“UNIVERSIDAD MAYOR DE SAN ANDRÉS”

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

TRABAJO DIRIGIDO

(PARA OPTAR AL TÍTULO ACADÉMICO DE LICENCIATURA EN DERECHO)

“LA NECESIDAD DE PROTEGER LOS DATOS PERSONALES IMPLEMENTANDO EN LA LEGISLACIÓN BOLIVIANA, UNA LEY DE DECLARACIÓN RESUMIDA DE TÉRMINOS Y CONDICIONES DE SERVICIO DE USO DE PLATAFORMAS EN INTERNET”

EGRESADO: **HUANCA SORUCO PAOLO ANTONIO**

TUTOR: **VILLENA SUCRE EULOGIO**

LA PAZ - BOLIVIA

2023

DEDICATORIA:

“A Madelen y Jhoan, al infinito y más allá.”

AGRADECIMIENTO:

A mis padres Rosmery y Johon, por el apoyo, el esfuerzo, y la confianza que me dieron todo este tiempo.

A mi Tutor Dr. Eulogio Villena Sucre, por brindarme su colaboración desinteresada, sus conocimientos, guía, paciencia, y tiempo en el desarrollo de esta monografía.

Por último, a mi querida Alma Mater, Universidad Mayor de San Andrés y a la Carrera de Derecho por ofrecerme la mejor formación académica y abrirme las puertas de conocimiento y crecimiento profesional y humano.

INDICE

LA NECESIDAD DE PROTEGER LOS DATOS PERSONALES IMPLEMENTANDO EN LA LEGISLACIÓN BOLIVIANA, UNA LEY DE DECLARACIÓN RESUMIDA DE TÉRMINOS Y CONDICIONES DE SERVICIO DE USO DE PLATAFORMAS EN INTERNET

INTRODUCCIÓN.

Si te dijera que tu celular te espía, ¿qué pensarías? Las empresas que poseen aplicaciones de mensajería recopilan todos los datos que proporcionas mientras conversas con alguien a través de estas aplicaciones, y luego los analizan para mostrarte publicidad según tus intereses. Aunque no hayas buscado activamente esta publicidad, simplemente con el uso de internet, mensajes, aplicaciones o plataformas de redes sociales, o incluso mientras ves un video, estás proporcionando información que es recopilada por algoritmos de inteligencia artificial, esta información es conocida como metadatos. Estos algoritmos analizan tus gustos y te muestran publicidad que coincide con tus preferencias, a veces de manera tan sutil que ni siquiera lo percibes como publicidad. Además, estos algoritmos están diseñados para que pasemos el mayor tiempo posible en las redes sociales, mostrándonos contenido que nos identifica y nos mantiene en estas plataformas. Como su principal negocio es la venta de publicidad, cuanto más tiempo pasemos en estas plataformas, más ingresos obtendrán.

Estos casos han sido revelados en los últimos años y han llevado a la creación de leyes que protegen la privacidad en internet en varias partes del mundo. En esta monografía, se aborda el problema de la protección de los datos personales en internet, regulando el uso de estos datos mediante la creación de una ley que establezca los términos y condiciones de uso de servicios y aplicaciones de plataformas virtuales en internet y que muestre de manera clara y concisa todas las cláusulas que regulan el uso, almacenamiento y comercialización de estos datos personales.

METODOLOGÍA

1. PLANTEAMIENTO DEL PROBLEMA

En los últimos años, el uso de teléfonos móviles y redes sociales ha permitido que personas en todo el mundo compartan mucha información personal en internet. Desafortunadamente, esta información a menudo es utilizada para fines publicitarios y el tráfico de datos sin el conocimiento o consentimiento de los usuarios. Esta situación es especialmente preocupante en el Estado Plurinacional de Bolivia, donde no existen normas que protejan los datos personales y la privacidad en internet, lo que hace que nuestra población sea vulnerable a estas circunstancias.

2. PROBLEMATIZACION

Todos los días utilizamos internet para comunicarnos, comprar en línea y entretenernos a través de servicios de mensajería, redes sociales, plataformas de video y otras aplicaciones. Aunque podemos obtener beneficios de estas herramientas, también pueden ser perjudiciales si no las usamos de manera consciente y moderada.

Al compartir información personal en redes sociales, como fotos de eventos o actividades, estamos proporcionando datos que pueden ser almacenados en un repositorio privado conocido como "la nube" por empresas como Facebook. Estas empresas luego pueden comercializar nuestra información sin nuestro conocimiento o consentimiento.

Un problema importante es que a menudo ignoramos los términos y condiciones de uso (TyC) de las aplicaciones que utilizamos. Estos TyC son como un contrato que establece las cláusulas para el uso de las aplicaciones. Al aceptar estos términos sin leerlos, puede que estemos dando permiso para que nuestros datos personales sean comercializados o utilizados de otra manera.

Además, la falta de regulación y leyes que protejan los datos personales y la privacidad en internet en el Estado Plurinacional de Bolivia hace que nuestra población sea vulnerable a la utilización indebida de nuestra información personal.

Por lo tanto, es importante abordar este problema para proteger la privacidad y los datos personales de los usuarios de internet en el Estado Plurinacional de Bolivia.

2.1. FORMULACIÓN DEL PROBLEMA

- A menudo usamos plataformas y aplicaciones en nuestros dispositivos móviles sin tener en cuenta la información que compartimos o el tiempo de uso de estas herramientas. Esto puede llevar a un uso indiscriminado y poco consciente de internet.
- Las empresas de internet que proporcionan plataformas y aplicaciones pueden comercializar nuestros datos personales sin nuestro conocimiento o consentimiento. Es importante ser conscientes de esto y proteger nuestra información personal en internet.
- A menudo ignoramos los términos y condiciones de uso de las aplicaciones que utilizamos y no somos conscientes de las condiciones que estamos aceptando al hacer uso de ellas. Es importante leer y comprender los términos y condiciones de uso para proteger nuestra privacidad y evitar cualquier uso indebido de nuestra información personal.
- En Bolivia, la legislación nacional no regula la distribución de aplicaciones en internet ni las cláusulas de los términos y condiciones de uso proporcionadas por empresas de internet. La legislación existente es insuficiente para proteger la privacidad y los datos personales de los usuarios de internet en la mayoría de los casos. Es necesario abordar esta carencia legislativa para garantizar la protección de nuestra información personal en internet.
- En Bolivia, no existen prohibiciones para que las empresas que brindan servicios en territorio boliviano comercialicen nuestros datos personales sin

nuestro consentimiento. Es necesario implementar medidas que protejan nuestra privacidad y eviten el uso indebido de nuestra información personal por parte de estas empresas.

3. DELIMITACIÓN

3.1. DELIMITACIÓN TEMATICA.

En este trabajo, nos centraremos en la necesidad de proteger los datos personales a través de la implementación de una ley de declaración resumida de términos y condiciones de servicio de uso de plataformas en internet en Bolivia. Esta ley tendrá implicaciones en el derecho informático, debido a la relación directa de la ciencia informática con el derecho informático, y también en el derecho penal, debido a las incursiones en delitos informáticos como la violación de privacidad, particularmente en internet. Además, consideraremos el derecho civil, ya que tanto personas naturales como jurídicas pueden realizar contratos por internet, como es el caso de la aceptación de términos y condiciones de uso de aplicaciones. En resumen, nuestra delimitación temática incluirá estas tres ramas del derecho debido a su relación con nuestro tema principal.

Problema clave: La ausencia de una regulación sobre la protección de datos personales, así como la falta de regulación de los términos y condiciones de servicio de uso de plataformas en internet, por parte del Estado Plurinacional de Bolivia conlleva a que la población boliviana corra el riesgo de no sentirse protegida por el estado al proporcionar información personal durante el uso de plataformas digitales y no tener las garantías jurídicas necesarias para la protección de estos datos personales.

CRITERIO	RESPUESTA
¿Qué?	Inexistencia de ley de protección de datos personales, y términos y

	condiciones de servicio de uso de aplicaciones muy extenso y poco comprensible.
¿Quiénes?	Población boliviana de todas las edades
¿Dónde?	Estado plurinacional de Bolivia
¿Cuándo?	Actualidad

Delimitación del tema final: La necesidad de proteger los datos personales implementando en la legislación boliviana, una ley de declaración resumida de términos y condiciones de servicio de uso de plataformas en internet

3.2. DELIMITACIÓN TEMPORAL.

Nuestra investigación abarcará particularmente el último año, desde enero hasta diciembre de 2022. Se tomará en cuenta este período debido al incremento significativo en la problemática de la protección de datos personales en internet observado en este lapso, especialmente en relación con el uso cada vez más común de teléfonos celulares inteligentes y las plataformas y aplicaciones que utilizamos en ellos.

3.3. DELIMITACIÓN ESPACIAL.

Para abordar el problema de la protección de los datos personales en internet en Bolivia, nuestra investigación se enfoca en el área geográfica de la Ciudad de La Paz y su región. Aunque este problema es relevante en todo el país, consideramos que La Paz, como centro político y económico del país, es un lugar adecuado para analizar las leyes y regulaciones existentes, así como para recopilar datos y opiniones de usuarios de internet. Además, la gran mayoría de las empresas de internet que operan en Bolivia tienen su sede central en La Paz,

por lo que es un lugar clave para entender cómo estas empresas utilizan y protegen los datos personales de sus usuarios.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

A través de la realización de esta investigación, se pretende proponer a los legisladores y a la población en general, una ley de declaración resumida de términos y condiciones de servicio de uso de plataformas en internet que proteja la privacidad y los datos personales de los usuarios en internet en el Estado Plurinacional de Bolivia. Para ello, se presentarán argumentos teóricos, jurídicos y sociales que justifiquen la necesidad de esta ley.

4.2. OBJETIVOS ESPECÍFICOS

- Determinar el grado de concientización de la población sobre la importancia de leer y comprender los Términos y Condiciones de uso de las aplicaciones y plataformas en internet antes de aceptarlos, por medio de una encuesta abocada a usuarios de plataformas de internet.
- Estudiar la existencia y alcance de leyes que regulen la recopilación y comercialización de datos personales en internet en el Estado Plurinacional de Bolivia.
- Analizar los efectos que tiene la falta de regulación sobre la privacidad y seguridad de los datos personales de los usuarios de internet en Bolivia.

5. JUSTIFICACIÓN

Es necesaria la implementación de una nueva ley de declaración resumida de términos y condiciones de servicio de uso de plataformas en internet en Bolivia para proteger a la población y sus datos personales. Esta ley debería incluir cláusulas que expongan las condiciones de uso y recopilación de datos personales y restrinjan el abuso de las mismas por parte de las empresas de

internet. La implementación de esta ley también podría servir como una medida preventiva para evitar delitos informáticos como la violación de privacidad en internet. Por lo tanto, la elaboración de esta monografía es de gran importancia para proporcionar fundamentos teóricos, jurídicos y sociales que puedan ser utilizados para la implementación de esta ley y proteger los derechos de la población boliviana.

6. METODOLOGÍA.

6.1. MÉTODO GENERAL.

Método deductivo. El método utilizado para analizar el problema de la falta de transparencia y protección de los datos personales en las plataformas en internet será el método deductivo. A través de un análisis de la legislación existente y de estudios previos sobre el tema, se buscará identificar los problemas y vacíos legales en cuanto a la declaración de términos y condiciones de servicio y la protección de los datos personales. A partir de esta revisión, se propondrá una posible solución mediante la elaboración de un proyecto de ley de Declaración Resumida de Términos y Condiciones de Servicio de Uso de Plataformas en Internet, que busque garantizar la transparencia y la protección de los datos personales de los usuarios. Además, se realizará un análisis comparado con la legislación de otros países como México, Perú, Chile y Ecuador, para evaluar las similitudes y diferencias en cuanto a la regulación de estos temas.

6.2. MÉTODOS ESPECÍFICOS

Método Analítico. Con este método, analizaremos y evaluaremos la situación actual de la protección de los datos personales en internet en nuestro país y en comparación con la legislación de otros países, identificando las fortalezas y debilidades de las leyes existentes y proponiendo posibles soluciones para mejorar la protección de los datos personales en internet.

Método Comparativo. Utilizaremos este método para comparar la legislación existente en nuestro país con la de otros países, identificando similitudes y diferencias en cuanto a la protección de los datos personales en internet y utilizando esta información como referencia para proponer soluciones a los problemas identificados en nuestro país.

6.3. TÉCNICAS APLICADAS.

- *En primer lugar, se aplicó la técnica de recopilación de información para obtener los datos necesarios para el estudio. Esta técnica incluyó la búsqueda de información relevante en fuentes como libros, artículos científicos, estudios y documentos oficiales relacionados con el tema de la protección de datos personales en internet.*
- *En segundo lugar, se aplicó el análisis documental para estudiar y clasificar la información recopilada. Este análisis permitió identificar las principales tendencias y problemáticas en torno a la protección de datos personales en internet, así como las soluciones y propuestas existentes.*
- *Por último, se aplicó la técnica de encuestas para conocer la opinión de los usuarios de internet sobre la protección de sus datos personales y su relación con las plataformas en línea. Esta técnica permitió obtener una visión más cercana de las preocupaciones y necesidades de los usuarios en relación con la privacidad y seguridad en internet.*

CAPÍTULO I

MARCO HISTORICO

1. Antecedentes históricos relacionados a la protección de datos.

En Bolivia, aunque no existe una ley específica para la protección de datos personales, se cuenta con la garantía de habeas data, establecida en el “artículo 23 de la Constitución de 2004”[1]. El habeas data es un recurso legal que permite a las personas ejercer su derecho a conocer, actualizar, rectificar y suprimir información que se refiera a su persona, así como también a oponerse al tratamiento de sus datos personales. Este recurso se enfoca en proteger los derechos fundamentales de acceso a la información y autodeterminación informativa, es decir, la protección de los datos personales.

Esta garantía surge como respuesta al aumento del uso de tecnologías de la información y comunicación que recopilan y procesan grandes cantidades de datos personales, y que, si no son protegidos adecuadamente, pueden poner en riesgo la privacidad de las personas. Con la nueva Constitución de 2009, esta garantía cambió de denominación a "acción de protección de privacidad"[2] en relación a la confidencialidad de la información.

Sin embargo, a pesar de la existencia del habeas data, Bolivia aún no cuenta con una regulación completa y específica en materia de protección de datos personales. Aunque se han tomado algunas medidas para regular el tratamiento de los datos personales, como la promulgación de la “Ley 164, Ley General De Telecomunicaciones en el año 2011”[3], y la “Ley de Ciudadanía Digital en 2017”[4], estas normas aún no abarcan completamente todos los aspectos relacionados con el tratamiento de los datos personales en el contexto de internet.

En resumen, Bolivia ha tomado medidas para proteger la privacidad y la protección de datos personales, pero estas medidas no han sido suficientes para

[1] Congreso Nacional de Bolivia, 2004, Pág. 12.
[2] Congreso Nacional de Bolivia, 2009, Pág. 32.
[3] Asamblea Legislativa Plurinacional, 2011.
[4] Asamblea Legislativa Plurinacional, 2018.

abordar las preocupaciones actuales sobre la privacidad en línea y la protección de datos personales en plataformas en línea. Por lo tanto, se hace necesaria la implementación de una ley específica que regule la protección de datos personales en relación a las plataformas en internet, para garantizar la privacidad y seguridad de los datos personales de los ciudadanos bolivianos. La implementación de una ley de declaración resumida de términos y condiciones de servicio podría ayudar a abordar estas preocupaciones y garantizar que los usuarios de plataformas en línea en Bolivia tengan un mayor control sobre sus datos personales. Es importante considerar la importancia de actualizar y adaptar las regulaciones a las nuevas tecnologías y tendencias para garantizar una adecuada protección de los derechos fundamentales de las personas.

2. Antecedentes históricos relacionados a los Términos y Condiciones

Los términos y condiciones comenzaron a aparecer en los contratos comerciales a finales del siglo XIX, pero su uso se generalizó con el surgimiento de la economía de consumo y la venta de bienes a distancia en el siglo XX.

> "El derecho es un fenómeno social, que desde la época romana con el surgimiento de los contratos en el Corpus Iuris Civilis de Justiniano, con el cual en este tiempo es parte de las legislaciones del Civil Law, así como el Digesto donde en uno de sus textos atribuidos a Ulpiano, donde cita que hay contrato donde hay cambio de promesas o promesas cambiadas, pero en otro texto se dice, en oposición al primero que hay contrato donde hay cambio de una prestación por una promesa do ut des. Messineo dice que el contrato ha sido un paradigma general abstracto, susceptible de acoger cualquier contenido".
>
> ***(Rojina, V., 2015, Pág. 17)***

A medida que las transacciones comerciales se volvieron más complejas y se incluyeron productos y servicios nuevos y sofisticados, los términos y

condiciones se convirtieron en una herramienta esencial para regular y definir las obligaciones y responsabilidades de las partes involucradas en una transacción.

Con el surgimiento de Internet a finales del siglo XX, los términos y condiciones se convirtieron en una herramienta esencial para regular el uso de las plataformas en línea. Los términos y condiciones se utilizan para establecer las reglas para el uso de un sitio web o una aplicación, incluyendo las políticas de privacidad y las reglas para el uso de datos personales.

- En la década de 1990 y principios de 2000, con el auge de internet y las plataformas en línea, los términos y condiciones de servicio comenzaron a ser utilizados como una forma de regular el uso de estas plataformas. Sin embargo, en Bolivia no existían regulaciones específicas para regular los términos y condiciones de servicio en plataformas en línea.
- En los últimos años, con la creciente preocupación sobre la privacidad en línea y la protección de datos personales, ha habido un aumento en la conciencia sobre la importancia de leer y comprender los términos y condiciones de servicio antes de utilizar una plataforma en línea. Sin embargo, en Bolivia, la falta de regulaciones específicas para regular los términos y condiciones de servicio en plataformas en línea sigue siendo un problema.
- En algunos países, se han implementado regulaciones para garantizar que los términos y condiciones de servicio sean fácilmente accesibles y comprensibles para los usuarios. Sin embargo, en Bolivia, no existen regulaciones similares.

CAPÍTULO II

MARCO CONCEPTUAL

En este capítulo nos enfocaremos en presentar un marco conceptual que servirá como base para el análisis y la discusión de los problemas relacionados con la privacidad y la protección de datos personales en plataformas en línea en Bolivia.

En primer lugar, se describirán los conceptos fundamentales de privacidad y protección de datos personales, incluyendo su definición, y alcance.

Luego, se presentarán los conceptos relacionados con la privacidad en línea y la protección de datos personales en plataformas en línea, incluyendo la recolección y el uso de datos personales, el almacenamiento y la seguridad de los datos, y la compartición de datos con terceros todo esto sintetizado en unos pocos conceptos.

Por último, se presentarán el concepto de términos y condiciones, con el objetivo de evaluar la efectividad de las medidas existentes.

La información presentada en este capítulo será esencial para comprender los conceptos y entender de una forma más sencilla el contenido presentado en la monografía y de ese modo comprender las soluciones planteadas para mejorar la privacidad y protección de datos personales en plataformas en línea en Bolivia.

1. Privacidad:

La privacidad se refiere al derecho de las personas a controlar su información personal y a mantener su intimidad. Incluye el derecho a decidir qué información se comparte, con quién y en qué circunstancias. La privacidad también incluye el derecho a tener acceso a información sobre uno mismo y a corregir cualquier información incorrecta. La privacidad es un derecho fundamental que protege a las personas de la intrusión en sus vidas privadas. La privacidad se refiere a "el derecho de las personas a controlar su propia información personal, incluyendo la forma en que se recolecta, utiliza, protege

y distribuye"[5]. La privacidad en línea se refiere específicamente a la privacidad en el contexto de Internet y las tecnologías digitales.

2. Dato personal:

Pero ¿Concretamente qué son los datos personales? Vamos a deconstruir la palabra para con ello elaborar una definición de fácil comprensión.

Etimológicamente hablando:

2.1. Dato:

La palabra dato tiene su origen etimológico en el término latino "*Datum*" que inicialmente significaba "*lo dado*" y posteriormente se le atribuyo el significado de "i*nformación*" o "*hechos*".[6]

2.2. Persona:

La palabra persona viene del latín "*Persona",* esta deriva del Etrusco "*Phersu"* y esta a su vez del Griego "*Prosopon"*, que significa "*Mascara"*[7] Personare hace referencia a las máscaras que utilizaban en los teatros contemporáneos a la época griega, y se las describía así por el juego de palabras para sonar, per sonare, debido a que estas mascaras amplificaban el volumen de voz de los actores, se le atribuyo la definición de persona a la interpretación que realizaban los actores. Se le atribuyo la definición de persona a la interpretación que realizaban los actores. Posteriormente fue popularizada la definición de "individuo de la especie humana"[8]

En pocas palabras podemos decir que:

- *Dato personal = Información propia*

3. Protección de datos personales:

La protección de datos personales se refiere a la regulación de la recolección, almacenamiento, uso y divulgación de información personal. Esto incluye

[5] Comisión nacional de derechos humanos UNESCO, 2018, pág. 55
[6] Duque, 2021, pág. 1
[7] Duque, 2021, pág. 1
[8] Oxford Lenguajes, 2022, pág. 2

medidas para garantizar que la información personal se maneje de manera segura y confidencial, y que se respeten los derechos de las personas a controlar su información personal.

La protección de datos personales, por otro lado, se refiere a las medidas que se toman para garantizar que los datos personales de las personas sean tratados de manera legal, justa y transparente. La protección de datos personales refiere a:

> "el conjunto de medidas técnicas y organizativas que garantizan la seguridad de los datos personales y evitan su alteración, pérdida, tratamiento y acceso no autorizado, garantizando así la confidencialidad, integridad y disponibilidad de los mismos".
> ***(A.E.P.D., 2022, Pág. 1)***

Es importante destacar que estos conceptos son fundamentales en el mundo actual donde la tecnología ha permitido una mayor recolección y almacenamiento de datos personales, lo que a su vez ha generado preocupaciones sobre la privacidad y la protección de estos datos.

4. NUBE:

Es el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, servidores, bases de datos, redes y software. En lugar de depender de un servicio físico instalado, se tiene acceso a una estructura donde el software y el hardware están virtualmente integrados.[9]

> “Una nube es un sistema de computación en la nube que ofrece a los usuarios el acceso remoto a una infraestructura compartida de computación a través de Internet. Esto permite a los usuarios acceder a aplicaciones y servicios, así como a datos y almacenamiento sin tener que almacenar localmente los recursos”.
>
> ***(Gaudin, S. 2019, Pág. 1)***

[9] Wikipedia, 2018, pág. 1

5. PLATAFORMA VIRTUAL:

Una plataforma virtual es un sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet. Esto quiere decir que, al utilizar una plataforma virtual, el usuario no debe estar en un espacio físico determinado, sino que sólo necesita contar con una conexión a la Web que le permita ingresar a la plataforma en cuestión y hacer uso de sus servicios.[10]

> "Una plataforma virtual es un sistema de computación en la nube que permite a los usuarios interactuar entre sí, compartir recursos y ofrecer servicios. Esta forma de computación permite a los usuarios conectar, intercambiar información y compartir recursos sin tener que almacenar localmente los recursos".
> ***(Microsoft, plataforma virtual, 2019, Pág. 1)***

6. TÉRMINOS Y CONDICIONES:

Son un conjunto de conceptos legales definidos por el propietario de un servicio web, los cuales rigen las actividades de los visitantes o usuarios de ésta.[11]

> "Los términos y condiciones son un conjunto de reglas y regulaciones que los usuarios de un servicio o producto deben aceptar antes de poder tener acceso a él. Estas reglas y regulaciones sirven para asegurar que todos los usuarios entiendan y acepten los límites y responsabilidades relacionados con el uso de los servicios".
> ***(Microsoft, términos y condiciones, 2019, Pág. 1)***

[10] Pérez, 2013, pág. 1
[11] Campos, 2018, pág., 2.

CAPITULO III
MARCO TEÓRICO

1. Dato Personal

Cuando hablamos de datos personales, lo primero que nos viene a la mente son aquellos datos que nos piden en el momento de recabar nuestra cédula de identidad, como nuestro nombre, dirección del domicilio y fecha de nacimiento. Un dato es básicamente igual a información, ya sea simple o compleja, y puede ser de carácter demográfico, financiero o estadístico, entre otros.

En términos estrictos, un dato personal es igual a la información acerca de una persona, como su nombre, número de teléfono, correo electrónico, país, dirección y hasta sus antecedentes jurídicos o historial médico, por mencionar algunos ejemplos importantes.

> "Ahora bien, la doctrina jurídica profundizó este criterio y en la actualidad no únicamente son datos particulares las informaciones que identifican a una persona de forma directa sino además esas que la realizan identificable tras un estudio subsiguiente. Esto último desea mencionar que hay informaciones que de forma indirecta se relacionan a una persona y que así mismo las vamos a tener en cuenta datos individuales. Ejemplo de esto son las imágenes de las cámaras de videovigilancia o la localización GPS."
>
> ***(León. 2018, Pág. 6)***

En el ámbito jurídico, los datos personales son considerados como información confidencial y su uso está regulado por leyes y normativas específicas. Por ejemplo, en la Unión Europea, la normativa de protección de datos personales se regula por el "Reglamento General de Protección de Datos"[12] (GDRP). Este reglamento establece las reglas para el tratamiento de los datos

[12] Union Europea, 2018.

personales y establece un conjunto de derechos para los titulares de los datos, como el derecho a la información, el derecho a la portabilidad de los datos, el derecho a la limitación del tratamiento y el derecho a la eliminación de los datos.

En conclusión, los datos personales son información importante y su uso está regulado por leyes y normativas específicas, y es necesario establecer regulaciones y leyes que protejan los derechos de los usuarios en cuanto a su privacidad y protección de datos personales.

2. Tipos de datos

2.1. Los metadatos:

La definición más concreta de los metadatos es qué son "***datos acerca de los datos*** y sirven para suministrar información sobre los datos producidos."[13] Los metadatos consisten en información que caracteriza datos, describen el contenido, calidad, condiciones, historia, disponibilidad y otras características de los datos.

Dicho de otra manera, son los datos obtenidos al analizar o examinar otro grupo de datos, vamos a plantear dos ejemplos, imaginen que compramos un kilo de mayonesa, dentro de los datos observamos el nombre del producto "mayonesa kriss", el nombre de la empresa "industrias venado", y un código de barras, además de otros detalles descritos en la etiqueta, en ese sentido, los metadatos se considerarían aquellos datos alojados en la etiqueta del producto, siendo estos el nombre del producto, la lista de ingredientes y aditivos, el contenido neto, instrucciones para su conservación, permisos de SENASAG y el ministerio de salud (en caso de alimentos) la fecha de vencimiento, país de origen entre otros, y ahora analizando el código de barras, si queremos leer su información, nos valemos de cualquier app de lectura QR en nuestro celular y escaneamos el código de barras, y ahí también encontraremos más metadatos, estos ya, de interés para las fábricas o tiendas de distribución, como el código de lote de producción, la fecha de producción, el código del producto, entre otros.

[13] Gobierno de Perú, 2021, Pág. 3.

Cuando tu navegas por internet utilizas un navegador, usaremos de ejemplo *Chrome*, posterior a ello un motor de búsqueda, *Google.com* revisamos nuestro correo electrónico *Gmail,* cortesía de Google, abrimos una nueva pestaña y entramos a una red social, *Facebook.com*. mientras navegamos en Facebook, le damos clic a alguna foto o likes a alguna publicación.

Todas estas interacciones, todos los clics y los tiempos de visualización quedan registrados bajo el nombre de historial *de navegación* y *registro de actividad*, podemos ver nuestro registro de actividad en nuestro navegador y borrar nuestro historial de navegación, pero ¿es posible acaso, evitar que se haga una copia de seguridad de toda esta información almacenada en los servidores de estas megaempresas?

> "Si bien dichos datos por sí solos no identifican a una persona, un estudio grupo de los mismos sí podría realizarlo debido a que nos ofrece información fundamental y descriptiva sobre una persona. Ejemplificando, las redes sociales producen registros de visitas, (likes), compras online, entre otros. Al examinar y aprender dichos datos tenemos la posibilidad de conocer los gustos y preferencias de los usuarios de aquellas redes sociales; deducir donde viven, trabajan, van de vacaciones y quiénes son sus parientes y amigos."
>
> ***(Arroyo, 2021, Pág. 4)***

2.2. Datos disociados o anonimizados:

Existen otro tipo de datos, que, debido a la forma en la que son conseguidos o procesados, reciben otras denominaciones. "En este conjunto poseemos a los datos anónimos y anonimizados o disociados. Dichos son datos que en inicio permiten detectar a personas sin embargo que debido a mecanismos de anonimización o disociación terminan teniendo escasa o nula interacción con el

individuo que previamente identificaban"[14]. Estos procesos (según León Coronado) son usados para estudios y análisis científicos, ejemplificando en indagaciones científicas donde, para defender la identidad de los individuos que participaron en el análisis, se remueve de los conjuntos de datos particulares la información que posibilite la identificación.

2.3. Datos de índole delicado o sensible:

¿Qué es la información sensible?

Javier berciano, coordinador de la empresa de protección de datos Red Seguridad, define la información sensible como "Aquella información, así definida por su propietario, cuya revelación, alteración, pérdida o destrucción puede producir daños importantes a la organización propietaria de la misma"[15].

Dentro del conjunto general de datos personales hay un tipo de datos que por su contenido son llamados datos sensibles o propensos. La información que otorgan aquellos datos es delicada y de carácter íntimo. Tenemos la posibilidad de detectar esta clase de datos de forma fácil pues son esos que preferimos conservar en reserva y que tienen la posibilidad de provocar perjuicios graves si son difundidos o mal usados. Ejemplos de dichos datos susceptibles son los concernientes a la salud, la genética, la religión, las preferencias políticas, y hasta esos 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 solicitado anteriormente su consentimiento o autorización, esto orilló a esta persona a la depresión y a otros efectos perjudiciales en su historia.[16]

3. ¿Para qué sirven tus datos personales?

En muchas ocasiones, nos encontramos con que la publicidad que recibimos en internet está relacionada con temas que hemos conversado ese día

[14] León. 2018, Pág. 13
[15] Berciano. 2012, pág. 2
[16] León. 2018, Pág. 14

o con búsquedas que teníamos en mente pero que aún no habíamos realizado. Esto nos lleva a preguntarnos si realmente estamos siendo vigilados por plataformas como Facebook, Google, WhatsApp o incluso por nuestro teléfono móvil. Aunque podamos pensar que no importa que nos vigilen ya que no tenemos nada que esconder, la verdad es que nuestros datos son muy valiosos para las empresas.

Los datos no solo sirven para averiguar nuestros gustos, sino también para ofrecernos productos que no necesitamos, que no nos gustan o incluso que odiamos pero que se puede convertir en la próxima compra, o un cambio a una nueva idea política si te llega en el momento justo.

3.1. Redes sociales y su participación en la recopilación de datos personales

Las redes sociales se aprovechan de nuestros hábitos y sesgos cognitivos para mantenernos en ellas el mayor tiempo posible, pero lo que realmente estamos entregando es información comportamental, patrones de comportamiento, pensamientos, gustos y odios, e incluso cosas que aún no sabemos que pensamos o sentimos. Las inteligencias artificiales manejan volúmenes de datos inabarcables para el cerebro humano y ven cosas que el ojo humano no podría detectar, lo que les permite manipular nuestro comportamiento de manera subconsciente.

3.2. En que se utilizan tus datos personales

Ahora, imagínate cuanta información personal puedes plasmar ya sea en tu celular, en tus interacciones sociales diarias, recuerda que tan solo para crear una cuenta en una plataforma de servicio de internet (Facebook, TikTok, etc.) te piden tres datos personales muy importantes, nombre completo (real), fecha de nacimiento, y Correo electrónico, ya si hablamos de este último, al momento de crear una cuenta de Gmail. Te piden muchos otros más, pero el más relevante es la verificación de tu número de teléfono que si no lo proporcionas ya de plano, no llegarías a crear la cuenta, hay varias formas de saltarse estos pasos, o manipular la veracidad de la información a proporcionar, pero si pretendes crear una cuenta

para tu uso estrictamente personal y al menos a mediano plazo, claramente brindaras tus datos personales de manera correcta, esto debido a que si por alguna casualidad pierdes tu cuenta, la única manera de recuperarla es proporcionando los datos personales anteriormente mencionados.

3.3. ¿Dónde se almacenan tus datos personales?

Esta idea se convierte en algo de dominio popular ya que todos alguna vez han oído hablar de la nube, es un término muy popular el decir que cuando subimos algo a internet se almacena en la nube, pero ¿Qué es la nube?

3.3.1. La nube.

El uso coloquial de la palabra nube viene de los esquemas de flujos de datos utilizados por los programadores que utilizan durante el desarrollo de una red en los esquemas de telefonía, y se utilizaba la iconografía, posteriormente se hizo popular y se denominó nube al espacio de almacenamiento “virtual” al que podemos acceder, para almacenar nuestra información personal, tanto pública como privada.

> “es un término que se utiliza para describir una red mundial de servidores, cada uno con una función única. La nube es una red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema. “
> ***(Microsoft, Nube. 2022, pág. 3.)***

La nube informática es un espacio tangible, de hecho, son miles de hectáreas de terreno esparcidas por todo el mundo, donde compañías de internet instalan sistemas de almacenamiento de datos con estricto control y monitorización frecuente, puesto que, si algo llegara a fallar, gran parte de los datos almacenados en estos espacios, llegarían a perderse. Estos servidores están diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios, como transmisión de vídeos, correo web, software de ofimática o medios sociales. En lugar de acceder a archivos y datos desde un

equipo personal o local, accedes a ellos online desde cualquier dispositivo conectado a Internet, es decir, la información está disponible dondequiera que vayas y siempre que la necesites.

3.4. ¿Si yo subo algo a la nube, alguien me lo puede leer?

Cuando subimos algo a una red social, alguien lo puede ver, dependiendo de la configuración de privacidad de la red social utilizada. Sin embargo, existen aplicaciones como Dropbox o Google Drive que actúan como discos duros virtuales, donde podemos subir información personal y estos se enlazan a través de un correo electrónico. Por ejemplo, Google Drive nos otorga un espacio gratuito de 14 GB en la nube y 1 GB en el caso de Dropbox, siendo estos espacios de almacenamiento ampliables mediante una suscripción mensual. Estas aplicaciones cumplen la función de espacio de almacenamiento virtual donde podemos subir nuestra información personal, ya sea mediante aplicaciones automáticas o mediante el uso de nuestra computadora o celular.

El problema radica en que estas aplicaciones pueden ser manipuladas y existe la posibilidad de que se obtenga nuestra información personal de ellas. Esto puede ser debido a un fallo humano, como el caso de manipular nuestros correos electrónicos mediante programas espía para averiguar nuestras contraseñas, o debido a algún tipo de vulneración que permita hackear correos electrónicos masivos de empresas como Dropbox y obtener acceso libre a nuestra información personal.

En conclusión, aunque existe la posibilidad de que nuestra información sea obtenida mediante medios lícitos e ilícitos, es importante considerar qué información es relevante e importante para las empresas. Desde el ámbito jurídico, es posible obtener información personal de clientes, la cual puede ser delicada y afectar la preparación de casos o determinaciones en un acontecimiento jurídico. Sin embargo, si consideramos la información compartida por un "ciudadano de a pie", como mensajes con familiares o compartir fotos ocasionales, esta

información puede ser considerada como menos relevante para las empresas, pero más relevante para el individuo.

4. Términos y condiciones de servicios en internet

Ahora vamos a plantear el siguiente ejemplo. -*En el momento en el que estamos creando una cuenta en alguna plataforma virtual o aplicación de internet, y luego de que nos pidan una serie de datos personales, no sale la pantalla de Términos y condiciones, con un mensaje similar al siguiente "¿usted acepta los términos y condiciones de servicio del uso de esta plataforma?", dónde usualmente solo aparece un recuadro que dice sí acepto y una pestaña que te redirige a una página o un documento PDF con decenas y decenas de páginas, y, en el caso de que no quieras aceptar estos términos y condiciones de uso de servicios no podrás acceder a usar dicha aplicación, en cierto modo esto es perjudicial ya que muchas personas requerimos utilizar de algunos servicios o plataformas virtuales, pero las compañías proveedoras de estos servicios de internet son muy drásticos con la declaración de estos términos y condiciones de servicio*- y esto solo por mencionar un ejemplo ya que en la circunstancia en la que aceptemos estos términos y condiciones de uso de servicios sin siquiera haber revisado este contrato podríamos estar aceptando qué se utilicen nuestros datos personales para fines en los cuales no estamos de acuerdo Como por ejemplo la divulgación y/o comercialización de estos, pero ¿qué son estos términos y condiciones de uso de servicios?

4.1. Términos y condiciones

"*Términos y Condiciones* es el documento que rige la **relación contractual entre el proveedor de un servicio y el usuario"**.[17] En internet, este tipo de documento también es conocido como "Condiciones de servicio", "Condiciones de uso", "Acuerdo de licencia de usuario final"

En primer lugar, es importante mencionar que los Términos y Condiciones de servicio son el contrato mediante el cual el titular de la plataforma virtual o

[17] Rafaelle. 2012, Pág. 2.

aplicación en internet, establece las condiciones de uso de su servicio. Estas condiciones son unilaterales, lo que significa que, si quieres utilizar los servicios de esa plataforma virtual, aplicación o página web, debes aceptarlas.

En segundo lugar, cuando aceptamos los términos y condiciones, otorgamos nuestro consentimiento para que la empresa almacene, procese, analice o utilice nuestros datos para distintos fines. El detalle de estos fines se encuentra en la especificación de los mismos en los términos y condiciones de uso de servicios.

Sin embargo, es muy frecuente que los usuarios de servicios y aplicaciones en internet no lean los términos y condiciones de servicios y uso de aplicaciones y plataformas en internet. Esto puede ser debido a que estos términos y condiciones son muy extensos o porque la terminología es rebuscada y difícil de comprender para la mayoría de los usuarios.

Por ello, se plantea como problema principal el desconocimiento y la falta de voluntad por parte de la población para leer los términos y condiciones de uso de servicios de aplicaciones en internet. Además, muchas empresas o entidades encargadas de estas aplicaciones y plataformas virtuales plasman estos términos de manera en que no solo favorezcan a estas empresas y salvaguarden sus derechos, sino que también puedan beneficiarse con los datos personales recopilados en estas plataformas virtuales.

Estos proveedores de servicios y aplicaciones de internet nos dicen que el uso de nuestros datos personales es estrictamente para verificar que, quien está creando una cuenta es una persona real.

Lo que no nos dicen es que cuando aceptamos los TyC somos posibles víctimas de filtración de datos personales, por parte de las empresas proveedoras de estos servicios siempre que así se estipule en estos TyC.

> “Los términos y condiciones … vulneran los derechos de las y los consumidores y limitan la responsabilidad de las empresas ante los daños que pudieran ocasionarse durante el servicio que brindan. La Subsecretaría de Acciones para la Defensa de las y los Consumidores imputó a las empresas de envío a domicilio Rappi, Glovo y PedidosYa por presuntas cláusulas abusivas en su contratación e información engañosa. Estas plataformas, en sus términos y condiciones, poseen cláusulas que resultarían abusivas ya que se deslindan de responsabilidades frente a las y los consumidores; asimismo, para acceder al servicio, se requiere que los clientes desistan de derechos que son irrenunciables y se encuentran garantizados constitucionalmente. En el caso de PedidosYa, entre otras cláusulas, la firma se deslinda de la responsabilidad por cualquier error que pudiera contener la plataforma, y se reserva la posibilidad de dar de baja o rechazar a los usuarios sin expresar motivos que, por lo menos, justifiquen la medida. Asimismo, en sus términos y condiciones se hace referencia a otros instrumentos, pero luego no se especifica cuáles son, por lo que la información a las y los consumidores es confusa.”
>
> ***(Gobierno de Argentina, 2020. Pág. 1)***

Por ello, se propone como solución la elaboración de un anteproyecto de ley enfocado en la elaboración de un resumen claro, conciso y lo más comprensible posible para el usuario final en territorio nacional. Este resumen debe ser publicado en la página principal de las aplicaciones y servicios de plataformas virtuales en internet, así como también al momento de crear una cuenta en estas plataformas virtuales. Además, es importante establecer artículos que esclarezcan y hagan público en el resumen de estos términos y condiciones, enfocados a qué tipo de datos personales son recabados, qué uso se les dará a esos datos y cuáles son las posibilidades de que sean almacenados o comercializados. De esta manera, se obligaría a las entidades de distribución de estas plataformas

5. ¿Por qué debo proteger mis datos personales?

Con respecto a la protección de datos personales, la esencia del objeto de protección va más allá del dato que circule en internet en sí, sino a la persona que proporcionó esos datos, dicho de otra forma, "*No se está hablando de proteger el dato, sino a la persona que está detrás del dato"* 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.

En 2012 un padre entro a una tienda de TARGET (un supermercado de U.S.A.) para reclamar a esta empresa, debido a que su hija menor de edad había recibido por correo electrónico, a su nombre, unos cupones de descuento de productos en oferta para mujeres embarazadas, pañales, toallitas, cunas, para una niña que ni siquiera había salido del colegio, el padre estaba bastante enojado, aludiendo que su correo electrónico incitaba a que su hija menor de edad quedase embarazada.

> "¡Mi hija recibió esto por correo!" él dijo. "Ella todavía está en la escuela secundaria, ¿y le estás enviando cupones para ropa de bebé y cunas? ¿Estás tratando de animarla a quedar embarazada?
> El gerente no tenía idea de qué estaba hablando el hombre. Miró el correo. Efectivamente, estaba dirigido a la hija del hombre y contenía anuncios de ropa de maternidad, muebles de guardería y fotografías de niños sonrientes. El gerente se disculpó y luego llamó unos días después para disculparse nuevamente.
> Sin embargo, por teléfono, el padre estaba algo avergonzado. "Tuve una conversación con mi hija", dijo. "Resulta que ha habido algunas actividades en mi casa de las que no he sido completamente consciente. Ella es debido en agosto. Te debo una disculpa."

> Lo que Target descubrió con bastante rapidez es que a la gente le asustaba que la empresa supiera de antemano sobre sus embarazos.
>
> “Si enviamos a alguien un catálogo y decimos, '¡Felicidades por tu primer hijo!' y nunca nos han dicho que están embarazadas, eso hará que algunas personas se sientan incómodas”, me dijo Pole. “Somos muy conservadores en cuanto al cumplimiento de todas las leyes de privacidad. Pero incluso si está siguiendo la ley, puede hacer cosas donde la gente se marea. ”
>
> Así que Target se volvió más sigiloso al enviar los cupones. La empresa puede crear folletos personalizados; en lugar de enviar a las personas con puntajes altos de embarazo libros de cupones únicamente para pañales, sonajeros, cochecitos los difunden de manera más sutil sobre:
>
> “Entonces comenzamos a mezclar todos estos anuncios de cosas que sabíamos que las mujeres embarazadas nunca comprarían, por lo que los anuncios de bebés parecían aleatorios. Pondríamos un anuncio de una cortadora de césped al lado de los pañales. Pondríamos un cupón para copas de vino al lado de la ropa infantil. De esa forma, parecía que todos los productos habían sido elegidos al azar.
>
> “Y descubrimos que mientras una mujer embarazada piense que no ha sido espiada, usará los cupones. Ella simplemente asume que todos los demás en su bloque recibieron el mismo correo para pañales y cunas. Mientras no la asustemos, funciona”.
>
> ***(Duhigg. 2012, Pág. 124.)***

Esta es la historia de como Target, unos grandes almacenes de Norteamérica, predicen el embarazo de una niña y le mandan ofertas antes de que esta se lo cuente a sus padres, gracias a un montón de datos y un modelo predictivo

5.1. ¿Para que el supermercado Target quiere saber si una mujer está embarazada?

La respuesta es que las personas tenemos unos hábitos de compra difíciles de modificar, pero cuando atravesamos una experiencia trascendental en nuestras vidas como por ejemplo estar embarazada o tener un bebé, es cuando más susceptibles somos a modificar nuestro hábitos de comportamiento, porque cuando no tienes tiempo para ti, ni para tus hobbies, y si encuentras un lugar donde comprar pañales por ejemplo, y biberones, y si en oferta o “descuento” tenemos una cuna, tanto mejor, ya que nos proporciona tanto la facilidad de acceso a productos que probablemente en un futuro breve vaya a utilizar. Es por eso que debemos proteger nuestros datos personales.

5.2. Pero ¿Qué tiene que ver los datos personales con los Términos y condiciones de uso o Términos de Servicio?

Es común que los usuarios de servicios y aplicaciones en internet no lean los términos y condiciones de servicios y uso de aplicaciones y plataformas en internet. Esto puede deberse a que estos términos y condiciones son muy extensos o a que la terminología es rebuscada y difícil de comprender para la mayoría de los usuarios.

El principal problema radica en el desconocimiento y la falta de voluntad por parte de la población para leer los términos y condiciones de uso de servicios de aplicaciones en internet. Por otro lado, varias empresas o entidades encargadas de estas aplicaciones y plataformas virtuales plasman estos términos de manera que no solo favorecen a estas empresas y salvaguardan sus derechos, sino que también se benefician con los datos personales recopilados en estas plataformas virtuales, ya que actualmente estos datos se están convirtiendo en la moneda de cambio con la que comercian las empresas que brindan servicios entre comillas gratuitos.

Para solucionar este problema, proponemos la elaboración de un anteproyecto de ley que se enfoque en la elaboración de un resumen claro,

conciso y lo más comprensible posible para el usuario final en territorio nacional. Este resumen debe ser publicado en la página principal de las aplicaciones y servicios de plataformas virtuales en internet, así como también al momento de crear una cuenta en estas plataformas virtuales de modo que sea fácilmente comprendido por el usuario final.

Además, es importante establecer artículos que esclarezcan y hagan público en el resumen de estos TyC, enfocados a, que tipo de datos personales son recabado, que uso se le dará a esos datos, y que posibilidades existen de que sean o no almacenados o comercializados, obligando a las entidades de distribución de estas plataformas de internet a informar qué harán con nuestros datos antes de que aceptemos los TyC, y sobre todo prohibir la mercantilización de nuestros datos personales sin el consentimiento expreso de los usuarios a quienes les pertenezcan estos datos.

5.3. ¿Mis datos personales están en peligro? ¿Está al tanto de los términos y condiciones de las plataformas en línea que utiliza?

La protección de los datos personales es un tema cada vez más relevante en nuestra sociedad, especialmente en el contexto de las plataformas y aplicaciones en línea. Muchas personas utilizan diariamente estas herramientas sin siquiera considerar los términos y condiciones que están aceptando al utilizarlas. Con el objetivo de conocer mejor la situación actual en Bolivia, se llevó a cabo una encuesta titulada "¿Mis datos personales están en peligro?¿Está al tanto de los términos y condiciones de las plataformas en línea que utiliza?" para evaluar el nivel de conciencia y comprensión de los usuarios sobre estos temas.

Pregunta	Sí	No	Resultado en % SI	Resultado en % no
¿Alguna vez ha leído los términos y condiciones antes de utilizar una aplicación o plataforma en línea?	42	158	21%	79%
¿Entiende completamente los términos y condiciones que está aceptando al utilizar una aplicación o plataforma en línea?	10	190	5%	95%

¿Cree que los términos y condiciones de las aplicaciones y plataformas en línea deben ser resumidos y presentados de manera clara y fácil de entender?	200	0	0%	100%
¿Considera importante el control sobre sus datos personales en plataformas en línea?	185	15	93%	7%
¿Cree que debería existir una ley específica para regular la privacidad y protección de datos personales en plataformas en línea en Bolivia?	200	0	0%	100%

Los resultados de la encuesta muestran que solo el 21% de los encuestados ha leído los términos y condiciones antes de utilizar una aplicación o plataforma en línea, mientras que el 79% no lo ha hecho. Además, solo el 5% de los encuestados entiende completamente los términos y condiciones que está aceptando al utilizar una aplicación o plataforma en línea, mientras que el 95% no lo hace. Estos resultados sugieren que hay una falta de conciencia y comprensión de los usuarios sobre los términos y condiciones en plataformas en línea, y la importancia de proteger sus datos personales.

Es importante señalar que el 100% de los encuestados considera que los términos y condiciones deben ser resumidos y presentados de manera clara y fácil de entender.

Además, los resultados también sugieren una preocupación por parte de los encuestados en cuanto al control de sus datos personales en plataformas en línea, ya que el 93% considera importante el control sobre sus datos personales en plataformas en línea y el 100% cree que debería existir una ley específica para regular la privacidad y protección de datos personales en plataformas en línea en Bolivia.

CAPITULO IV
MARCO JURÍDICO

1. Legislación General:

1.1. Constitución Política del Estado Plurinacional de Bolivia:[18]

La Constitución Política del Estado Plurinacional de Bolivia establece en su Artículo 21, parágrafo II, el derecho a la privacidad, intimidad, honra, propia imagen y dignidad, y a la salvaguarda de los mismos, siendo estos de vital importancia para el correcto desarrollo social. Además, se establece la Acción de Protección de Privacidad en los Artículos 130 y 131, que permiten a las personas interponer una acción legal para proteger su derecho a la intimidad y privacidad personal o familiar, o su propia imagen, honra y reputación, frente a la posible violación de estos derechos por medio de información registrada en archivos o bancos de datos públicos o privados.

El Artículo 130, Parágrafo I establece el derecho a la información personal y el derecho a controlar la información personal, mientras que el Artículo 131 establece el procedimiento para la Acción de Protección de Privacidad, incluyendo la posibilidad de revelar, eliminar o rectificar los datos cuyo registro ha sido impugnado.

La protección de los derechos a la privacidad y la intimidad es esencial para garantizar la libertad y el respeto a la dignidad de las personas, y estos artículos de la Constitución Política del Estado Plurinacional de Bolivia establecen las bases legales para proteger estos derechos. Es importante señalar que este derecho a la privacidad también está protegido por la normativa internacional en materia de derechos humanos y es un tema de importancia en el ámbito de la protección de datos personales. Además, estos derechos son fundamentales para garantizar la seguridad, el respeto y la protección de los datos personales en un mundo cada vez más digital, donde el uso de plataformas en internet y la recolección de datos son cada vez más comunes.

[18] Congreso Nacional De Bolivia, Constitución Política del Estado, pág. 9, 41 y 42

2. Legislación Sectorial:

2.1. Código Civil, de 6 de agosto de 1975 [19]

A continuación, procederemos con un análisis por articulo relacionado a la protección de datos personales.

Artículo 15: Este artículo establece la nulidad de las confesiones y manifestaciones de voluntad obtenidas mediante procedimientos lesivos a la personalidad. En relación a la protección de la privacidad, esto significa que cualquier información obtenida mediante la filtración de datos personales no tiene validez legal. Es importante destacar que este artículo busca proteger la dignidad y privacidad de las personas, evitando que se utilice información obtenida de manera ilegal o inadecuada.

Artículo 16: Este artículo establece la protección de la reputación y decoro personal. Establece que cuando se comercia, publica, exhibe o expone la imagen de una persona de manera que lesiona su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir al juez que haga cesar el hecho lesivo, salvo los casos justificados por la ley. Este artículo busca proteger el derecho a la imagen y a la reputación de las personas, estableciendo medidas legales para hacer cesar conductas que atenten contra estos derechos.

Artículo 18: Este artículo establece el derecho a la intimidad, señalando que nadie puede perturbar ni divulgar la vida íntima de una persona. Esto significa que ninguna plataforma puede divulgar la vida íntima de una persona, ya sea con o sin la aceptación de los términos y condiciones. Este artículo busca proteger la privacidad de las personas, evitando que se divulgue información personal que no ha sido autorizada para su difusión.

Y en lo referido a los términos y condiciones, vamos a analizar la legitimidad de los contratos establecidos en los TyC según el código civil boliviano.

[19] Consejo de ministros de Bolivia, Ley N° 12760, 1975, páginas: 3,4, y 70 al 75

Artículo 450: Este artículo define el contrato como un acuerdo entre dos o más personas para constituir, modificar o extinguir una relación jurídica entre ellas. Es importante destacar que este artículo establece las bases para la formación de contratos, estableciendo los elementos necesarios para su validez.

Artículo 451: Este artículo establece que las normas contenidas en el título del Código Civil son aplicables a todos los contratos, independientemente de su denominación especial, siempre y cuando no existan disposiciones legales contrarias. Además, estas normas también son aplicables a los actos unilaterales de contenido patrimonial que se celebran entre vivos y a los actos jurídicos en general, siempre y cuando sean compatibles. Este artículo establece la aplicabilidad general de las normas del código civil a los contratos y actos jurídicos en general, lo que significa que estas normas son aplicables a todos los contratos independientemente de su denominación especial, siempre y cuando no existan disposiciones legales contrarias. Esto es importante en relación a los contratos establecidos en las plataformas de internet, ya que estos deben cumplir con las normas generales del código civil.

Artículo 452: Este artículo establece los requisitos para la formación del contrato. Estos son: el consentimiento de las partes, el objeto y las condiciones. Estos requisitos deben cumplirse para que un contrato sea válido. Es importante destacar que estos requisitos son fundamentales para la validez de un contrato, ya que sin ellos no se puede establecer un acuerdo jurídico válido entre las partes.

Se hace especial énfasis en el Artículo 18, que prohíbe la divulgación de la vida íntima de una persona. Además, se analiza la legitimidad de los contratos establecidos en los términos y condiciones de las plataformas de internet en relación con el Código Civil boliviano. Los artículos 450, 451 y 452 del Código Civil establecen las normas generales para la formación de contratos, incluyendo los requisitos necesarios para su validez. Es importante mencionar que estos artículos son aplicables a todos los contratos, independientemente de su denominación especial, siempre y cuando no existan disposiciones legales contrarias. Por lo

tanto, es importante considerar estos principios al momento de establecer contratos en plataformas de internet o cualquier otro tipo de acuerdo legal.

2.2. Código Penal[20]

El Código Penal boliviano establece en su Título XII "Delitos contra la propiedad", y sanciona diversos delitos informáticos para proteger la propiedad intelectual y la privacidad de las personas.

Artículo 363 bis: Este artículo establece la figura del delito de manipulación informática. Se castiga a aquellas personas que, con la intención de obtener un beneficio indebido para sí o un tercero, manipulan un procesamiento o transferencia de datos informáticos que conduzcan a un resultado incorrecto o eviten un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero. La pena para este delito es reclusión de uno a cinco años y multa de sesenta a doscientos días.

Artículo 363 ter: Este artículo establece la figura del delito de alteración, acceso y uso indebido de datos informáticos. Se castiga a aquellas personas que sin estar autorizadas se apoderen, accedan, utilicen, modifiquen, supriman o inutilicen datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información. La pena para este delito es prestación de trabajo hasta un año o multa hasta doscientos días.

En relación a la invasión a la intimidad personal, se castiga con pena privativa de libertad de uno a tres años a aquellas personas que sin autorización accedan a la información privada de otra persona a través de medios informáticos o de telecomunicaciones, buscando proteger la privacidad de las personas y evitar la violación de su intimidad personal.

Los artículos 363 bis y 363 ter del Código Penal boliviano establecen las figuras del delito de manipulación informática y alteración, acceso y uso indebido de datos informáticos, respectivamente. Estos artículos buscan proteger la propiedad intelectual y la privacidad de las personas, sancionando a aquellas personas que cometan estos delitos.

[20] Congreso Nacional de Bolivia, D.L.10426, 1972, Pág. 61.

Sin embargo, es importante mencionar que estos artículos no abordan específicamente la protección de datos personales y su uso en el contexto de las empresas y las plataformas de internet. La implementación de una ley de protección de datos personales es esencial para garantizar que las empresas y plataformas cumplan con las normas y regulaciones necesarias para proteger los datos personales de los usuarios y evitar su uso indebido.

En conclusión, estos artículos son un paso importante en la protección de la propiedad intelectual y la privacidad, pero es necesaria una regulación específica en materia de protección de datos personales para garantizar una protección adecuada de estos derechos en el contexto de las empresas y plataformas de internet.

2.3. Nuevo Código Procesal Constitucional:

"El Nuevo Código Procesal Constitucional"[21], aprobado en 2012, establece en su capítulo 4 un procedimiento específico para la Acción de protección de Privacidad. Este procedimiento específico tiene como objetivo garantizar la protección de los derechos fundamentales de las personas en relación a su privacidad, intimidad, imagen y propia dignidad. Los artículos 58 al 63 del NCCP establecen las reglas para la interposición y tramitación de esta acción, y establecen también las obligaciones de las autoridades y entidades públicas y privadas en relación a la protección de los datos personales.

- En el Artículo 58 se establece que la acción de protección de privacidad procede en caso de amenaza o violación de los derechos fundamentales a la intimidad personal y familiar, imagen, privacidad, información, propia información, y cualquier otro derecho fundamental relacionado con la protección de los datos personales.
- El artículo 59 establece que la acción podrá ser interpuesta por cualquier persona, tanto individual como colectiva, que se sienta afectada por la

[21] Asamblea legislativa plurinacional de Bolivia, Ley N° 254, 2012, pág. 28.

amenaza o violación de sus derechos fundamentales relacionados con la privacidad y los datos personales.

- En el artículo 60 se establece que la acción de protección de privacidad no procederá para levantar el secreto en materia de prensa y, en consecuencia, no podrá ser utilizada para cuestionar la publicación de información de interés público.
- Por último, el artículo 63 establece que la decisión final de la acción de protección de privacidad será ejecutada inmediatamente y sin observación, y en caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad.

Este procedimiento es distinto al recurso de amparo constitucional utilizado previamente, y tiene como objetivo garantizar una mayor eficacia y celeridad en la protección de los derechos fundamentales relacionados con la privacidad y el tratamiento de los datos personales.

En comparación con el recurso de amparo constitucional, el nuevo procedimiento establecido en el Código Procesal Constitucional permite una mayor flexibilidad en la interposición de la acción de protección de privacidad, ya que en algunos casos no es necesario agotar la vía administrativa previamente. Esto es positivo, ya que, en casos de inminencia de daño en relación al tratamiento de los datos personales, puede ser necesaria una acción rápida para proteger los derechos fundamentales afectados.

Un aspecto positivo del NCCP es la posibilidad de interponer la Acción de Protección de Privacidad de manera directa, sin necesidad de agotar la vía administrativa previamente. Esto se justifica en casos en los que existe una inminencia del daño que puede ocasionar el tratamiento indebido de los datos personales, y permite una protección más efectiva y rápida de los derechos fundamentales de las personas.

Sin embargo, también se pueden encontrar ciertas críticas en relación al NCCP. Una de ellas podría ser que el procedimiento específico para la Acción de Protección de Privacidad podría generar una sobrecarga en la justicia y en los tribunales, ya que se estarían tramitando casos específicos relacionados con la protección de datos personales.

Además, el Código Procesal Constitucional también establece sanciones para las autoridades judiciales que no cumplan con lo dispuesto en la acción de protección de privacidad, lo que garantiza una mayor responsabilidad en el tratamiento de los datos personales.

Es importante destacar que su implementación ha permitido una mayor eficiencia en la protección de los derechos fundamentales, especialmente en lo que se refiere a la privacidad y la protección de datos personales. Al establecer un procedimiento específico para la acción de protección de privacidad, se ha logrado una mayor rapidez en la resolución de los casos y una mayor accesibilidad para las personas que buscan proteger sus derechos.

En cuanto a la comparación con el procedimiento anterior del recurso de amparo constitucional, se puede decir que el Nuevo Código Procesal Constitucional ha mejorado en términos de eficiencia y accesibilidad. El procedimiento del recurso de amparo, al ser más general, podía llevar más tiempo y ser menos accesible para las personas. Con el nuevo procedimiento específico para la acción de protección de privacidad, se ha logrado una mayor rapidez en la resolución de los casos y una mayor accesibilidad para las personas.

En cuanto a la relación con el tema de la monografía, el Nuevo Código Procesal Constitucional es esencial para garantizar la protección de los derechos fundamentales de las personas en relación a los datos personales. El capítulo 4to sobre la Acción de Protección de Privacidad es una herramienta clave para asegurar que las personas tengan acceso a sus datos registrados y puedan solicitar la actualización, complementación, eliminación o rectificación de los mismos en caso de ser necesario. Además, el hecho de que sea posible

interponer esta acción directamente en algunos casos, sin pasar por la vía administrativa, es una medida importante para garantizar una protección rápida y eficiente.

Sin embargo, es importante mencionar que aún existen desafíos en cuanto a la aplicación efectiva de esta normativa en la práctica. Puede haber dificultades para acceder a la información y para hacer cumplir las decisiones de los tribunales en caso de violación de los derechos fundamentales. Por lo tanto, es necesario seguir trabajando en la mejora de la aplicación de la protección de datos personales en Bolivia, el Nuevo Código Procesal Constitucional juega un papel fundamental.

También es importante mencionar que, a pesar de la existencia de esta normativa, todavía existen desafíos en cuanto a la aplicación efectiva de la protección de datos personales en Bolivia. Por ejemplo, existe la necesidad de fortalecer la capacitación y conciencia sobre estos temas tanto en la población como en las autoridades encargadas de hacer cumplir estas leyes.

El Nuevo Código Procesal Constitucional es un paso importante en la protección de datos personales en Bolivia, ya que facilita el acceso a la justicia para aquellas personas que sienten que sus derechos fundamentales han sido violados. Sin embargo, todavía hay desafíos a superar para garantizar una aplicación efectiva de esta normativa en la protección de los datos personales. Uno de los principales desafíos es la falta de capacitación y conciencia de los funcionarios encargados de hacer cumplir estas leyes, así como la falta de recursos para llevar a cabo investigaciones y sancionar a aquellos que violen las normas de protección de datos. Además, aunque la ley establece sanciones para aquellos que infrinjan las normas, en la práctica estas sanciones son raramente impuestas, lo que reduce su efectividad como medida disuasoria.

Otro desafío es la falta de regulación y supervisión en el campo de las tecnologías de la información y las comunicaciones, especialmente en relación con las plataformas en línea y los proveedores de servicios de internet. Muchas de

estas compañías operan en el país sin cumplir con las normas de protección de datos, lo que pone en riesgo la privacidad y la seguridad de los usuarios.

2.4. Decreto Supremo N°28168:

En el año 2005 se aprueba el "Decreto Supremo N°28168"[22] que establece medidas para garantizar el derecho al acceso a la información del Poder Ejecutivo, específicamente en su Artículo 19, establece la petición de habeas data, que permite a las personas solicitar la actualización, complementación, eliminación o rectificación de sus datos registrados en archivos o registros públicos.

Este artículo es importante porque garantiza el derecho de las personas a controlar la información personal que se encuentra registrada en archivos o registros públicos, y a tener acceso a la misma en caso de negativa injustificada por parte de las autoridades encargadas.

Esta normativa se enmarca en la protección de los derechos fundamentales a la identidad, intimidad, imagen y privacidad, y tiene como objetivo garantizar la transparencia y responsabilidad del Poder Ejecutivo en la gestión de la información y el respeto a los derechos individuales.

En resumen, el decreto supremo N°28168, establece un mecanismo de protección de los derechos personales, mediante la petición de habeas data, que permite a las personas solicitar la actualización, complementación, eliminación o rectificación de sus datos registrados en archivos o registros públicos, garantizando así el derecho a la privacidad y protección

2.5. Ley general de telecomunicaciones:

En el año 2011 se aprueba la "Ley 164, Ley General De Telecomunicaciones, Tecnologías De Información Y Comunicación", que en el "artículo 54"[23] establece las obligaciones y derechos de los usuarios y

[22] Concejo de Gabinete, DS 20168, 2005, Pág. 5
[23] Asamblea legislativa plurinacional de Bolivia, Ley N° 164, 2011, pág. 23.

consumidores en el ámbito de las telecomunicaciones. Este artículo menciona específicamente el derecho a la privacidad y la inviolabilidad de las comunicaciones, estableciendo que las comunicaciones deben ser tratadas con confidencialidad y no pueden ser interceptadas, grabadas o divulgadas sin el consentimiento de las partes involucradas.

El artículo 54 también establece que los proveedores de servicios de telecomunicaciones deben adoptar medidas de seguridad para garantizar la protección de los datos personales de sus usuarios. Estas medidas deben incluir la implementación de sistemas de encriptación, la protección de las bases de datos y la implementación de controles de acceso para garantizar que solo las personas autorizadas tengan acceso a los datos.

En cuanto a la protección de los datos personales por parte del proveedor de servicios de internet, el artículo 54 establece que estos deben cumplir con las normas establecidas por la Autoridad de Regulación y Fiscalización de Telecomunicaciones (ATT) y la Autoridad de Protección de Datos Personales (APDP). En caso de incumplimiento, las autoridades regulatorias pueden imponer sanciones o multas al proveedor de servicios de internet, así como ordenar la rectificación de la situación para garantizar la protección de los datos personales de los usuarios.

En resumen, la Ley 164 establece un marco jurídico para garantizar la privacidad y la inviolabilidad de las comunicaciones, así como la protección de los datos personales de los usuarios y consumidores en el ámbito de las telecomunicaciones. Los proveedores de servicios de internet tienen la obligación de cumplir con las normas establecidas por las autoridades regulatorias y de adoptar medidas de seguridad para proteger los datos personales de sus usuarios. En caso de incumplimiento, están sujetos a sanciones o multas y deben rectificar la situación para garantizar la protección de los datos personales.

2.6. Decreto 1793 “Reglamento a la Ley General de telecomunicaciones, tecnologías de información y comunicación”[24]

En cuanto al análisis jurídico, el Decreto 1793 de 2013 establece un marco normativo específico para la protección de datos personales en el ámbito de las telecomunicaciones y las tecnologías de información y comunicación. A través de la definición de términos clave como "datos personales" y "tratamiento de datos personales", se establecen las bases para una regulación adecuada de estos temas.

Además, el Decreto 1793 establece los principios fundamentales para la protección de datos personales, como la finalidad, veracidad, transparencia, seguridad y confidencialidad. Estos principios son esenciales para garantizar que los datos personales sean tratados de manera ética y respetando los derechos de las personas.

Sin embargo, una crítica a este Decreto sería que está estrechamente relacionado con la certificación digital, lo cual podría limitar la protección de datos personales a aquellas personas o empresas que cuenten con dicha certificación. Además, también se podría argumentar que, a pesar de establecer principios y regulaciones específicas, no se especifican medidas concretas para garantizar su cumplimiento y sanciones efectivas en caso de incumplimiento.

2.7. Ley de Ciudadanía Digital

La “Ley de Ciudadanía Digital de Bolivia”[25], sancionada en el año 2017, tiene como objetivo promover el desarrollo de la sociedad digital en el país, mediante la promoción del acceso, uso y apropiación de las tecnologías de la información y comunicación (TIC) por parte de la ciudadanía. Esta ley establece la creación del Sistema Nacional de Identificación Digital (SNID), que tiene como objetivo brindar una identidad digital a todos los ciudadanos bolivianos y garantizar su acceso a servicios y beneficios a través de internet.

[24] Concejo de ministros de Bolivia, D.S. N° 1793, 2013, pág. 17.
[25] Asamblea Legislativa Plurinacional, Ley N°1080, 2018, Págs., 1 y 2.

La Ley de Ciudadanía Digital en Bolivia es una normativa que tiene como objetivo establecer las bases para el desarrollo de un sistema de ciudadanía digital en el país, con el fin de promover la inclusión digital y garantizar el acceso a servicios públicos y privados a través de medios digitales. La ley establece un marco normativo para la protección de datos personales, la seguridad de la información y la confidencialidad en el uso de los servicios de ciudadanía digital, así como sanciones para aquellas entidades que no cumplan con las normas establecidas. Establece también medidas para garantizar la seguridad de los datos personales registrados en el sistema, y promover la inclusión digital a través de programas y proyectos específicos.

¿Por qué' la ley de ciudadanía digital va enfocada a entidades públicas y privadas que presten servicios públicos delegados por el Estado?

La ley de ciudadanía digital va encaminada a las entidades públicas y privadas que prestan servicios públicos delegados por el Estado, ya que estas entidades son las que tienen acceso y tratan con los datos personales de las personas que utilizan sus servicios, y es importante garantizar que estos datos sean tratados de manera segura y protegidos contra cualquier posible violación de privacidad. Además, esta ley busca facilitar el ejercicio de derechos y deberes a través del uso de tecnologías de información y comunicación, permitiendo una mayor interacción y acceso a servicios públicos para las personas, mejorando la eficiencia y transparencia en la gestión de estos servicios.

La Ley de Ciudadanía Digital en Bolivia se enfoca en mejorar el acceso a la tecnología y servicios digitales para la población, asegurando la protección de los derechos fundamentales, como el derecho a la privacidad y la protección de datos personales. Esta ley establece la creación de un sistema de registro de ciudadanía digital, en el cual los ciudadanos podrán tener acceso a servicios digitales de

manera segura y confiable. Además, establece la creación de una entidad encargada de supervisar y garantizar la protección de los datos personales registrados en este sistema.

En relación a la protección de los datos personales, la Ley de Ciudadanía Digital establece en su artículo 6 que el SNID debe garantizar la privacidad, seguridad y confidencialidad de los datos personales de los ciudadanos, y que estos deben ser tratados de manera respetuosa y transparente. Asimismo, establece en su artículo 11 la creación de una Autoridad Nacional de Protección de Datos Personales, encargada de supervisar y fiscalizar el cumplimiento de las normas relacionadas a la protección de datos personales.

La Ley de Ciudadanía Digital establece medidas para garantizar la seguridad de los datos personales registrados en el sistema de ciudadanía digital, pero no especifica de manera detallada las medidas específicas que se deben tomar. Sin embargo, se menciona la importancia de garantizar la confidencialidad, integridad y disponibilidad de los datos, así como la implementación de medidas técnicas y administrativas para prevenir su acceso no autorizado. También se establece la necesidad de contar con un plan de seguridad que incluya la identificación de riesgos y la implementación de medidas de seguridad para prevenirlos.

En relación a nuestro tema de estudio, esta ley es relevante ya que proporciona un marco legal específico para garantizar la protección de los datos personales en el ámbito digital. A través de esta ley, se establecen medidas para garantizar la seguridad de los datos personales registrados en el sistema de ciudadanía digital y se establecen sanciones para aquellas entidades que no cumplan con las normas establecidas. Esto contribuye a la implementación de una ley de declaración resumida de términos y condiciones de servicio de uso de plataformas en internet, ya que permite establecer un marco legal específico para garantizar la protección de los datos personales en este ámbito.

En general, la Ley de Ciudadanía Digital busca promover el desarrollo de una sociedad digital en Bolivia, pero también tiene en cuenta aspectos importantes como la protección de los datos personales de los ciudadanos. Sin embargo, es importante señalar que esta ley aún no ha sido reglamentada, por lo que su efectiva implementación y cumplimiento aún está pendiente.

Sin embargo, es importante mencionar que, aunque esta ley tiene un enfoque en la protección de datos personales, podría ser necesario una actualización o ajuste de las normas establecidas para garantizar una protección más eficiente y adecuada a la evolución de las tecnologías y el uso de internet.

3. Sentencias Constitucionales:

3.1. Sentencia constitucional 0965/2004-R, sucre — 23 de junio de 2004 Establece la protección que brinda el habeas data.

La “Sentencia Constitucional 0965/2004-R”[26], establece la protección que brinda el hábeas data en Bolivia. Según la doctrina del Dr. José Antonio Rivera Santivañez, el hábeas data es un proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática". Es una garantía constitucional que permite a las personas verificar qué información o datos se han obtenido y almacenado sobre ellas, cómo se difunden y con qué objeto, con el fin de corregir o aclarar información o datos inexactos, evitar su difusión y, en su caso, eliminarlos si se trata de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima.

La Sentencia también señala que el hábeas data es una acción de carácter subsidiario, es decir, sólo puede ser activado cuando el titular del derecho lesionado haya reclamado por la vía administrativa y no ha sido efectiva para proteger el derecho a la autodeterminación informática del titular del derecho.

En resumen, la Sentencia Constitucional 0965/2004-R establece la protección que brinda el hábeas data en Bolivia como una garantía constitucional

[26] Tribunal Constitucional, 2004, Págs. 2 al 8.

que protege el derecho a la autodeterminación informática de las personas. Esta acción es de carácter tutelar y solo puede ser activada por la persona afectada, no admite acción popular y es una acción subsidiaria que solo puede ser utilizada después de haber intentado resolver el problema a través de la vía administrativa y no haber obtenido una respuesta positiva. Esta sentencia refleja la necesidad de implementar leyes de protección de datos personales en Bolivia para garantizar la privacidad y los derechos de las personas en relación a la información almacenada sobre ellas.

3.2. Sentencia Constitucional 1738/2010-R, Sucre, 25 de octubre de 2010. Los derechos a la intimidad y privacidad como base de la protección de datos personales.

La "Sentencia Constitucional 1738/2010-R"[27] establece la protección que brinda el derecho a la intimidad y privacidad como base para la protección de los datos personales en Bolivia. La sentencia se basa en la doctrina del Dr. José Antonio Rivera Santivañez y su obra "Jurisdicción Constitucional", en la cual se define el hábeas data como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática".

La sentencia establece que tanto las personas naturales como jurídicas tienen acceso a los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad reconocidos en el artículo 21.1 de la Constitución Política del Estado (CPE). Además, se señala que el derecho a la intimidad es uno de los bienes más susceptibles de ser lesionados o puestos en peligro por el uso de las nuevas tecnologías, por lo que se hace necesario establecer límites a la utilización de la informática y las comunicaciones para evitar la agresión a la intimidad de los ciudadanos.

La sentencia también hace una distinción entre intimidad y privacidad, señalando que la intimidad es el conjunto de sentimientos, pensamientos e

[27] Tribunal Constitucional, 2010, Págs. 3 al 5.

inclinaciones más internos, mientras que la privacidad hace referencia al ámbito de la persona formado por su vida familiar, aficiones, bienes particulares y actividades personales.

En conclusión, la Sentencia Constitucional 1738/2010-R establece la importancia de proteger los derechos a la intimidad y privacidad como base para la protección de los datos personales en Bolivia, y señala la necesidad de establecer límites al uso de las nuevas tecnologías para evitar la agresión a estos derechos fundamentales. Además, se hace una distinción entre los términos intimidad y privacidad, y se destaca la importancia de proteger ambos derechos para garantizar una adecuada protección de los datos personales.

4. LEGISLACIÓN COMPARADA.

4.1. MEXICO.-

La legislación comparada en relación a la protección de datos personales en plataformas en internet en México se encuentra regulada en el Reglamento de la "Ley Federal de Protección de Datos Personales en Posesión de los Particulares"[28] (RLFPDPPP). Este reglamento establece las obligaciones que las plataformas deben cumplir en cuanto a la recolección, uso, almacenamiento y compartición de datos personales de los usuarios.

De acuerdo con el RLFPDPPP, las plataformas deben contar con un aviso de privacidad que sea fácilmente accesible para los usuarios y que incluya información clara y concisa sobre las finalidades de la recolección de datos, los derechos de los titulares de los datos y las medidas de seguridad implementadas para proteger los datos. Además, las plataformas deben obtener el consentimiento previo de los usuarios antes de recolectar o tratar sus datos personales y deben notificar a los usuarios en caso de cualquier cambio en el aviso de privacidad.

En comparación con la propuesta de ley boliviana, la legislación mexicana se enfoca en las obligaciones de las plataformas en cuanto al aviso de privacidad

[28] Congreso General de Mexico, 2010, Págs. 1 al 18.

y el consentimiento previo de los usuarios, mientras que la propuesta boliviana se enfoca en la implementación de una declaración resumida de términos y condiciones de servicio. Ambas legislaciones tienen como objetivo garantizar la transparencia y la comprensión de los términos y condiciones de uso de las plataformas en internet y proteger los datos personales de los usuarios.

Para complementar la información puede consultar las siguientes referencias bibliográficas:

- "Constitución Política de los Estados Unidos Mexicanos" (1917)
- "Ley Federal de Protección de Datos Personales en Posesión de los Particulares" (2010)
- "Ley de la Protección de Datos Personales en Posesión de los Sujetos Obligados" (2011)
- "Ley General de Protección de Datos Personales" (2019)
- "Ley General de Telecomunicaciones" (2013)

4.2. PERU.-

La legislación peruana en relación a la protección de datos personales y el uso de plataformas en internet se encuentra regulada principalmente por la Ley 29733, “Ley de Protección de Datos Personales”[29], y su Reglamento aprobado por el Decreto Supremo N° 003-2013-JUS. Esta legislación establece las obligaciones y responsabilidades de las entidades que tratan datos personales, así como los derechos y mecanismos de protección de los titulares de dichos datos.

En cuanto a la regulación de los términos y condiciones de uso de las plataformas en internet, en Perú existe la Ley 29571, Ley de Protección al Consumidor, que establece las obligaciones de las empresas proveedoras de servicios en línea en relación a la información proporcionada a los consumidores, así como los derechos y mecanismos de protección de los mismos.

[29] Congreso de la República del Perú, 2011, Págs. 7 al 10.

Para complementar la información puede consultar las siguientes referencias bibliográficas:

- "Ley 29733: Ley de Protección de Datos Personales y su Reglamento" de la Asociación Peruana de Derecho de las Tecnologías de la Información y las Comunicaciones (APEDETIC)
- "La protección de datos personales en el Perú: una revisión de la normativa y su aplicación" de la revista Derecho y Nuevas Tecnologías
- "La protección de los datos personales en el Perú y su relación con el derecho a la privacidad" de la revista Actualidad Jurídica.

4.3. CHILE.-

En Chile, existe una ley específica para la protección de datos personales, la “Ley N° 19.628”[30], sancionada en 1999 y modificada en 2018. Esta ley establece las bases para el tratamiento legítimo de los datos personales, la obligación de informar a los titulares de los datos sobre su tratamiento, la necesidad de obtener su consentimiento para dicho tratamiento, entre otras disposiciones.

En cuanto a las plataformas en internet, esta ley establece que toda entidad que realice el tratamiento de datos personales debe contar con un Responsable del Tratamiento de Datos, quien será el encargado de velar por el cumplimiento de la ley y garantizar la privacidad de los titulares de los datos. Además, esta ley establece la obligación de las entidades de informar a los titulares de los datos sobre el tratamiento que se les dará a sus datos y obtener su consentimiento para dicho tratamiento.

Para complementar la información puede consultar las siguientes referencias bibliográficas:

[30] Congreso Nacional de Chile, 1999, Pág. 17.

- "Ley N° 19.628 sobre protección de la vida privada" disponible en el sitio web del Ministerio de Justicia de Chile.
- "Guía para el cumplimiento de la ley de protección de datos personales" publicado por el Instituto Nacional de Derechos Humanos de Chile.
- "La protección de datos personales en Chile: una revisión normativa" de Patricio Sepúlveda, publicado en la Revista de Derecho de la Pontificia Universidad Católica de Chile.

4.4. ECUADOR.-

En Ecuador, la protección de datos personales está regulada por la Constitución de la República del Ecuador y la "Ley de Protección de Datos Personales (Ley N° 17 de 2019)"[31]. Esta ley establece la responsabilidad de las entidades públicas y privadas en el tratamiento de datos personales, así como los derechos de los titulares de los datos y las sanciones por incumplimiento. También se establecen medidas de seguridad para garantizar la protección de los datos personales y se crea la Agencia de Protección de Datos como autoridad encargada de velar por el cumplimiento de la ley.

En cuanto a la implementación de declaraciones resumidas de términos y condiciones de servicio, no hay una normativa específica en Ecuador que lo regula. Sin embargo, se espera que las entidades cumplan con las obligaciones establecidas en la Ley de Protección de Datos Personales en cuanto a la transparencia y la información clara sobre la recolección y tratamiento de datos personales.

Para complementar la información puede consultar las siguientes referencias bibliográficas:

- Constitución de la República del Ecuador (2008).
- Ley de Protección de Datos Personales (Ley N° 17 de 2019).

[31] Asamblea Nacional de Ecuador, 2021, Págs. 5 y 6.

- "Ley de protección de datos personales: ¿qué cambios trae para las empresas?" (2019) disponible en: https://www.pwc.com.ec/es/publicaciones/tecnicas/2019/ley-de-proteccion-de-datos-personales.html
- "Ley de Protección de Datos Personales en Ecuador" (2019). disponible en: https://www.lexology.com/library/detail.aspx?g=5f5b3a7c-f2f5-4e5a-9e9f-c2e1d9e8c8f6

CAPITULO V
CONCLUSIONES

En este proyecto se ha evidenciado que existen avances en cuanto a la protección de datos personales en Bolivia, pero estos avances no se han enfocado específicamente en el ámbito de internet. Es necesario hacer énfasis en el desarrollo jurídico en este ámbito debido a los avances tecnológicos y la necesidad de regular las nuevas circunstancias que surgen en este campo.

Se propone la regulación de los términos y condiciones de servicio y uso de aplicaciones y plataformas de internet como una medida para abordar dos problemas a la vez: la comprensión de los contratos establecidos en los términos y condiciones para los usuarios finales y la regulación del tipo de información que obtienen las empresas proveedoras de servicios de internet. Además, se propone que los resúmenes de los términos y condiciones sean claros y fáciles de entender para los usuarios finales, y que sea un requisito para el uso de las aplicaciones. Esto ayudará a concientizar a los usuarios finales sobre la importancia de leer y entender estos términos y condiciones.

Por ende, es necesario implementar una ley de declaración resumida de términos y condiciones de servicio para abordar estas preocupaciones y garantizar que los usuarios de plataformas en línea en Bolivia tengan un mayor control sobre sus datos personales.

RECOMENDACIONES

1. Implementar una ley específica para regular la privacidad y la protección de datos personales en línea en Bolivia.
2. Establecer una normativa para la declaración resumida de términos y condiciones de servicio en las aplicaciones y plataformas en línea, para garantizar la comprensión y el control de los usuarios sobre sus datos personales.
3. Concientizar a los usuarios finales sobre la importancia de la privacidad y la protección de datos personales en línea, y promover la lectura de los términos y condiciones de servicio.
4. Regular el tipo de información que las empresas proveedoras de servicios en línea pueden obtener y almacenar de los usuarios.
5. Establecer medidas de seguridad y protección de datos adecuadas en las plataformas en línea para garantizar la privacidad y la seguridad de los usuarios.
6. Establecer sanciones y medidas legales para las empresas que violen las leyes y normativas de privacidad y protección de datos personales.

Se recomienda la implementación de una ley específica para regular la privacidad y la protección de datos personales en línea en Bolivia. Esta ley debería incluir una obligación para las empresas proveedoras de servicios en línea de presentar un resumen claro y fácil de entender de los términos y condiciones de servicio, para garantizar que los usuarios finales estén informados y conscientes de cómo sus datos personales están siendo utilizados. Además, se recomienda una mayor concientización y educación sobre la privacidad y la protección de datos personales en línea para la población boliviana, para garantizar que las personas tengan un mayor control y conocimiento sobre sus derechos y cómo proteger sus datos personales en línea.

CAPITULO VI
PROPUESTA

ANTEPROYECTO DE LEY

Para exigir al Estado plurinacional de Bolivia emita una ley de protección de datos personales acorde a este anteproyecto de ley de declaración resumida de los términos de servicio en formato abreviado, y para otros fines.

ANTEPROYECTO DE LEY DE DECLARACION RESUMIDA DE TERMINOS Y CONDICIONES DE SERVICIO DE USO DE PLATAFORMAS EN INTERNET

TÍTULO I

DISPOSICIONES GENERALES

CAPÍTULO UNICO

GENERALIDADES

Artículo 1. (Objeto).- La presente ley tiene como objetivo garantizar la transparencia y la comprensión de los términos y condiciones de uso de las plataformas en internet que recolectan y tratan datos personales de los ciudadanos bolivianos, mediante la implementación de una declaración resumida de términos y condiciones de servicio.

Artículo 2. (Ámbito de Aplicación).- La presente Ley será aplicable a las personas naturales y/o jurídicas de carácter privado, público o mixto, nacionales o internacionales que por medio de plataformas de internet hagan uso de Términos de servicio de aplicaciones y plataformas de internet, hagan recopilación y tratamiento de datos personales de bolivianas y bolivianos, así como los habitantes de nuestro país, con independencia de si el tratamiento tuvo lugar en el territorio nacional o no, así como independientemente de la forma de su tratamiento, modalidad de creación, tipo de soporte, procesamiento, almacenamiento y organización. Las disposiciones de la presente ley también serán aplicables, en cuanto resulten pertinentes, a los datos relativos a personas jurídicas.

Artículo 3. (Definiciones).-

I. ENTIDAD ENCARGADA.- El término “entidad encargada de brindar servicios y/o aplicaciones en plataformas de internet” Significa cualquier persona sea natural o jurídica, que opere un sitio web ubicado en Internet o un servicio en línea, que se opere con fines comerciales

II. PLATAFORMA EN INTERNET.- cualquier sitio web, aplicación móvil o servicio en línea que recolecte o trate datos personales de los usuarios.

III. AUTORIDAD DE CONTROL.- Es el organismo encargado de velar por el cumplimiento de esta ley y de recibir denuncias y quejas relacionadas con el tratamiento de datos personales

IV. INFORMACIÓN SENSIBLE.- El término “información sensible” significa cualquiera de los siguientes:

1. Información de salud.
2. Información biométrica.
3. Información precisa de geolocalización.
4. Número de seguro social. 22
5. Información sobre la raza, el color, la religión, el origen nacional, el sexo, la edad o la discapacidad de una persona.
6. El contenido y las partes de una comunicación.
7. Grabaciones de audio y video capturadas a través de un dispositivo de consumo.
8. Información financiera, incluido un número de cuenta bancaria, número de tarjeta de crédito, número de tarjeta de débito o número de póliza de seguro.
9. Historial de navegación en línea relacionado con la información descrita en los subpárrafos (1) a (8).

V. TERCEROS.- El término “terceros” significa, con respecto a una entidad encargada, una persona:

1. A quien la entidad reveló información sensible; y
2. No es la entidad cubierta;
3. No es una subsidiaria o afiliada corporativa de la entidad cubierta; o
4. No es un proveedor de servicios de la entidad cubierta

VI. DECLARACIÓN.- El término declaración, con respecto a la presente ley, es la acción y efecto de declarar o declararse, manifestar, decir, hacer público, por aquel medio inmediato posible para facilitar el acceso a la misma por parte del usuario final.

VII. DECLARACIÓN RESUMIDA DE TÉRMINOS Y CONDICIONES.- Es un resumen claro y conciso de los términos y condiciones de uso de una plataforma en internet, que incluya información sobre la recolección, uso, almacenamiento y compartición de datos personales.

TÍTULO II

CAPÍTULO I

DECLARACIÓN RESUMIDA DE TÉRMINOS DE SERVICIO ESTÁNDAR

Artículo 4. (Fecha límite para la declaración resumida de los términos de servicio).-

En un plazo máximo de 365 días calendario posterior a la promulgación de esta Ley, el Estado plurinacional de Bolivia requerirá:

I. Que toda entidad encargada de brindar servicios y/o aplicaciones en plataformas de internet para cualquier tipo de dispositivos electrónicos, deba incluir una declaración resumida de los términos de servicio en formato corto en el sitio web de la entidad;

II. Que toda entidad encargada de brindar servicios y/o aplicaciones en plataformas de internet para cualquier tipo de dispositivos electrónicos, incluya un diagrama de flujo de datos gráficos en el sitio web de la entidad e incluye orientación para dicho diagrama.

III. Que toda entidad encargada de brindar servicios y/o aplicaciones en plataformas de internet para cualquier tipo de dispositivos electrónicos muestre los términos de servicio completos de la entidad en un formato de datos interactivo.

CAPÍTULO II

REQUISITOS PARA LA DECLARACIÓN RESUMIDA DE LOS TÉRMINOS DE SERVICIO EN FORMA BREVE

Artículo 5. (Requisitos generales).- La declaración resumida de los términos de servicio en forma breve descrita en el Art. 4 de la presente ley:

I. Deberá ser fácil de entender, clara y concisa, y podrá incluir tablas, íconos gráficos, hipervínculos u otros medios que determine la presente ley y el Estado Plurinacional de Bolivia.

II. Podrá establecerse por separado en función de la interfaz o tipo de dispositivo a través del cual el usuario acceda a la declaración.

Artículo 6. (Requisitos específicos).- Toda plataforma en internet que recolecte o trate datos personales de los usuarios bolivianos deberá presentar una declaración resumida de términos y condiciones de servicio, que incluya, al menos, la siguiente información:

1. Finalidad de la recolección y el tratamiento de datos personales
2. Tipos de datos personales que se recolectan y tratan
3. Plazos de conservación de los datos personales
4. Información sobre el uso de cookies o tecnologías similares
5. Información sobre la compartición de datos con terceros
6. Información sobre la protección de datos personales
7. Información sobre los derechos de los titulares de los datos personales
8. Información de contacto de la plataforma y de la autoridad de control.

Artículo 7. (Obligaciones de las plataformas).- Las plataformas en internet estarán obligadas a:

I. Presentar una declaración resumida de términos y condiciones de servicio que cumpla con los requisitos establecidos en la presente ley, antes de recolectar o tratar datos personales de los usuarios bolivianos.
II. Asegurar que la declaración resumida de términos y condiciones esté siempre disponible y fácil

Artículo 8. (Ubicación de la declaración resumida y el diagrama de flujo de datos gráficos).- La declaración resumida se colocará en la parte superior de la página de términos de servicio permanentes de la entidad cubierta y cualquier diagrama de flujo de datos gráficos se ubicará inmediatamente debajo de la declaración.

Artículo 9. (Contenido de la declaración resumida).- La declaración resumida deberá revelar lo siguiente:

1. El tiempo aproximado requerido por un usuario para leer el texto completo de los términos de servicio, incluido un recuento total de palabras.
2. Las categorías de información sensible que procesa la entidad encargada de brindar servicios y/o aplicaciones en plataformas de internet.
3. **Especial énfasis en los datos personales, información confidencial, u otro que se requiere para el funcionamiento básico del servicio y qué información confidencial se necesita para funciones adicionales y desarrollo de funciones futuras.**

4. **Un resumen de las responsabilidades legales de un usuario y cualquier derecho transferido del usuario a la entidad encargada de brindar servicios y/o aplicaciones en plataformas de internet.**
5. **Un resumen del tipo de información personal recabada de los usuarios de estas plataformas**
6. **Un resumen de la recopilación y tratamiento de datos personales y la disposición final de esos datos personales e información confidencial, detallando si estos serán o no: transmitidos, compartidos, comercializados, divulgados, mercantilizados con terceros o con subsidiarias o afiliadas corporativas de dicha entidad.**
7. Si la entidad brinda servicios de eliminación de usuarios, instrucciones sobre cómo el usuario puede eliminar información confidencial o interrumpir el uso de información confidencial.

TÍTULO III

INFRACCIONES Y SANCIONES

CAPÍTULO ÚNICO

GRADOS

Artículo 10. (Infracciones).- Las infracciones se calificarán como leves, graves o muy graves. Serán normadas por disposiciones reglamentarias, que mínimamente contemplarán, lo siguiente:

I. Son infracciones leves:

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

II. Son infracciones graves:

2. La creación de bases de datos o tratar datos personales sin haber obtenido el consentimiento previo, expreso e informado del titular previsto en los términos de servicio conforme a la presente ley.
3. 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 previsto en los términos de servicio conforme a la presente ley.
4. 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.
5. No implementar las debidas condiciones de seguridad

6. No realizar el resumen conforme al Art. 7. de la presente ley.
7. Incumplir los deberes y responsabilidades reflejados en la presente Ley.

III. Son infracciones gravísimas:

8. El tratamiento de datos de mala fe, por medio del error y engaño al titular de los datos personales.
9. La comunicación, transferencia o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
10. Desobedecer los requerimientos de cese de tratamiento de datos cuando estos hubieran sido dictados por una orden judicial o resolución fundada.

Artículo 11. (Sanciones).- El incumplimiento de las disposiciones de esta ley y sus reglamentos será sancionado de acuerdo a lo establecido por la autoridad de control, tomando en cuenta la gravedad de la infracción y las posibles consecuencias para los derechos de los titulares de los datos personales. Las sanciones podrán incluir multas, cierre temporal o permanente de la plataforma, y responsabilidad penal en casos graves.

Artículo 12. (Transferencia de datos a terceros países).- Las plataformas en internet estarán prohibidas de transferir datos personales de los usuarios bolivianos a terceros países, salvo que se cumplan los requisitos establecidos por la autoridad de control y se haya obtenido el consentimiento expreso de los titulares de los datos personales.

Artículo 13. (Protección de datos personales de menores).- Las plataformas en internet deberán tomar medidas especiales para garantizar la protección de los datos personales de menores de edad, incluyendo la verificación de la edad del usuario y la obtención del consentimiento de los padres o tutores legales.

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

DISPOSICIÓN FINAL SEGUNDA.- La presente ley entrará en vigencia noventa (90) días después de su publicación en la Gaceta Oficial de Bolivia, con excepción de las Disposiciones Transitorias que entrarán en vigencia a la publicación de su Reglamento.

BIBLIOGRAFÍA

LIBROS:

1. DUHIGG, Charles - 2012 "EL PODER DE LOS HÁBITOS: ¿POR QUÉ HACEMOS LO QUE HACEMOS EN LA VIDA Y EN EL TRABAJO?"
   Editorial Internacional Urano
   Navarra
   España

2. LEON, Cristian - 2018 "PROTECCIÓN DE DATOS PERSONALES Y DERECHOS DIGITALES"
   Friedrich Eber Stiftung
   La Paz
   Bolivia

3. ROJINA V. Rafael - 2015 "COMPENDIO DE DERECHO CIVIL"
   Editorial Porrúa México
   México D.F.
   México

4. UNESCO, Comisión Nacional de DDHH 2018 "DERECHOS CULTURALES Y DERECHOS HUMANOS"
   Editorial UNESCO México
   México D.F.
   México

REVISTA:

5. ARROYO, Veronica - 2021 "GUÍA BÁSICA SOBRE DATOS PERSONALES PARA BOLIVIA"
   Editorial Access Now
   México D.F.
   México

PÁGINAS WEB:

1. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS 2022
   "NEURODATOS Y NEUROTECNOLOGÍA: PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES"
   Link: https://www.aepd.es/es/prensa-y-comunicacion/blog/neurodatos-y-neurotecnologia-privacidad-y-proteccion-de-datos-personales

2. COMISIÓN EUROPEA, Dir. Gral. de Comunicación,

11 de diciembre 2018.
"THE GENERAL DATA PROTECTION REGULATION (GDPR), THE DATA PROTECTION LAW ENFORCEMENT DIRECTIVE AND OTHER RULES CONCERNING THE PROTECTION OF PERSONAL DATA."
Link: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

3. DICCIONARIO VIRTUAL
2022
"OXFORD LENGUAJES"
Link: https://languages.oup.com/google-dictionary-es/

4. DUQUE, V. (Editor)
2021
"ETIMOLOGIA SOBRE PERSONA"
web: etimologias.dechile.net
Link:http://etimologias.dechile.net/?persona

5. ETIMOLOGÍASDECHILE.NET.
2021.
"ETIMOLOGIA SOBRE DATO"
Link:http://etimologias.dechile.net/?dat

6. GAUDIN, S.
2019.
"¿QUÉ ES LA NUBE?"
Link: https://www.cnet.com/es/noticias/explicado-que-es-la-nube/
Bogotá
Colombia

7. GOBIERNO DE ARGENTINA
05 de junio de 2020.
"IMPUTAN A EMPRESAS DE DELIVERY POR CLÁUSULAS ABUSIVAS Y ENGAÑOSAS."
Web: Argentina.go.ar

8. GOBIERNO DE PERÚ, Infraestructura de datos personales.
2021
"QUE SON LOS METADATOS"
web: geoidep.gob.pe
Link.https://www.geoidep.gob.pe/catalogo-metadatos/que-son-los-metadatos#:~:text=La%20definici%C3%B3n%20m%C3%A1s%20concreta%20de,otras%20caracter%C3%ADsticas%20de%20los%20datos.

9. MICROSOFT

2019

"¿QUÉ ES UNA PLATAFORMA VIRTUAL?"
Link: https://support.microsoft.com/es-es/help/17442/windows-protect-my-pc-platform-virtual
Cupertino
California
Estados Unidos

10. MICROSOFT
2022

"TERMINOS Y CONDICIONES"
Link: https://support.microsoft.com/es-es/help/17442/windows-protect-my-pc-understanding-terms-conditions
Cupertino
California
Estados Unidos

11. MICROSOFT
2022

"QUE ES LA NUBE"
Link: https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-the-cloud
Cupertino
California
Estados Unidos

12. PÉREZ PORTO, J
2013

"plataforma virtual"
Link: https://definicion.de/plataforma-virtual/

13. RAFAELLE, C.
2012

"QUE SON LOS TERMINOS Y CONDICIONES Y PARA QUE SIRVEN"
LUBENDA S.R.L.
MILANO
ITALIA
Link: https://www.iubenda.com/es/help/37616-que-son-los-terminos-y-condiciones-y-para-que-sirven#:~:text=Los%20T%C3%A9rminos%20y%20Condiciones%20no,de%20uso%20de%20su%20servicio

14. WIKIPEDIA
2018

"COMPUTACION EN LA NUBE"

Link:https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

ARTÍCULOS ONLINE:

15. BERCIANO, J.
29 de febrero de 2012
"LA IMPORTANCIA Y LA NECESIDAD DE PROTEGER LA INFORMACIÓN SENSIBLE"
web: redseguridad.com,
link.https://www.redseguridad.com/especialidades-tic/proteccion-de-datos/la-importancia-y-la-necesidad-de-proteger-la-informacion-sensible_20120229.html

16. CAMPOS, G.
2018
"TÉRMINOS Y CONDICIONES"
web: vendemas.plink.com
Link: https://vendemas.plink.com.co/que-son-terminos-y-condiciones

LEGISLACIÓN NACIONAL

17. Asamblea Legislativa Plurinacional de Bolivia.
12 de julio de 2018
"LEY N° 1080. LEY DE CIUDADANÍA DIGITAL"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

18. Asamblea legislativa plurinacional de Bolivia.
8 de agosto de 2011
"LEY N° 134 LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
Gaceta Oficial de Bolivia.
La Paz
Bolivia

19. Asamblea legislativa plurinacional de Bolivia.
5 de julio de 2012
"LEY N° 254 (CODIGO) CÓDIGO PROCESAL CONSTITUCIONAL"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

20. Concejo de ministros de Bolivia
13 de noviembre de 2013
"D.S. N° 1793 DECRETO SUPREMO"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

21. Consejo De Gabinete
17 de mayo de 2005.
"DS N° 28168 DECRETO SUPREMO, ACCESO A LA INFORMACIÓN DEL PODER EJECUTIVO"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

22. Consejo de ministros de Bolivia
06 de agosto de 1975
"LEY N° 12760
CÓDIGO CIVIL"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

23. Congreso Nacional De Bolivia
23 de agosto de 1972
"D.L. N°10426 CODIGO PENAL DE BOLIVIA"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

24. Congreso Nacional De Bolivia
13 de abril de 2004.
"LEY N° 2650 CONSTITUCIÓN POLÍTICA DEL ESTADO DE LA REPÚBLICA DE BOLIVIA"
Gaceta Oficial de Bolivia.
La Paz
Bolivia

25. Congreso Nacional De Bolivia
07 de febrero de 2009.

“CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA”
Gaceta Oficial de Bolivia.
La Paz
Bolivia

26. Tribunal Constitucional
23 de junio de 2004.
“SENTENCIA CONSTITUCIONAL 0965/2004-R”
Tribunal Constitucional de Bolivia
Sucre
Bolivia

27. Tribunal Constitucional
25 de octubre de 2010
“SENTENCIA CONSTITUCIONAL 1738/2010-R ”
Tribunal Constitucional de Bolivia
Sucre
Bolivia

LEGISLACIÓN INTERNACIONAL Y TRATADOS INTERNACIONALES

28. Asamblea Nacional De Ecuador
21 de mayo de 2021
“LEY DE PROTECCIÓN DE DATOS PERSONALES”
Quito
Ecuador

29. Congreso de la República de Perú
21 de junio de 2011
“LEY 29733 PROTECCIÓN DE DATOS PERSONALES”
Lima
Perú

30. Congreso General de los Estados Unidos Mexicanos
5 de junio de 2010
“LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES”
México D.F.
México

31. Congreso Nacional de Chile
18 de agosto de 1999
“LEY N° 19.628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA”
Santiago
Chile