Estudio Centroamericano de Protección de Datos,

PANAMÁ

Diagramación: Isabel Valladares
Edición: Raúl Altamar
Coordinación: Sara Fratti
Autoría: Krizia Matthews

Enero 2019.

IPANDETEC
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS

Instituto Panameño de Derecho y Nuevas Tecnologías -IPANDETEC- es una organización sin fines de lucro basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital, a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

1. Marco jurídico constitucional

Las garantías constitucionales que conforman el conjunto de derechos relacionados con la intimidad en Panamá se encuentran en los artículos 29, 42 al 44 de la Constitución Política de la República de Panamá[1], que son a su vez el fundamento del derecho a la protección de los datos personales.

En su Artículo 29 se establece que: "La correspondencia y demás documentos privados son inviolables y no pueden ser ocupados o examinados sino por disposición de autoridad competente, para fines específicos y mediante formalidades legales. (...) se guardará reserva sobre los asuntos ajenos al objeto de la ocupación o del examen. Igualmente, las comunicaciones telefónicas privadas son inviolables y no podrán ser interceptadas (...)".

En los artículos 42 y 43 del texto constitucional se determina lo relativo al derecho de acceso a la información.

Artículo 42. "Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley".

La información contenida en dicho Articulo sólo podrá ser recogida para fines específicos mediante consentimiento de su titular, o por disposición de autoridad competente con fundamento en lo previsto en la Ley.

Por su parte, el Artículo 43 menciona: "Toda persona tiene derecho a solicitar información de acceso público o de interés colectivo que repose en bases de datos o registros a cargo de servidores públicos o de personas privadas que presten servicios públicos, siempre que ese acceso no haya sido limitado por disposición escrita y por mandato de la Ley, así como para exigir su tratamiento leal y rectificación".

Por su parte, el Articulo 44 hace referencia al Hábeas Data estableciendo lo siguiente: "Toda persona podrá promover acción de hábeas data con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información. Esta acción se podrá interponer, de igual forma, para hacer valer el derecho de acceso a la información pública o de acceso libre, de conformidad con lo establecido en la Constitución. Mediante la acción de hábeas data se podrá solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o datos que tengan carácter personal. La Ley reglamentará lo referente a los tribunales competentes para conocer del hábeas data, que se sustanciará mediante proceso sumario y sin necesidad de apoderado judicial".

[1] Constitución Política de la República de la República de Panamá. Reformada por los Actos Reformatorios de 1978, el Acto Constitucional de 1983 y los Actos Legislativos de 1994. Disponible en: https://www.oas.org/juridico/spanish/pan_res2.doc

2. Marco jurídico ordinario

Actualmente, Panamá no posee una Ley General de Protección de Datos. Se cuenta con un proyecto de ley que ha sido presentado por la Autoridad Nacional de Transparencia y Acceso a la Información y la Autoridad Nacional para la Innovación Gubernamental de la República de Panamá ante la Asamblea de Diputados.

2.1. Ley No.6 de 2002 sobre Transparencia y Acceso a la Información Pública

La Ley No.6 del 22 de enero de 2002[2] sobre Transparencia y Acceso Información Pública establece la acción de Hábeas Data, la cual fue creada con el objetivo de reforzar los derechos fundamentales contenidos en la Constitución Política de Panamá.

La Ley cuenta con disposiciones tales como el derecho de acceso a la información, así como indica el tipo de información que es considerada de carácter público, siendo esta la información de alguna persona que ha sido recabada por alguna institución o entidad del Estado sin necesidad de sustentar justificación o motivación[3].

De igual manera, se considera información de carácter publico a toda información que se encuentre en archivos, registros o expedientes del Estado, y a corregir o eliminar información que sea incorrecta, irrelevante, incompleta o desfasada, a través de los mecanismos pertinentes como se establece en el artículo 3 de la mencionada Ley.

[2] Asamblea Nacional, Ley No. 6 del 22 de enero de 2002, Que dicta normas para la transparencia en la gestión pública establece la acción de Habeas Data y dicta otras disposiciones. Disponible en: http://www.mef.gob.pa/es/transparencia/Documents/Ley%20No%206%20de%2022%20enero%20de%202002.pdf

[3] Ibid, articulo 2.

2.3. Ley No.24 de 2004 que regula el servicio de información sobre el historial de crédito

La Ley No. 24 del 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito establece en su artículo 1 que el objetivo de la misma es proteger y garantizar la confiabilidad, la veracidad, la actualización y el buen manejo de los datos personales de consumidores o clientes, relativos a su historial de crédito, incorporados o susceptibles de ser incorporados a una agencia de información de datos administrada por una persona natural o jurídica, debidamente autorizada conforme a la presente.

Adicionalmente, la misma regula la actividad de las personas naturales y jurídicas, públicas o privadas, que se dediquen a administrar las agencias de información de datos y a los agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores o clientes.

Mediante esta Ley, la Autoridad de Protección al Consumidor y Defensa de la Competencia puede conocer y resolver las quejas de los consumidores o clientes velando por la protección y garantizara el buen manejo de los datos personales de los consumidores que se encuentran en la base de datos de una Agencia de Información, por lo que se podrán imponer sanciones a aquellas agencias.

Pese a no existir ley especial, entendemos que dentro de los supuestos de esta norma se encontrarían, por ejemplo, a los datos de nacimiento, defunción, estado civil o domicilio electoral contenidos en el Registro Civil, el registro de morosidad patronal de la Caja Costarricense del Seguro Social, o los diversos Registros que componen el Registro de la Propiedad. El hecho de que para acceder a estos datos se pueda requerir la creación de un usuario y contraseña no es un elemento relevante, siempre y cuando cualquier persona pueda obtener una cuenta con el fin de acceder a datos personales. Habría sido deseable que la Ley o el Reglamento enlistaran cuáles de las bases de datos que hoy, de facto, son de acceso irrestricto mantendrían dicha condición una vez promulgada la Ley.

[4] Asamblea Nacional, Ley No. 24 del 22 de mayo de 2002, Que regula el servicio de información sobre el historial de crédito de los consumidores o clientes. Disponible en: http://www.legalinfo-panama.com/legislacion/00297.pdf

2.4. Ley No. 51 de 2009 para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones.

Ley N. 51 de 18 de septiembre de 2009[5] que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones.

Esta Ley tiene por objeto que los agentes económicos que comercialicen o presten servicio de telecomunicaciones cuenten con un registro de datos que proporcione la identificación y dirección suministradas por los usuarios que contraten sus servicios. Esta ley contiene principios propios de la protección de datos, como lo son clara determinación de la finalidad, calidad y limitación al plazo de conservación.

En su artículo 3 se establece que estos agentes económicos deben adoptar medidas para garantizar que los datos se conversen de forma debida en las empresas por el termino señalado en la ley que es de 6 meses según el artículo 6 de la Ley. Dicho periodo puede ser extendido a solicitud de autoridad judicial por un plazo de 6 meses adicionales.

La Ley establece que los datos obtenidos y conservados no pueden ser utilizados para fines distintos que los establecidos en la ley. Se debe garantizar su integridad, y tienen carácter confidencial tal y como se establece en los artículos 8, 9 y 10 de la referida Ley.

[5] Asamblea Nacional, Ley N. 51 de 18 de septiembre de 2009 que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones. Disponible en: https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf

2.5. Ley No. 3 de 2000 sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida.

Ley No. 3 del 5 de enero de 2000 considera las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida[6].

La Ley se creó con objeto de establecer el marco jurídico para la educación y promoción de la salud; para la investigación, prevención, capacitación, detección, vigilancia epidemiológica y atención integral sobre las infecciones de transmisión sexual (ITS), el virus de la inmunodeficiencia humana (VIH) y el síndrome de inmunodeficiencia adquirida (SIDA), y para establecer los derechos y deberes de la persona enferma o portadora de infección de transmisión sexual y del virus de la inmunodeficiencia humana, así como de las demás personas en todo el territorio nacional.

La Ley aborda aspectos relacionados con la protección de datos, específicamente aquellos principios sobre confidencialidad que se pueden encontrar en los artículos 21 que establece que se deberá respetar la confidencialidad del paciente (artículo 21). Así como el articulo 34, el cual establece que “la confidencialidad es un derecho fundamental de la persona enferma o portadora de infección de transmisión sexual o del virus de la inmunodeficiencia humana. Nadie podrá, pública ni privadamente, hacer referencia a estos padecimientos, sin el previo consentimiento del paciente o la paciente, excepto para las cónyuges, los cónyuges, los compañeros y las compañeras de actividad sexual, así como para los representantes”.

Así mismo, la Ley contiene disposiciones de sanción a aquellos que violen dicha confidencialidad al que facilite información sin consentimiento ni justa causa, ya sea de manera privada o pública.

[6] Asamblea Nacional, Ley General No. 3 de 5 enero de 2000 sobre las infecciones de transmisión sexual, el virus de la inmunodeficiencia humana y el sida. Disponible en: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127734.pdf

2.6. Proyecto de Ley de Protección de Datos de Carácter Personal

El Proyecto No. 465 de Ley de Protección de Datos de Carácter Personal[7] busca dotar a los ciudadanos en general de un instrumento legal de protección y defensa, tal y como se establece en el preámbulo del Proyecto de Ley que cuenta con 34 artículos.

Dicho Proyecto de Ley tiene como objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de Datos Personales, considerando también su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas o no, que traten Datos Personales (artículo 1 del Proyecto de Ley).

En la misma se abordan cuestiones sobre la utilización de datos personales relativos a obligaciones de carácter comercial, tratamiento de los datos personales por partes de los Organismos Públicos, así como las responsabilidades derivadas de las infracciones de la Ley.

Este Proyecto de Ley fue presentado por primera vez en el año 2017[8] y fue abierto a consulta pública, en la cual participaron distintas partes interesadas y surgieron dudas sobre temas estructurales, e inclusive presupuestarios, lo que llevo a que el Proyecto de Ley fuera retirado de la Asamblea Nacional de Diputados. El 20 de agosto de 2018 una versión revisada del Proyecto fue presentada por el Ministerio de la Presidencia a la Asamblea Nacional de Diputados.

El proyecto de Ley No. 665 de Protección Datos de Carácter Personal se encuentra aprobado en tercer debate en la Asamblea Nacional de Diputados de Panamá.

[7] Asamblea Nacional, Proyecto de Ley No.465 de Protección de Datos Personales de 20 de agosto de 2018. Disponible en: http://www.asamblea.gob.pa/proyley/2018_P_665.pdf

[8] Asamblea Nacional, Proyecto de Ley No. 463 de Protección de Datos de carácter personal, 8 de febrero de 2017. Disponible en: http://www.asamblea.gob.pa/proyley/2017_P_463.pdf

3. Definición de datos personales

La Ley No. 6 del 22 de enero de 2002 sobre Transparencia y Acceso Información Pública establece acción de Hábeas Data, la Ley No. 3 del 5 de enero de 2000 sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida, y la Ley No. 51 de 2009 que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones, no establecen definiciones sobre datos personales y datos sensibles. Lo mismo aplica para la Ley No. 24 del 22 de mayo de 2002, que regula el servicio de información sobre el historial de crédito pero que tampoco contiene una definición sobre datos personales y datos sensibles. Sin embargo, esta última define el concepto de dato y su tratamiento.

En cuanto a Proyecto de Ley No. 465 de Protección de Datos de Carácter Personal, en su artículo 3 numeral 9, establece explícitamente la noción de dato personal como “Dato de carácter personal o datos personales: Es cualquier información concerniente a personas naturales, que las identifica o las hace identificables”.

Otros numerales del referido Proyecto de Ley también proporcionan definiciones, como el Artículo 9, numeral 6, señalando a los datos de acceso restringido o confidencial como aquellos “Datos bajo responsabilidad del custodio cuyo tratamiento será permitido para fines de la administración pública o si se cuenta con el consentimiento expreso del titular, sin perjuicio de lo dispuesto por leyes especiales”.

Otros datos, como aquellos de importancia crítica estatal, se encuentran en el numeral 10, el cual establece que “La información asociada a datos personales, en poder de entidades del Estado, cuyo tratamiento resulta fundamental para el funcionamiento de éste en cualquiera de sus niveles de gobierno, los cuales serán definidos como tal por cada institución del Estado, de acuerdo a la Ley y según sus competencias”.

La ley también brinda otras definiciones. Tal es el caso del “Dato sensible”, recogida en el numeral 13 siendo, este “Aquel dato que se refiere a características físicas o morales de las personas naturales o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual, tal cual lo establezcan las leyes especiales”.

4. Principios de tratamiento de datos personales

El Proyecto de Ley contiene en sus disposiciones el respeto a principios de tratamiento de datos personales que forman parte de la Declaración de Principios, la Comisión Interamericana de Derechos Humanos y derechos reconocidos en la Convención Americana de Derechos Humanos, donde se protege el derecho a la privacidad, la honra y la reputación de las personas.

También recoge otros principios como la calidad y confidencialidad, al establecer que las bases de datos que contengan Datos Personales y que reposen en custodia del Estado deberán ser resguardadas de manera segura, ya sea que se encuentren ubicadas dentro o fuera del territorio nacional, como complemento a las legislaciones especiales que crean y reglamentan las bases de Datos Personales. En cuanto a los datos de importancia crítica estatal, se establece que los mismos deben hospedarse en servidores ubicados dentro del territorio nacional.

Otros principios como legalidad también se encuentran recogidos en el Proyecto de Ley, donde se reconocen los derechos de las personas a la información, modificación, cancelación o bloqueo de sus datos personales, estableciéndose el plazo de 10 días hábiles para que los responsables de las bases de datos faciliten su tramitación y contestación, y la posibilidad de que el titular de los datos pueda recurrir a la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) en caso de que su derecho no haya sido atendido.

5. Derechos ARCO

El proyecto de Ley de Protección de Datos de Carácter Personal en su artículo 12 hace referencia a los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), los cuales pueden ser ejercidos en cualquier momento siendo estos irrenunciables salvo excepciones contempladas en las leyes especiales.

El Articulo 12 del Proyecto de Ley No. 465 recoge los “derechos que tienen los titulares de los Datos Personales, de ejercer sobre los responsables del Tratamiento de bases de datos, así:

- **Derecho de Acceso:** Permite al titular obtener los Datos Personales que se encuentren almacenados o sujetos a Tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados.
- **Derecho de Rectificación:** Permite al titular solicitar la corrección de sus Datos Personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.
- **Derecho de Cancelación:** Permite al titular solicitar la eliminación de sus Datos Personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.
- **Derecho de Oposición:** Permite al titular, por motivos fundados y legítimos relacionados a una situación en particular, negarse a proporcionar sus Datos Personales o a que sean objeto de determinado Tratamiento, así como a revocar su consentimiento”.

6. Consentimiento

Sobre el consentimiento, la legislación actual es la anteriormente señalada Ley No. 6 del 22 de enero de 2002 sobre Transparencia y Acceso Información Pública, que establece acción de Habeas Data, junto con la Ley N. 51 de 2009, la cual dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones, y adopta otras disposiciones no tratan la noción del consentimiento.

Sin embargo, la Ley No. 24 del 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito, en su Título III sobre Derechos y Deberes del Consumidor y Cliente, en su artículo 23 numeral 4, abarca la necesidad de consentimiento para la recopilación de la información y transmisión de la información.

Artículo 23, numeral 4: "Consentir la recopilación de la información. Los datos sobre historial de crédito brindados por los consumidores o clientes a los agentes económicos, sólo podrán ser recopilados y/o transmitidos a las agencias de información de datos y suministrados por éstas a los, agentes económicos con el consentimiento expreso de los consumidores o clientes, con excepción de las obligaciones de carácter económico, financiero, bancario, comercial o industrial, siempre que ellas consten en cheques protestados por falta de fondos o por haber sido girados contra cuenta corriente cerrada o por orden de suspensión de pagos...".

En cuanto a la Ley No. 3 del 5 de enero de 2000, Ley General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida, en ella se hace la mención al consentimiento en su capítulo II, Sección Primera sobre el Diagnóstico, así como en el artículo 15 para el tratamiento, artículo 16 sobre la investigación y sobre la confidencialidad

Artículo 5. "El resultado de la prueba para el diagnóstico clínico de las infecciones de transmisión sexual, del virus de la inmunodeficiencia humana y del sida, será confidencial.

Con las excepciones previstas en esta Ley, la prueba para el diagnóstico de las infecciones de transmisión sexual, del virus de la inmunodeficiencia humana y del sida, deben realizarse con el consentimiento de la persona o su representante legal".

Artículo 15. "La transfusión de sangre y sus derivados, así corno los trasplantes de órganos y tejidos, que constituyen una medida excepcional para salvar y / o mejorar la calidad de vida del paciente o la paciente, requieren:
1. El consentimiento del paciente o la paciente o de sus familiares, en los casos en que sea posible
2. Cuando el paciente o la paciente no esté en capacidad física o mental de emitir su consentimiento, privará el criterio del médico o la médica tratante".

Artículo 26. (.....): "Ninguna persona infectada con el virus de la inmunodeficiencia humana, podrá ser objeto de experimentación para la aplicación de medicamentos o técnicas, asociados con este virus, sin haber sido advertida de su condición experimental y de sus riesgos y sin su consentimiento previo o el de su representante legal".

Articulo 34. “Con las excepciones establecidas por esta Ley, la confidencialidad es un derecho fundamental de la persona enferma o portadora de infección de transmisión sexual o del virus de la inmunodeficiencia humana. Nadie podrá, pública ni privadamente, hacer referencia a estos padecimientos, sin el previo consentimiento del paciente o la paciente, excepto para las cónyuges, los cónyuges, los compañeros y las compañeras de actividad sexual, así como para los representantes o las representantes legales de menores. La persona portadora de infección de transmisión sexual o del virus de la inmunodeficiencia humana o, en su defecto, su representante legal, tiene el deber de comunicar su situación, a sus contactos y a las personas en riesgo de contagio. De lo contrario, las autoridades de salud procederán a notificarlos”.

En cuanto al Proyecto de Ley, en su artículo 3 numeral 4, define consentimiento como ”Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos”.

Se pueden encontrar otras menciones en los siguientes artículos:

Artículo 5. “El titular tiene el derecho a que sus datos personales no sean utilizados de forma asociada para otros fines que no hayan sido expresamente informados, tales como publicidad, promociones, mercadeo, investigación, estudios, consultas o encuestas, y podrá oponerse al uso no expresamente informado o autorizado de sus datos personales, con las consecuentes responsabilidades civiles y penales”.

En toda recolección de datos personales realizada a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta Ley regula, se deberá informar a las personas del carácter no obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas.

Este artículo 5 requiere información expresa sobre las finalidades del tratamiento, en donde se sugiere la aplicación de medidas penales en caso de infracción.

Por su parte, el Artículo 6 señala: “El tratamiento de los datos personales sólo puede efectuarse cuando esta Ley u otras disposiciones legales lo autoricen o el titular consienta de manera previa, irrefutable y expresa en ello. La persona que consienta dicho tratamiento, debe ser debidamente informada respecto del propósito del uso de sus datos personales. El consentimiento podrá obtenerse en forma que permita su trazabilidad mediante documentación, sea esta electrónica o mediante cualquier otro mecanismo que resulte adecuado al medio de que se trate el caso y el mismo puede ser revocado, aunque sin efecto retroactivo. No requiere autorización para el tratamiento de datos personales, en los siguientes casos: (..... Cuando el consentimiento se refiera a datos personales sensibles de salud, el consentimiento será previo, irrefutable y expreso. (.....)”.

7. Sujetos obligados

Las normas sectoriales que han sido mencionadas en el apartado de marco jurídico establecen cada una dentro de su competencia los sujetos regulados.

En cuanto al Proyecto de Protección de Datos, los sujetos regulados son las personas naturales y jurídicas, de carácter público o privado, con o sin fines de lucro, que lleven a cabo el tratamiento y/o custodia de datos personales. Esto se refleja en el artículo 1.

Artículo 1: “Toda persona, natural o jurídica, de derecho público o privado, lucrativa o no, puede efectuar el tratamiento de datos de carácter personal, siempre que lo haga con arreglo a la presente Ley y para los fines permitidos en el ordenamiento jurídico. En todo caso, deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta Ley les reconoce”.

8. Obligaciones y responsabilidades de los sujetos obligados

El Proyecto de Ley, en su Artículo 3, menciona una serie de sujetos obligados sin especificar las obligaciones de los custodios y responsables para el tratamiento de datos personales.

El Proyecto de Ley de Protección de Datos en el Artículo 7 especifica responsabilidades de los sujetos obligados, como el establecimiento de los protocolos y procedimientos de gestión y transferencia segura. En su Artículo 8 se menciona la obligación de guardar la confidencialidad de los datos, y el Artículo 12 establece la obligación de cuidar los datos con debida diligencia y designa las responsabilidades por daños o perjuicios ocasionados que le sean exigibles.

El Proyecto de Ley, en su Capítulo III sobre la utilización de Datos Personales, también incluye responsabilidades a los sujetos obligados como la necesidad de contar con consentimiento previo, informado y expreso del titular, salvo lo establecido en las leyes especiales (Artículo 23).

La necesidad de establecer las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de la red o en la prestación de los servicios, con el fin de garantizar los niveles de protección de los datos personales (Artículo 24). La prohibición de por parte del responsable del tratamiento de datos personales y/o el custodio de la base de datos de transferir o comunicar los datos que se relacionen con una persona identificada o identificable luego de transcurridos siete (7) años desde que se extinguió la obligación legal de conservarla, salvo que el titular de los datos personales expresamente solicite lo contrario tal y como se establece en el Artículo 25 del referido proyecto de ley.

9. Disposiciones sobre la transferencia y cesión de datos

El Proyecto de Ley, en su Capítulo III sobre la utilización de Datos Personales, específicamente en el Artículo 23, se abordan cuestiones relativas a la transferencia o cesión de datos al establecer que solo podrán trasmitir información sobre los mismos cuando cuenten con el consentimiento previo, informado y expreso del titular, salvo lo establecido en las leyes especiales. Así lo establecido en el Artículo 25 sobre la prohibición por parte del responsable del tratamiento de datos personales y/o el custodio de la base de datos de transferir o comunicar los datos que se relacionen con una persona identificada o identificable, luego de transcurridos siete (7) años desde que se extinguió la obligación legal de conservarla, salvo que el titular de los datos personales expresamente solicite lo contrario.

Se aborda de igual manera en el Artículo 29 que los responsables y/o custodios de bases de datos que transfieran datos personales almacenados en bases de datos a terceros, deben llevar un registro de estas. Estas bases de datos deberán estar a disposición de la ANTAI en caso de que ésta lo requiera, para cumplir con las facultades que le otorgara el proyecto de ley. Sus Artículos 27 y 28 abordan cuestiones sobre que el tratamiento de datos personales por parte de una entidad pública solo podrá efectuarse respecto de las materias de su competencia, y en los casos de condenas por delitos, infracciones administrativas o faltas disciplinarias; no podrán comunicarlos una vez prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena, salvo autorización expresa por el titular del dato.

10. Autoridad competente

Cada una de las leyes mencionadas en normas sectoriales contiene su propia autoridad de control. El Proyecto de Ley de Protección de Datos establece las autoridades competentes en su Artículo 7.

Artículo 7. “El responsable del tratamiento de datos personales contenidos en bases de datos, establecerá los protocolos y procedimientos de gestión y transferencia segura, protegiendo los derechos de los titulares sobre sus datos bajo los preceptos de esta Ley”.

El procedimiento de almacenamiento de información será fiscalizado y supervisado por la Autoridad de Transparencia y Acceso a la Información (ANTAI), con el apoyo de la Autoridad Nacional para la Innovación Gubernamental (AIG), cuando trate de aspectos relacionados a las tecnologías de la información y comunicación, con excepción de aquellas que se realicen mediante leyes especiales, las cuales serán fiscalizadas y supervisadas por las autoridades correspondientes.

La ANTAI es el ente rector en materia de derecho de petición y acceso a la información pública, protección de datos personales, transparencia, ética y prevención contra la corrupción a nivel gubernamental. Fue establecida como una nueva institución pública, descentralizada del Estado, con capacidad para actuar con plena autonomía funcional de forma administrativa, legal y con presupuesto independiente en el ejercicio de sus funciones, sin recibir instrucción de ninguna autoridad, órgano del Estado o persona.

La Autoridad contará con un director general, además de las unidades administrativas necesarias que requiera para el ejercicio de sus funciones. Así se establece en el artículo 10 de la Ley 33 de 25 de abril de 2013, que crea la “Autoridad Nacional de Transparencia y Acceso a la Información”[9].

El director general será nombrado por el Órgano Ejecutivo y ratificado por la Asamblea Nacional, para un periodo de siete años prorrogable por una sola vez (Artículo 12 de la ley anteriormente mencionada). El director general dirigirá y administrará la Autoridad y será su representante legal (Artículo 13), y el director general tendrá la consideración de alta autoridad del Estado a nivel nacional y una remuneración equivalente a la de ministro de Estado. A nivel internacional tendrá el título de embajador plenipotenciario de la República de Panamá para el debido cumplimiento de sus funciones, como se establece en el Artículo 14.

[9] Asamblea Nacional, Ley 33 de 25 de abril de 2013, que crea la Autoridad Nacional de Transparencia y Acceso a la Información. Disponible en: http://www.digeca.gob.pa/tmp/file/1202/Ley%20No-33%20DE%2025%20abril%20de%202013%20-Que%20crea%20la%20Antai.pdf

La Autoridad Nacional para la Innovación Gubernamental (AIG) se establece mediante la Ley 65 de 30 de octubre de 2009[10]. Es la entidad competente del Estado para planificar, coordinar, emitir directrices, supervisar, colaborar, apoyar y promover el uso óptimo de las tecnologías de la información y comunicaciones en el sector gubernamental para la modernización de la gestión pública, así como recomendar la adopción de políticas, planes y acciones estratégicas nacionales.

La autoridad tendrá personalidad jurídica, patrimonio propio y autonomía en su régimen interno, así como la capacidad de adquirir derechos y contraer obligaciones, administrar sus bienes y gestionar sus recursos, sujeta a las disposiciones que regulan la contratación pública y la fiscalización de la Contraloría General de la República. La Autoridad será representada ante el Órgano Ejecutivo por conducto del Ministerio de la Presidencia, como se establece en un su Artículo 2.

La AIG está bajo la dirección de un Administrador General y un Subadministrador General nombrados por el presidente de la República (Artículo 4). Adicionalmente, se cuenta con un Consejo Nacional de Innovación (Artículo 5).

[10] Asamblea Nacional, Ley 65 de 30 de octubre de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental, Disponible en: http://www.innovacion.gob.pa/descargas/Ley65.pdf

11. Procedimientos y Sanciones

El Proyecto de Ley de Protección de Datos reconoce la facultad de ANTAI para sancionar a la persona natural o jurídica, propietaria o responsable del manejo o administración de bases de datos que, por razón de la investigación de las quejas que se le presenten, se les compruebe que han infringido los derechos del titular de los datos personales. Las cuantías de las sanciones y el procedimiento sancionador a llevar a cabo serán reguladas posteriormente.

Artículo 26: “La infracción de cualquiera de estas obligaciones será del conocimiento de la ANTAI, quien aplicará las sanciones correspondientes de conformidad con el respectivo reglamento, salvo aquellas que competan a otras entidades públicas contempladas en leyes especiales”. El Artículo 33 otorga facultades a la ANTAI “para sancionar a la persona natural o jurídica, responsable del tratamiento de los datos personales, así como también al custodio de la base de datos, que por razón de la investigación de las quejas o denuncias que se le presenten, se les compruebe que han infringido los derechos del titular de los datos personales”.

La ANTAI fijará los montos de las sanciones aplicables a las respectivas faltas, acorde a la gravedad de las faltas. También reglamentará el procedimiento correspondiente. Las sanciones pecuniarias que imponga la ANTAI, en el ejercicio de las facultades establecidas en esta Ley, que no hayan sido pagadas en el término concedido, se remitirán para su cobro a la Dirección General de Ingresos (DGI) del Ministerio de Economía y Finanzas.

Todas las leyes contemplan sanciones si se presentan contravenciones a lo establecido. En lo específico al Proyecto de Ley, en su artículo 35 se establece que “las sanciones que imponga la ANTAI a los responsables de las bases de datos y demás sujetos alcanzados por el régimen de la presente Ley y sus reglamentos, se graduarán en atención a la reincidencia de la infracción cometida.

1. Las sanciones se clasifican así:
2. Amonestación verbal.
3. Amonestación escrita.
4. Multas.
5. Clausura de los registros de la base de datos.
   Para ejecutar esta acción, la ANTAI deberá contar con la opinión formal del Consejo Consultivo de Protección de Datos Personales, sin perjuicio de los recursos que esta ley le concede al afectado.
6. Suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de datos personales.

Para hacer cumplir la sanción de suspensión o clausura, la ANTAI podrá requerir el auxilio de la Fuerza Pública. Los hechos que acarreen una sanción serán documentados de acuerdo a las formalidades legales y se realizarán informes estadísticos que permitan a la ANTAI establecer la gravedad, reiteración o reincidencia de la infracción cometida.

Se debe proceder a la retención de documentos y archivos inspeccionados cuando la infracción o situación investigada sea de alto riesgo o amenaza y así lo requiera, hasta por un lapso de treinta días hábiles. La medida será formalmente documentada y sólo podrá prorrogarse por los órganos jurisdiccionales competentes cuando sea imperioso.

Se debe suspender en cualquier etapa de la investigación que se realice en la sede administrativa, y aún luego de promovido el proceso judicial ante la autoridad competente, la investigación o desistir del proceso judicial mediante la realización de transacciones, previo cumplimiento de los requisitos legales, siempre que los encargados o responsables del tratamiento de datos investigados o demandados acepten medidas en torno a las conductas o actos investigados, incluyendo clausulas penales que garanticen el cumplimiento del acuerdo.

Se debe ejercer la jurisdicción coactiva sobre las multas impuestas por violación a las normas determinadas en la presente Ley y sus reglamentos.

12. La computación en la nube y los servicios financieros

El Proyecto de Ley de Protección de Datos Personales excluye de su aplicación a las empresas de servicios financieros, los bancos y las compañías de tarjetas de crédito. Por lo que los datos financieros están actualmente excluidos de este Proyecto de Ley.

Actualmente, se ha presentado a la Asamblea Nacional de Diputados un proyecto de ley para la Modernización y Competitividad Internacional del Sistema Financiero de la República de Panamá. Este proyecto de ley tiene como objetivo cumplir con compromisos regulatorios junto con la innovación en los servicios legales y financieros al ser Panamá un centro financiero.

Este tema no había sido objeto de revisión desde el año 1998, cuando se realizó la última reforma a la Ley bancaria. Este proyecto de Ley incluye todo lo relacionado al financiamiento tecnológico FINTECH, y también incluye figuras financieras novedosas como el “crowdfunding” o micromecenazgo, es decir, una red de financiación colectiva, normalmente online, que a través de donaciones económicas o de otro tipo consiguen financiar un determinado proyecto a cambio de recompensas, participaciones de forma altruista y también la tipología “crowdlending” como alternativa a la financiación tradicional. Estas figuras estarán autorizadas a ofrecer distintos servicios como emisión de dinero electrónico y proyectos en plataformas de financiamiento colectivo, entre otros, como se menciona en el preámbulo del proyecto. Por lo que se busca es que se puedan brindar estos servicios sin menoscabar los principios de competencia y de protección de los consumidores.

El Proyecto de Ley busca reafirmar la privacidad de las transacciones financieras salvaguardando la información de los particulares o de las empresas. En su Artículo 22 se abordan cuestiones relacionadas a la seguridad informática donde se menciona la necesidad de designar un oficial de seguridad informática el cual establecerá las reglas adicionales de capital, seguridad en el tratamiento de datos de clientes u otras reglas de cumplimiento obligatorio que considere necesarias para garantizar razonablemente la prestación de los servicios en condiciones de seguridad y fiabilidad. Además contiene una sección sobre normas aplicables a las entidades de administración de mercados y de provisión de servicios de custodia y/o almacenamiento de criptomonedas.

Con el objetivo de dar cumplimiento al objetivo 13 de la Agenda Digital PANAMÁ 4.0 2014-2019 del gobierno nacional, la Autoridad Nacional para la Innovación Gubernamental (AIG) en Panamá lanzó el proyecto de la nube computacional gubernamental en el año 2011. Se trata de una plataforma para montar servicios en la nube de diversas instituciones públicas, en las cuales los recursos y servicios informáticos son ofrecidos y consumidos como servicios a través de la Internet o intranet, garantizando su disponibilidad.

La futura ley de protección de datos establecerá el marco legal para la interoperabilidad y la posibilidad de desarrollo de Centros de Datos para aplicaciones de nube, tanto a nivel gubernamental como a nivel de entorno empresarial. A su vez les brindará seguridad a las instituciones en la implementación de nubes gubernamentales. Con esto la AIG busca modificar la ley de Compras y los Convenios Marco con el objetivo de facilitar la implementación de nubes computacionales, la contratación de horas de programación, expertos tecnológicos, ERPs y períodos plurianuales para la contratación de mantenimiento de plataformas TI, tal y como se establece en la Agenda Digital PANAMA 4.0.

Esta nube computacional gubernamental se encuentra en plataformas de seguridad privadas del Estado, utilizando como medio de conectividad los servicios de la RNMS. Es un plan a 3 fases para potenciar, fortalecer y desarrollar una NCG que brinde servicios de infraestructura (IaaS), plataforma (PaaS) y aplicaciones (SaaS) a todas las entidades de gobierno.

La nube computacional gubernamental permite la reducción de costos de operación y mantenimiento, por lo que contribuye a una mayor generación de ingresos al atraer la inversión.

13. Agenda Digital

La Agenda Digital 4.0[11] tiene como objetivo darle continuidad a los trabajos que iniciaron en el año 2002 que buscan la modernización de las entidades gubernamentales a través de una política común estratégica, en la cual se incorpore el uso de las Tecnologías de la Información y Comunicaciones (TIC) en los distintos procesos de las entidades del Estado.

La Agenda Digital 4.0 fue elaborada siguiendo los criterios contenidos en la Ley 83 de 2012[12], denominada de Gobierno Electrónico, la cual establece los parámetros legales que deben seguir las entidades del Estado para facilitar y simplificar, por vía de los medios digitales, aquellos trámites que realizan los ciudadanos y empresas, incluyendo la obligatoriedad de las entidades de elaborar anualmente su Agenda Digital, el Plan de Simplificación de Trámites y el Plan Operativo Anual[13]. Para su creación se tomaron en cuenta otras Agendas Digitales, como las de Unión Europea, España, Chile, Perú, México y la Agenda Digital eLAC2018.

En su elaboración, como se menciona en la sección de stakeholders de la Agenda Digital, se han tenido en cuenta los principales segmentos de interés para establecer acciones concretas de cómo el Gobierno interactuará con los mismos. Tal es el caso del Gobierno al Ciudadano (G2C), principal objeto de una Agenda Digital centrada en el ciudadano, o del Gobierno a los Negocios o empresas (G2B), las relaciones entre instituciones (I2I), los intercambios de Gobierno a Gobierno (G2G) y la atención de las consultas que se hagan al Gobierno desde cualquier parte del Mundo (G2W)[14]. Esta agenda Digital comprende tópicos que son el resultado de aspectos que fueron solicitados por los stakeholders como lo son la necesidad de mayor transparencia, servicios de gobierno digital, planificación, capacitación, interoperabilidad y normativa.

11 Autoridad Nacional para la Innovación Gubernamental, Agenda Digital 2014-2019, Disponible en: http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf

12 Asamblea Legislativa, Ley N° 83 de 9 de noviembre de 2012, Que regula el uso de medios electrónicos para los trámites gubernamentales y modifica la ley 65 de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental, Disponible en: http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2012/2012_598_1356.pdf

13 Autoridad Nacional para la Innovación Gubernamental, Agenda Digital 2014-2019, Antecedentes, pág. 5, Disponible en: http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf

14 Ibidem, pág.24

Sobre la normativa, las partes interesadas o stakeholders manifestaron la necesidad de la modernización gubernamental, el acceso a la información, la protección de los datos personales, la seguridad en las transacciones, mejorar los procesos de pago, gestión de tributos, minería de datos, entre otros.

La importancia de contar con leyes sobre Ciberseguridad y Protección de Datos recae en la meta de atraer la inversión extranjera a Panamá, proporcionando un ambiente legal estable y predecible. En este sentido, cabe mencionar la solicitud que presentaron para la revisión y modificación de la Ley de Compras, la revisión de leyes de comercio en línea con nuevos tratados internaciones, o nuevas inquietudes como la trazabilidad, la agilización de trámites aduaneros, creación de empresas, restricciones a la competencia[15].

Los principales objetivos de la agenda digital son:

1. Líneas estratégicas y valores para desarrollar las acciones prioritarias.
2. Definir el marco de actuación de la AIG y de las entidades en cada caso.
3. Reorganizar a la AIG, preparándola para los exigentes retos a conseguir en el quinquenio, y en adelante.
4. Las principales carencias de la entidad, preparar un plan para desarrollar competencias y fortalezas que auguren el éxito, coordinando los esfuerzos internos y externos.
5. Establecer una serie de acciones a desarrollar y validar las principales iniciativas con el resto de las entidades.
6. Desarrollar una serie de nuevos instrumentos y herramientas que ayuden en la innovación y transformación gubernamental.
7. Perfeccionar los métodos de planificación, seguimiento de las acciones, la determinación de métricas, indicadores para su seguimiento, a través del instrumento de la Agenda Digital institucional y la Ley 83 de Gobierno Electrónico[16].

La Agenda Digital contiene una serie de proyectos que buscan cumplir con los objetivos antes mencionados, como lo son una mejor articulación de la tecnología, cambios y mejoras normativas, gobierno electrónico móvil, el desarrollo de la Sociedad de la Información y el Conocimiento entre otros la iniciativa de Gobierno Abierto, que busca aumentar la competitividad y la transparencia.

15 Ibidem, pág.26 f

16 Ibidem, pág.32

Entre los pilares básicos de este programa se encuentra la política de datos abiertos, en la que se ha establecido que la ANTAI y la AIG, con el apoyo de la Contraloría General de la República, juegan un rol clave en la divulgación y acompañamiento para la aplicación de la metodología de apertura de datos, habilitando la generación y poblamiento del Portal de Datos Abiertos de Gobierno por parte de las instituciones del gobierno nacional, con una apertura de datos en formatos accesibles y abiertos.

La apertura de datos elaborados, tanto como de datos no procesados para su posterior análisis y la generación de procesos estandarizados a nivel nacional en el tema de apertura de datos[17].

El documento menciona que para cumplir este objetivo, entre otras iniciativas, se debe trabajar en una Ley de Protección de Datos que establezca el marco legal para la interoperabilidad y la posibilidad de desarrollo de Centros de Datos para aplicaciones de nube, tanto a nivel gubernamental como a nivel de entorno empresarial[18]. Se buscan certezas jurídicas para las instituciones al compartir datos personales, mayor establecimiento de negocios basados en datos por parte de empresas extranjeras que ofrezcan servicios basados en la nube, y garantías jurídicas a los usuarios en relación con el uso de sus datos.

Este es uno de los elementos contenidos en la Agenda Digital, el cual busca la aumentar la prestación de servicios, trámites, transparencia y participación ciudadana a través de inversiones conjuntas del Gobierno y el sector privado, impactando significativamente en la reducción de la brecha digital, la inclusión social y la competitividad del país[19].

17 Ibidem, pág 47

18 Ibidem, pág. 60

19 Autoridad Nacional para la Innovación Gubernamental, AIG expone Agenda Digital PANAMÁ 4.0 en CADE 2017, Disponible ne: http://www.innovacion.gob.pa/noticia/2924

Referencias

Constitución Política de la República de la República de Panamá. Reformada por los Actos Reformatorios de 1978, el Acto Constitucional de 1983 y los Actos Legislativos de 1994. Disponible en: https://www.oas.org/juridico/spanish/pan_res2.doc

Ley No. 6 del 22 de enero de 2002, Transparencia y Acceso Información Pública. Establece acción de Habeas Data. Disponible en: http://www.redipd.es/legislacion/common/legislacion/panama/ley_num_6.pdf

Ley No. 24 del 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito. Disponible en: http://www.oas.org/es/sla/ddi/docs/P7%20Ley%2024%20de%202002.pdf

Ley No. 3 del 5 de enero de 2000, Ley General sobre las Infecciones de Transmisión Sexual, el Virus de la Inmunodeficiencia Humana y el Sida. Disponible en: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_127734.pdf

Ley N. 51 de 2009 que dicta normas para la conservación, la protección y el suministro de datos de usuarios de los servicios de telecomunicaciones y adopta otras disposiciones. Disponible en: https://docs.panama.justia.com/federales/leyes/51-de-2009-sep-23-2009.pdf

Asamblea Nacional, Ley 65 de 30 de octubre de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental, Disponible en: http://www.innovacion.gob.pa/descargas/Ley65.pdf

Asamblea Nacional, Proyecto de Ley No. 463 de Protección de Datos de carácter personal, 8 de febrero de 2017. Disponible en: http://www.asamblea.gob.pa/proyley/2017_P_463.pdf

Autoridad Nacional para la Innovación Gubernamental, Agenda Digital 2014-2019, Disponible en: http://innovacion.gob.pa/descargas/Agenda_Digital_Estrategica_2014-2019.pdf

Asamblea Legislativa, Ley N° 83 de 9 de noviembre de 2012, Que regula el uso de medios electrónicos para los trámites gubernamentales y modifica la ley 65 de 2009, que crea la Autoridad Nacional para la Innovación Gubernamental, Disponible en: http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2010/2012/2012_598_1356.pdf

Asamblea Nacional, Proyecto de Ley No.465 de Protección de Datos Personales de 20 de agosto de 2018. Disponible en: http://www.asamblea.gob.pa/proyley/2018_P_665.pdf