Curso “Ciudadanía y Derechos Humanos en la era digital”

Módulo 2: Vulneraciones de privacidad y protección de datos personales

Documento de contenido

Docentes: Camilo Arratia y Verónica Salinas

1. Objetivo de aprendizaje

El objetivo de este módulo es identificar los tipos de bases de datos existentes en Bolivia, las inequidades en el aprovechamiento de la datificación, la importancia de la protección de los datos personales y los diferentes mecanismos de protección y prevención que se pueden aplicar en nuestro contexto para evitar vulneraciones de privacidad.

2. Contenido y estructura del curso

1. ¿Qué es un dato personal?
2. Tipos de bases de datos en Bolivia: públicas y privadas.
3. Extractivismo de datos con fines comerciales.
4. Protección de datos personales.
5. Mecanismos de protección.

3. Justificación

La producción, recolección y tratamiento de los datos personales y no personales se ha acelerado como producto de la digitalización. Producimos datos todo el tiempo, por ejemplo, cuando usamos Whatsapp o cualquier otra aplicación o red social estamos produciendo datos. Tomemos el caso de una llamada para lo que usamos Whatsapp, son datos la persona que llama, la que recibe recibe la llamada, la duración de la llamada, el lugar donde está cada uno de los celulares, la hora, la frecuencia de contacto, las empresas que dan el servicio de Internet y también la conversación y archivos que se intercambian. De esta manera, todo lo que hacemos produce datos que son captados, recolectados, analizados y utilizados para tomar decisiones empresariales y de gobierno. Estas decisiones no son malas en sí mismas porque facilitan nuestro acceso a información, compra de cosas u obtener servicios pero pueden ser mal utilizadas vulnerando Derechos Humanos tales como la privacidad, el acceso a información pública, la libertad de expresión, entre otros; y generando discriminación y estigmatizaciones.

Acerca de la aceleración en los volúmenes de recolección de datos, el Banco Interamericano de Desarrollo[1], reporta que solo en el año 2012, se calcula que se crearon más datos que todos los datos producidos hasta la fecha en la historia de la humanidad.

Así, tenemos una primera clasificación: los datos personales y los datos personales. En este módulo estudiaremos con más detalle lo que se refiere a los datos personales pero no

[1] Durante el año 2018, se produjo 2,4 EB (Exabytes) de información cada día (2,5 quintillones de bytes de datos o el número 25 seguido de 17 ceros), se trata de números difíciles de imaginar. BID (2022) Curso Datos para la efectividad de las políticas públicas.

debemos olvidar que existe una problemática acerca de datos que no son personales y que definen políticas de datos abiertos[2].

Entonces, los datos personales se han convertido en uno de los activos más valiosos y a la vez más controversiales porque tanto las empresas como los gobiernos buscan tener el acceso a esos datos, muchas veces sin tomar en cuenta que el tratamiento de esos datos está potencialmente en conflicto con el derecho humano a la privacidad.

De esta manera, el uso intensivo de la información personal cuando se accede a Internet, puede conllevar riesgos y exposición a amenazas o violaciones a la privacidad, por ejemplo:

- Uso de datos con finalidades para las que no fueron recolectados.
- Tratamiento de datos personales a través de páginas “pirata” de Internet.
- Envío masivo de correos electrónicos no deseados, de promoción de productos o servicios de diversa índole.
- Suplantación de identidad digital.
- Decisiones tomadas por inteligencias artificiales en base a perfiles (generalizaciones) como puede ser contrataciones de personal u ofertas de descuentos.

Para Bolivia y los países del Sur Global en general, esta aceleración del uso de los datos personales impone dos retos: generar innovación tecnológica y además, resolver temas pendientes en la política tecnológica como la brecha digital. En Bolivia, aún existen muchas personas y organizaciones que no tienen una conexión estable y asequible. Si bien el nivel de uso de Internet el año 2017 era del 67% (AGETIC) y después de la pandemia, es muy probable que se haya incrementado a un 75% a 80%, la conexión más común es móvil y prepago, que es cara y se compra a diario dependiendo de las necesidades y dinero que la gente disponga, por lo que la calidad de conexión es cara y al menos mediocre.

4. Marco teórico

La protección de datos personales tiene dos actores principales: los titulares y los responsables del tratamiento de las bases de datos.

- Los ***titulares*** son las personas de quienes se extraen los datos personales.
- Los ***responsables*** son las entidades públicas o privadas que realizan el tratamiento de las bases de datos personales.

¿A quién le pertenecen los datos personales? A los titulares, es decir, a cada uno de nosotras y nosotros.

[2] En Bolivia, no existe una política de datos abiertos en el gobierno central y tampoco contamos con una Ley de Acceso a la Información, por lo que se hace más difícil reclamar la apertura de datos públicos. El portal www.datos.gob.bo es un repositorio con solo 43 conjuntos de datos que están desactualizados y el portal www.geo.gob.bo que es valioso por los más de 1.000 capas de datos geolocalizados o mapas, ahora no tiene personal público dedicado a su actualización desde hace un año y medio. En todo caso, no se trata solo de abrir bases de datos y obsesionarse con la calidad de los datos sino que también hay una necesidad urgente de mejorar las habilidades de recopilación y análisis de datos para crear valor agregado con los datos. De lo contrario, se corre el riesgo de invertir recursos públicos para abrir datos que serán utilizados sólo por países y empresas del Norte Global. Esto tendría como resultado el aumento de la brecha económica y digital entre los países del Sur y los países del Norte.

¿Qué es el consentimiento? Ya que los datos personales les pertenecen a las personas, los responsables deben pedir consentimiento libre, previo e informado a los titulares para usar sus datos personales.

A continuación vamos a desarrollar varios aspectos relativos a esta relación entre responsables y titulares pero antes, revisemos qué es un dato personal y qué tipos de datos personales existen.

4.1 ¿Qué es un dato personal?

- Un dato personal es la información sobre una persona que permite identificarla, localizarla o contactarla por sí solo o en combinación con otros datos personales. El nombre, domicilio, edad, lugar de estudio o trabajo, lugar donde se encuentra, gustos, entre otros, son **datos personales generales** y pueden ser expresados en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Estos datos describen, dan identidad, caracterizan y diferencian a un individuo de otro.

- Existe un tipo de datos personales que son delicados porque pueden llevar a estigmatizaciones, discriminación o serios riesgos de seguridad individual, estos son los **datos personales sensibles**. El estado de salud, creencias religiosas, filosóficas y morales, filiación sindical, ideología política, orientación sexual son ejemplos de este tipo de datos. En ese sentido, estos datos requieren de especial protección y cuidado, por parte del Estado y de las empresas privadas que acceden a este tipo de datos.

- Por otro lado, están los **datos biométricos,** son los referidos a las características físicas, fisiológicas o conductuales de una persona que posibilitan o aseguran su identificación inequívoca. Por ejemplo: huella dactilar, reconocimiento facial, reconocimiento del iris, reconocimiento de la geometría de la mano, reconocimiento de retina, reconocimiento de voz, datos genéticos, entre otros. Utilizarlos para ingresar a un sistema pone en riesgo porque si la base de datos se filtra no es posible cambiar estos como se cambiarían una contraseña.

- También existen los **datos anonimizados o disociados** que son datos que en principio permiten identificar a personas pero que, gracias a mecanismos de anonimización o disociación, terminan teniendo poca o nula relación con la persona que antes identificaban. Estos procesos son utilizados por ejemplo en investigaciones científicas donde, con el fin de proteger la identidad de las personas que participaron en el estudio, se elimina de los conjuntos de datos personales la información que permita la identificación.

- Por otro lado, están los **metadatos** o “datos sobre los datos” se obtienen al analizar otros conjuntos de datos, por ejemplo, cuando se mantiene una conversación por Internet, el contenido de la conversación son los datos y los metadatos son el tiempo de la llamada, la frecuencia con la que esos dos números se contactan, el nombre de quien llama y de quién recibe la llamada, etc. Si bien estos datos por sí solos no

identifican a una persona, un análisis conjunto de los mismos sí podría hacerlo ya que brinda información importante y detallada sobre una persona.

Todo tipo de dato personal revela detalles íntimos sobre la vida personal y familiar. A nivel social, muestra tendencias que pueden permitir el estudio y de comportamientos colectivos. Por eso entender qué tipos de datos existen y cómo protegerlos es esencial.

4.2. Tipos de bases de datos en Bolivia.

La clasificación del tipo de bases de datos personales depende de quién recopila, registra y gestiona los datos, es decir, quién es el responsable del tratamiento de los datos. Se han identificado cuatro tipos de entidades que gestionan bases de datos: públicas, privadas, ONGs y otras organizaciones civiles, y finalmente, organizaciones internacionales de cooperación.

Las bases de datos públicas son las más reguladas y algunas del sector privado como las de la banca y de telecomunicaciones pero varias privadas y las de ONGs y de organizaciones internacionales de cooperación no cuentan con regulación o son regulaciones poco claras o elaboradas para otros países.

4.2.1 Bases de datos públicas.

Las bases de datos públicas se crean con el propósito de brindar servicios a la población y se dividen en dos grupos: primarias y sectoriales.

Las bases de datos primarias están relacionadas con la identidad, hay dos oficinas principales. El Servicio General de Identificación Personal (SEGIP), que es la única institución facultada por ley para expedir cédulas de identidad en todo el país. Otro es el Servicio de Registro Cívico (SERECI), su misión principal es organizar y gestionar el registro de personas, específicamente nombres y apellidos, filiación, nacimiento, estado civil y defunción.

El segundo grupo de bases de datos públicas son las sectoriales. Existen aproximadamente 200 bases de datos de administración pública en el gobierno central creadas por ley. Por ejemplo están las bases de datos de antecedentes policiales, de propiedad de bienes, de infracciones de tránsito, entre varias otras.

4.2.2 **Bases de datos privadas**.

Se pueden distinguir tres grandes sectores en Bolivia que se están dinamizando en la recolección e incluso el análisis de bases de datos personales:

- El sector financiero.
- Los supermercados.
- Las empresas de reparto.

Es importante mencionar que algunas de estas empresas tienen el mismo problema y limitaciones que el sector público y es que cuentan con escasos recursos humanos calificados, herramientas e infraestructura tecnológica para analizar los datos que recolectan. Muchas veces solo los almacenan y no los aprovechan. Uno de los pocos

ejemplos de empresas que analizan los datos personales que recolectan e incluso desarrolla algunos otros servicios a partir de eso es la app de *delivery* PedidosYa.

Por otro lado, existen algunas otras empresas privadas que también están recolectando datos pero sin evidencia de que las analicen. Algunos ejemplos son las empresas de telecomunicaciones, la información generada en la Cámara Nacional de Comercio, la Confederación de Empresarios Privados, fondos de pensiones, instituciones académicas y farmacias.

4.2.3. ONG y organizaciones de sociedad civil.

Se ha identificado la generación de datos y administración de datos personales por parte de ciertas organizaciones de la sociedad civil como algunas especializadas en el análisis de políticas públicas pero esta recolección y análisis se produce en menor escala. Ejemplo puede ser la ONG Ciudadanía de Cochabamba que anonimiza los datos que recolecta para la encuesta LAPOP pero también están las listas de asociados de un sindicato, por ejemplo.

4.2.4. Agencias internacionales de cooperación.

Estas organizaciones internacionales han sido identificadas como recolectoras y gestoras de datos generados a partir de encuestas o sondeos de opinión que elabora como parte de su rol de apoyo a las políticas públicas y también como analistas de datos para el gobierno.

4.3. Extractivismo de datos.

La extracción de datos personales puede tener fines lícitos e ilícitos. Las bases de datos personales se venden y es uno de los negocios que más dinero da en Internet[3].

El término extractivismo de datos se usa como un paralelo de industrias extractivistas de Recursos Naturales en las que las industrias extraen Datos/Recursos Naturales sin dejar ningún beneficio a las poblaciones locales y para lucrar con esos bienes reproduciendo relaciones injustas e históricas que vivimos desde la Colonia cuando los países del norte invadieron países del sur para extraer sus riquezas, esclavizando a las personas locales.

Esta es una idea compleja y requiere de mayor reflexión, sin duda. Si tiene consultas o comentarios al respecto, la sesión sincrónica del 1 de septiembre será un buen momento para conversar.

4.3.1. ¿Cómo se obtiene información personal?

La información personal puede ser obtenida de distintas maneras. Tres de ellas son:

- **A través de la entrega directa:** Esta es la más frecuente en la era digital. Debido a que es muy común que para tener acceso a alguna página web o el uso de alguna aplicación móvil como Facebook, Whatsapp, Tiktok, Netflix, etc. o para hacer gestiones en oficinas públicas, bancos, farmacias, entre otros. Es común que estas

[3] Un ejemplo controversial de la última década del extractivismo de datos para fines políticos fue el de Facebook Inc. y Cambridge Analytica/Strategic Communications Laboratories en referencia a las elecciones presidenciales de los Estados Unidos y el referéndum del Reino Unido -Brexit- en 2016, que abrió la pregunta de cuánto peso tiene el uso de datos para manipular las voluntades de los votantes.

organizaciones soliciten datos personales como el nombre completo, el correo electrónico y edad.

- **A través de medios tecnológicos:** Esto a través del llamado *webtracking*, es decir, el monitoreo constante de los hábitos de navegación en línea. Mediante los clics, la publicidad que vemos y aceptar *cookies* las compañías como Google o Youtube pueden tener un registro de los gustos de sus usuarios y usuarias, y así ofrecer una publicidad personalizada. Lamentablemente esto también implica que las compañías tienen un registro de los gustos y hábitos de consumo en línea.
- **Comprándolos u obteniéndolos a través de entidades que obtuvieron los datos previamente**: Existen empresas que funcionan legalmente en Bolivia y en el mundo dedicadas a vender bases de datos, además existen otras personas y entidades que comercializan estas bases de datos ilegalmente. Al no existir en Bolivia, una ley de protección de datos personales es difícil saber quiénes venden y quiénes compran bases de datos personales y garantizar derechos de privacidad.

4.3.2. Desbalances de poder del tratamiento de los datos personales.

El informe de investigación acerca de Datos Justos (*Data Justice* por su nombre en inglés)[4] de la Fundación de InternetBolivia.org concluye que el extractivismo de datos personales en Bolivia es una práctica que genera más injusticia y desbalances de poder entre actores poderosos (empresas tecnológicas y algunos gobiernos) y actores débiles (la ciudadanía, en general, y poblaciones vulnerables, en específico). Como resultado de este proceso -aún lento- grupos históricamente vulnerados como las personas que viven en zonas rurales, las mujeres, personas con discapacidades son marginados de los procesos de innovación tecnológica, y eso los hace más pobres y los excluye más. Esto conduce a la extracción injusta de datos y la falta de información de los titulares sobre sus derechos.

Algunas de las dinámicas de poder del extractivismo de datos son las siguientes:

- **Escasa posibilidad ciudadana de influir en las decisiones de la gestión de datos personales.** En general, la escasa posibilidad de la ciudadanía para influir en la gestión de las bases de datos personales es la expresión más frecuente de este desequilibrio de poder. Se puede pensar en varios momentos en los que este desequilibrio se expresa, por ejemplo, en la decisión de contratar un servicio de Internet para un celular cuando se obtiene un contrato impreso en el que es muy difícil cambiar algo y solo queda firmar o quedarse sin el servicio.
- **Dinámica de poder basada en la tecnología.** Esta dinámica de poder es ejercida por personas o entidades que conocen de tecnología o tienen recursos tecnológicos. Esto podría ser infraestructura o software. Entidades que tienen servidores donde se almacenan los datos o personas/organizaciones que saben cómo analizar los datos tienen más influencia y capacidad de decisión por encima de otras organizaciones o personas. Un ejemplo cotidiano es la diferencia entre una persona que sabe cómo llenar un formulario en línea y otra que no sabe, la persona que no sabe está en

[4] La Fundación InternetBolivia.org participó de una investigación global acerca de justicia de datos liderada por el Instituto Alan Turing y el Centro Internacional de Montreal en Inteligencia Artificial (CEIMIA). Elaboró el documento acerca de Bolivia que se puede acceder en este enlace en la versión en inglés https://advancingdatajustice.org/wp-content/uploads/2022/04/Advancing-Data-Justice-Research-and-Practice-Final-Report%E2%80%94Internet-Bolivia.pdf

desventaja frente a la que sí sabe hacerlo. Esto puede llevar a la pérdida de oportunidades laborales entre otros efectos.

- **Regulaciones complicadas.** Las Leyes y contratos muy complicados que son desarrollados por algunas empresas e instituciones públicas, y que la ciudadanía no entiende generan desequilibrios de poder. Estos contratos son comunes en servicios de telecomunicaciones y financieros, por ejemplo.
- **Corredores de datos y mercados negros de datos.** En Bolivia, existen intermediarios que comercializan bases de datos que recopilan de diversas fuentes legal e ilegalmente. Legales como los consorcios de datos financieros, e ilegales como son emprendedores y empresas tecnológicas. Las ofertas que a veces se reciben para incrementar seguidores en redes sociales son producto de bases de datos obtenidas fraudulentamente.

  La posibilidad de garantizar el derecho a la privacidad cuando se trata de actividades legales es muy difícil pero en el caso de mercados negros, es imposible.

4.4. Protección de datos personales en Bolivia.

Debido a los efectos potencialmente dañinos del extractivismo de datos, la protección de los datos personales adquiere marcada relevancia actualmente. Es necesario que el Estado disponga en favor de sus ciudadanos y ciudadanas, normas y políticas públicas que protejan del tratamiento abusivo de datos personales y garanticen el derecho fundamental a que las personas decidan qué parte de su vida quieren hacer pública y cuál desean mantener en privado.

Por otro lado, al regular las bases de datos privados las empresas y gobiernos tienen un marco legal fortalecido que les permite hacer un tratamiento legal y con respeto a los Derechos Humanos.

En Bolivia, no tenemos una Ley de Protección de Datos Personales pero la Fundación Internet Bolivia ha elaborado un anteproyecto de Ley y está haciendo gestiones para que la debatan en la Asamblea Legislativa. Si desea consultarla, puede bajar el documento de este enlace https://misdatos.internetbolivia.org/

4.4.1. El derecho a la privacidad como derecho fundamental.

En Bolivia no tenemos una Ley de Protección de Datos Personales pero la Constitución Política del Estado (CPE) reconoce en su artículo 21 el derecho *"A la privacidad, intimidad, honra, honor, propia imagen y dignidad".*

Además, el artículo 130 (I) de la CPE se refiere a la Acción de Protección de Privacidad como una acción de defensa:

> *"Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y*

privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad".

El concepto de **privacidad** se basa en los derechos fundamentales del honor, la dignidad, la intimidad, la propia imagen, así como en la libertad de expresión, pensamiento, opinión y asociación. Muchos de ellos, regulados en los Instrumentos Internacionales de Derechos Humanos[5] y en la CPE, también se desarrollan en ámbitos digitales.

En ese orden de ideas, el derecho a tener una vida privada asegura la libertad y la dignidad de las personas, y en algunos contextos es también requisito para el ejercicio de otras garantías fundamentales (trabajo, salud, entre otros).

Asimismo, la Acción de Protección de Privacidad resguarda la autodeterminación informativa, debido a que cada persona es dueña de sus datos, y es quien debe determinar qué se hace con ellos. Mediante este dispositivo constitucional la protección de datos personales es considerada como un derecho fundamental.

Por otro lado, la mayoría de los ordenamientos jurídicos a nivel global, así como el boliviano, han establecido que el derecho a la privacidad no es absoluto y que puede tener limitaciones razonables[6].

4.4.2. Formas de tratamientos de datos personales.

El uso y tratamiento de datos personales no son actividades nuevas, la recolección de datos de estudiantes, archivos laborales, historias clínicas se han utilizado desde hace varias décadas. Y con mayor razón ahora que la economía de datos ha acelerado los procesos.

El anteproyecto de Ley presentado por la Fundación InternetBolivia.org desarrolla el concepto de tratamiento de los datos personales de la siguiente manera:

"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".

4.4.3. Responsables del tratamiento de datos personales.

---

[5] En el Sistema Interamericano de Derechos Humanos estos derechos están claramente establecidos en la Declaración Americana de los Derechos y Deberes del Hombre de 30 de abril de 1948 en su artículo V, y en la Convención Americana sobre Derechos Humanos conocida como "Pacto de San José" de 22 de noviembre 1969 en sus artículos 11 y 13. Así mismo la Corte Interamericana de Derechos Humanos se ha referido a ellos en varias de sus Sentencias, como el Caso de las Masacres de Ituango vs. Colombia y el Caso Atala Riffo vs. Chile, entre otros.

[6] Al respecto la Declaración Americana de los Derechos y Deberes del Hombre de 30 abril de 1948 se refiere a ellos en su artículo IV y la Convención Americana sobre Derechos Humanos o Pacto de San José de 22 de noviembre 1969 en su artículo 13.

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 que están a cargo de la recopilación, aplicación de medios de seguridad y tratamiento de datos personales, según corresponda.

Por ejemplo, en Bolivia el Servicio General de Identificación Personal (SEGIP) es responsable del tratamiento de la base de datos de identificación de las y los bolivianos, emitiendo carnets de identidad.

De la misma manera, un supermercado puede ser responsable del tratamiento de los datos personales contenidos en la base de datos de sus clientes. En determinadas circunstancias puede requerir contratar a otra empresa para que estudie las bases de datos del supermercado para que analice a qué hora hay más afluencia de clientes, qué producto se compra más, entre otros temas.

Estos terceros tienen acceso a los datos personales y los tratan pero lo hacen a nombre del responsable respetando la finalidad y los medios determinados por el responsable. Estos encargados usualmente celebran un contrato con el responsable del tratamiento en el cual se determina la finalidad, modalidad, tipo de datos, duración y otras particularidades del tratamiento para cada base de datos. Estos contratistas se llaman **encargados o exportadores**.

4.4.4. ¿Qué derechos sobre los datos personales tienen las y los titulares?

El derecho que tienen todas las personas para decidir sobre el uso y manejo de su información personal, esta facultad, en términos jurídicos, se reconoce como “titularidad”.

Esto implica el derecho a tener el control sobre los propios datos, una parte de la doctrina jurídica lo asume como el ejercicio de la autodeterminación informativa (la libertad de decidir sobre la propia información); otra parte de la doctrina entiende este control de la información personal como un desarrollo del derecho a la privacidad, derecho que está más relacionado a proteger los espacios de intimidad.

Los derechos ciudadanos relativos a la protección de datos son los siguientes:

- **Derechos ARCO.** Son los derechos de acceso, rectificación, cancelación y oposición.
    - **Derecho de acceso.** Este derecho nos permite conocer qué datos nuestros tiene una empresa o el gobierno. Un ejemplo es el acceso al historial médico, algo que en la actualidad es difícil de hacer.
    - **Derecho de rectificación.** Los datos personales que manejan estas entidades deben ser exactos, por tanto, este derecho nos da la posibilidad de corregir y actualizar los datos personales que estén almacenados en bases de datos, por ejemplo, si existe un o más datos erróneos en el formulario de Registro Único de Estudiantes (RUDE) que facilita el Ministerio de Educación o cualquier otro trámite, deberían existir los mecanismos para corregirlo.
    - **Derecho a la cancelación.** Así como se da el consentimiento para que los datos personales sean tratados, este derecho permite solicitar la cancelación

o supresión de datos personales de los archivos, registros, expedientes o sistemas donde se encuentran. Por ejemplo, en Bolivia, cuando una persona ya ha cumplido su condena y pasa una cantidad de años, puede pedir la cancelación de sus antecedentes penales.

- **Derecho de oposición.** Este derecho permite a las personas oponerse a la recolección o tratamiento de su información personal siempre que sea con una razón legítima.

- **Derecho a la portabilidad de los datos personales.** Cuando se traten datos personales por vía electrónica o medios automatizados, la persona tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable y transferirlos a otro responsable, en caso de que lo requiera.
- **Derecho a no ser objeto de decisiones individuales automatizadas.** Es el 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. El ejemplo clásico es de selección de personal realizado únicamente por inteligencia artificial.
- **Derecho a la limitación del tratamiento de los datos personales.** Es el derecho a que el tratamiento de datos personales se limite al plazo y finalidad otorgado en el consentimiento para ello.
- **Derecho de indemnización.** Este consiste en ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación a cualquiera de los derechos establecidos anteriormente.

4.5. Mecanismos de protección.

4.5.1. Rol del Estado

El principal actor llamado a garantizar los derechos de la ciudadanía es el Estado. En ese sentido, el Estado debe promover mecanismos que permitan garantizar los derechos de las personas con relación a sus datos personales, principalmente contar con una Ley de Protección de Datos Personales y políticas públicas para capacitar a la población y a los funcionarios sobre los derechos ciudadanos que apoyen su implementación.

4.5.2. Marco Normativo: enfoque desde las y los usuarios y principios

Varios países en la región de América Latina cuentan con una Ley General de Protección de Datos Personales. Algunas de estas leyes fueron elaboradas hace más de dos décadas y naturalmente a la fecha, requieren actualizaciones debido a la evolución tecnológica.

Anteriormente, las leyes de protección de datos seguían el principio de territorialidad de las normas, que dice que las normas se aplican dentro del territorio de un Estado. De esta manera, se decidía qué ley se aplicaba de acuerdo a donde se encontraba el responsable del tratamiento y/o su base de datos.

Posteriormente, en un nuevo contexto, la Unión Europea propuso el enfoque desde el usuario. Ello significa que no importa dónde los datos personales de esa persona estén almacenados o donde esté el responsable del tratamiento. Por consiguiente, se optó por

una mirada extraterritorial de la aplicación de las normas. De esta manera, se aplicarán las leyes de donde se encuentre el usuario.

Otro punto importante es la inclusión de principios. Algunas leyes en la región ya incluyen principios rectores[7]. Lo cual es bueno y debe repetirse en las nuevas propuestas legislativas porque los principios se mantienen en el tiempo.

4.5.3. Autoridad Competente

Además de contar con una Ley General de Protección de Datos Personales, los Estados también deben crear una autoridad con capacidad de hacer cumplir la norma legal. Se recomienda que esta autoridad sea independiente en todo sentido, para que pueda realizar investigaciones, fiscalizaciones y pueda sancionar a cualquier entidad sea esta pública o privada. Asimismo, esta autoridad debe contar con mecanismos robustos de control que le permitan actuar sin retraso.

La importancia de contar con una autoridad de protección de datos adecuada se puede ver en Chile y Brasil, países donde existe legislación pero no se cuenta con una autoridad independiente, haciendo que la ley y sus disposiciones se queden en el papel.

4.5.4. ¿Cuál es la situación en América Latina?

En muchas partes del mundo, incluida América Latina, los países cuentan desde hace varios años con leyes generales de protección de datos. Bolivia es uno de los países que aún no cuenta con una Ley de Protección de Datos Personales.

Tabla 1. Países y leyes de protección de datos personales

País	¿Tiene LPDP(*)?	¿Tiene APDP(**)?
Argentina	Sí, desde 2000	Sí
Brasil	Sí, desde 2020	Sí
Chile	Sí, desde 1999	No
Colombia	Sí, desde 2012	Sí
Costa Rica	Sí, desde 2011	Sí
Ecuador	Sí, desde 2021	Sí
México	Sí, desde 2010	Sí
Panamá	Sí, desde 2019	Sí

[7] Algunos de estos principios son: Principio de Licitud, Principio de Lealtad, Principio de Transparencia, Principio de Diversidad Cultural, Principio de Finalidad, Principio de Proporcionalidad, Principio de Calidad, Principio de Responsabilidad, Principio de Seguridad, Principio de Confidencialidad, Principio Pro Persona, Principios Comerciales, Principio de Conservación limitada, Principio de Datos Personales Sensibles y Datos Biométricos.

Paraguay	Sí, desde 2020	Sí
Perú	Sí, desde 2011	Sí
República Dominicana	Sí, desde 2013	No
Uruguay	Sí, desde 2008	Sí

Fuente: Guerrero Argote, Carlos: Conectados y protegidos. P. 40
Referencias: (*Ley de Protección de datos) (**Autoridad de protección de datos)

Por su parte, cabe destacar la experiencia Europea emitió un Reglamento General de Protección de Datos Personales (RGPD) que cuenta con nuevas y más sofisticadas herramientas para garantizar un uso adecuado de los datos personales más allá de los límites geográficos, porque la atención primordial está puesta en el interés y los derechos de los usuarios. El RGPD entró en vigor en mayo de 2018.

4.5.5. Marco normativo para protección de datos en Bolivia.

Bolivia aún no cuenta con una Ley de Protección de Datos Personales, sin embargo, aunque no son suficientes existen artículos en leyes, decretos supremos y resoluciones en los cuales se puede apoyar respecto a la protección de datos. Hacemos una breve revisión a continuación.

Constitución Política del Estado, Artículo 130.

I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

Artículo 131.

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las **veinticuatro horas** siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley

Código Procesal Constitucional

Capítulo Cuarto - Acción de Protección de Privacidad

Artículo 58°.- (Objeto) **:** La Acción de Protección de Privacidad tiene por objeto garantizar el derecho de toda persona a conocer sus datos registrados por cualquier medio físico, electrónico, magnético o informático, que se encuentre en archivos o bancos de datos públicos o privados; y a objetar u obtener la eliminación o rectificación de éstos cuando contengan errores o afecten a su derecho a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación.

Artículo 59°.- (Legitimación activa) La Acción de Protección de Privacidad podrá ser interpuesta por:

Toda persona natural o jurídica que crea estar afectada en su derecho, u otra persona a su nombre con poder suficiente. Las herederas o herederos de una persona fallecida, que crean que ésta ha sido afectada en su derecho a la privacidad, imagen, honra y reputación, cuando dicho agravio genere directamente la vulneración de los derechos de ellas o ellos, en virtud del vínculo de parentesco con la difunta o difunto.

Artículo 60°.- (Legitimación pasiva) La Acción de Protección de Privacidad podrá ser interpuesta contra: Toda persona natural o jurídica responsable de los archivos o bancos de datos públicos o privados donde se pueda encontrar la información correspondiente.
Toda persona natural o jurídica que pueda tener en su poder datos o documentos de cualquier naturaleza, que puedan afectar al derecho o la intimidad y privacidad personal, familiar o a la propia imagen, honra y reputación. En ambos casos, tendrá legitimación pasiva la persona natural o jurídica, pública o privada, que compile datos personales en un registro, que independientemente de tener o no una finalidad comercial, esté destinado a producir informes, aunque no los circule o difunda.

Artículo 61°.- (Interposición directa de la acción) La Acción de Protección de Privacidad podrá interponerse de forma directa, sin necesidad de reclamo administrativo previo, por la inminencia de la violación del derecho tutelado y la acción tenga un sentido eminentemente cautelar.

Artículo 62°.- (Improcedencia) La Acción de Protección de Privacidad no procederá cuando se haya interpuesto para levantar un secreto en materia de prensa, cuando hayan cesado los efectos del acto reclamado y cuando sea aplicable lo previsto en el Artículo 53 del presente Código.

Artículo 63°.- (Efectos de la resolución) Si el Órgano Jurisdiccional considera probada la violación del derecho, podrá establecer la existencia de indicios de responsabilidad civil o penal de la accionada o accionado de conformidad al Artículo 39 del presente Código.
Si la acción fuese promovida por un acto ilegal o indebido, que impida conocer los datos registrados por cualquier medio físico, electrónico, magnético o informático en archivos de datos públicos o privados, la sentencia ordenará la revelación de los datos cuyo registro fuera impugnado.

Si la acción fuese promovida por un acto ilegal o indebido, que impida objetar los datos registrados por cualquier medio físico, electrónico, magnético informático en archivos de datos públicos o privados, la sentencia determinará se admita la objeción del accionante.

Si la acción fuese promovida por un acto ilegal o indebido, que impida obtener la eliminación o rectificación de datos registrados por cualquier medio físico, electrónico, magnético o informático en archivos de datos públicos o privados, la sentencia ordenará la eliminación o rectificación de los datos del accionante a ley.

Decreto Supremo Nº 1793

Capítulo II Tratamiento de los datos personales

Artículo 56.- (protección de datos personales). A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

a) La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

b) El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;

c) Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

d) Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;

e) El responsable del tratamiento de los datos personales, tanto del sector público como del privado, deberá adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento no autorizado, las que deberán ajustarse de conformidad con el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Ley Ciudadanía Digital

Bolivia LEY No 1080 del 11 de Julio de 2018

Artículo 12.- (protección de datos personales y seguridad informática)
I. Las y los servidores y funcionarios de las instituciones previstas en la presente Ley,

utilizarán los datos personales y la información generada en la plataforma de interoperabilidad y ciudadanía digital únicamente para los fines establecidos en normativa vigente.

II. El incumplimiento de la anterior previsión, será sujeto a responsabilidad por la función pública; para el caso de instituciones privadas que presten servicios públicos delegados por el Estado, el ente que ejerza supervisión respecto a sus funciones deberá establecer los mecanismos pertinentes a fin de dar cumplimiento a esta norma.