GUÍA BÁSICA SOBRE DATOS PERSONALES PARA BOLIVIA

accessnow.org

accessnow

Este documento contiene una presentación de la problemática de la protección de datos personales en Bolivia y ofrece algunos conceptos básicos, principios y reglas que deberían tenerse en cuenta en la futura legislación sobre el tema. Ha sido elaborado por **Access Now**, organización internacional de derechos humanos en internet en colaboración con **InternetBolivia.org**, organización boliviana dedicada a la defensa y promoción de los derechos humanos en contextos digitales.

Importancia de la protección de datos personales

Todos los días usamos aplicaciones móviles y el navegador de internet para diversas actividades como comunicarnos, mantenernos informados, realizar compras y ventas, entretenernos, efectuar operaciones bancarias, trabajar, entre otras. Claramente, vivimos en un mundo interconectado.

Como usuarios reconocemos fácilmente las ventajas de vivir conectados. No obstante, existe otro aspecto que no siempre es evidente porque sucede detrás de nuestras pantallas. Hablamos del uso y tratamiento de nuestros datos personales.

Cuando navegamos o usamos aplicaciones vamos dejando rastros de información. Esa información puede revelar quienes somos y cómo usamos la tecnología. Muchas veces entregamos datos personales (como nuestro nombre, hábitos de consumo y localización) porque páginas y aplicaciones nos lo solicitan. En otros casos, los datos personales son deducidos o generados a partir de nuestro uso. Estos datos personales también son analizados por quienes nos brindan servicios en Internet para diversos fines que incluyen desde brindar una mejor experiencia de uso hasta clasificarnos discriminatoriamente. Esta situación se repite todo el tiempo.

Por ello, hace algunos años los gobiernos y activistas empezaron a preocuparse sobre el uso de los datos personales. En muchas partes del mundo (incluida América Latina) los países cuentan, desde hace varios años, con leyes generales de protección de datos, que ponen límites a la recolección y análisis de información personal y reconocen derechos a los usuarios para evitar abusos y controlar el funcionamiento de la tecnología.

Sin embargo, como la tecnología avanza y cada vez estamos más interconectados, las leyes suelen quedar desactualizadas. La Unión Europea entendió esta situación y emitió un Reglamento General de Protección de Datos Personales ("RGPD" en adelante) 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.

La entrada en vigor de este reglamento en mayo de 2018 generó expectativas y dudas. De la noche a la mañana, empresas de todo el mundo pusieron sus ojos en el cumplimiento del RGPD. De la misma manera, otros Estados fuera de la Unión Europea empezaron a analizar si sus marcos normativos estaban a la altura de los desafíos que impone la tecnología actual. Inclusive aquellos países que aún no cuentan con una ley de datos personales comenzaron a dialogar con mayor seriedad sobre la necesidad de contar con una.

Bolivia es uno de los países que aún no cuenta con una ley general de protección de datos personales. Por esa razón, el equipo de Access Now con la colaboración de la organización InternetBolivia.org elaboró esta guía para promover el debate y una regulación general sobre la protección de los datos personales en Bolivia.

En este trabajo, proponemos definiciones básicas y ejemplos de la vida diaria para poder comprender mejor cómo la protección de datos es un elemento indispensable para el uso y aprovechamiento de la tecnología en un marco de protección de derechos humanos.

En la actualidad, las y los bolivianos cuentan con leyes que tocan algunos temas de datos personales pero lo hacen de manera incompleta y no integral. Por ello, buscamos que esta guía ayude a promover un diálogo centrado en una visión completa y con los derechos de los usuarios en el centro de la discusión. Pues son los usuarios los dueños de su información y quienes tienen el derecho de conocer, autorizar o negar los usos que se hagan de ella. Junto a InternetBolivia.org proponemos impulsar el trabajo por una ley general de protección de datos personales.

¿Qué es un dato personal?

El dato personal = mi información

Cuando se habla sobre este tema siempre se menciona "la protección de los datos personales". La misma frase puede causar confusión y por lo tanto empezaremos desarrollando el concepto.

En términos sencillos, **un dato es igual a información**. Un dato contiene información que puede ser de carácter estadístico, financiero, demográfico, entre otros. Cuando se habla de datos personales, nos estamos refiriendo a datos que contienen información sobre o relativos a una persona.

De esta manera, **un dato personal es igual a la información sobre una persona**. Algunos ejemplos bastantes conocidos son el nombre, la dirección, el teléfono, el correo electrónico y hasta el historial médico y los antecedentes penales. Estos datos nos dan información sobre una persona en particular.

Ahora bien, la doctrina legal profundizó este concepto y actualmente no sólo son datos personales las informaciones que identifican a una persona directamente sino también aquellas que la hacen identificable tras un análisis posterior. Esto último quiere decir que hay informaciones que indirectamente se relacionan a una persona y que de igual manera las vamos a considerar datos personales. Ejemplo de esto son las imágenes de las cámaras de videovigilancia o la ubicación GPS.

Toda esta información es clave y 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 que tipos de datos existen y cómo protegerlos es esencial para la vida democrática en un marco de creciente digitalización.

Tipos de datos

Como podemos ver, los datos personales dan a conocer informaciones diversas. Es por ello que a nivel legislativo y de análisis técnico se ha diferenciado entre distintos tipos de datos personales.

Los sensibles: Dentro del grupo general de datos personales hay un tipo de datos que por su contenido son denominados datos sensibles. La información que proporcionan esos datos es delicada y de carácter íntimo. Podemos identificar este tipo de datos fácilmente porque son aquellos que preferimos mantener en reserva y que pueden causar daños graves si son difundidos o mal utilizados. Ejemplos de estos datos sensibles son los concernientes a la salud, la genética, la religión, las

preferencias políticas, y hasta aquellos que denotan ingresos económicos o preferencias sexuales. Hubo un caso donde se difundió que una autoridad era portadora del virus de la inmunodeficiencia humana (VIH) sin haber requerido previamente su consentimiento o autorización, esto orilló a esta persona a la depresión y a otros efectos dañinos en su vida.

Datos anonimizados o disociados: Existen también otros tipos de datos que, por la forma en la que son obtenidos o procesados, reciben otras denominaciones. En este grupo tenemos a los datos anónimos y anonimizados o disociados. Estos 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. Sin embargo, esta práctica no quita que los principios de protección de los datos personales, que veremos más adelante, deban ser aplicados, en especial el de minimización de la recolección y análisis de datos; ya que existen procedimientos técnicos para revertir la anonimización y volver a identificar a las personas, en algunos casos.

Los metadatos: Estos son los llamados "datos sobre los datos", puesto que son datos que se obtienen al analizar otros conjuntos de datos. Esto incluye, por ejemplo, algunos datos de navegación en internet e información sobre comunicaciones entre personas (a qué hora se mandó un SMS, en qué ubicación GPS se tomó una foto, etc). Si bien estos datos por sí solos no identifican a una persona, un análisis conjunto de los mismos sí podría hacerlo ya que nos brinda información importante y detallada sobre una persona. Por ejemplo, la redes sociales generan registros de visitas, reacciones (likes), compras en línea, entre otros. Al analizar y estudiar estos datos podemos conocer los gustos y preferencias de los usuarios de esas redes sociales; deducir donde viven, trabajan, van de vacaciones y quienes son sus familiares y amigos.

Formas de tratamiento

Ante todo, debemos tener en claro que usar y trabajar con datos personales no es una actividad nueva. Recordemos las estanterías donde se solían guardar archivos de trabajadores, estudiantes y pacientes, por ejemplo. Aquellas personas que trabajaban usando esos archivos hacían (y aún hacen) lo que llamamos "tratamiento de datos personales".

El tratamiento de datos personales es toda actividad que se realiza con los datos personales, y comprende desde su recopilación y almacenamiento hasta actividades más complejas como un análisis con inteligencia artificial[1].

1 - Actualmente, no existe una definición fija sobre inteligencia artificial. Para algunos, es cuando las máquinas empiezan a realizar tareas que de hacerlas los humanos habrían requerido inteligencia, para otros es hacer máquinas inteligentes, e inclusive otros señalan que son las tecnologías que están inspiradas en el sistema nervioso y el cuerpo del ser humano. Sin embargo, podemos decir que la inteligencia artificial es más considerada como un todo que algo en específico. Dentro de este todo encontramos subtemas como: aprendizaje automático (machine learning), robótica, redes neuronales, visión, natural procesamiento del lenguaje, procesamiento de discursos. Para conocer más sobre inteligencia artificial y su impacto en los derechos humanos les recomendamos revisar la publicación Human Rights in the Age of Artificial Intelligence de Access Now

Dicho tratamiento puede ser manual (como el que se hace en papel) o automatizado que es aquel que emplea software para analizar información a gran escala. Hoy en día, la tecnología hace que el tratamiento sea más sofisticado y veloz, habilitando el tratamiento de cantidades enormes de datos personales sin mucho esfuerzo y obteniendo resultados más exactos. Es por eso que el análisis de *big data* [2]se ha convertido en una actividad relevante para todo aquel que quiera conocer más sobre un mercado, los consumidores, o las preferencias políticas de un grupo demográfico.

Responsable y encargados del tratamiento

Los datos personales suelen ser almacenados en bases de datos que pueden ser archivos físicos o estar en algún sistema computarizado. Cuando se crea una base de datos se le otorga una finalidad, una razón de ser, que puede incluir desde el registro de los visitantes a un lugar o ayudar a cumplir con la prestación de servicios médicos mediante historias clínicas, hasta elaborar perfiles detallados de usuarios de servicios y sus preferencias de consumo.

La entidad que determina los fines (para qué) y medios (cómo) del tratamiento de los datos es considerada: "responsable del tratamiento". Esa entidad puede ser una persona natural, jurídica, organismo público o no gubernamental. Y será responsable por todo lo que pueda pasar con los datos personales almacenados en la base de datos, además de otras obligaciones que la ley le pueda dar.

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 que permite que tengamos carnets de identidad. De la misma manera, un supermercado es responsable del tratamiento de los datos personales contenidos en la base de datos "compras de clientes".

Naturalmente, en ocasiones dicha entidad no tiene la capacidad de realizar todo el tratamiento por sí sola y necesita de terceros que le ayuden. 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. Según la doctrina y la legislación estos terceros son llamados "encargados del tratamiento". 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. Sin perjuicio de ello, las leyes de datos personales exigen que ese encargado también cumpla con la ley general de protección de datos personales.

En el ejemplo del supermercado y la base de datos "compras de clientes", un encargado del tratamiento podría ser una empresa de análisis de datos que haya contratada por el supermercado para estudiar las bases de datos y saber a qué hora hay más afluencia de clientes, qué producto se compra más, entre otros temas.

2 - "Big Data" hace referencia a un gran volumen de datos que se caracteriza por ser muy variado, tener gran valor y a la vez haber sido recolectado velozmente.

¿Por qué me debe importar proteger y tener control sobre mis datos personales?

Pensemos en aquella vez que recibimos una llamada en la cual nos ofrecen un producto o servicio. La persona que nos llama conoce nuestro nombre, nuestro número de teléfono y al parecer hasta conoce nuestras necesidades. Nunca antes habíamos hablado con esa persona ni tenemos relación con la empresa a la cual representa. La simple llamada suele ser molesta y hasta impertinente. Pero más allá de eso, es posible preguntarnos: ¿cómo es que tiene mi número y porqué no deja de llamarme?

Otro ejemplo cercano a estas fechas de elecciones son los padrones electorales. Últimamente en Bolivia como parte del proceso de elecciones primarias para habilitar binomios de candidatos a presidencia y vicepresidencia se han conocido denuncias de personas que han encontrado su nombre como militantes en el padrón de un partido político donde no militan. ¿Cómo llegó ese nombre al padrón de cada partido?

En ambos casos la empresa y el partido político está haciendo tratamiento de nuestros datos personales sin que tengamos conocimiento ni lo hayamos autorizado, lo cual de por sí es incómodo. Pero demos un paso más y respondamos la pregunta ¿cómo obtuvieron ellos mi nombre? Podemos empezar a encontrar algunas respuestas en las noticias.

Se ha reportado un caso en Argentina de infiltrados en la administración pública que tenían acceso a datos personales y que gracias a una aplicación lograron vender la información a terceros. Un situación similar se reportó en Brasil, donde un ente de la propia administración pública vendía bases de datos de una oficina de gobierno que contenían: nombre completo, número de identificación, fecha de nacimiento, sexo, nombre de la madre y dirección, entre otros. También hay situaciones donde, por fallas o negligencias en la seguridad, los datos quedan expuestos libremente. Una situación de ese tipo se dió en Perú donde, desde el 2015 hasta el 2018 se podía descargar la foto, nombre completo, dirección, sexo, estado civil, grupo de votación, y datos sobre donación de órganos sin levantar ninguna alerta en el sistema del registro nacional de identificación de ese país.

La filtración de datos también puede darse desde las empresas. Por ejemplo, en Chile se reportó una filtración de más de 14 mil datos sensibles de tarjetas de crédito y débito. Asimismo, en México, una empresa de telemedicina habría dejado expuestos los datos personales sobre la salud de 2.373.764 personas, un daño tan grave que la Autoridad de datos personales estaba considerando una multa de más de 1 millón de dólares estadounidenses.

Adicionalmente, se han reportado casos de venta de bases de datos por parte de particulares. En Perú, un noticiero reportó la venta, en plena calle, de bases de datos de empresas telefónicas y bancos a un precio de 60 dólares estadounidenses. La falta de fiscalización hace que esto sea posible. Esta situación, es aún peor en países donde ni siquiera hay ley de protección de datos que permita fiscalizar estos negocios. Por ejemplo, en Bolivia, también hay uso no autorizado de bases de datos

personales por parte de particulares; la venta o cesión de bases de datos personales de supermercados, empresas de seguros, entre otros está a la orden del día.

Las situaciones descritas son sólo muestras de todo lo que está sucediendo, en muchos casos, sin darnos cuenta. Los datos personales, al revelar información importante de nosotros, son muy valiosos para distintos finalidades y actores. Es por ello que resulta de mucha importancia que nosotros, como usuarias y usuarios, tengamos conocimiento de esta situación y conozcamos nuestros derechos para no ser las próximas víctimas de un tratamiento indebido de nuestros datos personales.

¿Qué derechos tengo sobre mis datos?

Control sobre mis datos: mi derecho

El término que utilizamos en esta materia es el de "derecho a la protección de los datos personales". Aquí cabe una aclaración, puesto que a simple vista parecería que queremos proteger el dato; sin embargo el concepto va más allá. **No se está hablando de proteger el dato, sino a la persona que está detrás del dato**[3], es decir a la persona a la cual ese dato identifica o hace identificable. Por lo tanto, a fin de generar esa protección se le brindan herramientas para que controle la información que está relacionada a su persona.

Dicho control sobre los datos personales es entendido por una parte de la doctrina jurídica como un ejercicio de autodeterminación informativa, esto es, la libertad de decidir sobre la propia información. Lo cual permite que la persona pueda, por ejemplo, conocer de qué forma y con qué finalidades se están tratando sus datos personales y así evitar daños económicos y sociales, entre otros. 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. Independientemente de qué doctrina se prefiera, lo cierto es que este control sobre los datos personales ha seguido su propio desarrollo.

Es así que debemos mencionar la expresión básica del control de nuestros datos personales: el consentimiento. Para algunos el consentimiento es un principio, mientras que para otros es una base jurídica que autoriza el tratamiento de datos personales, al igual que una ley o un contrato. Sin entrar en detalles jurídicos porque este no es el espacio para hacerlo, queremos que quede claro que el consentimiento es una expresión explícita, informada, que hacemos de manera libre a fin de dar nuestra aprobación a un tercero para que realice tratamiento de nuestros datos personales.

Ahora, para ejercer ese control sobre nuestros datos personales, la doctrina y las legislaciones han planteado nuevos derechos y principios. Los cuales nos sirven de herramientas para tener información, trasladar nuestros datos, impedir que terceros usen nuestros datos, entre muchas cosas más. Veamos a continuación los derechos más comunes que tenemos para controlar nuestros datos personales. [4]

3 - FERNANDEZ DE MARCOS, Isabel Davara. 2011. Hacia la estandarización de la protección de datos personales. Madrid: La Ley Actualidad.
4 - Las legislaciones de cada país podrían crear otros derechos según lo requieran.

Derecho a la información: Este derecho nos garantiza poder obtener información sobre el tratamiento de nuestros datos directamente del ente responsable del tratamiento, sin demoras ni trámites burocráticos. Esto incluye, entre otros, el derecho a saber quiénes, cómo, con qué fines y por cuánto tiempo recolectan y analizan nuestra información.

Derecho de acceso: Este derecho nos permite conocer de primera mano si un ente privado o de gobierno tiene o trata nuestros datos. Este derecho incluye el de obtener una copia de ese archivo. Por ejemplo, si quieres ejercer este derecho podrías pedir a tu centro de salud el historial de las visitas médicas que realizaste y este centro deberá entregarte una copia de dicho historial.

Derecho a la rectificación: Este derecho fue pensado en consonancia a otro principio que es el de exactitud y del que hablaremos más adelante. Los datos que se manejen deben ser exactos, por lo tanto se nos da la posibilidad de corregir y actualizar los datos personales que estén almacenados en bases de datos. Por ejemplo, podríamos querer actualizar nuestro estado civil o el registro de deudas que figura en servicios de información crediticia.

Derecho a revocar el consentimiento o cancelación: Como comentamos líneas arriba, una de las expresiones base de la protección de los datos personales es el consentimiento. Así como damos nuestro consentimiento para que nuestros datos sean tratados, también podemos retirar dicho consentimiento cuando el tratamiento sea excesivo, no pertinente, inadecuado, entre otros. Ello significa que el responsable del tratamiento deberá dejar de tratar nuestros datos personales.

Derecho de supresión: Este derecho garantiza que luego de terminado el uso de un servicio, podamos solicitar que el responsable elimine todos los datos personales que nos conciernen. En marcos regulatorios como el RGPD, también puede reclamarse la eliminación cuando el responsable de los datos los haya usado ilegalmente.

Derecho al olvido: Este derecho está lleno de controversias. El derecho al olvido apareció en un caso judicial ante la Corte Europea de Justicia[5] y consiste en que la persona puede pedir que se disocie de los buscadores en internet aquella información personal que ya no sea relevante. Si bien parece una causa noble, la misma ha generado ciertas discusiones. La más importante de ellas es con respecto al derecho a la información: al disociar dicha información se reducen las posibilidades que otras personas puedan conocer hechos que eventualmente puedan resultar de interés público. Si deseas conocer más sobre este derecho puedes consultar el documento de posición de Access Now sobre el derecho al olvido.

Derecho a la oposición: Este derecho permite a las personas oponerse a la recolección o tratamiento de su información personal ante ciertos casos puntuales, que cada legislación determina en función de objetivos de política pública. Ejemplo de esto son los casos en los que podemos oponernos previamente al tratamiento de nuestros datos con fines de marketing o si se hace para la toma automatizada de decisiones que nos conciernen.

5 - En España, el señor Mario Costeja solicitó que el motor de búsqueda Google desindexara el contenido que mostraba cuando buscaba su nombre en dicho motor, puesto que mostraban noticias pasadas sobre un problema

Derecho a la portabilidad: Este es un nuevo derecho que se incluyó recientemente en el RGPD. Según este derecho, tenemos el poder movilizar nuestros datos personales de una base de datos a otra. Ello puede implicar solicitar al responsable del tratamiento una copia o el original de toda nuestra información en un formato compatible que permita trasladarla a otro proveedor de servicios. En algunos casos también puede pedirse que el responsable del tratamiento de datos haga ese traslado por nosotros. Por ejemplo se podría solicitar a un banco que mueva todos nuestros datos a otro banco. Así, no perderíamos historial de nuestros movimientos financieros, ni de lo créditos que obtuvimos.

Derecho a la explicación: Este también es otro derecho que fue plasmado por primera vez en el RGPD. Cabe resaltar que no hay un artículo en específico asignado a este derecho, sino que proviene de la interpretación de varios. Este derecho nos permite obtener explicaciones sobre las decisiones que se realizan mediante el tratamiento automatizado de nuestra información personal. Es el caso de las decisiones que se toman mediante sistemas de inteligencia artificial o algoritmos.

Si deseas conocer más sobre estos derechos, puedes revisar la guía en inglés "A User Guide to Data Protection in the European Union – Your Rights and How to Exercise Them" que Access Now publicó para la Unión Europea.

¿Cómo se protegen los datos personales?

Rol del Estado

El principal actor llamado a garantizar nuestros derechos es el Estado. En ese sentido, el Estado debe promover mecanismos que nos permitan controlar nuestros datos personales. Uno de estos mecanismos es el contar con una ley general sobre la materia, otro factor adicional son políticas públicas para capacitar a la población sobre los derechos que tiene, e inclusive el Estado podría trabajar mano a mano con las empresas para asegurar que respeten los derechos de las personas. Claramente, el Estado puede implementar un sinfín de mecanismos. En los siguientes puntos hablaremos de dos de ellos.

Marco Normativo: enfoque desde el usuario y principios

Como comentamos anteriormente, varios países en la región de América Latina cuentan con una ley general sobre protección de datos personales. Algunas de estas leyes fueron elaboradas hace más de una década y naturalmente a la fecha requieren actualizaciones debido a la evolución tecnológica y el enfoque actual del uso de datos en la economía digital. Esto último se debe básicamente a la forma en que están planteadas estas leyes, es decir, el enfoque que se utilizó.

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. Por ejemplo, si el responsable y/o la base de datos estaban en Bolivia entonces se aplicaba la ley de Bolivia. Siguiendo el ejemplo, el problema surgió cuando esas bases comenzaron a tener responsables de tratamiento o estar situadas fuera de Bolivia. Internet y la transmisión de datos

personales a servidores que están situados fuera del país presentan un desafío en este sentido.

En este contexto, la Unión Europea propuso un nuevo 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 aplicará 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. Lo cual es bueno y debe repetirse en las nuevas propuestas legislativas. Ello porque los principios son fundamentos y límites básicos que se mantienen en el tiempo.

A continuación listamos los principios más usados:

Lealtad y legalidad: Los datos personales deben ser procesados de manera justa y legal; lo que implica que exista una ley, y que el tratamiento de datos se realice de una manera justa y transparente, para que podamos informarnos sobre cómo las entidades recopilan, usan y almacenan nuestros datos personales.

Limitación de la finalidad: Los datos personales deberán ser tratados solo para fines específicos y legítimos. El propósito debe ser explícito, y de duración limitada.

Minimización de datos: El tratamiento de datos personales debe limitarse a lo que sea suficiente, pertinente y no excesivo en relación con una finalidad específica y definida.

Exactitud: Los datos personales deben ser precisos y, cuando corresponda, deben ser actualizados. Recordamos aquí el derecho que tenemos de rectificación.

Conservación limitada: Los datos personales procesados por cualquier propósito no deben ser mantenidos por más tiempo del necesario.

Derechos de los usuarios: Los datos personales deben ser tratados respetando nuestros derechos.

Integridad y confidencialidad: Los datos personales deben ser tratados de forma segura, protegiéndolos contra accesos no autorizados o ilegítimos, pérdida accidental, destrucción o daño de los mismos.

Adecuación: Los datos personales no deben ser transferidos a un país o territorio tercero, a menos que el país o territorio en cuestión garantice un nivel adecuado de protección para nuestros derechos en relación al tratamiento de los datos personales.

Autoridad Competente

Además de contar con una ley general sobre 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[6], países donde existe legislación pero no se cuenta con una autoridad independiente, haciendo que la ley y sus disposiciones se queden en el papel.

A fin de conocer más sobre cómo los legisladores deben actuar para crear e implementar un marco efectivo de protección de datos personales, le recomendamos leer la publicación de Access Now: "La creación de un marco para la protección de datos: una guía para los legisladores sobre qué hacer y qué no".

¿Y cuál es la situación en Bolivia?

Bolivia es uno de los países que aún no cuenta con una legislación general y completa sobre protección de datos personales. Otros son por ejemplo: Paraguay y Ecuador. Sin embargo, cuenta con otras disposiciones que de una u otra manera abordan el tema.

De un lado, encontramos en algunos artículos en la Constitución legislación acerca de este tema, como el Artículo 21.2 que señala que las y los bolivianos tienen derecho a la privacidad, intimidad, honra, propia imagen y dignidad. Este artículo establece la base para entender que las y los bolivianos también tienen derecho a controlar sus datos personales puesto que pueden afectar la honra, la imagen, dignidad y privacidad.

Otro artículo que vale comentar es el 130 llamado Acción de Protección de Privacidad. Esta es una acción constitucional que ya se encontraba prevista desde el 2004 pero que aparece con ese nombre en la nueva constitución del 2009. Durante esos años dos sucesos marcaron el avance en este tema: la sentencia constitucional 0965/2004-R de junio de 2004 donde se menciona a los datos sensibles y a las personas jurídicas y la ley del 2005 sobre acceso a la información.

Conforme a esta nueva acción constitucional, las y los bolivianos pueden ejercer esta acción cuando consideren que están siendo impedidos de conocer, objetar la eliminación o rectificar los datos registrados en un banco de datos ya sea público o privado y que por lo tanto se le esté afectado la intimidad, privacidad, imagen honra y reputación. Actualmente, el Código procesal Constitucional prevé como deberá desarrollarse una Acción de Protección de Privacidad.

6 - El 28 de diciembre de 2018, el poder ejecutivo de Brasil publicó la Orden Ejecutiva Nª 869 que modifica algunas disposiciones de la ley actual de datos personales de Brasil y crea la Autoridad Nacional Brasileña de Protección de Datos Personales. La autoridad formaría parte de la presidencia, lo cual crea un problema cuando quiera controlar y fiscalizar el tratamiento de lo datos que hace el gobierno y las entidades públicas, pues no es independiente. Según las leyes de Brasil, las órdenes ejecutivas son de aplicación inmediata pero para convertirse en Ley deben ser ratificadas por el Congreso Nacional en un plazo de 120 días. A la fecha de publicación de esta guía aún no tenemos certeza sobre esta ratificación. Más información en el artículo de Renato Leite Monteiro "Changes to Brazil's Data Protection Law and the establishment of the DPA"

Por otro lado, otras leyes y códigos tiene menciones sobre la privacidad; entre ellos cabe destacar el artículo 54 de la Ley General de Telecomunicaciones y Tecnologías de la información y Comunicación, sobre los derechos de los usuarios a la privacidad, y a decidir sobre los datos que se incluyen en las guías de números telefónicos que están disponibles al público. Asimismo, la modificación al Artículo 79 de la Ley del Órgano Electoral que permite interoperar el Servicio de Registro Cívico (SERECI) con el Servicio General de Identificación (SEGIP) contiene disposiciones sobre la seguridad de los datos personales y les concedes a las y los bolivianos poder consultar los datos personales almacenados para poder autenticar y validar la información.

Adicionalmente, tenemos el Artículo 56 del Reglamento para el Desarrollo de Tecnologías de la Información y Comunicación, el cual al referirse al certificado digital le brinda a la persona un marco de control sobre sus datos basándose en la idea del consentimiento. Finalmente, la reciente Ley de ciudadanía digital en su Artículo 12 dispone el tratamiento de los datos personales se debe limitar a la finalidad que establece la ley.

Al revisar estas normas legales podemos comentar lo siguiente:

- En primer lugar, se ve que los legisladores son conscientes de la necesidad de colocar mecanismos de seguridad, límites al tratamiento y hasta otorgar derechos cuando se trata de datos personales.

- En segundo lugar, notamos que no existe una visión normativa integral sobre datos personales. Cada norma contiene artículos que mencionan temas de datos personales pero desde su propio enfoque, que en algunos casos puede resultar descoordinado y contradictorio. Para graficarlo es como si se intentara armar el rompecabezas de los datos personales sólo con unas cuantas piezas.

- Como tercer y último punto, al ver en detalle los artículos citados, percibimos que en sí mismos también se encuentran incompletos. Algunos no incluyen todos los derechos que ya mencionamos, no incorporan mecanismos de seguridad, y en otros tampoco se hace mención a todos los principios.

Por lo tanto, es necesario un trabajo conjunto de todos los sectores para armar un marco normativo general. Esta discusión ya empezó en el segundo Foro de Gobernanza de Internet de Bolivia (2018), el cual dedicó una de sus sesiones a comentar la situación de los datos personales en el país. Este tipo de eventos sirven para acercar a todos los sectores a conversar sobre temas importantes como lo es la protección de datos y para ver cuál es el estado de las cosas. En Bolivia, la preocupación de los asistentes de ese evento se centró tanto en cómo incrementar la concientización sobre el tratamiento de nuestros datos personales y la posibilidad de tener una autoridad de protección de datos personales que vele por el cumplimiento de una ley general en el tema. Es fundamental la participación de todos los interesados en diálogo abierto y democrático sobre la norma de protección de datos indicada para Bolivia. La sociedad civil, el sector privado, el sector académico, la comunidad técnica y el gobierno tienen mucho para aportar al debate. Y una ley efectiva deberá contar con la legitimidad y apoyo de todos los sectores para su eficiente creación e implementación.

Es nuestro momento

Esperamos que luego de leer esta guía haya podido comprender de manera sencilla todo lo relacionado a la protección de nuestros datos personales. Es importante que entendamos y otras personas también conozcan sobre el tema; pues mientras más informados estemos, más fácil será pedir que se respeten nuestros derechos. Por ello, le invitamos a que comparta el conocimiento ya adquirido con sus familiares, amigos, vecinos, compañeros de trabajo, entre otros. Para ello, puede utilizar esta guía como base para concientizar, hablar y hasta cuestionar a las autoridades y empresas sobre el tratamiento de nuestros datos.

Contacto

Verónica Arroyo
Asociada de Políticas Públicas para América Latina | veronica@accessnow.org

Roxana Pérez Del Castillo y Eliana Quiroz
Fundación Internet Bolivia.org | info@internetbolivia.org

Para más información por favor visite

www.accessnow.org
www.internetbolivia.org

accessnow

Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

https://www.accessnow.org