ASAMBLEA LEGISLATIVA PLURINACIONAL DE BOLIVIA
CÁMARA DE DIPUTADOS

CÁMARA DE DIPUTADOS
PRESIDENCIA
RECIBIDO
20 OCT 2021
HORA 10:55 | FIRMA
Nº REGISTRO | Nº FOJAS 90

CÁMARA DE DIPUTADO
SECRETARIA GENERAL
RECIBIDO
5775
21 OCT 2021
HORA 8:38 | FIRMA
Nº REGISTRO | Nº FOJAS

La Paz, 19 de octubre de 2021
CITE: CCLYSE/INT N° 0320/2020 - 2021

Señor:
Dip. Freddy Mamani Laura
PRESIDENTE DE LA CÁMARA DE DIPUTADOS
ASAMBLEA LEGISLATIVA PLURINACIONAL
Presente. -

REF.- PROYECTO DE LEY

PL- 349-20

De mi mayor consideración:

En el marco del Reglamento General de la Cámara de Diputados, remito a su Investidura el Proyecto de Ley "**LEY PROTECCION DE DATOS PERSONALES**" a fojas 30.

Asimismo, en observancia a los requisitos establecidos al efecto, adjunto cuatro ejemplares del proyecto de Ley y el medio magnético correspondiente.

Con este motivo, saludo a usted con las consideraciones más distinguidas.

Dip. I. Renán Cabezas Veizán
PRESIDENTE
COMISIÓN DE CONSTITUCIÓN, LEGISLACIÓN

PROYECTO DE LEY PROTECCIÓN DE DATOS PERSONALES

Exposición de motivos

En el transcurso de las últimas décadas, se ha producido en el mundo una revolución tecnológica y comunicativa de una magnitud tan grande que ha atravesado distintos ámbitos, tanto a nivel público como privado. La aparición de tecnologías como Internet ha creado múltiples oportunidades en casi todos los aspectos de la vida, permitiendo ser un instrumento de comunicación, información y desarrollo.

Es innegable que este avance tecnológico tiene repercusiones positivas en la sociedad, trayendo beneficios inéditos y permitiendo democratizar el acceso a mecanismos de información que pueden conllevar un mayor y mejor desarrollo. Así también, las entidades públicas han podido beneficiarse de estos cambios, que les han permitido realizar y facilitar diferentes servicios, como los trámites gubernamentales que realiza la ciudadanía, y también el intercambio de datos entre instituciones lo que permiten una mejora en el funcionamiento del Estado, así como una visión integrada del manejo público.

De igual manera, en el ámbito privado ha existido un desarrollo sin precedentes de servicios relacionados con la tecnología que determinan incluso relaciones de personas nacionales con empresas domiciliadas en el extranjero. Esto ha hecho que las actividades comerciales se hayan internacionalizado, promoviendo un ámbito de mayor competencia y crecimiento para todos.

No obstante, a pesar de todos estos beneficios que ha traído la denominada *Era Digita*l, también existen dificultades y peligros que deben ser considerados. Sobre algunos de ellos, existe además una imperiosa necesidad de regular normativamente, teniendo en cuenta que una obligación irrenunciable del Estado es precautelar y garantizar los derechos de las personas, en todos los ámbitos. Acciones que además

ya han sido adoptadas en la mayoría de países del mundo.Tal vez uno de los temas más urgentes de esta agenda regulatoria es el régimen de protección de los datos

grupos indígenas, por ejemplo), hasta el uso de información personal con la finalidad de manipular la opinión pública o los procesos electorales, pasando por el incremento de la violencia de género que ahora se ejerce en nuevos ámbitos digitales multiplicando daños y violencias a través de las tecnologías de la información y comunicación. Conforme el uso de las nuevas tecnologías va en aumento, de igual forma ocurre con los casos relacionados con la seguridad de los datos y el uso indebido de los mismos, tanto a nivel nacional como internacional, y en muchas ocasiones no existen las sanciones correspondientes debido a la ausencia de una norma clara y específica.

Sin embargo, es preciso reconocer que desde hace algunos años ya se vienen dando algunos cambios importantes en este ámbito. Por ejemplo, la Constitución Política en el artículo 20 determina el derecho de todas las personas de acceder a los servicios básicos, entre ellos, las telecomunicaciones. Por otro lado, el artículo 21 establece que, entre los derechos civiles reconocidos se encuentran los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad, todos ellos relacionados con la autodeterminación informativa, un derecho que se protege a través de la Acción de Protección de Privacidad.

También existen normas conexas en el ámbito tecnológico que impactan en la protección de los datos personales. Por ejemplo en la Ley 164 "Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación" y la Ley 1080 "Ley de ciudadanía digital", entre otras. No obstante, la dispersión de todas estas regulaciones, dificulta la comprensión y defensa integral de los datos personales. Además, impide visibilizar la actualidad de la temática y determinar claramente los derechos y obligaciones de las personas y entes relacionados con su uso y tratamiento.

Por otro lado, tanto las instituciones públicas como las entidades privadas tienen acceso a datos personales, y en muchas ocasiones, los utilizan con el fin de mejorar la calidad de los servicios que brindan. En ese sentido, el país tiene un reto pendiente referido a lograr la interoperabilidad de datos, aspecto de especial relevancia en el ámbito público con relación a la mejora de la calidad de los servicios que se brinda a la ciudadanía, la promoción de una integración real de las diversas entidades públicas y la formulación de políticas públicas bajo criterios objetivos obtenidos en base a datos.

Para ello, es necesario establecer estándares técnicos y procedimentales que a la larga permitan una mayor eficacia gubernamental y por ende una reducción de los costos en el

servicio público, tanto para la administración como para la ciudadanía; además, se debe considerar que la interoperabilidad de datos puede fortalecer la transparencia de los servicios públicos y fomentar la confianza del ciudadano hacia el aparato estatal. Las falencias que se producen en la gestión pública y en el sector privado al brindar servicios menos eficientes, también atenta contra los derechos de la ciudadanía de recibir servicios eficientes que no requieran gastos onerosos de desplazamientos y largas colas.

Se debe considerar también que, las personas naturales son titulares de los datos personales, que son aquellos que permiten identificar, localizar o contactar de forma directa o indirecta a personas naturales. Además, dentro de los datos personales, se encuentran algunos de naturaleza sensible, que pertenecen a la esfera íntima de las personas y que pueden llevar a estigmatizaciones o discriminación, entre ellos, de manera enunciativa: creencias religiosas, opiniones políticas, datos relacionados con la salud, orientación sexual, etc.

Distintos países de la región han ido desarrollando normativa específica relacionada con la protección de datos, estableciendo leyes concretas sobre esta temática. Así, por ejemplo, Argentina cuenta con una Ley de Protección de Datos desde el año 2000 y Perú desde el año 2011. De igual manera, otros países han avanzado en estos temas de forma muy reciente, como es el caso de Brasil, que recién cuenta con una ley de este tipo que ha entrado en vigencia el año 2020; o Ecuador, que el 10 de mayo de 2021 aprobó en su Asamblea Nacional la Ley de Protección de Datos Personales. Son pocos los países de la región que aún no cuentan con una norma de esta naturaleza, entre ellos Bolivia, Paraguay y Venezuela.

No solo en Latinoamérica, sino en todo el mundo, las leyes de protección de datos son un instrumento que permite salvaguardar los derechos de las personas, facilitar la creación de políticas por parte del Estado y ofrecer certeza jurídica al sector privado. Es por ello que, se hace ineludible regular la temática, tanto por la obligación de resguardar los derechos establecidos en la Constitución Política del Estado y los tratados de derechos humanos de los cuales el Estado Plurinacional de Bolivia es parte, como también, por la necesidad de actualizar la normativa boliviana a las exigencias de un mundo en constante cambio tecnológico.

En ese sentido, la presente ley tiene por objeto regular el tratamiento de datos personales que se efectúan en el Estado Plurinacional de Bolivia, y por ende, garantizar los derechos de protección de datos personales, privacidad, intimidad, honra, propia imagen y autodeterminación informativa de las personas titulares de datos personales. De igual manera,

dar un marco normativo a la gestión de bases de datos personales administradas por el sector público y privado para que interoperándolas puedan proveer mejores servicios a la ciudadanía.

Así, la ley abarca distintos aspectos, entre ellos, las definiciones que permitirán comprender a cabalidad la naturaleza de las normas y de los aspectos regulados. Por otro lado, enfatiza en el consentimiento que deben brindar los titulares de los datos personales para poder realizar el tratamiento de los mismos, además de brindar el pleno reconocimiento a los derechos de acceso, rectificación, cancelación, oposición y portabilidad, denominados derechos ARCOP.

También, se determina las obligaciones que tienen las personas naturales o jurídicas que se encuentran involucradas en el tratamiento de datos, incluyendo la manera en la que se debe proceder con relación a la interoperabilidad de los datos. De igual manera, se determina la creación del Consejo Plurinacional para la Protección de Datos Personales – CPPDP y de la Autoridad de Protección de Datos Personales – APDP que formarán parte del aparato del Estado, como encargadas de que se cumplan las disposiciones de la ley, de acuerdo a las atribuciones correspondientes.

Así, la presente Ley regula un aspecto de suma relevancia de acuerdo al contexto actual, permitiendo que el Estado Plurinacional de Bolivia cuente con un instrumento normativo específico que garantice los derechos de las personas con relación al tratamiento de datos personales que se constituye en una acción cada vez más común, la cual debe ser regulada.

Dip. I. Renán Cabezas Veizaga
PRESIDENTE
COMISION DE CONSTITUCIÓN
LEGISLACION Y SISTEMA ELECTORAL
CAMARA DE DIPUTADOS
Asamblea Legislativa Plurinacional

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
GENERALIDADES

PL- 349-20

Artículo 1. (Objeto).- La presente ley tiene por objeto regular el tratamiento de datos personales que se efectúan en el Estado Plurinacional de Bolivia, así como regular los métodos de seguridad, los derechos, las responsabilidades y sanciones aplicables a cada caso.

Artículo 2. (Finalidad).- La presente ley tiene por finalidad garantizar los derechos de protección de datos personales, privacidad, intimidad, honra, propia imagen y autodeterminación informativa de las personas titulares de datos personales.

Artículo 3. (Ámbito de Aplicación).-

I. La presente ley será aplicable al tratamiento de datos personales de personas individuales que se encuentren en territorio boliviano realizado por personas naturales y/o jurídicas de carácter privado, público o mixto, nacionales o internacionales, con independencia de si el tratamiento tuvo lugar en el territorio nacional o no, de la forma de su tratamiento, modalidad de creación, tipo de soporte, procesamiento, almacenamiento y organización.

II. Se excluye la aplicación de la presente ley cuando resulte aplicable la legislación o jurisdicción extranjera en virtud de un contrato, instrumento jurídico o de las regulaciones vigentes del derecho internacional público.

III. La legislación y jurisdicción que sea aplicable según el caso debe garantizar un nivel adecuado de protección de los datos de conformidad con los principios y estándares internacionales referidos a protección de datos personales.

Artículo 4. (Excepciones).- Las disposiciones de la presente ley no serán aplicables:

1. En el caso de personas particulares que formen archivos, registros o bancos de datos personales que sean de uso exclusivamente personal.
2. Personas fallecidas, sin perjuicio de lo establecido en el artículo 27 de la presente Ley.
3. Datos disociados, en tanto no sea posible identificar a su titular. En el momento en que los datos dejen de ser anónimos o seudonomizados, su tratamiento estará sujeto a las disposiciones de la presente ley.
4. En ningún caso podrán afectar las fuentes de información periodística, el secreto en materia de prensa y el ejercicio de la función periodística. Sin perjuicio de ello, las personas titulares pueden ejercer los derechos establecidos en la presente ley, siempre y cuando no afecten el ejercicio periodístico. Esta disposición incluye otros ejercicios legítimos del ejercicio del derecho a la libertad de expresión, como ser, de forma enunciativa pero no limitativa: las investigaciones realizadas por organizaciones no gubernamentales o personas u organizaciones académicas.

Artículo 5. (Definiciones).- A efecto de la aplicación de la presente Ley, se entiende por:

1. **Base de datos:** Conjunto organizado de datos personales, cualquiera que sea su forma o modalidad de creación, almacenamiento, organización, acceso, tratamiento y difusión. Se divide en:
    a. **Base de Datos Automatizadas:** Es el conjunto organizado de datos personales que son creados, tratados y/o almacenados a través de programas de computadora o software.
    b. **Base de Datos no Automatizadas:** Es el conjunto organizado de datos personales que son creados, tratados y/o almacenados de forma manual, con ausencia de programas de computadora o software.
2. **Consentimiento:** Manifestación de la voluntad, libre, expresa, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza con un determinado fin y tiempo específico, el tratamiento de los datos personales que le pertenecen. Debe ser realizado previamente al tratamiento de datos.
3. **Datos Personales:** Datos de cualquier tipo que permitan identificar, localizar o contactar a personas naturales. Se divide en:
    a. **Datos Personales Generales:** Datos de cualquier tipo que permitan identificar, localizar o contactar de forma directa o indirecta a personas naturales, expresados en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo.
    b. **Datos Personales Sensibles:** Aquellos datos personales que se refieran a la esfera íntima de una persona natural y que pueden llevar a estigmatizaciones o discriminación. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual.
    c. **Datos biométricos:** Aquellos datos personales referidos a las características físicas, fisiológicas o conductuales de una persona que posibiliten o aseguren su identificación única. De forma enunciativa pero no limitativa: Huella dactilar, reconocimiento facial, reconocimiento del iris, reconocimiento de la geometría de la mano, reconocimiento de retina, reconocimiento de voz, datos genéticos, entre otros.

    En la presente ley, cuando se contemple "Datos Personales", se entenderá que abarca los datos personales, datos personales sensibles y datos biométricos, a menos de que se especifique lo contrario. Sin embargo, los responsables deben considerar que los datos personales sensibles y los datos biométricos, debido a sus características e implicaciones deben tener un tratamiento especialmente cuidadoso.

4. **Metadato:** Los metadatos son datos descriptivos de las bases de datos. Describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos. Se caracterizan por:
    a. Ser altamente estructurados.
    b. Describir características, circunstancias y atributos de los datos.

c. Ser útiles para la estandarización de las bases de datos, la búsqueda de datos y su análisis, y acelerar los cambios en las bases de datos.

5. **Derechos ARCOP (Derechos de acceso, rectificación, cancelación, oposición y portabilidad):** Derechos personalísimos y fundamentales de acceso, rectificación, cancelación, oposición y portabilidad al tratamiento de datos personales. En todo momento el titular o su representante podrá solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen. El ejercicio de cualquiera de los derechos ARCOP no es requisito previo, ni impide el ejercicio de otros.

6. **Disociación de Datos:** Todo tratamiento de datos personales generales, sensibles y/o biométricos, donde por la manera en que la información ha sido obtenida no pueda asociarse a persona determinada o determinable. Se divide en:
   a. **Anonimización:** Proceso irreversible mediante el cual los datos identificativos se disocian de los datos personales generales, sensibles y/o biométricos. Existen tres tipos: generalización, aleatorización y eliminación. Tiene la finalidad de minimizar la posibilidad directa o indirecta de identificación del titular.
   b. **Seudonimización:** Proceso reversible de disociación de datos personales del titular, sustituyéndolos por códigos, palabras u otros similares, con la finalidad de resguardar los datos personales generales, sensibles y/o biométricos.

7. **Información de acceso público:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.

8. **Información previa sobre el tratamiento de datos personales:** Información relativa al tratamiento de datos que es brindada al titular al momento de solicitar sus datos cuando el responsable es una institución pública. La misma debe establecer de manera clara la finalidad del tratamiento y los mecanismos de seguridad.

9. **Responsables del Tratamiento de Datos Personales:** Son las personas naturales o jurídicas encargadas de obtener el consentimiento de los titulares de forma directa o indirecta y están a cargo de la recopilación, aplicación de medios de seguridad y tratamiento de datos personales, según corresponda. Se dividen en:
   a. **Responsable:** Persona natural o jurídica privada, pública o mixta, que sólo o en conjunto con otros, define los fines, medios y realiza el tratamiento de datos personales a nombre propio, de forma directa o por intermedio de terceros encargados.
   b. **Encargado:** Es la persona natural o jurídica privada, pública o mixta a la cual se delega el tratamiento de datos personales a nombre del responsable.
   c. **Exportador:** Persona natural o jurídica privada, pública o mixta, que efectúa transferencias de datos personales a nivel internacional.

   Una persona natural o jurídica podrá tener, al mismo tiempo, la condición de exportador y de responsable o encargado.

Cuando en la presente Ley se estipula una obligación aplicable al "responsable" del tratamiento de datos personales, tendrá alcance a todas las divisiones contempladas en el presente numeral.

10. **Titular:** Persona natural sobre quien recae el derecho propietario (la titularidad y pertinencia) de los datos personales.
11. **Tratamiento:** Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionados, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento, eliminación y en general cualquier uso o disposición de datos personales.

CAPÍTULO II
GARANTÍAS Y PRINCIPIOS

Artículo 6 (Interpretación).- Los principios de la presente ley se encuentran relacionados entre sí y deben interpretarse de manera conjunta. Las disposiciones de la presente ley deben interpretarse y aplicarse en conformidad a los principios dispuestos.

Artículo 7. (Principios y Garantías Constitucionales).- El Estado, en el marco de lo dispuesto por el bloque de constitucionalidad, garantizará a los titulares de los datos personales, el ejercicio de todos los derechos reconocidos por la Constitución y los tratados internacionales de derechos humanos; así como el cumplimiento por parte de personas naturales, jurídicas privadas, públicas o mixtas, nacionales e internacionales, de la presente Ley, con el propósito de impedir efectivamente el tratamiento y/o tráfico ilícito de datos personales, lesivo a la dignidad y derecho del/la afectado(a).

Artículo 8. (Principios).- Son principios de la presente ley y de la protección de los datos personales:

1. **Principio de Licitud.-** El tratamiento de datos personales debe cumplir con elementos de veracidad de los datos, legitimidad de los fines del tratamiento, adopción de las medidas de seguridad, cumplimiento de los deberes de conservación, información, consentimiento, concretados en la calidad y legitimación de los datos a través del estricto apego y cumplimiento de lo dispuesto en la Constitución, las leyes bolivianas y los tratados internacionales de derechos humanos aplicables a la materia.
2. **Principio de Lealtad.-**
    a. Exige que se informe el tipo de tratamiento y manejo de los datos personales y/o sensibles, incluyendo los medios de seguridad aplicables. Notificando al titular del derecho cada vez que un servidor público y/o persona natural de derecho privado ingrese a consultar o tratar sus datos, haciéndole conocer el fin o los fines de dicho tratamiento, obteniendo un consentimiento del titular de manera previa, privilegiando la protección de los intereses del titular y absteniéndose de

tratar éstos a través del consentimiento obtenido a través medios engañosos o fraudulentos.

b. Son desleales aquellos tratamientos de datos personales y/o sensibles que den lugar a actos, hechos de cualquier naturaleza, contrarios a los intereses del titular de los datos, ya sea una discriminación injusta o arbitraria, u otras. Queda prohibido cualquier tratamiento desleal.

3. **Principio de Transparencia.-** El responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales y/o sensibles, a fin de que pueda tomar decisiones informadas al respecto. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión.
4. **Principio de Diversidad Cultural.-** El tratamiento de datos debe considerar la diversidad cultural del país, promoviendo en el marco de su actuación el respeto de la misma. El titular de los datos personales y/o sensibles podrá solicitar que tanto el consentimiento expreso, como la información relativa al tratamiento de sus datos, se realice en su idioma nativo.
5. **Principio de Finalidad.-** Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas. El responsable, sus dependientes o terceras personas relacionadas al responsable, no podrán tratar los datos personales y/o sensibles, en su posesión, para finalidades distintas a aquéllas que motivaron el consentimiento expreso del titular y por ende el tratamiento original de éstos.
6. **Principio de Proporcionalidad.-** El responsable tratará únicamente los datos personales y/o sensibles que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a la(s) finalidad(es) que justifican su tratamiento y que se invocan en el consentimiento expreso del titular.
7. **Principio de Calidad.-** El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos. Esto conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable.

   El principio también implica que la persona titular brinde de manera veraz los datos personales que haya consentido, evitando inducir en error al responsable.

8. **Principio de Responsabilidad.-**

   a. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en la presente Ley, así como rendirá cuentas sobre el tratamiento de datos personales al titular y a la Autoridad de Protección de Datos Personales – APDP, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro

mecanismo que determine adecuado para tales fines. Esta obligación, aplicará también cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

b. El responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable.

9. **Principio de Seguridad.-**
   a. El responsable establecerá y mantendrá medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
   b. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.
10. **Principio de Confidencialidad.-** El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.
11. **Principio Pro Persona.-** Criterio interpretativo que establece que se debe aplicar la norma o la interpretación más favorable a la persona o titular de los datos personales, considerándose la protección y la prohibición de la limitación de Derechos Humanos, aplicando la norma, interpretación o situación menos restrictiva y más favorable al titular.
12. **Principios Comerciales.-** Las relaciones jurídicas de naturaleza comercial se regirán por las normas corporativas vinculantes y los principios de buena fe, transparencia, equidad, minimización de datos, democratización, autonomía de voluntad, independencia, sostenibilidad, seguridad jurídica, simplicidad y celeridad, así como aquellos principios contemplados en la presente norma, la Constitución, los tratados de derechos humanos a momento de procesar el tratamiento de datos de manera nacional e internacional, debiendo prevalecer los derechos de los titulares en todo momento y contexto.

13. **Principio de Conservación limitada:** Los datos personales se conservarán solo durante el tiempo necesario para cumplir con la finalidad de su tratamiento. Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

    La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.

14. **Principio de Datos Personales Sensibles y Datos Biométricos:** Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Para el tratamiento de las categorías de datos personales sensibles y datos biométricos, los responsables deben adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.

Artículo 9. (Normativa especializada).- Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión u otros derechos fundamentales, sectores regulados por normativa específica y los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, estarán sujetos a los principios y disposiciones establecidos en sus propias normas. Los principios y disposiciones de la presente Ley, serán aplicados en los casos que corresponda. En todo caso deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y la protección de datos personales, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

TÍTULO II

BASES JURÍDICAS PARA EL TRATAMIENTO LEGÍTIMO Y LÍCITO DE DATOS PERSONALES

CAPÍTULO I
TRATAMIENTO LEGÍTIMO Y LÍCITO DE DATOS PERSONALES

Artículo 10. (Tratamiento legítimo y lícito de datos personales).- El tratamiento será legítimo y lícito cuando se cumpla al menos una de las siguientes condiciones:

1. El titular brindó su consentimiento para el tratamiento de sus datos personales, para una o varias finalidades específicas;
2. Que el tratamiento sea realizado por el responsable en cumplimiento de una obligación legal o el mandato específico de instituciones públicas establecido en ley, debiendo cumplir con los criterios de legalidad, proporcionalidad y necesidad;
3. Que el tratamiento sea realizado por el responsable para el cumplimiento de una orden judicial o requerimiento fiscal fundado y motivado, en atención a un proceso abierto y en curso, de autoridad pública competente, debiendo observarse los principios de la presente ley;
4. Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;

5. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.
6. Que el tratamiento sea necesario para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad; y
7. Para tratamiento de datos personales que consten en bases de datos correspondientes a información de acceso público.

CAPÍTULO II
CONSENTIMIENTO

Artículo 11. (Condiciones para el Consentimiento).-

I. Se podrán tratar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo.
II. El consentimiento debe ser expreso, previo, libre, específico e informado; por tanto, el responsable deberá contar con el consentimiento del titular de manera inobjetable, previamente al tratamiento de los datos personales. El mismo para no contar con vicios, deberá ser informado, especificar la finalidad, los mecanismos de seguridad que se emplearán en el tratamiento de los datos personales y el tiempo de vigencia de dicho consentimiento.
III. El consentimiento será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias.
IV. El titular podrá revocar en cualquier momento el consentimiento otorgado. El responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos para este fin. La revocatoria no tendrá efecto retroactivo.
V. El consentimiento otorgado por el titular de datos personales no otorga el derecho a terceros de hacer uso del tratamiento consentido, a menos de que el consentimiento incluya esta posibilidad.
VI. La información previa al consentimiento deberá ser otorgada en el idioma nativo del titular de los datos personales, pudiendo solicitar un traductor para el efecto. Asimismo, para las personas en situación de discapacidad se les otorgará la información en los medios idóneos para su comprensión, asegurando dicho extremo de manera documental.

Artículo 12. (Tratamiento de Datos Personales de niñas, niños, adolescentes y personas interdictas).- El consentimiento para el tratamiento de datos personales de niñas, niños, adolescentes y personas interdictas, será obtenido a través del consentimiento de los tutores, titulares de la patria potestad o guarda, cumpliendo rigurosamente las condiciones del consentimiento y principios consagrados por la presente ley.

Artículo 13. (Consentimiento de adolescentes).- Las y los adolescentes a partir de los 14 años de edad, podrán otorgar como titulares, su consentimiento explícito para el tratamiento de sus datos personales. El responsable debe considerar las características especiales de las y los adolescentes para este fin, debiendo resguardar sus derechos como grupo especialmente vulnerable.

Artículo 14. (Excepciones).- Excepcionalmente, el tratamiento de datos personales podrá realizarse sin el consentimiento del titular pero con su conocimiento informado cuando se cumpla alguna de las condiciones para que el tratamiento de datos personales sea legítimo y lícito, de acuerdo a los establecido en el artículo 10 de la presente ley.

Artículo 15. (Información previa sobre el tratamiento de datos).- Debido a la naturaleza de las instituciones públicas, el consentimiento no será requerido en base al mandato específico de cada institución pública establecidas o previstas en ley. No obstante, las instituciones públicas deben informar al titular sobre el tratamiento de datos que se realizará, considerando las condiciones establecidas para el consentimiento en aquello que sea aplicable.

TÍTULO III

DERECHOS

CAPÍTULO I
DERECHOS DEL TITULAR DE DATOS PERSONALES

Artículo 16. (Derechos del titular de los datos personales).- En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen. El ejercicio de cualquiera de los derechos referidos anteriormente no es requisito previo, ni impide el ejercicio de otros.

Artículo 17. (Derecho de acceso).- El titular tendrá el derecho de solicitar el acceso a los datos personales que estuviesen en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento. Los responsables deberán comunicar mediante mecanismos digitales a la Autoridad de Protección de Datos Personales – APDP de todo tratamiento y acceso que se realice sobre datos personales, indicando los aspectos generales del tratamiento; dicha comunicación no implica un traspaso de las bases de datos personales manejadas por los responsables.

Artículo 18. (Derecho de rectificación y actualización).- El titular tendrá el derecho a obtener del responsable, la rectificación, corrección o actualización de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

Artículo 19. (Derecho de cancelación).- El titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del

responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

Artículo 20. (Derecho de oposición).- El titular podrá oponerse al tratamiento de sus datos personales cuando:

1. Tenga una razón legítima derivada de su situación particular.
2. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

Artículo 21. (Derecho a la portabilidad de los datos personales).-

I. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

II. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.

III. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

IV. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

Artículo 22. (Derecho a no ser objeto de decisiones individuales automatizadas).-

I. El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

II. Lo dispuesto en el parágrafo anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por normativa legal vigente, o bien, se base en el consentimiento del titular de acuerdo a las condiciones de consentimiento dispuestas por esta Ley.

III. No obstante, cuando sea necesario para la relación contractual o el titular hubiere manifestado su consentimiento tendrá derecho a obtener la intervención humana; recibir una explicación sobre la decisión tomada; expresar su punto de vista e impugnar la decisión.

IV. El responsable no podrá llevar a cabo tratamientos automatizados de datos personales que tengan como efecto la discriminación de los titulares por su origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; género; datos relativos a la salud, a la vida, preferencia u orientación sexual, así como datos genéticos o datos biométricos.

Artículo 23. (Derecho a la limitación del tratamiento de los datos personales).-El titular tendrá derecho a que el tratamiento de datos personales se limite al plazo y finalidad otorgado en el consentimiento para ello. Asimismo, su almacenamiento se limitará al periodo que medie, entre una solicitud de rectificación u oposición hasta su resolución por el responsable. El titular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el responsable, pero los necesite para formular una reclamación.

Artículo 24. (Derecho a la información).-

I. El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio sobre:
   1. Los fines del tratamiento;
   2. La base jurídica para el tratamiento;
   3. Tipos de tratamiento;
   4. Tiempo de conservación;
   5. La existencia de una base de datos en la que consten sus datos personales;
   6. El origen de los datos personales cuando no se hayan obtenido directamente del titular;
   7. Otras finalidades y tratamientos ulteriores;
   8. Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, número de teléfono y correo electrónico;
   9. Cuando sea del caso, identidad y datos de contacto del Oficial de protección de datos personales, que incluirá: dirección, número de teléfono y correo electrónico;
   10. Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas;
   11. Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;
   12. El efecto de suministrar datos personales erróneos o inexactos;
   13. La posibilidad de revocar el consentimiento;
   14. La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, rectificación y actualización, cancelación, oposición, portabilidad, no ser objeto de decisiones individuales automatizadas y limitación.
   15. Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales, y;
   16. La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

II. En el caso que los datos se obtengan directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal. Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de información de acceso público, el titular deberá ser informado dentro de los siguientes cuarenta y cinco (45) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas.

La información proporcionada al titular podrá transmitirse de cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión. El titular puede solicitar que la información sea proporcionada en castellano u otro idioma oficial.

Artículo 25. (Derecho de indemnización).- El titular tiene derecho a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación a cualquiera de los derechos establecidos en la presente ley, normas conexas y aquellas que otorguen mayor protección a los derechos humanos.

CAPÍTULO II

EJERCICIO DE DERECHOS

Artículo 26. (Ejercicio de los Derechos ARCOP).-

I. El responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación,y oposición y portabilidad.
II. Estos mecanismos y procedimientos no podrán exceder los plazos que vayan a ser establecidos en el reglamento de la presente ley. Los procedimientos establecidos por la Autoridad de Protección de Datos Personales serán en todo caso supletorios ante la ausencia de medios y procedimientos dictados por el responsable.
III. Para el ejercicio de los derechos ARCOP no se requerirá otro requisito que la identificación del solicitante.
IV. El responsable únicamente podrá determinar la no procedencia de la solicitud en los casos de rectificación, cancelación, oposición y portabilidad al amparo de las siguientes causales:
    1. El responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.
    2. El tratamiento sea necesario para el cumplimiento de una disposición legal.

Artículo 27. (Datos personales de personas fallecidas).- Los titulares de derechos sucesorios de las personas fallecidas, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación, actualización o cancelación de los datos personales del causante, siempre que el titular de los datos no haya, en vida, indicado otra utilización o destino para sus datos, mediante documento notarial.

Las personas o instituciones que la persona fallecida haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso, su rectificación, actualización o cancelación.

Artículo 28. (Ejercicio de los derechos frente a la Administración Pública).- El ejercicio de los derechos mencionados frente a la Administración Pública será interpretado y aplicado considerando la naturaleza de la misma, de acuerdo al mandato específico que tenga cada institución establecido por ley.

TITULO IV

BASE DE DATOS Y TRANSFERENCIA DE DATOS PERSONALES

CAPÍTULO I
BASES DE DATOS PÚBLICAS Y PRIVADAS

Artículo 29. (Creación y Tratamiento de Bases de Datos Públicas).- La creación y tratamiento de bases de datos por parte de las administraciones públicas, sólo podrán realizarse en razón a las materias de su competencia y en estricto cumplimiento a lo descrito en la presente ley. No se generarán bases de datos o su tratamiento, que vulneren los principios y derechos consagrados en la presente ley.

Artículo 30. (Interoperabilidad de Datos entre Administraciones Públicas).-

I. Las entidades públicas dentro del desempeño de sus funciones pueden realizar la comunicación de datos de carácter personal a terceras entidades públicas de forma justificada.
II. La interoperabilidad de datos entre administraciones públicas no requiere el consentimiento del titular, de acuerdo al mandato específico de las instituciones públicas establecidos en ley; sin embargo, a través de la información previa sobre el tratamiento de datos se debe informar si los datos son interoperados con terceras entidades públicas.
III. En caso de que la interoperabilidad haya iniciado de manera posterior a la entrega de la información previa sobre el tratamiento de datos, la institución pública deberá informar sobre la interoperabilidad a través de los medios con los que cuente para informar a la población, de manera enunciativa pero no limitativa: páginas web, plataformas de redes sociales, entre otras. En la medida de lo posible, se informará de manera personal a los titulares, a través de medios físicos o digitales, sobre la interoperabilidad de datos entre administraciones públicas.
IV. A través de sus páginas web, redes sociales y otros medios de comunicación institucional se informará a la población sobre la interoperabilidad de datos.

Artículo 31. (Creación y Tratamiento de Bases de Datos Privadas).-

I. Las personas naturales y jurídicas podrán crear y tratar bases de datos que contengan datos de carácter personal cuando sea congruente con la finalidad del servicio que brindan, con estricto cumplimiento a las disposiciones contenidas en la presente ley.

II. Toda ampliación o solicitud de datos adicionales deberá recabar el consentimiento expreso, previo, libre, específico e informado, pudiendo éste último oponerse, revocar el consentimiento y en cualquier momento ejercer el derecho de cancelación sobre dicho tratamiento, así como todos los derechos reconocidos por la presente ley.

III. Los datos personales almacenados en listas de cámaras, entes colegiados o agrupaciones profesionales deberán limitarse a los usos para los cuales fueron recogidos y tratados, en el marco de los principios y derechos enunciados.

Artículo 32. (Interoperabilidad de Datos por parte de entidades privadas).- Las entidades privadas en el marco de las funciones específicas del servicio que brindan, solo podrán realizar la comunicación de datos de carácter personal a terceras entidades públicas o privadas de forma justificada y previo consentimiento expreso, previo, libre, específico e informado del titular.

Artículo 33. (Bases de datos abiertos).-

I. Las bases de datos que se hagan públicas, independientemente de la finalidad que cumplan, deberán utilizar mecanismos de disociación de datos, ya sea de anonimización o seudonimización, para garantizar la privacidad e intimidad de los titulares de los datos personales.

II. Se exceptúan de la disposición anterior aquellos datos personales que sean públicos por consentimiento del titular.

III. También se exceptúan aquellas bases de datos referidas a datos personales que por mandato de ley deben ser públicas.

IV. Los responsables del tratamiento deben utilizar todos los mecanismos técnicos y administrativos para garantizar la seguridad de los datos tratados.

Artículo 34. (Información obtenida en bases de datos de acceso público).-

I. Los datos personales que consten en bases de datos de acceso público comunicados a través de medios de comunicación convencionales y difusión masiva como la televisiva, radial, escrita, plataformas web, entre otras, podrán ser tratados siempre y cuando no sea para fines comerciales o publicitarios. Se podrán tratar los datos de acceso público cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica y número de teléfono profesional.

II. En caso de que los datos personales hayan sido obtenidos en bases de acceso público y sean utilizados con fines comerciales o publicitarios, deberá notificarse sobre la obtención de los datos personales de acuerdo a lo establecido en el artículo 24 parágrafo II. Esta disposición no impide que el titular pueda oponerse al tratamiento de datos personales.

III. Los datos personales que se encuentran en bases de acceso público, deben enmarcarse en todo momento a los principios y derechos consagrados en la

Constitución Política del Estado Plurinacional de Bolivia, la presente ley, normas conexas y tratados de derechos humanos.

Artículo 35. (Tratamiento de Datos Personales con Fines Publicitarios).-

I. Las entidades que se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, gestión comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos hayan sido facilitados por los titulares y hayan sido otorgados a través de un consentimiento expreso, previo, libre, específico e informado. Bajo ninguna circunstancia el silencio puede ser interpretado como aceptación.

II. Es necesario contar con consentimientos diferenciados, uno para el tratamiento de datos personales y la respectiva política de privacidad, y otro, para recibir información publicitaria y de marketing. De ningún modo, el consentimiento para el tratamiento de datos personales implica un consentimiento para la recepción de información publicitaria. Los consentimientos pueden ser obtenidos en un solo documento, pero deberá diferenciarse claramente la finalidad de cada uno.

III. Los mensajes publicitarios y comerciales deberán ser claramente identificados con esa naturaleza.

IV. Los titulares tendrán derecho a conocer el origen de sus datos personales cuando hayan recibido comunicaciones comerciales o mensajes publicitarios.

V. Los titulares tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les concierne, en cuyo caso serán dados de baja del tratamiento de forma inmediata, cancelándose las informaciones que sobre ellos figuren, a simple solicitud.

VI. Las comunicaciones deberán indicar claramente la forma en la que el destinatario puede aceptar o rechazar el envío de futuras comunicaciones del remitente, para que los usuarios puedan habilitarse o deshabilitarse en el caso de que no deseen continuar recibiendo estos mensajes, correos u otras formas de comunicación.

CAPÍTULO II
TRANSFERENCIA DE RESPONSABILIDADES DE TRATAMIENTO DE DATOS PERSONALES

Artículo 36. (Delegación del Tratamiento de Datos Personales por el Responsable).-

I. La delegación del tratamiento de datos personales del responsable en favor de un tercero por fuera de su estructura organizacional, deberá formalizarse mediante la suscripción de un contrato o instrumento jurídico suscrito por las partes, bajo los lineamientos dictados por la autoridad.

II. El contrato o instrumento jurídico establecerá, al menos, el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento; el tipo de datos personales; las categorías de titulares, así como las obligaciones y responsabilidades del responsable y encargado.

III. Se debe contar con el consentimiento del titular para la delegación del tratamiento de datos personales.

IV. El Encargado o Exportador están obligados a verificar la existencia del consentimiento de los titulares de los datos personales que tratará por encargo del responsable.

V. Una vez concluida la relación con el responsable, el encargado o exportador deberá destruir la información, sin importar el medio de soporte que la contenga, referente a los datos personales y la base de datos delegada por el responsable.

VI. La delegación del tratamiento, no exonera de responsabilidad al responsable, contando todas las partes intervinientes en la obtención y tratamiento de los datos personales, responsabilidades frente al titular.

Artículo 37. (Subcontratación de Servicios).- El Encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito y específica del responsable, a través del contrato o instrumento jurídico suscrito entre este último y el encargado. Instrumento legal que deberá enmarcarse a los lineamientos establecidos en la presente ley.

Artículo 38. (Reglas Generales para las Transferencias de Datos Personales).-

I. El responsable podrá realizar transferencias internacionales de datos personales cuando se cumpla cualquiera de los siguientes supuestos:
   1. En el país donde se hará el tratamiento de los datos personales hubiere reconocido un nivel adecuado de protección de datos personales por parte de la Autoridad de Protección de Datos Personales.
   2. El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento mínimo de las condiciones establecidas en la presente ley. Para ello se deben suscribir cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. Se deberá informar a la Autoridad de Protección de Datos Personales, las transferencias realizadas bajo este supuesto, de acuerdo a las disposiciones que vayan a establecerse en el reglamento de la presente ley.

Artículo 39. (Autorización para la transferencia internacional).- Para todos los casos no contemplados en los artículos precedentes, en los que se pretenda realizar una transferencia internacional de datos personales, se requerirá la autorización de la Autoridad de Protección de Datos Personales.

CAPÍTULO III
OBLIGACIONES EN EL TRATAMIENTO DE DATOS PERSONALES

Artículo 40. (Oficial de Protección de Datos Personales).-

I. El responsable, Encargado y/o el Exportador, deberán designar a un oficial de protección de datos personales cuando exista cualquiera de las siguientes situaciones:
   1. Sea una entidad pública.
   2. Lleve a cabo tratamientos de datos personales que tengan habitualidad, aplicación sistemática o que el tratamiento de datos personales sea su rubro de servicios.
   3. Realice tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, entre otros factores y de manera únicamente enunciativa más no limitativa, el tratamiento de datos personales sensibles o datos genéticas; debiendo registrar y estar al alcance del titular a simple petición, las transferencias que se efectúen; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos y los servidores públicos que hayan accedido a dichos datos personales.

II. El responsable que no se encuentre en alguna de las causales previstas en el parágrafo anterior, podrá designar a un oficial de protección de datos personales si así lo estima conveniente.

III. El responsable estará obligado a otorgar al oficial de protección de datos personales en el desempeño de sus funciones, los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de éstos.

IV. El oficial de protección de datos personales tendrá al menos, las siguientes funciones:
   1. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
   2. Coordinar al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la normativa relativa a la protección de datos.
   3. Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional que resulte aplicable en la materia.

Artículo 41. (Privacidad en el Tratamiento de Datos Personales).- El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la presente Ley.

El responsable garantizará que sus programas, servicios, sistemas, plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique un tratamiento de datos personales, cumpla por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la presente Ley.

Artículo 42. (Mecanismos de Autorregulación).- El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante.

Artículo 43. (Evaluación de Impacto a la Protección de Datos Personales).- Cuando el responsable pretenda tratar datos personales sensibles, biométricos o que por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa a la implementación del recojo y tratamiento, una evaluación del impacto a la protección de los datos personales, aplicable al caso en concreto, estipulando medidas específicas de seguridad que permitan la mayor protección para los titulares. Informe que será presentado ante la Autoridad de Protección de Datos Personales – APDP para su correspondiente aprobación.

Artículo 44. (Notificación de vulneración de seguridad).-

I. El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales, tan pronto sea posible, y a más tardar en el término de diez (10) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de diez (10) días, deberá ir acompañada de indicación de los motivos de la tardanza.
II. El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de tres (3) días contados a partir de la fecha en la que tenga conocimiento de ella.
III. En caso de que el responsable del tratamiento de los datos personales no cumpliese oportunamente y de modo justificado con la notificación será sancionado conforme al régimen sancionatorio previsto en esta ley.

Artículo 45. (Notificación de vulneración de seguridad al titular).-

I. El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de quince (15) días contados a partir de la fecha en la que tuvo conocimiento del riesgo.
II. No se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos:
    1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas;
    2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, no ocurrirá; y,
    3. Cuando se requiera un esfuerzo desproporcionado para hacerlo; en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.
III. La procedencia de las excepciones de los numerales 1 y 2 del parágrafo anterior, deberá ser calificada por la Autoridad de Protección de Datos, una vez informada esta

tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Artículo 44.

IV. En caso de que el responsable del tratamiento de los datos personales no cumpliese oportunamente y de modo justificado con la notificación será sancionado conforme al régimen sancionatorio previsto en esta ley.

TÍTULO V
REGULACIÓN DEL TRATAMIENTO DE DATOS PERSONALES

CAPÍTULO I

CONSEJO PLURINACIONAL PARA LA PROTECCIÓN DE DATOS PERSONALES

Artículo 46. (Consejo Plurinacional para la Protección de Datos Personales).- Se crea el Consejo Plurinacional para la Protección de Datos Personales – CPPDP que formará parte del aparato del Estado. Se constituye en la instancia máxima de coordinación y representación, para formular, aprobar y ejecutar políticas públicas para la protección de datos personales.

Artículo 47. (Conformación y estructura).-

I. El Consejo Plurinacional para la Protección de Datos Personales-CPPDP estará conformado por:

1. El Órgano Ejecutivo a través de los siguientes Ministerios:
   a. Ministerio de Justicia y Transparencia Institucional.
   b. Ministerio de la Presidencia y la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC).
   c. Ministerio de Obras Públicas, Servicios y Vivienda.
2. El Órgano Judicial a través de:
   a. Representación del Tribunal Constitucional Plurinacional.
   b. Representación del Tribunal Supremo de Justicia.
3. Instituciones de defensa de la sociedad:
   a. Representación de la Defensoría del Pueblo.
4. Sociedad civil organizada, de acuerdo a disposiciones reglamentarias.

II. La estructura y funcionamiento del Consejo Plurinacional para la Protección de Datos Personales, será establecido a través de disposiciones reglamentarias.

Artículo 48. (Atribuciones).- El Consejo Plurinacional para la Protección de Datos Personales-CPPDP tiene las siguientes atribuciones, además de aquellas que sean inherentes al ejercicio de sus funciones:

1. Garantizar el cumplimiento de la presente ley.

2. Formular y aprobar políticas públicas para la protección de datos personales.

3. Ejecutar en coordinación con otras instituciones públicas, tanto a nivel central como con las entidades territoriales autónomas las políticas públicas para la protección de datos personales.

4. Supervisar y evaluar la ejecución de las políticas públicas para la protección de datos personales.

5. Gestionar recursos económicos para la implementación de la presente ley y las políticas de protección de datos personales.

6. Supervisar y fiscalizar el trabajo y acciones realizadas por la Autoridad de Protección de Datos Personales.

7. Conocer y resolver los recursos jerárquicos contra las resoluciones emitidas por la Autoridad de Protección de Datos Personales.
8. Celebrar acuerdos o convenios con otros organismos extranjeros de regulación y supervisión del tratamiento de datos personales, para la cooperación, capacitación y el intercambio de información.
9. Autorizar la incorporación al ámbito de la regulación a otro tipo de servicios y empresas que tengan relación con el tratamiento de datos personales.
10. Establecer un canon de montos a ser cobrados por los diferentes registros, servicios prestados e infracciones a ser cobradas. Misma que deberán ser aprobadas por el Directorio de la Autoridad de Protección de Datos Personales – APDP.

11. Otras funciones que asigne el Consejo Plurinacional para el cumplimiento del objeto y los fines de la presente Ley, de acuerdo a Reglamento.

CAPÍTULO II

AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

Artículo 49. (Autoridad de Protección de Datos Personales).- Se crea la Autoridad de Protección de Datos Personales –APDP, como Secretaría Técnica del Consejo Plurinacional para la Protección de Datos Personales-CPPDP. La organización y forma de funcionamiento de la Autoridad de Protección de Datos Personales será determinada mediante disposiciones reglamentarias.

Artículo 50. (Objeto).-

I. La Autoridad de Protección de Datos Personales –APDP tiene como objeto ejecutar la regulación y supervisión del recojo y tratamiento de los Datos Personales, con la

finalidad de velar por el sano funcionamiento y desarrollo de las bases de datos personales con dichas características, bajo los postulados y derechos expuestos en la presente ley.

II. La Autoridad de Protección de Datos Personales –APDP es la instancia encargada de ejercer las funciones de regulación, supervisión y control de las personas naturales y jurídicas de derecho privado, público y mixto, en base a las disposiciones de la presente Ley y su respectiva reglamentación.

Artículo 51. (Requisitos de la Autoridad de Protección de Datos Personales).- Para optar al cargo de Autoridad de Protección de Datos Personales se requerirá, además de los requisitos generales para el acceso al servicio público, contar por lo menos con ocho años de experiencia profesional y tener especialización o experiencia acreditada en temáticas de protección de datos personales. Las disposiciones reglamentarias deberán asegurar que el ejercicio de las funciones de la Autoridad de Protección de Datos Personales se desarrollen bajo principios de imparcialidad, idoneidad y transparencia.

Artículo 52. (Atribuciones).- La Autoridad de Protección de Datos –APDP tiene las siguientes atribuciones, además de aquellas que sean inherentes al ejercicio de sus funciones:

1. Garantizar y defender los derechos e intereses de los titulares de los datos personales.
2. Registrar, regular, supervisar y sancionar a las personas naturales y jurídicas de cualquier naturaleza, que tengan bases de datos públicas y privadas en las que se almacenen y traten datos personales.
3. Normar y vigilar la correcta aplicación de las normas aplicables a la materia, así como la presente ley.
4. Emitir reglamentación específica y supervisar su cumplimiento en el marco de la normativa aplicable.
5. Conocer y resolver acciones que se interpongan contra los actos definitivos de las instancias que recojan y traten Datos Personales.
6. Conocer y resolver los recursos de revocatoria contra las resoluciones o actos administrativos definitivos.
7. Establecer sistemas preventivos de control y vigilancia para la protección de datos personales.
8. Ejercer supervisión consolidada de grupos comerciales, en materia de protección de datos personales.
9. Imponer sanciones por infracción de las disposiciones legales y reglamentarias.
10. Disponer la regularización obligatoria y la intervención de las personas naturales y/o jurídicas que incumplan el marco normativo aplicable en concordancia con la presente ley.
11. Diseñar e implementar ofertas de formación y capacitación en temas de datos personales dirigidas a funcionarios, ciudadanía, empresarios, académicos y otros públicos interesados.
12. Instruir mejoras y ajustes en los sistemas de seguridad aplicados por los responsables, Encargados y/o Exportadores.

13. Suspender determinadas operaciones en el tratamiento de datos personales de manera fundamentada.
14. Supervisar el control de riesgos y el cumplimiento a las disposiciones legales específicas aplicables al tratamiento de datos personales.
15. Instruir acciones a los responsables, Encargados y/o Exportadores, para resolver reclamaciones y denuncias que presenten los titulares.
16. Emitir normativa prudencial de carácter general y específico, extendiéndose a la regulación de normativa para aplicación de los responsables, Encargados y/o Exportadores.
17. Emitir normativa para regular la información, publicidad o propaganda relacionada con datos personales, y prohibir o suspender la publicidad o propaganda cuando vulneren derechos fundamentales y ARCOP de los titulares, con mayor énfasis cuando se trate de niñas, niños y adolescentes.
18. Pronunciarse e imponer sanciones ante el rechazo inadecuado u omisión en el pronunciamiento en plazo respecto al reclamo de los derechos del titular ante el responsable del tratamiento de datos personales.
19. Realizar actividades de fiscalización sobre los responsables, encargados y exportadores del tratamiento de datos personales. Estas tareas, entre otras, incluirá la realización de auditorías y pericias técnicas.
20. Determinar bajo criterios técnicos y jurídicos, los países en los que exista un nivel adecuado de protección de datos personales para la transferencia de datos personales.
21. Aprobar y registrar los contratos y documentos legales de transferencia de datos personales entre responsables, Encargados y/o Exportadores.
22. Registrar las vulneraciones de seguridad a las bases de datos personales de acuerdo a las notificaciones recibidas por parte de los responsables del tratamiento.
23. Otras funciones que le asigne el Consejo Plurinacional de Protección de Datos Personales para el cumplimiento del objeto y los fines de la presente Ley, de acuerdo a lo dispuesto en el reglamento de la presente ley.

Artículo 53. (Auditoría de Protección de Datos).- La Autoridad de Protección de Datos – APDP estará facultada para realizar auditorías de protección de datos tanto a personas naturales, empresas o instituciones privadas, instituciones y empresas públicas y/o mixtas que traten datos personales, ante reclamaciones fundamentadas de los titulares de datos personales como posibles afectados, a fin de evaluar que las bases de datos y los respectivos datos personales que alberguen se estén tratando en apego a los derechos y principios insertos en la presente ley, en la Constitución Política del Estado Plurinacional y normas conexas.

Artículo 54. (Auditoría de oficio a instituciones públicas).- La Autoridad de Protección de Datos –APDP, realizará auditorías periódicas de oficio a instituciones públicas que traten datos personales, con la finalidad de detectar el incumplimiento al marco legislativo aplicable a la materia y la vulneración a derechos de los titulares.

TÍTULO VI
RECURSOS ADMINISTRATIVOS

CAPÍTULO I

GENERALIDADES

Artículo 55. (Características).-

I. Los recursos contemplados por el Consejo Plurinacional para la Protección de Datos Personales-CPPDP y la Autoridad de Protección de Datos –APDP gozarán de las siguientes características:
   1. Primará el principio de informalidad;
   2. Serán gratuitos;
   3. Con procedimientos abreviados;
   4. Accesibles y con medios idóneos para permitir a los titulares procesar los mismos en cumplimiento a todos los principios y derechos otorgados a los titulares de datos personales;
   5. Serán sustentados fundamentadamente;
   6. Se regirán por el debido proceso y derechos constitucionales;
   7. El titular tendrá acceso a todos los documentos necesarios que requiera para hacer prevalecer sus derechos;
   8. Será sustentado bajo el principio pro homine.

II. Asimismo, cualquier duda será interpretada a favor del ejercicio de los derechos del titular afectado o que se considere afectado.

TÍTULO VII

INFRACCIONES Y SANCIONES

CAPÍTULO I
GRADOS

Artículo 56. (Infracciones).- Las infracciones se calificarán como leves, graves o muy graves. Serán normadas por disposiciones reglamentarias, que mínimamente contemplarán lo siguiente:

1. Son infracciones leves:
   a. No dar contestación a las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales.

b. No proporcionar o colaborar con las solicitudes de información que solicite la autoridad competente en el ejercicio de sus facultades.

2. Son infracciones graves:
   a. La creación de bases de datos o tratar datos personales sin haber obtenido el consentimiento expreso, previo, libre, específico e informado del titular.
   b. La creación de bases de datos de titularidad privada o el tratamiento de datos de carácter personal con finalidades distintas a las que fueron comunicadas y que derivaron en el consentimiento obtenido del titular.
   c. El impedimento o la obstaculización por parte de los responsables del tratamiento para el ejercicio de los derechos reconocidos en la presente ley y normas conexas.
   d. No rectificar o eliminar los datos de carácter personal cuando éstos se hubieran informado como inexactos o el titular se hubiera opuesto al tratamiento.
   e. No implementar las debidas condiciones de seguridad previstas en las disposiciones reglamentarias.
   f. No notificar sobre las vulneraciones de seguridad de las bases de datos personales a la Autoridad de Protección de Datos Personales y a los titulares cuando corresponda.
   g. Incumplir los deberes y responsabilidades reflejados en la presente Ley.

Son infracciones gravísimas:

   h. El tratamiento de datos de mala fe, por medio del error y engaño al titular de los datos personales.
   i. La comunicación, transferencia o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
   j. Desobedecer los requerimientos de cese de tratamiento de datos cuando estos hubieran sido dictados por la Autoridad de Protección de Datos o por una orden judicial o resolución fundada de autoridad competente.

CAPÍTULO II
SANCIONES

Artículo 57. (Sanciones).- Las sanciones serán definidas a través de disposiciones reglamentarias. Las sanciones pueden incluir multas pecuniarias que serán establecidas de manera proporcional al volúmen de ingreso que tenga el responsable de tratamiento de datos personales.

DISPOSICIÓN TRANSITORIA PRIMERA.-. El Órgano Ejecutivo en el plazo de doscientos (200) días de publicada la presente Ley, desarrollará la reglamentación correspondiente para su aplicación.

DISPOSICIÓN TRANSITORIA SEGUNDA.- El gobierno en sus distintos niveles y en coordinación con organizaciones de la sociedad civil y el sector privado, promoverá y gestionará la implementación de programas de formación dirigidos a funcionarios públicos y a la ciudadanía en general, relacionados con el contenido de la presente ley y la protección de datos personales.

DISPOSICIÓN FINAL PRIMERA.- Se derogan y abrogan todas las normas contrarias a la presente ley.