley de protección de datos personales que se han recibido en la Asamblea Legislativa: la "Ley de Protección de Datos Personales y Hábeas Data" presentado por ARENA y la "Ley General de Protección de Datos Personales", presentado por el FMLN, cuyos comentarios fueron solicitados. La opinión incorpora una serie de referencias a la economía digital, con base en la cual funcionan muchas de las actividades económicas modernas, al marco constitucional y normativo que rige la protección de datos personales actualmente, elementos de derecho comparado y, finalmente, las observaciones puntuales sobre cada uno de los proyectos de ley, con sus respectivas conclusiones. Para facilitar su lectura, se ha dividido en 2 partes. En este documento se presentan las contenidos de la parte I.

1. Introducción

En el mundo digitalizado que se vive, cada individuo produce una cantidad masiva de datos. Tan solo en un minuto se envían 16 millones de mensajes de texto y 156 millones de correos electrónicos[1]. Los teléfonos móviles y tarjetas de crédito dejan estelas de cada movimiento y compra durante el día. Es una realidad que la evolución de las nuevas tecnologías ha facilitado la incorporación de datos de crácter personal a ficheros informáticos de fácil copia y distribución. **Los "datos" se han convertido en un producto global clave y son considerados en el mundo como el aceite de la economía digital. Los datos se utilizan, procesan, intercambian, y analizan cada vez más en cantidades masivas para potenciar el contenido, los bienes y los servicios digitalizados.** Cuando los datos estaban únicamente en formato papel, era mucho más fácil protegerlos; ahora con la evolución tecnológica, se ha vuelto más complejo garantizar el resguardo apropiado de los datos personales y, por ello, la necesidad de dar respuesta a este nuevo reto de la era digital.

1 https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#6eae968d60ba

Los datos personales son todos aquellos que permiten, directa o indirectamente, identificar a un individuo distinguiéndolo de otros (OECD, 2013a; Reglamento UE 2016/679). Estos incluyen su nombre, su número único de identificación, sus datos de posicionamiento (GPS), cualquier identificador en línea, así como uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de una persona. Por otra parte, los datos sensibles son un subgrupo de los anteriores, en particular aquellos que una persona no tiene obligación de compartir con terceros (ejemplo: problemas de salud, creencias religiosas, afiliación política, etc.).

Hay grandes cantidades de datos personales que están circulando mundialmente y cabe hacerse las preguntas sobre: ¿quién tiene mi información?, ¿quién tiene acceso a esta?, ¿qué pueden hacer con esta información?, ¿qué derecho tienen las personas para asegurar que se les proteja esta información? Estas solo son algunas de las preguntas que servirán de base para iniciar el análisis de la importancia que tiene en el país contar con una Ley de Protección de Datos Personales que brinde respuestas a estas interrogantes, y dimensionar, asimismo, la importancia de la gestión ética del manejo de los datos personales[2].

Según el estudio "La digitalización del mundo: de borde a núcleo", realizado por IDC a solicitud de Seagate Technology, la esfera de datos globales (cantidad de datos creados, capturas y replicados en todo el mundo) podría crecer hasta 175 zettabytes para 2025, impulsados por los sectores financiero, de manufactura, salud y entretenimiento ayudarían a definir esta nueva era de crecimiento de datos[3]. De acuerdo con el "Informe de Riesgos de Negocios Globales de 2018" del Foro Económico Mundial, se clasifican los ataques cibernéticos como el riesgo global número 3 en términos de probabilidad, detrás de fenómenos meteorológicos extremos y desastres naturales[4]. En la edición de 2019 de este mismo informe, el riesgo de un ciberataque baja a 5º lugar, pero aparece en el lugar número 4 el riesgo de fraude o de robo de datos[5].

Lo anterior ha conllevado a que alrededor del mundo, la protección de datos se ha convertido en un punto fundamental para la comunidad empresarial, los organismos reguladores y los consumidores, llevándolos a adoptar normas para la protección de los mismos.

La protección de datos tiene múltiples propósitos como privacidad y seguridad, en parte, debido a fuertes preocupaciones de los ciudadanos sobre su privacidad y de los gobiernos sobre la seguridad nacional.

Para los países, proteger datos requiere un equilibrio delicado entre muchos factores, entre los cuales cabe destacar: seguridad nacional, vigilancia, política sobre competencia, innovación, la integridad del proceso electoral y la protección del consumidor. Encontrar este adecuado balance es uno de los retos mayores que enfrentan los países al momento de discutir las leyes de protección de datos personales, que por una parte resguarden el derecho fundamental de la privacidad de las personas, y a su vez, no se vuelva un candado a la innovación y desarrollo de los países.

2 *https://blogs.iadb.org/conocimiento-abierto/es/quien-es-el-dueno-de-mis-datos-personales/*

3 Reinsel, D. y otros (2018). The Digitization of the World From Edge to Core, an IDC White paper, sponsored by Seagate, November 2018, disponible en *www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf* [Consultado el 17.09.2019].

4 WEF (2018). The Global Risks Report 2018, disponible en *http://www3.weforum.org/docs/WEF_GRR18_Report.pdf* [Consultado el 17.09.2019].

5 WEF (2019). The Global Risks Report 2019, disponible en *http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf* [Consultado el 17.09.2019]

2. Antecedentes normativos relacionados con la protección de datos personales en el país

2.1 Marco constitucional

La Constitución establece en el Art. 2. "Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, a ser protegida en la conservación y defensa de los mismos.

Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Art. 24. "La correspondencia de toda clase es inviolable. Interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comuicaciones telefónicas".

Ambos artículos brindan garantía consitucional al derecho a la intimidad personal y privacidad, derecho fundamental del que emana el derecho a la protección de datos personales.

Asimismo, existen varias leyes secundarias que hacen referencia a la protección de datos personales. No obstante, esta dispersión es parte de lo que no ha permitido que a la fecha exista una verdadera protección y regulación del manejo y resguardo de los datos de personas, lo que hace necesario homologar esta regulación e impulsar la aprobación de un marco normativo homogéneo y especializado en la materia, que cuente con la institucionalidad adecuada que vele por la implementación de la misma y una política nacional enfocada en el desarrollo tecnológico, enmarcada en el resguardo de los derechos personales. A continuación, se hace referencia a este marco normativo.

2.2 Leyes vigentes

El país cuenta con dos grupos de leyes; por una parte, los cuerpos normativos que regulan la protección de datos de carácter personal en manos de entidades públicas y, por otra parte, las leyes que regulan la protección de datos personales en sectores específicos, entre ellos, el sector financiero y el sector de telecomunicaciones[6], así como leyes que protegen los datos, sus titulares y los registros, desde una óptica sancionadora, como la Ley Especial Contra los Delitos Informáticos y Conexos, tal como se aprecia en la tabla en la siguiente página.

3. Análisis de Proyectos de Ley relativos a la protección de datos personales

Las observaciones sobre los elementos más relevantes respecto del proyecto de "Ley de Protección de Datos Personales y Hábeas Data", presentado por ARENA y del proyecto de "Ley General de Protección de Datos Personales", presentado por el FMLN, se han agrupado por temas o rubros de ambos documentos, ya que se ha detectado que, en su mayoría, están estructurados de forma muy similar en cuanto al orden y fondo de sus contenidos, siendo la mayor diferencia detectada -no la única- la autoridad garante de este derecho propuesta por cada partido.

De forma transversal, se considera de mucha importancia la necesidad de incorporar en forma detallada, todos los aspectos que se refieren a los retos que la tecnología, la inteligencia artificial y el tratamiento automatizado de la información global plantea actualmente para las personas

6 Estudio Centroamericano de Protección de Datos, Capítulo El Salvador. José Edmundo Osorio Morales. Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC). Enero 2019.

Leyes	Artículo	Naturaleza de entidad que maneja los datos	Regulación
Ley de Acceso a la Información Pública	Art. 31-39	Pública	Establece el derecho que tienen las personas de saber si las entidades gubernamentales están procesando sus datos y recoge derechos para tener acceso a ellos, rectificarlos, etc.
Ley de Firma Electrónica	Art. 5	Pública	Establece mecanismos electrónicos para resguardar los datos personales en su relación con las empresas que prestan un servicio de almacenamiento de datos electrónicos.
Ley de Regulación de Servicios de Información sobre el Historial de Créditos de las Personas	Art. 1	Privada	Garantiza que haya un buen manejo de los datos del consumidor o cliente relativos a su historial crediticio.
Ley de Protección al Consumidor	Art. 18/ lit. g	Privada	Regula cómo las empresas pueden compartir información del consumidor entre distintos agentes.
Ley General de Telecomunicaciones	Art. 29	Privada	Protege la intimidad y datos personales de los usuarios en sus comunicaciones.
Ley Especial Contra los Delitos Informáticos y Conexos	Arts. 15 al 26	Pública y privada	Sanciona penalmente los delitos contra los registros y titulares de datos personales

Fuente: elaboración propia con base en la investigación del Estudio Centroamericano de Protección de Datos, Capítulo El Salvador. José Edmundo Osorio Morales. IPANDETEC, enero 2019 **e investigaciones propias.**

en materia de recolección, uso, resguardo, transmisión, procesamiento de sus datos, así como las obligaciones que esto impone a los responsables de los registros de datos, tanto públicos como privados, sobre todo porque en el siglo XXI los datos personales se han convertido en un bien comercializable de alta valía, muchas veces sin conocimiento ni autorización de sus titulares. En ese sentido, la Ley Especial contra los Delitos Informáticos y Conexos ya prohíbe y sanciona penalmente varias conductas que atentan en contra de los datos que se encuentran en registros o bases de datos digitales. No obstante, habrá que actualizar dicha ley para garantizar que considere todas las opciones posibles, ya que los delitos digitales evolucionan exponencialmente a la par de la tecnología.

También deberán hacerse las reformas necesarias a la Ley de Acceso a la Información Pública, en la parte de información confidencial y en toda la parte relativa a protección de datos personales, tal como se explica en detalle en los apartados finales de esta opinión.

En primer lugar, se hará referencia a los estándares internacionales que cualquier proyecto de ley debería contener, sobre todo en materia de principios y de reglas de seguridad, que ante los avances tecnológicos actuales se vuelve uno de los retos principales en el resguardo y manejo adecuado de los datos personales de los salvadoreños, así como a 3 ejemplos de derecho comparado, de los cuales pueden extraerse buenas prácticas.

En segundo lugar, se hará referencia a la jurisprudencia constitucional reciente sobre este tema, con el objeto de asegurarse que los proyectos cumplan con los parámetros fijados por la Sala de lo Constitucional para el derecho fundamental a la protección de los datos personales y para las garantías de este derecho. El análisis de los 2 proyectos se articulará en 5 grandes rubros: principios aplicables, derechos de los titulares de los datos, medidas de seguridad, procedimientos aplicables y entes rectores.

3.1 Principios internacionales aplicables a la protección de datos personales

3.1.1 Sistema Interamericano de Derechos Humanos

El Comité Jurídico de la Organización de Estados Americanos (OEA) se encuentra trabajando desde hace varios años en un proyecto de Ley Modelo de Protección de Datos Personles, por mandato de la Asamblea General de la OEA[7]. A la fecha, el proyecto no está concluido, pero sí se ha logrado acordar que este deberá articularse alrededor de 12 principios básicos, partiendo del supuesto de que la protección de datos personales es un derecho humano que debe ser garantizado por todos los Estados[8].

1. Propósitos Legítimos y Justos;
2. Claridad y Consentimiento;
3. Pertinencia y Necesidad;
4. Uso Limitado y Retención;
5. Deber de Confidencialidad;
6. Protección y Seguridad;
7. Fidelidad de la Información;
8. Acceso y Corrección;
9. Información Sensible;
10. Responsabilidad;
11. Flujo Transfronterizo de Información y Responsabilidad; y
12. Publicidad de las Excepciones.

3.2 Sistema Europeo de Proteción de los Derechos Humanos

La normativa marco en la Unión Europea es el Reglamento (UE) 2016/79 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, conocido como el "Reglamento General de Protección de Datos" o "GDPR" (por sus siglas en inglés), relativo a la protección de datos personales y a la libre curculación de esos datos, entrando en vigor en mayo de 2018[9]. Sin embargo, en dicho sistema existen otras directivas especiales relativas a datos personales de personas privadas de libertad[10] y a la protección de los datos personales en las comunicaciones electrónicas[11] y un reglamento específico para el tratamiento de datos personales por parte de las entidades y organismos de la Unión Europea[12].

7 INFORME DEL COMITÉ JURÍDICO INTERAMERICANO PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES del 26 de marzo de 2015 disponible en http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-doc_474-15_rev2_26_03_15.pdf [Consultados el 24.07.2019]

8 Departamento de Derecho Internacional de la OEA, Ley Modelo Interamericana de Protección de Datos Personales (en elaboración) *http://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo_documentos.asp* [Consultados el 30 de julio de 2019].

9 Disponible en https://publicationseuropea.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1/language-en

10 En mayo de 2018 también entró en vigor la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, reltiva a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre curculación de dichos datos, y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

11 Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de la comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) disponible en *https://eur-lex-europa.eu/legal-content/ES/ALL/?uri=CELEX:32002L0058* [Consultada el 30.07.2019].

12 Reglamento UE 208/1725 del 23.10.2018 disponible en *https://eur.lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725*

Este sistema es el que más ha perfeccionado la protección de datos personales y el que tiene el régimen más garantista en favor de la privacidad de las personas naturales y el derecho a poder controlar su información. En la práctica, la Unión Europea espera que su reglamento se convierta en el estándar que puedan adoptar otras economias y socios estratégicos como América Latina[13].

En el art. 5 del Reglamento 2016/679, se establece una serie de principios básicos que rigen la protección de datos personales dentro de los países miembros de la Unión Europea, también partiendo del supuesto de que se está en presencia de un derecho humano que debe ser protegido tanto por los estados a título individual, como por el sistema europeo de protección de los derechos humanos:

"1. Los datos personales serán:

*a) tratados de manera lícita, leal y transparente en relación con el interesado ("**licitud, lealtad y transparencia**");*

*b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (**"limitación de la finalidad"**);*

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimizción de datos");

*d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (**"exactitud"**);*

*e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado ("**limitación del plazo de conservación**");*

*f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas ("**integridad y confidencialidad**").*

*2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo ("**responsabilidad proactiva**").*

3.3 Observaciones sobre los principios rectores de ambos sistemas

Al analizar ambos sistemas, puede observarse que en el Sistema Interamericano la lista de principios parece más larga, pero en realidad existe un consenso alrededor de los principios medulares, como la licitud de los

13 Agencia Española de Protección de Datos (2018). LATINOAMÉRICA Y EL MODELO EUROPEO DE PROTECCIÓN DE DATOS del 03.07.2018, disponible en https://www.reglamentodatos.es/index.php/blog/143-latinoamerica-y-el-modelo-europeo-de-protección de datos [Consultado el 16.09.2019].

datos, la libertad del consentimiento y la seguridad en su resguardo, y la responsabilidad de los dueños o administradores de los registros, ficheros o bases de datos, los cuales servirán como punto de referencia para analizar los proyectos bajo examen.

Cabe agregar que ls directrices de la Organización de las Naciones Unidas (ONU) para la Regulación de los Archivos de Datos Personales Informatizados, adoptadas mediante resolución 45/95 de la Asamblea General de 14 de diciembre de 1990, establecenun principio adicional que no se encuentra en los 2 sistemas regionales examinados: el de no discriminación, en el cual se establece que "no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato"[14].

4. Entidades garantes de la protección de los datos personales en el derecho internacional y en el derecho comparado

4.1 Sistema Interamericano de Derechos Humanos

En el Sistema Interamericano de Derechos Humanos, las entidades garantes son la Comisión y la Corte Interamericana de Derechos Humanos y aunque la Convención Americana de Derechos Humanos no haga referencia expresa a la protección de datos personales, la misma puede derivarse implícitamente del art. 11 en el que se establece que *"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."*

4.2 Sistema Europeo de Derechos Humanos

En la Unión Europea (EU) la institución llamada a proteger en primer lugar los datos personales es una entidad administrativa denominada el Supervisor Europeo de los Datos Personales, cuyas funciones esenciales son las siguientes[15]:

- Supervisa el tratamiento de los datos personales por parte de la administración de la UE, a fin de garantizar el cumplimiento de las normas de protección de la intimidad.
- Asesora a las instituciones y los organismos de la UE, sobre todo lo relativo al tratamiento de los datos personales y las políticas y legislación al respecto.
- Se ocupa de las reclamaciones y realiza investigaciones.
- Colabora con las autoridades nacionales de la UE para garantizar la coherencia en la protección de datos.
- Supervisa las nuevas tecnologías que puedan tener una incidencia en la protección de datos.

En segundo lugar, la instancia jurisdiccional que garantiza la protección de los datos personales en la

14 Disponibles en http://transparencia.udg.mx/sites/default/files/Directrices%20para%20la%20regulaci%C3%B3n%20de%20los%20archivos%20de%20datos%20personales%20informatizados.pdf [Consultada el 30.07.2019].

15 Supervisor Europeo de los Datos Personales en https://edps.europa.eu/edps-homepage_en?lang=es [Consultado el 30.07.2019].

UE es la Corte Europea de Derechos Humanos[16]. Este tribunal ha pronunciado abundante jurisprudencia sobre el tema, siendo uno de los casos más recientes, relevantes y polémicos, el caso que la Agencia de Protección de Datos Española llevó y ganó en contra de Google, en el que se estableció un derecho "al olvido" que ha generado polémica en muchos ámbitos académicos y en la comunidad jurídica porque, en forma muy resumida, permite alterar de alguna forma la historia y afecta la neutralidad de la red[17]. A pesar de ser polémico, es un derecho garantizado por el Sistema Europeo de Proteción de los Derechos Humanos y por lo tanto, también por cada una de las leyes de los países que forman parte de la UE.

4.3 Derecho comparado

En el derecho comparado se han analizado las leyes de Argentina y México, por ser países parecidos con El Salvador, por estar en la misma región y por tener algunas de las mejores leyes en la materia, pero también Estonia, por ser este uno de los países considerados más avanzados en materia de digitalización de la gestión gubernamental, el cual ha sabido compatibilizar estos avances con la protección de datos personales. A partir del estudio de otros modelos, se han extraído algnos elementos comunes, útiles para el análisis de los proyectos bajo estudio en la Asamblea Legislativa. Se han agrupado las consideraciones en principios, derechos, medidas de seguridad, entes garantes y procedimientos para la protección de los datos personales.

Argentina

La Ley 25.326 de Protección de Datos Personales de Argentina entró en vigencia en 2000 y en sus principios contiene elementos muy similares a los que establece el Comité Jurídico Interamericano, con algunas especificidades como el caso de los datos sobre la salud: 1) licitud, 2) calidad de los datos, 3) consentimiento libre, expreso e informado, 4) debe de informar a los titulares sobre sus datos personales, 5) categorías de datos (prohibición de obligar a dar datos sensibles y protección reforzada de su custodia), 6) datos relativos a la salud, 7) seguridad de los datos, 8) deber de confidencialidad, 9) medidas para la cesión de los datos, y 10) transferencia internacional[18].

Como dato curioso, Argentina expresamente establece que las bases de datos y las fuentes de información periodística no podrán ser afectadas por esta ley.

En relación con los derechos, la ley argentina también establece las facultades provenientes de los llamados derechos "ARCO"[19], con algunos matices: derecho a conocer qué datos están en poder de determinados registros, de acceso a dicha información, a que la información le sea proporcionada de forma completa, clara y en el formato solicitado por el titular de los datos, derecho de actualización, rectificación y supresión. Esta ley también regula casos de excepción en los que el responsable de la base de datos puede negar el acceso u otros derechos al titular de los datos.

En materia de seguridad, la ley argentina no tiene mayor desarrollo y únicamente aborda el tema como un principio en el que se establece que el responsable de las bases de datos debe tomar las medidas necesarias

16 Corte Europea de Derechos Humanos disponible en *https://www.echr.coe.int/Pages/home.aspx?p=home* [Consultada el 30.07.2019]

17 TEJ, asunto C-131/12, SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala), de 13 de mayo de 2014 (*) disponible en *http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES* [Consultada el 30.07.2019].

18 Ley 25.326 del 4 de octubre de 2000 disponible en *http://www.informatica-juridica.com/anexos/legislacion-de-argentina-ley-25-326-de-habeas-data/*

19 Derechos ARCO: acceso, rectificación, cancelación y oposición o supresión (arts. 14 a 16 de la Ley de Protección de Datos Personales, Ley 25.326 del 4 de octubre de 2000).

técnicas y organizativas que resulten necesarias para la seguridad y confidencialidad de los datos, que eviten su pérdida, adulteración, desviaciones intencionales o accidentales, ya sea que los riesgos provengan de acciones humanas o automatizadas.

Finalmente, el ente garante establecido para el modelo argentino es un "Órgano de Control", al que le corresponden las facultades de supervisar, controlar, verificar e imponer sanciones. El Órgano de Control gozará de autonomía funcional y actuará como ente descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación. Estará a cargo de un Director nombrado por el Poder Ejecutivo con acuerdo del Senado de la República, debiendo ser seleccionado entre personas con antecedentes o conocimientos en la materia. En materia de procedimientos, la ley argentina prevé una acción de hábeas data directamente ante la autoridad judicial, según las reglas de competencia comunes (domicilio del demandado, domicilio del demandante, lugar del hecho o lugar establecido en el contrato). El procedimiento aplicable será el del amparo común y supletoriamente las del juicio sumarísimo previsto en el Código Procesal Civil y Comercial de la Nación.

México

La Ley Federal de Protección de Datos Personales en Posesión de Particulares, del 2010, se combina con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, ya que, si bien la segunda regula la protección de datos en poder de entidades públicas, el ente garante en ambos casos es el mismo: el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales[20]. La ley marco es complementada con una cantidad muy amplia de guías y lineamientos para el sector privado sobre temas específicos, incluidos esquemas de autorregulación, criterios mínimos para el tratamiento informático de los datos, para el manejo de incidentes de seguridad, para el manejo de datos biométricos, entre otros muchos temas[21]. También existe una serie de guías similares para el sector público[22].

Esta ley regula principios muy similares a las otras 2 leyes estudiadas para este análisis: 1) licitud, 2) consentimiento, 3) información, 4) calidad, 5) finalidad, 6) lealtad, 7) proporcionalidad, y 8) responsabilidad.

En materia de derechos, los titulares de los datos tienen derecho de acceso, rectificación, cancelación y oposición o derechos "ARCO". En materia de cancelación la ley establece excepciones tasadas que incluyen que su tratamiento obedece a una disposición legal, sean necesarios para realizar una función de interés público, sean necesarios para el tratamiento, prevención o dignóstico médico, amparados por el secreto profesional.

No regula aspectos específicos sobre la seguridad en la Ley Federal de Protección de Datos Personales, pero sí en las guías y lineamientos sobre temas específicos a los que se hizo referencia al inicio de este apartado sobre México.

El ente garante es el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales o INAI. Este organismo tiene rango constitucional (art. 6 de la Constitución Política de México) y su mandato, competencias y obligaciones se encuentran desarrollados con un alto nivel de detalle. En la parte pertinente del art. 6 Cn., se establece lo siguiente: *"VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir*

20 Disponible en http://corpusiurispdp.inai.org.mx/Pages/home.aspx [Consultado el 30.07.2019].

21 Disponibles en http://inicio.inai.org.mx/SitePages/Documentos-de-Interes.aspx?a=m3 [Consultado el 30.07.2019].

22 Idem.

sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley".

En México, el titular de los datos debe, primero, ejercer cualquiera de sus derechos ante el responsable de la base o registro de datos. Solo en caso de no recibir una respuesta satisfactoria, tiene 15 días para acudir al INAI, en cuyo procedimiento impera la informalidad y simplicidad para facilitar el acceso a los usuarios. En contra de las resoluciones del INAI procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

El INAI tiene funciones educativas, de vigilancia y supervisión, de solución de conflictos, de emisión de lineamientos y demás normativa operativa, pero sobre todo, conocer y resolver los procedimientos de protección de datos personales e imponer las sanciones establecidas en la ley.

Estonia

La nueva Ley de Protección de Datos Personales es muy reciente, entró en vigencia en enero de 2019[23]. En relación con los principios, Estonia prevé elementos muy similares a los establecidos en el Sistema Europeo, ya que por ser parte de la UE debe adaptar su derecho interno a dicha normativa: 1) legalidad, 2) finalidad, 3) calidad, 4) veracidad, 5) temporalidad de la retención de los datos, y 6) seguridad. En materia de derechos también prevé los derechos, estándar conocidos como "ARCO": acceso, rectificación, cancelación y oposición o solicitud de eliminación, pero especificados en forma sumamente detallada, sometida a plazos y con un nivel de detalle de las obligaciones de los responsables de los registros sumamente elevado. La Ley de Estonia toma en cuenta de forma expresa todos los riesgos que el tratamiento automatizado o digital de la información supone, por lo que exige a los responsables de registros algunas obligaciones específicas, ya que en dicho país toda la gestión gubernamental y muchos trámites de índole privado se hacen por vía digital.

En particular, se prevén las siguientes obligaciones para los responsables de bases de dtos, ficheros o registros:

a) Que elaboren un mapa de riesgos de errores en el manejo o de infiltraciones en las bases de datos, así como las medidas de prevención y correcciones que se adoptarán, las cuales deben ser informadas al ente garante.

b) Los responsables de registros deben informar al ente garante las medidas físicas y tecnológicas de seguridad implementadas para el tratamiento ordinario de datos personales, así como aquellas medidas reforzadas para los datos sensibles, tales como religión, afiliación política, grupo étnico, por ejemplo. Estas medidas deben, entre otros, garantizar la anonimización o pseudonimización de los titulares de los datos. Cualquier violación a las medidas de seguridad debe ser informada al ente garante de forma inmediata (*hackers* o fallas tecnológicas).

c) Esta ley señala una serie de bitácoras que cada entidad púbica o privada que trate con datos personales debe llevar, como por ejemplo, sobre datos recopilados, datos corregidos, ingresos al sistema, revelación de datos a terceros, transmisión de datos a terceros, datos borrados o cancelados. Estas deberán ser puestas a disposicón de la autoridad garante a solicitud de esta última.

23 Estonia Personal Data Protection Act, disponible en https://www.riigiteataja.ee/en/eli/523012019001/consolide

Finalmente, en Estonia el ente garante es un Inspector de Protección de Datos Personales, el cual es una entidad completamente independiente y autónoma en lo administrativo. La persona que se nombre como Inspector deberá tener conocimiento en la materia, no tener ningún vínculo político partidario, ni ejercer ninguna otra labor durante su cargo, pero previo a ser nombrado deberá someterse a una serie de controles y verificaciones de seguridad, con la Policía y el Ministerio de Justicia. Una vez superado el control de seguridad, el Ejecutivo consultará con el Comité Constitucional del Parlamento la viabilidad del nombramiento. Las multas por casos de violaciones a los derechos de los titulares de los datos son sumamente elevadas y alcanzan varios millones de dólares.

Los reclamos se presentan inicialmente ante los responsables de los registros o bases de datos. En caso de no obtener una respuesta favorable, pueden acudir con una queja ante el Inspector de Datos Personales, quien tiene la obligación de resolver en plazo máximo de un mes, en un lenguaje sencillo. Si el titular de los datos no se encuentra satisfecho con la decisión del Inspector, puede acudir a los tribunales. El Inspector tiene también funciones de consulta.

En la parte II de este estudio, se analizará la jurisprudencia constitucional y los elementos concretos de los 2 proyectos bajo estudio de la Comisión de Economía de la Asamblea Legislativa, para concluir con algunas consideraciones finales sobre el tema.

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