UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

(PETAENG)

TRABAJO DIRIGIDO

Para optar al Título Académico de Licenciatura en Derecho

"CONDICIONES Y TÉRMINOS DEL USO DE FACEBOOK A LA LUZ DE NUESTRA LEGISLACIÓN ACTUAL"

POSTULANTE : Abuná Poma Rocio Mariela

TUTOR : M.S.C. DAEN Abog. Rubén Ramiro Rodríguez Jemio

La Paz - Bolivia

2023

DEDICATORIA

A mi familia, por ser el pilar fundamental de todo lo que soy, de mi educación académica, como de mi preparación para la vida, en especial a mi padre Rodolfo Abuná Salcedo. A mi psiquiatra Betania Aguilar y a mi psicóloga Ingrid Maldonado, debido a que sin su orientación habría sido imposible iniciar y continuar con los objetivos y metas trazados en mi vida.

AGRADECIMIENTO

Me gustaría agradecer la valiosa colaboración de amigos y colegas durante el proceso de investigación y redacción de este trabajo. Agradezco a mis padres y a mi tutor, Dr. Rubén Ramiro Rodríguez Jemio, por haberme orientado en todos los momentos que necesité sus consejos, y al Dr. Eulogio Villena y la Dra. Karina Ingrid Medinaceli Díez, debido a que sin su orientación este trabajo no habría podido culminarse.

INDICE

RESUMEN

El presente trabajo pretende analizar las Condiciones y términos de Uso de la Red Social Facebook en relación al Derecho de Protección de datos personales a la luz de nuestro ordenamiento jurídico nacional vigente. Intenta ofrecer interpretaciones con bibliografía tanto jurídica como doctrinaria, con el afán de encontrar necesidades y posibles soluciones.

Se hizo un acápite de Metodología para abordar el tema a investigar de manera ordenada con el fin de lograr tanto el objetivo general como los objetivos específicos. También se hizo una descripción de los métodos y técnicas a utilizar.

Posteriormente se realizó un Marco Conceptual que abordó los principales conceptos que sirvieron como referencia en la presente investigación utilizando tanto normativa jurídica como teoría.

Asimismo, se estableció con la colaboración del trabajo de expertos en el tema un Marco Teórico especificando la teoría necesaria para de este modo abordar las implicancias jurídicas de la Relación Jurídica de Facebook para con el usuario residente en Bolivia. Y determinar si efectivamente existe una protección adecuada a la autodeterminación informativa, por parte de los organismos propios de nuestro Estado.

Entre las conclusiones observamos la insuficiencia de nuestra normativa para proteger los datos personales de los usuarios en cualquier red social pero en concreto en Facebook. La única herramienta jurídica que tenemos en nuestro ordenamiento es la Acción de Protección de Privacidad. Sin embargo, esta garantía jurídica no viabiliza medios de prevención. Vale decir, que es aplicable únicamente posterior al daño.

INTRODUCCIÓN

El presente trabajo de investigación se denomina: "**CONDICIONES Y TÉRMINOS DEL USO DE FACEBOOK A LA LUZ DE NUESTRA LEGISLACIÓN ACTUAL**". El mismo, ha sido estructurado en una serie de segmentos o capítulos que permitieron que por medio del análisis tanto de la doctrina como de la normativa positiva, hayamos logrado con éxito los objetivos planteados.

En primer lugar presentamos el diseño de la investigación el cual está comprendido del enunciado del tema del trabajo dirigido, identificación del problema, y la problematización, así mismo, la delimitación del tema temática, espacial y temporal, finalmente se encuentra la fundamentación e importancia del tema de investigación, los objetivos tanto el general como los específicos, y las técnicas y métodos usados en el presente trabajo.

Posteriormente, se encuentran el Marco Histórico, el Marco Conceptual y el Marco Teórico los cuales permiten dar una referencia de aquello que la doctrina ha estudiado sobre la temática de la presente investigación. Seguidamente, enunciamos el Marco Jurídico, el cual, nos ha permitido reconocer y señalar la normativa jurídica nacional para así cumplir con el objetivo de analizar las implicancias jurídicas y si este marco permite una adecuada protección en cuanto a la autodeterminación informativa. De la misma manera, en este apartado, fue establecida normativa internacional.

Finalmente, realizamos el análisis de los hechos consistentes en la Política de Datos y Condiciones de Servicios de Facebook en contraste a nuestro ordenamiento jurídico. Con base a este análisis hicimos una propuesta de la investigación que contribuya a solucionar los problemas y falencias existentes. Así, pudimos arribar a conclusiones y recomendaciones.

METODOLOGÍA

1.1.- ENUNCIADO DEL TEMA DEL TRABAJO DIRIGIDO

Presento esta investigación bajo el enunciado: “Condiciones y términos del uso de Facebook a la luz de nuestra legislación actual”. Por medio de la misma investigación indagaremos sobre: la relación jurídica de Facebook con el usuario; la existencia o carencia de herramientas jurídicas de protección de datos personales dentro de nuestro ordenamiento jurídico actual; posibles vulneraciones al derecho a la protección de datos personales, un análisis de la Ley Nro.164 del 8 de agosto del 2011 que regula las telecomunicaciones en nuestro país y su reglamento, el Decreto Supremo Nro. 1793 del 2013; y normativa en cuanto a derecho comparado, considerando la existencia de los Estándares de protección de datos personales de la Red Iberoamericana de protección de datos; el Reglamento Europeo de protección de datos personales (GDPR) y demás normativa pertinente.

1.2.- IDENTIFICACIÓN DEL PROBLEMA

Con la invención de la Web 2.0, el internet ha pasado de ser un amplio soporte de información a convertirse en un medio imprescindible de comunicación multilateral. Una muestra de este hecho es la existencia y el uso masivo de las denominadas redes sociales. En este entendido, Facebook se ha constituído en una plataforma digital que permite una interacción social más allá de las fronteras geográficas. Facilita a sus usuarios hacer conexión, compartir fotografías, pensamientos personales, mensajería “privada”, entre otras funciones. A pesar de que el usuario no debe realizar ningún tipo de paga monetaria a cambio de estos servicios, Facebook utiliza un modelo de negocio cuyo medio de obtención de réditos es por la venta de publicidad y el tratamiento de los datos personales obtenidos a través de sus usuarios. Así, en el presente trabajo analizaremos las Condiciones y Términos del uso de

Facebook a la luz de nuestra legislación actual. Y de este modo, determinar si la misma es suficiente o si se requiere la creación de normativa jurídica.

1.3.- PROBLEMATIZACIÓN

La Relación Jurídica de la Red social Facebook y sus implicancias jurídicas en el Derecho a la protección de datos personales.

1.4.- DELIMITACION DEL TEMA

1.4.1. Delimitación temática

Analizaremos las Condiciones de Servicio y las Políticas de Datos que el usuario debe aceptar para crear y utilizar un perfil en Facebook, en ese entendido el presente trabajo de investigación se delimita en el Derecho Informático.

1.4.2. Delimitación espacial

Esta relación jurídica será analizada en el contexto de nuestro país, vale decir, nuestro ordenamiento jurídico nacional, sin perjuicio del análisis de normativa internacional que sirva como referencia.

1.4.3. Delimitación temporal

Si bien Facebook fue oficialmente creado el año 2004, las Condiciones de uso[1] han tenido una serie de modificaciones. Por lo que el análisis que proponemos se ubica, temporalmente, desde el 2022 hasta la actualidad.

[1] Antes denominadas: Declaración de derechos y responsabilidades.

1.5.- FUNDAMENTACIÓN E IMPORTANCIA DEL TEMA

En la era digital, la interacción social ha sufrido una serie de transformaciones debido a las nuevas tecnologías de la información y comunicación que funcionan como nuevos medios para satisfacer esta necesidad humana. La ética de la publicidad siempre ha sido cuestionada, incluso antes de Internet. Si un modelo de negocio plantea el tratamiento de datos personales de millones de personas para realizar publicidad segmentada y de este modo generar ganancias exorbitantes, es deber de los gobiernos, asegurar la protección de los derechos de cada uno de los usuarios. El tratamiento de los datos personales podría permitir una serie de beneficios para la desburocratización de la justicia, la implementación de políticas públicas en el sector de la salud o, la gestión del tráfico por el análisis de datos de ubicación geográfica (Frigerio, 2018). Sin embargo, los datos personales identifican o hacen identificable a una persona, por lo que su protección implicaría la salvaguarda de otros derechos tales como la dignidad, la privacidad, la intimidad, etc. Vale decir, todo aquello que lo hace humano.

Realizar un análisis de las implicaciones jurídicas con el uso de internet y en particular con el uso de las redes sociales es una necesidad urgente e imprescindible. El Internet no dejará de ser parte de nuestra vida actual y futura, por el contrario, vamos hacia un uso progresivo de las funciones y herramientas que nos ofrece. El conocimiento de las posibles vulneraciones sobre nuestros derechos es imperativo para encontrar soluciones a los problemas que pueden suscitar, pero sobre todo para prevenirlos. Por medio de la autocritica y el análisis de la realidad es posible determinar falencias o lagunas jurídicas. Y dado que cada realidad es diferente, con la revisión de nuestro ordenamiento jurídico vigente, en relación con esta problemática, es posible identificar la caducidad o actualidad del mismo.

1.6.- OBJETIVOS DEL TEMA

1.6.1. Objetivo general

Analizar las Condiciones y Términos de uso de la red social Facebook y nuestra legislación actual.

1.6.2. Objetivos específicos

- Determinar los términos en los que empieza una relación jurídica con la red social Facebook, señalando las implicaciones y consecuencias jurídicas de esta relación, así como las posibles vulneraciones al derecho a la protección de datos personales.
- Analizar la vigencia, caducidad o insuficiencia de la normativa nacional que regula la protección de datos personales para posteriormente realizar las propuestas de solución pertinentes.
- Determinar las conclusiones y recomendaciones en cuanto a todo lo estudiado en el presente trabajo.

1.7.- MÉTODOS

1.7.1 Métodos Generales

Método inductivo

De acuerdo al Portal Digital del Diccionario Jurídico el método inductivo:

> *"(…) La inducción es el razonamiento que parte de fenómenos particulares y se eleva a conocimientos generales; por ejemplo, tenemos a un sujeto, a éste se le estudia a profundidad para saber qué hecho a cometido o qué conducta ha llevado a cabo, a sí mismo se estudian los factores que influyeron en la*

> *realización de determinado hecho. Del estudio de diversos casos individuales, se pasa a lo que son inducciones estadísticas, se pasa a lo general, de esta manera es como se han elaborado los Códigos Penales y los Manuales de Conducta, de la repetición, así tenemos que si muchos sujetos no se adaptan a la sociedad, la destruyen o no respetan los derechos de los demás, hablamos de una conducta general antisocial, si varios sujetos se apoderan de bienes ajenos de manera ilegal, comenten el delito de robo. Se va de cada caso individual a elevarlos a conductas generales (…)"* (Diccionario Jurídico, 2023).

Para Donatella della Porta la deducción es un proceso mediante el cual se sacan conclusiones directamente de sus premisas mediante la lógica. En cambio, la inducción implica *"(…) el estudio de casos reales, de los cuales se sacan conclusiones generales.*" (Della Porta & Michael, 2013)

Las redes sociales son una realidad actual en nuestra sociedad, por lo tanto, en la presente investigación utilizaremos el Método Inductivo. El motivo por el que me permito el uso de este método es porque las redes sociales son una parte de internet que utiliza de forma descontrolada los datos personales de los usuarios. Además para realizar un adecuado análisis de las problemáticas de internet, es muy importante hacer una revisión caso por caso. Por lo que considero que debe existir una revisión de cada caso en concreto para determinar adecuadamente una doctrina general, que permita llegar a soluciones más optimas.

En la presente investigación, me limito al análisis de un caso en particular, es decir, las condiciones y usos de la red social Facebook, para de este modo hacer un contraste con nuestra legislación nacional y determinar de este modo si existe o no la necesidad de crear normativa jurídica específica, lo que en relación al método inductivo, vendría a ser una generalidad, consecuencia del

análisis de un caso particular. De este modo, obtendremos pautas para construir conclusiones generales que se traducirán en necesidades y posibles soluciones

1.7.2 Métodos específicos

Método Exegético

Para el profesor Ramos Nuñez *"(…) Constituye el estudio lineal de las normas tal como ellas aparecen dispuestas en el texto legislativo (…)"* (Ramos Nuñez, 2007). Utilizaremos este método para hacer una revisión de la normativa sobre protección de datos personales aplicable al caso particular que son Las Condiciones y Términos de la red social Facebook.

1.7.3.- Técnicas de investigación

Recopilación Documental o escrita

Ezequiel Ander-Egg señala que la recopilación documental es *"(…) un instrumento o técnica de investigación social cuya finalidad es obtener datos e información a partir de documentos escritos y no escritos, susceptibles de ser utilizados dentro de los propósitos de una investigación en concreto (…)"* (Ander-Egg, 1995)**.** Debido a los objetivos del presente trabajo, la recopilación documental es la técnica principal que utilizaremos para la obtención de datos. Se realizará una recolección de material bibliográfico, teórico y doctrinal, así como jurídico.

Fichaje

Es una técnica de investigación documental que *"(…) sirve tanto para registrar y ordenar la documentación consultada, analizada y contrastada, como para la correcta redacción del informe final (…)"* (Barragán & Et.al., 2007). Es una

técnica de organización de datos, tanto bibliográficos como de resumen, análisis, textual, etc.

En el presente trabajo, hice un uso amplio de esta técnica, debido a la amplia información que existe sobre la temática. Me permitió organizar la información y de este modo pude analizarla y hacer uso de ella.

CAPÍTULO I

MARCO HISTÓRICO

Historia de Facebook

En los inicios del internet, la dinámica virtual era eminentemente estática y unidireccional, donde pocos creaban contenido web y la mayoría únicamente recibía información. Con la creación y el uso de la web 2.0 esta dinámica se transformó en colaborativa y multidireccional, permitiendo así la interacción entre usuarios.(Roa Navarrete, 2013)

> *"(…) La Web 2.0 (…) se caracteriza por tener una base comunitaria de usuarios, contando con un amplio abanico de herramientas web para fomentar la colaboración, participación, relación, intercambio y generación de contenidos, como son las redes sociales, blogs, wikis, y otros espacios compartidos. (…)"* (Roa Navarrete, 2013)

Bajo este contexto aparece Facebook, una red social creada por Mark Zuckererg en octubre del 2003. Cuya configuración difiere de aquello que se acostumbraba en internet. Sus *"(…) contenidos, la navegación y el comportamiento de usuario, producen impacto en la propia plataforma*" (Roa Navarrete, 2013).

Crea una serie de nuevas realidades en el ámbito del Derecho relacionadas sobre todo con la privacidad y sus componentes, los Derechos de autor y el Derecho penal en cuanto a la creación de nuevas formas de delitos: los "ciberdelitos".

A pesar de haber sido creada como un espacio de interacción social virtual, en la actualidad, Facebook es una empresa altamente lucrativa que se encarga de

la difusión de publicidad para obtener ingresos, para este fin utiliza estratégicamente la información proporcionada por sus mismos usuarios a quienes va destinada la publicidad.

En la Tesis: “Facebook un espacio de interacción virtual” Cárdenas Ramírez, autor de la obra, hace un breve relato del inicio de esta Red Social. Señala que Zuckerberg -creador de Facebook- era un universitario de 25 años nacido en White Plains en Estados Unidos, quien junto con sus compañeros de habitación creó thefacebook.com, que posteriormente sería conocida simplemente como Facebook.com (Cárdenas Ramírez, 2009). Incentivado por la herramienta Ágora25 que solo permitía publicar una fotografía, el número de habitación en la cual sus compañeros de universidad vivían dentro del campus y su correo electrónico. El autor señala que la plataforma fue concebida para la construcción de una base de datos universal y de interacción social.

> *“(…) Tras noches y semanas de arduo trabajo de programación, en febrero 4 de 2004 thefacebook.com fue lanzado al mundo universitario. Rápidamente Facebook se convirtió en una herramienta usada por gran parte de los estudiantes universitarios de Norteamérica, tan sólo diez meses después de haber sido lanzado, Facebook había alcanzado el millón de usuarios. Para el año 2006 Facebook había logrado abrirse a cualquier persona que quisiera unirse, en 2007 Facebook lanza su aplicación para poder acceder a la página desde teléfonos móviles, durante el 2008 la página es lanzada en español, lo cual provocaría una gran expansión hacia los usuarios de habla hispana y en 2009 se da un hito histórico en la transmisión de eventos por Internet (…)”* (Cárdenas Ramírez, 2009)

Facebook básicamente empezó a generar ingresos monetarios desde sus inicios en 2004 por medio de la venta de pequeños espacios publicitarios. Sin embargo, fue el 2007 cuando oficialmente creo su plataforma de publicidad

permitiendo que empresarios puedan crear perfiles empresariales y así poder interactuar con los usuarios. Asimismo, introdujo el “Social Ads” que permite que el empresario pueda saber si un usuario particular visitó su página. Permite, además que se pueda identificar a usuarios objetivo y los “amigos” de estos y su información personal. De esta manera la publicidad aparece tanto en el feed de cualquier usuario como en un espacio designado para ello en la plataforma. (Fuchs, 2020)

El 2011, Facebook implementó las “Sponsored Stories” que posibilitó la aparición de publicidad pagada directamente en el feed del usuario que derivan de páginas o amigos a quienes el usuario ya dio *like*. No obstante, recién a partir del 2012, habilitaron la publicidad para celulares. (Fuchs, 2020)

El 2014, implementó una nueva estructura publicitaria que consistía en tres niveles: campañas publicitarias, set de publicidad y la publicidad en concreto. Con esta nueva estructura cada anuncio publicitario tenía un objetivo, un presupuesto, un horario y un segmento de usuarios seleccionados. (Fuchs, 2020)

En 2016, introdujeron bots para Messenger que daba la oportunidad de que sus “clientes” incorporaran mensajes con esponsor o “Click-to-messenger” ads. Ya para 2018 y 2020 expandieron el formato publicitario, dando la opción de que este pueda ser: fotografía, video, stories, por Messenger, carousel, slideshow, collection o playable content. (Fuchs, 2020)

El año 2021, Fabebook anunció el rebranding de Facebook por Meta, bajo la intención de, en el lapso de 10 a 15 años, trabajar en realidad virtual (Ramírez, 2021).

El escándalo de Cambridge Analytica

El año 2018 se descubrieron diversas afectaciones al Derecho a la protección de datos por parte de Facebook hacia los usuarios. Los medios de difusión New York Times, The Guardian junto al canal británico Chanell 4 difundieron investigaciones periodísticas que revelaban como se usaron de manera ilegal los datos personales de usuarios de Facebook para manipular resultados electorales en el 2016 para el triunfo de Trump en Estados Unidos, así como en el Brexit. (Vercelli, 2018)

Esto inició cuando una empresa de análisis psicométrico implementó dentro del API de Facebook una aplicación[2] denominada: "This is my digital life" fue que aparentemente buscaba realizar un estudio psicológico para identificar rasgos de personalidad, y conducta del usuario en la red social que incluía ubicación, género, cumpleaños, etc. Obteniendo esta información se contactó con Cambridge analítica y Strategical communication laboratories que se encargaban de marketing y publicidad electoral. De acuerdo a las investigaciones pudieron ser más de 80 millones de usuarios afectados, a quienes se les expuso propaganda electoral por medio de micropublicidad personalizada, vale decir, adecuada a cada usuario por medio de toda la base de datos recopilada por Global Science Research. (Vercelli, 2018)

Las consecuencias de estas investigaciones fueron audiencias con el Parlamento Europeo hacia los responsables directos de estas empresas incluidos personal de Facebook Ink. A partir de este suceso, las políticas de tratamiento de datos personales en la plataforma de Facebook fueron modificadas y Cambridge Analytica se declaró en quiebra arguyendo excesivos gastos legales y la pérdida de clientes. (Vercelli, 2018)

[2] Sin embargo, de acuerdo a los testimonios de los extrabajadores de Cambridge Analytica es posible que hayan sido muchas aplicaciones.

Cabe resaltar que esta vulneración de derechos no fue descubierta por ningún gobierno, sino por periódicos privados y la confesión de un ex trabajador de Cambridge Analytica.

CAPÍTULO II

MARCO CONCEPTUAL

Dato

De acuerdo a la RAE puede ser entendido desde tres definiciones: Primero, como *"(…) información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho (…)"*. Segundo como *"(…) documento, testimonio, fundamento (…)",* y tercero como *"(…) información dispuesta de manera adecuada para su tratamiento por una computadora (…)"*. (Real Academia Española, s.f. definición 1, 2 y 3)

Dato de carácter Personal

De acuerdo a Elena Gil Gonzales un dato de carácter personal es *"(…) cualquier información concerniente a personas físicas identificadas o identificables (…)"* (Gil, 2016). Así mismo, de acuerdo a los Estándares de Protección de Datos Personales un dato personal es identificable cuando *"(…) su identidad pueda determinarse directa o indirectamente siempre y cuando esto no requiera plazos o actividades desproporcionadas (…)*" (RIPD, 2017). El reglamento de la Ley 164 o Reglamento para el desarrollo de Tecnologías de Información y comunicación señala que datos personales son "(…) *toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable (…)"* (Decreto Supremo N° 1793, 2013, Artículo 3).

Big data

Elena Gil Gonzales indica que es un *"(…) conjunto de tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, con el objetivo de poder otorgarles una utilidad que proporcione valor. (…)"* (Gil, 2016)

Metadato

Senso y De la Rosa definen un metadato *como "(…) toda aquella información descriptiva sobre el contexto, calidad, condición o características de un recurso, dato u objeto que tiene la finalidad de facilitar su recuperación, autentificación, evaluación, preservación o interoperatividad (…)"* (Senso y De la Rosa, 2003) Los autores señalan como ejemplos a: índices de documentos contenidos en una intranet, direcciones IP o DNS, o términos extraídos por los motores de indización/búsqueda (Senso y De la Rosa, 2003).

Intimidad

Viene a ser una esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas o conocimiento de terceros, salvo excepciones muy concretas contenidas en la Ley. Protege elementos físicos e instrumentales; como la vivienda, la correspondencia o las comunicaciones privadas; y elementos sustanciales o datos sensibles sobre el individuo como su ideología, religión, creencias, vida sexual o salud. (Salgado, 2010)

Privacidad

Facultad de una persona de prevenir la difusión de datos pertenecientes a su vida privada que, sin ser difamatorios ni perjudiciales, esta desea que no sean divulgados.(Diccionario panhispánico del español jurídico, 2020). Para Víctor Salgado, la privacidad apareció recién el 2001 dentro de la Real Academia de nuestra lengua. El autor explica que fue sacado del derecho anglosajón como un instrumento que trasluce el derecho a estar solo, a que el Estado nos deje estar solos. Si bien, tenía un contenido parecido a la intimidad, en la actualidad sirvió para denominar a la privacidad de nuestros datos personales en contenidos informáticos o electrónicos. Su esfera de protección abarcaría todos los datos que una entidad tenga sobre un ciudadano. (Salgado, 2010)

Minería de datos

"El Data Mining es un conjunto de técnicas y tecnologías que permiten explorar grandes bases de datos, de manera automática o semiautomática, con el objetivo de encontrar patrones repetitivos que expliquen el comportamiento de estos datos."[3]

Red social

Para Javier Sanchez Iregue, red social es "*un conjunto de personas que interactúan a partir de intereses comunes."* Así, divulgan información relacionada con su vida personal, gustos, profesiones opiniones, etc.(Sanchez Iregui, 2018). Bajo este análisis, las redes sociales pondrían en tela de juicio muchas concepciones jurídicas y reglas establecidas respecto de diversas áreas del derecho, principalmente por ser plataformas y actividades no reguladas, al menos no directamente. (Roa Navarrete, 2013)

Pueden clasificarse de diversas maneras. Pablo Fernández Burgueño (Fernandez B., 2009), distingue principalmente dos tipos de redes sociales: analógicas o Redes sociales Off-Line en donde las relaciones sociales, con independencia de su origen, se desarrollan sin mediación de aparatos o sistemas electrónicos; y las digitales o Redes sociales On-Line que tienen su origen y se desarrollan a través de medios electrónicos. (Fernandez B., 2009). En referencia a nuestra investigación, propone la siguiente clasificación:

Por su público objetivo y temática:

- **Redes sociales Horizontales:** dirigidas a todo tipo de usuario y sin una temática definida. Su estructura permite la entrada y participación libre y genérica sin un fin definido.

[3] https://www.iebschool.com/blog/data-mining-mineria-datos-big-data/

- **Redes sociales Verticales:** tiene el objetivo de agrupar un colectivo de personas con base en una temática especializada concreta. Estas pueden ser redes profesionales; como LinkenIn; de ocio y mixtas.
- **Redes sociales Verticales Profesionales:** Están dirigidas a generar relaciones profesionales entre los usuarios. Los ejemplos más representativos son Viadeo, Xing y LinkedIn.

Por el sujeto principal de la relación:

- **Redes sociales Humanas:** buscan fomentar relaciones entre individuos según sus perfiles sociales individuales de gustos, aficiones, y otras actividades.
- **Redes sociales de Contenidos:** los usuarios se interconectan por medio de contenidos, como el caso de Scribd.

Por su localización geográfica:

- **Redes sociales Sedentarias:** se transforma de acuerdo a las relaciones entre sus usuarios, lo que comparten o los eventos.
- **Redes sociales Nómadas:** incluye, además de las relaciones entre usuarios, su ubicación geográfica.

Habeas data.- Acción constitucional que puede ejercer cualquier persona incluida en un registro de datos para acceder al mismo y recabar la información que le afecte, así como para solicitar su eliminación o corrección si tal información fuera falsa o estuviera desactualizada. (Diccionario panhispánico del español jurídico, 2020). En nuestro ordenamiento jurídico constitucional se denomina Acción de Protección de Privacidad.

Protección de datos

Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y

los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.(Diccionario panhispánico del español jurídico, 2020)

Contrato de adhesión.- Es aquel acuerdo entre partes en donde *"(…) queda excluida toda posibilidad de regateo y discusión entre las partes. (…) las cláusulas son previamente determinadas por uno solo de los contratantes, de modo que el otro contratante no tiene poder de introducirle modificaciones (…)"* (Mélich-Orsini, 1985)

Durante la gestión 2011, fue promulgada la Ley General De Telecomunicaciones, Tecnologías De Información Y Comunicación o Ley N° 164; la cual, en su artículo 6, presenta una serie de definiciones. En este entendido, las siguientes son las que conciernen a la presente investigación:

- **Tecnologías de Información y Comunicación – TIC.** Comprende al conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.
- **Telecomunicaciones.** Comprende la transmisión, emisión y recepción, de señales, símbolos, textos, imágenes, video, voz, sonidos, datos o información de cualquier naturaleza o aplicaciones que facilitan los mismos, por cable o línea física, radioelectricidad, ondas hertzianas, medios ópticos u otros sistemas radioeléctricos de cualquier índole o especie, a través de una red pública o privada.
- **Usuaria o usuario.** Es la persona natural o jurídica que utiliza los servicios de telecomunicaciones y tecnologías de información y comunicación, como destinatario final. Para

efectos de esta Ley, se considera a los socios de las cooperativas de telecomunicaciones como usuarias o usuarios.

- **Comercio electrónico.** Es toda relación de índole comercial sea o no contractual, con la intervención o a partir de la utilización de una o más comunicaciones digitales.

Asimismo, el Decreto Supremo 1793 del 13 de noviembre de 2013, que aprueba el Reglamento de la Ley 164, presenta las siguientes definiciones que serán de utilidad para nuestro trabajo:

- **Contenido digital:** Información digitalizada generada bajo cualquier modo o forma de expresión que puede ser distribuida por cualquier medio electrónico y es parte de un mensaje que el sistema de transferencia o soporte no examina ni modifica, salvo para conversión durante el transporte del mismo.
- **Aplicaciones digitales:** Programas de software modulares, específicos e interactivos de usuario o multiusuario, utilizados sobre plataformas de prestación de servicios digitales en general o equipos terminales destinados a comunicaciones personales, fines educativos, productivos o de entretenimiento, entre otros.
- **Mensaje electrónico de datos:** Es toda información de texto, imagen, voz, video y datos codificados digitalmente, creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que pueden ser intercambiados por cualquier sistema de comunicación electrónico.
- **Tratamiento de los datos personales:** Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Correo electrónico comercial:** Todo mensaje, archivo, dato u otra información electrónica, enviada por cualquier medio electrónico con el fin de difundir, ofertar y publicitar bienes o servicios.

- **Correo electrónico no deseado:** Todo mensaje, archivo, dato u otra información enviada periódicamente, por cualquier medio electrónico dirigido a un receptor con quien el emisor no tiene relación alguna y es enviado sin su consentimiento.
- **Seguridad informática:** Es el conjunto de normas, procedimientos y herramientas, las cuales se enfocan en la protección de la infraestructura computacional y todo lo relacionado con ésta y, especialmente, la información contenida o circulante.
- **Seguridad de la información:** La seguridad de la información es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio y confiabilidad.
- **Plan de contingencia:** Es un instrumento que comprende métodos y el conjunto de acciones para el buen gobierno de las Tecnologías de la Información y Comunicación en el dominio del soporte y el desempeño, contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del servicio y las operaciones de una entidad, en circunstancias de riesgo, crisis y otras situaciones anómalas.
- **Soberanía tecnológica:** Es la posesión del control por parte de una nación y/o estado sobre la tecnología que utiliza. Se caracteriza por el acceso al conocimiento sobre el contenido y los procedimientos, procesos y técnicas necesarios para el desarrollo y uso de dicha tecnología, el mismo que le permite auditar, mejorar, desarrollar, modificar y ajustar a sus necesidades específicas la misma, sin la intervención ni autorización específica de terceros; de modo que se garantice la total independencia en cuanto al control de la tecnología utilizada por dicha nación o estado con respecto a compañías, empresas, personas, naciones o estados.
- **Descolonización del conocimiento tecnológico e informacional:** Es el proceso social y científico que permite

romper los lazos de dependencia tecnológica e informacional de una nación y/o estado con respecto a terceras personas, empresas, naciones o estados y desarrollar conocimiento y tecnología propia, acorde a sus necesidades, retos y características, partiendo del diálogo entre los conocimientos locales y universales disponibles. Es un proceso de intercambio cultural, de conocimientos y tecnologías, con otras sociedades, naciones y/o estados dispuestos a compartir sus propios desarrollos e interiorizar los externos, respetando el derecho de los otros a conocer los contenidos y los procedimientos, procesos y técnicas necesarios para el desarrollo y uso de las tecnologías en general y de las tecnologías de la información y la comunicación en particular. La descolonización del conocimiento tecnológico e informacional está directamente relacionada con el desarrollo de capacidades científicas e institucionales para garantizar el manejo y aprovechamiento soberano de los recursos naturales y el desarrollo económico del Estado Plurinacional de Bolivia en la construcción del vivir bien.

- **Mensaje de datos:** La información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos – EDI, el correo electrónico, el telegrama, el télex o el telefax.
- **Intercambio electrónico de datos:** La transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto.

La Red iberoamericana de Protección de datos personales, al ser un referente para la creación de normativa para la protección de datos personales en Iberoamerica, señala, en su artículo 3, ciertas definiciones (RIPD, 2017). Las siguientes serán de utilidad para el presente trabajo:

- **Anonimización:** la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.
- **Consentimiento:** manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen.
- **Datos Personales**: cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.
- **Datos personales sensibles:** aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.
- **Encargado:** prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste.
- **Exportador:** persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

- **Responsable:** persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales.
- **Titular:** persona física a quien le conciernen los datos personales.
- **Tratamiento:** cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.

CAPÍTULO III

MARCO TEÓRICO

4.1.- LA IMPORTANCIA DEL DATO PERSONAL

En el capítulo referido al Marco conceptual, siguiendo la línea de Gil Gonzáles y los Estándares de Protección de Datos Personales, se define como Dato de Carácter Personal como cualquier información que le concierna a una persona física como identificada o identificable (Gil, 2016), es decir, cuando directa o indirectamente puede determinarse su identidad y esto no requiera plazos o actividades desproporcionadas (RIPD, 2017).

El término: "cualquier información" tiene como característica principal el sentido amplio de interpretación que otorga al concepto de dato personal. Puede involucrar *"(…) elementos objetivos y subjetivos a partir de los cuales se puede lograr la identificación de la persona (…)"* (Fernández, et al., 2019)

La palabra "concerniente" implica que está vinculado a una persona física. En este entendido, Fernández et al., haciendo referencia al Grupo de trabajo del artículo 29 (GTA29) de la Comisión Europea de Protección de Datos, señala que para la vinculación a una persona se debe tomar en cuenta 3 elementos: elemento contenido, elemento finalidad y elemento resultado, que no necesariamente aparecen de manera simultánea, sino de manera alternativa. Así, contenido se refiere a los datos "(…*) sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero o de la repercusión de esa información en el interesado (…)"* (Fernández et al., 2019). Siguiendo la misma línea del GTA29, la finalidad determina que los datos se utilizan; o probablemente se utilicen; para evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona. En cuanto al resultado, el GTA29 determina que *"(…) basta que la persona pueda ser tratada diferente por otras personas*

como consecuencia del tratamiento de tales datos (…)" (Fernández et al., 2019). Es decir, que independientemente de que se produzca los elementos de finalidad y contenido, el uso de los datos, repercutan en los derechos e intereses de la persona física (Fernández et al., 2019).

De acuerdo a Richter, existen diferentes categorías atendiendo a las legislaciones sobre el tema. El autor señala las siguientes: de identificación; como el nombre o el teléfono, laborales; ser PEP[4], patrimoniales, académicos, ideológicos y filosóficos, de salud, los que definen características personales; como el ADN, los que representan características físicas y "*(…) los que configuran vida y hábitos sexuales, origen (étnico y racial.); entre otros (…)*" (Richter, 2015). Sin embargo, hay una categoría que merece un tratamiento especial, esta categoría son los datos personales sensibles.

4.1.1.- DATO PERSONAL SENSIBLE

Un Dato personal sensible, adoptando la definición de los Estándares de Protección de Datos personales, son *"(…) aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste (…)*" (RIPD, 2017). Asimismo, los Estándares señalan que Tratamiento es "*(…) cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizados sobre datos personales (…)*" (RIPD, 2017). Este tipo de operaciones pueden ser el almacenamiento, análisis y combinación de Datos personales para fines de segmentación publicitaria, como hace Facebook en su modelo de negocio.

> Los datos personales sensibles *"(…) forman parte de un determinado grupo de informaciones susceptibles de una reconsideración respecto a una categoría general y homogénea por sus especiales peculiaridades y*

[4] Persona públicamente expuesta. De acuerdo a la EDV: *"Boliviano que desempeña o ha desempeñado funciones públicas destacadas y prominentes en un país, por elección o nombramientos ejecutivos; así como los individuos de alto perfil público ya sea por afiliación política o de actividad privada vinculada al poder político."*

características, que los constituye en una categoría especial de datos, protegidos bajo reglas específicas (…)" (Fernández et al.,2019)

Este tipo de información personal puede estar referida a creencias religiosas, enfermedades, posición política, preferencias sexuales y un largo etc. Que se encuentra en la esfera más intima de una persona. Por lo que su tratamiento equívoco o abusivo puede generar daños de mayor impacto para el individuo en particular.

Los datos personales son la información que refleja nuestra identidad personal. Se encuentra tanto en nuestra esfera íntima, como los datos de salud; como en nuestra esfera privada, como nuestros datos biométricos. Nos hacen ser personas únicas. Reflejan nuestros intereses más profundos. Nos diferencian del resto y permiten que nos hagamos distinguibles de y para los demás.

Con el Internet y las nuevas tecnologías de la información y comunicación, se ha hecho mucho más sencilla la obtención de estos datos de forma masiva. Pero, donde radica la mayor ventaja para los almacenadores de datos, está en el análisis de los mismos para diferentes fines. Facebook, es una de las empresas que más datos personales ha almacenado y con el tratamiento de los mismos ha sabido lucrar de tal manera que, según el portal Statista, para 2020 obtuvo un total de 86.000 millones de dólares y un incremento del 21% durante el 2021 (Fernández, 2021)

4.2.- TRATAMIENTO DE DATOS Y EL BIG DATA

Las nuevas tecnologías permiten un sin fin de oportunidades de negocio, investigación e innovación frente a la vida y sus desafíos. Por años, el análisis y recolección de datos debía realizarse de forma manual por diversos métodos y estrategias estadísticas. La posibilidad de automatizar estos procesos ha facilitado el análisis de grandes cantidades de datos, sin tener que realizar muestreos para la obtención de resultados y correlaciones.

> *La informática ha abierto una gama de posibilidades: a) la rapidez en el archivo y formación de datos; b) la casi instantánea transmisión de datos; c) la simultánea comunicación de todos en un acto; d) el almacenamiento completo y abarcador en poco espacio; e) la posibilidad, por lo tanto de conformar a la persona humana; f) construir una proyección del porvenir; g) comunicar al mundo de dicha realidad virtual; h) rapidez en la búsqueda y encuentro de los resultados.* (Richter, 2015)

Bajo este entorno, se ha hecho urgente repensar el Derecho, en cuanto; garantía de derechos subjetivos individuales.

De acuerdo a al Diccionario de protección de datos personales del INAI[5] Tratamiento viene a ser "(…) las actividades que involucran la ejecución de determinados procedimientos o acciones tendientes a la utilización de datos personales por parte del responsable, el encargado del tratamiento o un tercero (…)" (Fernández, et al., 2019). Para que estas actividades afecten directamente el Derecho de autodeterminación informativa, el tipo de tratamiento de datos personales debe cumplir la finalidad de creación de un perfil personal y la posible predicción de preferencias, comportamientos y actitudes (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 2016)

El perfil personal se genera por medio de la obtención, por medio de métodos informáticos de correlaciones por la penetración en las aptitudes de comportamiento individuales, como señala Francois Rigaus, citado por Garriga. Estas correlaciones, o el perfil personal, encasillan a una persona en función del tratamiento informatizado de sus datos y de la manera en que se repartan los roles en el grupo social en el que se encuentre, es decir, su contexto. De este resultado pueden surgir actos discriminatorios hacia la persona cuando busque un trabajo, o un crédito (Garriga, 2009)

> "(…) el uso desviado de la tecnología de tratamiento de datos personales supone claros peligros para la libertad, para el derecho a no ser

[5] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de los Estados Unidos Mexicanos.

discriminado y, asimismo, para la propia dignidad personal." (Garriga, 2009)

Actualmente, es posible la utilización de tecnologías, como el big data, el machine learning y la minería de datos, para la obtención de resultados e información mucho más específica y exacta.

Para autores como Elena Gil, el big data no es una tecnología sino un planteamiento de trabajo que permite obtener valor y beneficios a través del tratamiento de grandes volúmenes de datos por parte de compañías, autoridades y otras organizaciones cuyo análisis se basa en el uso de algoritmos. Lo relevante es el valor comercial que esta tecnología puede explotar en el descubrimiento de conocimientos ocultos de estos datos. *"(…) cuando transformamos la realidad en datos, podemos transformar la información en nuevas formas de valor. Un ejemplo de estos nuevos servicios son los motores de recomendaciones automatizados (…)"* (Gil, 2016) de los que se vale la publicidad.

Asimismo, permite la *datificación* que implica transformar información no estructurada que antes no podía cuantificarse como la localización, fotografías, imágenes, etc. En Facebook, tal y como lo declaran en su Política de Datos *"(…) incluso nuestras amistades y gustos son transformados en datos, a través de los gráficos de relaciones sociales o los «likes» (…)"* (Gil, 2016).

Desde la óptica de Gil sus principales atributos son:

- Volumen, sustituyendo el uso de la muestra en la estadística tradicional, debido a que con el big data se puede analizar grandes cantidades de datos.
- Velocidad, lo que posibilita la rapidez de transferencia, de forma barata y eficiente, de datos en tiempo real y datos que ya fueron almacenados.
- Variedad, es decir, los datos provienen de fuentes estructuradas como no estructuradas.

- Veracidad, la confiabilidad de los datos se regula con base a la incertidumbre, creando un contexto entorno a los datos combinando diversas fuentes.
- Visualización, con el big data se puede combinar datos para de este modo predecir o visualizar eventos futuros.
- Valor, tanto económico como en términos de innovación.
- Utilización intensiva de algoritmos, por medio de un proceso denominado *machine learning* es posible encontrar correlaciones o información nueva sin la necesidad de plantear una hipótesis previa a esta búsqueda y de hallar correlaciones nuevas y más específicas.

Por otro lado, la Minería de Datos es una actividad usada en varias áreas como la prevención de enfermedades o la mejora de seguridad, sin embargo, *"(…) debe tenerse presente que el tratamiento de la información tiene implicaciones éticas cuando se trata de datos sobre personas (...)"* (Franganillo, 2010). Otra de las disciplinas que utiliza esta tecnología es la publicidad. De acuerdo a López Jiménez, esta herramienta prepara, sondea y explora los datos. De este modo, saca información oculta con la finalidad de obtener los datos de potenciales consumidores (Hand, 19998; Mena, 1999 citados por López, 2011) a quienes se les oferta productos con base en lo anteriormente adquirido y su perfil personal (López, 2011). En pocas palabras, se almacena y analiza la información para vender, prediciendo posibles actividades comerciales, es decir; el comportamiento.

> *"(…) La recopilación de información personal es preocupante porque se realiza de forma deliberadamente silenciosa. Y el ser humano suele ignorar los peligros que no le son evidentes: cree tener su vida bajo control sin tener presente que personas ajenas a su entorno toman ciertas decisiones que les afectan, basándose en datos personales que no ha proporcionado de manera consciente, o que creía olvidados o secretos (…) La minería de datos revela cómo se puede influir sobre las personas y cómo se las puede*

> *manipular para obtener un beneficio que no suele ser mutuo, sino exclusivo de quien posee y explota esos datos."* (Franganillo, 2010)

Por su parte, Victor Salgado Seguin, si bien no da una definición de minería de datos, señala una serie de riesgos de las redes sociales; como por ejemplo: que las empresas "(…) dirigen sus campañas de promoción y publicidad a las redes sociales, tratando muchos de los datos de los interesados para confeccionar perfiles de gustos y compras potenciales." (Salgado, 2010) Una diversidad de entidades acceden a estas redes para obtener información de sus usuarios para "(…) procesos de selección, control de productividad y bajas de empleados, perfiles de personalidad, evaluación de solvencia y crédito, evaluación de concesión de subvenciones, seguros, etc." (Salgado, 2010) Aclara que los datos obtenidos pueden ser transferidos a países diferentes a la residencia del usuario. (Salgado, 2010)

Así como el bigdata y la minería de datos, existen otras como el frontendverification, utilizado para contrastar la exactitud de información personal con información similar (Clarke, 1994 citado por López, 2011); el computer profiling, que combina datos elementales generando valor al conocer perfiles comerciales de los clientes (Ford, 2010 citado por López, 2011); el database marketing, vinculado especialmente a la relación del receptor y el anunciante, busca almacenar información de clientes actuales y potenciales (Ramonet, 2002 citado por López, 2011). Los factores comunes de cada una de estas tecnologías es el manejo de una base de datos personales, la creación de un perfil personal por medio de correlaciones de datos, y la predicción potencial de comportamientos.

> *"Estas posibilidades tienen como contracara peligros tales como: 1) recopilación de datos sensibles en instituciones no autorizadas para recabar estos datos; 2) cesión a terceros de la información, vulnerando los fines para los cuales fue recogida; 3) impedir que la persona interesada tome conocimiento de los datos que se manejan sobre ella; 4) mantener*

eternamente la información, sin dar lugar al llamado derecho al olvido." (Richter, 2015)

El peligro, como indica Denninger citado por Garriga, no se encuentra en el carácter del dato, ni si es o no secreto, "lo que importa es su utilidad y la posibilidad de su aplicación" (Garriga, 2009). Podemos concluir, acoplándonos a la postura de Ana Garriga, que la falta de control sobre el tratamiento de los datos personales y el uso abusivo de los bancos de datos personales no solo pone en juego la intimidad, sino, principalmente: la identidad personal.

4.4.- El Derecho de Protección de Datos o Derecho de autodeterminación informativa

4.4.1.- Origen

El derecho a autodeterminación informativa surgió en Alemania por medio de la Sentencia del 15 de diciembre de 1983 dictada por el Tribunal Constitucional alemán, bajo un contexto de protesta en donde el gobierno exigía la recopilación exhaustiva de datos personales. Dicha Sentencia fue dictada debido a una "Reclamación Constitucional" propuesta por la abogada Wild y Stadler-Euler arguyendo que la Ley de Censo de 1983 vulneraba el libre desenvolvimiento de la personalidad, la dignidad humana, la libertad de expresión y garantías procesales, siendo todos estos derechos constitucionales. (BCJ, 2008)

Previamente, existía ya en Alemania la Ley Federal de protección de datos del 27 de febrero de 1977, que en su artículo 5 que prohibía la comunicación, elaboración, utilización o facilitación a terceros de datos protegidos de índole personal para fines que no sean legalmente autorizados. Sin embargo, La Ley de Censo no prescribía la existencia de ninguna oficina específica que elaborara las estadísticas municipales, por lo que "no había garantía de que se utilizasen los datos exclusivamente para finalidades estadísticas" (BCJ, 2008)

Entre otras vulneraciones que fueron el argumento para la creación de la Sentencia del 15 de diciembre de 1983 en contra de la Ley de Censo están:

- Anonimato Estadístico: no se debe establecer relación alguna entre los datos recopilados y la persona individualizada.
- Especificidad: la ley no esclarecía con precisión los fines por los cuales los datos recopilados podían ser utilizados, por lo que su tratamiento podía ser amplio y sin control, pudiendo generar múltiples perjuicios.
- Recopilaba datos personales sensibles, en específico la pertenencia a una asociación religiosa.
- Imprecisión en cuanto a los objetivos en el tratamiento de los datos, vale decir; quien los trata, quien dispone, donde, cómo y qué datos.

4.4.2.- Derivación de la intimidad a Derecho Autónomo

Es sabido que los Derechos Humanos involucran diferentes generaciones de derechos que han ido surgiendo a partir de la aparición de realidades y problemáticas. Así los Derechos de primera generación salvaguardan los derechos individuales, los derechos de segunda generación los Derechos sociales, económicos y culturales. Los derechos de tercera generación, tal como lo explica Aristeo García Gonzales aparecen como emergencia de la contaminación de libertades surgida por las nuevas tecnologías. (García Gonzales, 2007)

> "(…) La intimidad, marcada por un matiz individualista, era la facultad destinada a salvaguardar un determinado espacio con carácter exclusivo, y que consistía en un derecho del individuo a la soledad y a "tener una esfera reservada en el cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella" (…)" (García Gonzales, 2007)

Así, el Derecho a la Autodeterminación Informática, inicialmente aparece como un derivado del Derecho a la Intimidad, para posteriormente cobrar autonomía como Derecho Humano. Según García Gonzales, la protección de la intimidad resulta insuficiente cuando en su concepción garantista defiende las invasiones indebidas. Al mismo tiempo debe ser contemplada también como un "Derecho

activo de control". Esta concepción vendría a denominarse como estatus positivo que controla el flujo de informaciones y datos que involucran a cada individuo (García Gonzales, 2007).

> "(…) Al tratarse de un derecho con un carácter abierto y dinámico que está frente a una sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura actual, Frossini, señalaba acertadamente que el control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro de crédito, así como de las reservas de viajes, representan muestras conocidas de la omnipresente vigilancia informática de la existencia habitual de la persona. Por lo que la vida individual y social corre el riesgo de hallarse sometida a un "juicio universal permanente" (…)" (García Gonzales, 2007)

En este entendido, García adopta la definición de Protección de Datos de Hondius que señala que es *"aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos"* (García Gonzales, 2007).

Señala García que aquello que diferenciaba al ser humano, su inteligencia, ha sido expropiada por las computadoras creándose así la "inteligencia artificial". Es esta quien permite tratar, transmitir y elaborar información. García citando a Benda, indica que el peligro radica en la imposibilidad del ser humano de disponer sobre sus datos, y tener pleno conocimiento de quien y con qué objeto se transmiten. *"(…) Dicha facultad de elección de la persona sobre la revelación o no de informaciones que le conciernen constituyen el núcleo de la autodeterminación informativa (…)"* (García Gonzales, 2007).

El Derecho de autodeterminación informativa no solo se fundamenta bajo el argumento de no querer compartir la información personal para mantener la vida privada lejos de los demás, sino también porque el tratamiento de datos personales puede implicar tanto consecuencias beneficiosas como dañinas (Garriga, 2004). En este sentido, *"(…) el uso exclusivamente del perfil*

informático en la toma de decisiones que afecten a un individuo significará normalmente su discriminación en muchas de las actividades de la vida cotidiana (…)" (Garriga, 2004)

No implica solo la falta de información que tienen los otros sobre los demás, sino el control que tenemos sobre la información que nos concierne. Pasa a ser de cerrado y estático a abierto y dinámico por el contexto social que ha cambiado (García Gonzales, 2007). Así, la protección de datos, especialmente si se trata de datos personales sensibles, implica el uso democrático de las nuevas tecnologías de la información y comunicación (García Gonzales, 2007).

> "(…) en las sociedades informatizadas del presente, el poder ya no reposa sobre el ejercicio de la fuerza física, sino en el uso de las informaciones que permiten influir y controlar la conducta de los ciudadanos, sin necesidad de recurrir a medios coactivos (…) El derecho a la intimidad ha pasado de ser una libertad negativa –esto es, una libertad propia del individualismo que exige el respeto a los demás; es decir, un derecho de defensa- a una libertad positiva en donde el individuo cuenta con la facultad de poder controlar toda aquella información que le sea relevante y le concierna a él mismo." (García Gonzales, 2007)

CAPÍTULO IV

MARCO JURÍDICO

5.1.- Consideraciones previas

El Derecho a la protección de datos personales o derecho a la autodeterminación informativa no está especificado en nuestra normativa jurídica. De ahí viene la urgencia de crear una ley de protección de datos personales. No obstante, ha habido casos en nuestro país en los cuales se ha utilizado la vía constitucional de la Acción de protección de Privacidad para el resguardo de este derecho.

De la misma manera, si bien existe normativa como la Ley 164 y su reglamento aprobado por el D.S. 1793, que regula aspectos relacionados a internet, no especifican ninguna regulación sobre el tratamiento de datos. Estas normas jurídicas se refieren en mayor medida a las telecomunicaciones y a la firma y certificado electrónico.

A pesar de esta limitación, se hizo el ejercicio de extraer de nuestro ordenamiento jurídico, posibles Derechos e instrumentos procesales que puedan; aunque de manera insuficiente; amparar la autonomía informática en relación a la revisión de las condiciones de servicio y las políticas de Datos de Facebook.

5.2.- Legislación Nacional

Debido a que el presente trabajo pretende hacer un análisis de nuestra normativa nacional en relación a Facebook y el derecho a la Protección de Datos Personales, a continuación se detalla la normativa relacionada.

Acción de Protección de Privacidad

La Acción de Protección de Privacidad está regulada por la CPE, por el art. 130 y 131 y por el CPC; art. 58 a 63. Es una de las Acciones de defensa constitucional, que en este caso, es la única herramienta jurídica para la protección de datos personales en nuestro país.

Presenta dos dimensiones de protección. En primer lugar está la protección de potestades del ciudadano boliviano, frente a actos ilegales o indebidos. Estas potestades involucran datos registrados en archivos o bases de datos y se desglosan bajo los siguientes verbos:

- Conocer
- Objetar
- Obtener la eliminación
- Obtener la rectificación

La segunda dimensión protege la afectación a los Derechos de:

- Privacidad personal
- Privacidad familiar
- Propia imagen
- Honra
- Reputación

Si bien, la CPE determina su procedimiento por el de la Acción de Amparo Constitucional. El CPC señala, que debido a su naturaleza cautelar, puede interponerse de forma directa.

En cuanto a la legitimación activa, esta puede ser interpuesta tanto por la persona directamente afectada, como por sus herederos, por la Defensoría del pueblo, y la Defensoría de la Niñez y Adolescencia. Puede interponerse frente a personas naturales o jurídicas que sean responsables del archivo o banco de datos, o que tengan en su poder los datos o documentos pasibles de afectar los derechos que protege.

Las únicas limitaciones son el secreto de prensa y el Derecho de huelga.

Código Civil

Nuestro Código Civil no regula la protección de datos personales, sin embargo, enuncia una serie de derechos, como los derechos de la personalidad, que; en su afectación y nivel de protección; pueden engendrar la utilización de datos de de carácter personal, de acuerdo al caso concreto.

Sobre los derechos de la personalidad, indica que son inherentes al ser humano y se hallan fuera del comercio y que cualquier limitación a su libre ejercicio es nula cuando afecta al orden público o a las buenas costumbres. Estos, de acuerdo a la normativa civil, se ejercen por las personas individuales sin ninguna discriminación. Asimismo, son inviolables por lo que cualquier hecho contra ellos confiere al damnificado la facultad de demandar el cese de ese hecho, aparte del resarcimiento por el daño material o moral.

Asimismo, nuestro Código Civil establece en su artículo 12 la protección del nombre cuando este se dispute o el titular sufra algún perjuicio por su uso indebido, por lo que se otorga la potestad de pedir judicialmente el reconocimiento de este derecho o la cesación del uso lesivo. El artículo 13 le otorga esta misma protección al seudónimo cuando este adquiere por su difusión igual importancia.

Sobre el Derecho a la Imagen, al honor y a la intimidad suscribe lo siguiente:

> “ARTÍCULO 16. (DERECHO A LA IMAGEN).- I. Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga

> cesar el hecho lesivo. II. Se comprende en la regla anterior la reproducción de la voz de una persona.
>
> ARTÍCULO 17. (DERECHO AL HONOR).- Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.
>
> ARTÍCULO 18. (DERECHO A LA INTIMIDAD).- Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley (…)" (Código Civil, 1975)

A su vez, el Código Civil en su artículo 19 suscribe que la correspondencia epistolar y otros papeles privados son inviolables y no pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente, y al mismo tiempo, señala que no surten ningún efecto legal las cartas y otros papeles privados que han sido violados o sustraídos, ni las grabaciones clandestinas de conversaciones o comunicaciones privadas.

En el artículo 20 de la misma normativa se prohíbe al destinatario de una carta misiva de carácter confidencial la divulgación del contenido sin el asentimiento expreso del autor o de sus herederos forzosos, pero puede presentarla en juicio si tiene un interés personal serio y legítimo.

En el caso de fallecimiento del destinatario, el autor o sus herederos forzosos pueden pedir al juez ordene se restituya, o sea destruida, o se deposite la carta misiva en poder de persona calificada, u otras medidas apropiada.

Ley 164 o Ley General de Telecomunicaciones, Tecnologías de información y comunicación

La Ley 164 fue promulgada el 8 de agosto de 2011. General de Telecomunicaciones señala, por mandato del artículo 54 de esta Ley, exigir respeto a la privacidad e inviolabilidad de las comunicaciones, es un derecho del usuario, exceptuando los expresamente señalados por la Constitución Política del Estado y la Ley.

Crea el Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC), para la proposición de políticas y planes nacionales de desarrollo del sector de tecnologías de información y comunicación. Dicho Comité está integrado por los Ministerios de Obras Públicas, Servicios y Vivienda; Comunicaciones, Educación, Planificación del desarrollo y la ADSIB[6]. Así mismo, instaura el Consejo Sectorial de Telecomunicaciones y Tecnologías de información y comunicación (COSTETIC), instancia consultiva de proposición y concertación entre los diferentes niveles de gobierno nacionales.

Frente a la protección de datos personales, la Ley 164 señala como un Derecho de las usuarias o usuarios la potestad de solicitar la exclusión, sin costo alguno, de las guías de usuarias o usuarios disponibles al público, ya sean impresas o electrónicas; de decidir sobre cuáles datos personales se incluyen, así como comprobarlos, corregirlos o suprimirlos; de reclamar ante los proveedores de servicios y acudir ante las autoridades competentes en aquellos casos que la usuaria o usuario considere vulnerados sus derechos, mereciendo atención oportuna; y de recibir protección del proveedor del servicio sobre los datos personales contra la publicidad no autorizada por la usuaria o usuario.

Decreto Supremo 1793

Fue promulgado el 13 de noviembre de 2013, y aprueba el Reglamento a la ley 164 para el desarrollo de la tecnología de la información y comunicación. Con

[6] Agencia de Desarrollo para la sociedad de la Información en Bolivia

respecto al presente tema de investigación podemos mencionar el artículo 3 en su parágrafo IV que describe definiciones sobre datos personales, de la siguiente manera:

- Datos personales: toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable.
- Autorización: consentimiento previo expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada."
- Tratamiento de datos personales como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

En este mismo artículo en el parágrafo VII se señalan definiciones respecto a la soberanía: la dependencia tecnológica, la soberanía tecnológica y la descolonización tecnológica. En términos generales, se refieren al control o la falta de este, sobre la tecnología por parte del Estado y su población sobre diferentes acciones como el control, el uso, la modificación, ajuste o auditorias sobre la tecnología y su conocimiento.

El artículo 4, numeral II menciona los principios para el tratamiento de datos personales, sin embargo, limita este tratamiento a actos de certificación personal. Estos son el principio de finalidad, veracidad, transparencia, seguridad y confidencialidad.

En el artículo 8 manda a las entidades públicas la promoción de seguridad informática para la protección de datos por medio de planes de contingencia.

El título II regula específicamente la conformación y las funciones del Comité Plurinacional de Tecnologías de información y comunicación (COPLUTIC) y, al Consejo Sectorial de Telecomunicaciones y Tecnologías de información y comunicación (COSTETIC). Cabe resaltar que a la COPLUTIC, entre otras, se le asigna la función de:

- Proponer programas de capacitación, sensibilización y socialización ene le uso y aprovechamiento de las TIC
- Proponer líneas de acción para la seguridad informática”
- Promover la adaptación y apropiación por parte de la sociedad boliviana de saberes y conocimientos relacionados a las TIC.
- Proponer normas adecuadas para la protección y defensa de los usuarios de medios, mensajes y recursos informáticos.

Del mismo modo, la COSTETIC tiene la función de “proponer y coordinar mecanismos necesarios para fomentar el acceso, uso y apropiación social de las tecnologías de información y comunicación” (D.S. 1793, 2011), entre otras.

Ley de ciudadanía digital

Tiene la finalidad de regular el acceso y ejercicio de la ciudadanía digital, que viene a ser “(…) el ejercicio de derechos y deberes a través del uso de tecnologías de información y comunicación en la interacción de las personas con las entidades públicas y privadas que presten servicios públicos delegados por el Estado (…)” (Ley N° 1080, 2018). En este entendido, busca la desburocratización causada por la presencia física del interesado en cuanto a servicios públicos o trámites. Otorga validez a la firma digital, y a las notificaciones digitales con el previo consentimiento del administrado. Hace imperativo para los funcionarios e instituciones que utilizan datos personales, que no desvíen el tratamiento de datos a otros fines que no sean los establecidos por la ley.

Decreto Supremo 28168

Fundando sus postulados en los Derechos fundamentales de Petición y Transparencia, este Decreto supremo busca garantizar el acceso a la información de toda persona respecto a los datos de las instituciones que conforman el Poder ejecutivo. Hace responsable a todo servidor público; del Poder ejecutivo; a que otorgue al peticionante toda información que no esté previamente declarada como secreta, reservada o confidencial por autoridad

competente. Del mismo modo, y sin perjuicio de la Acción de protección de privacidad, otorga al interesado el instrumento de la Petición de Habeas Data por la vía administrativa para actualizar, rectificar, eliminar o complementar sus datos.

Sentencia Constitucional 0819/2015-S3

La sentencia 0819/2015-S3 fue realizada el 10 de agosto de 2015 en atención a una Acción de Protección de Privacidad interpuesta por Belmonte contra Medinaceli. La accionante busca protección constitucional debido a la difusión en internet en 21 plataformas digitales por parte de Medinaceli de un video de contenido sexual en el que se evidenciaba su participación, sin consentimiento de Belmonte.

En líneas generales la acción denegó la tutela frente a Medinaceli bajo el argumento de no poder considerarlo como sujeto a legitimación pasiva de la acción, dado que existía un proceso penal en curso, interpuesto por Belmonte contra Medinaceli por diferentes delitos. Por lo que, se encuentra amparado bajo la garantía de la presunción de inocencia.

No obstante, el Tribunal Constitucional reconoce que incluso sin existir legitimación pasiva, tratándose de un hecho que vulnera gravemente los derechos fundamentales de privacidad, intimidad, honra y honor, propia imagen, dignidad y autodeterminación informática, de la accionante, la tutela debe realizarse inmediatamente.

De este modo, sin establecer responsabilidad, ordena al Fiscal General del Estado y al Fiscal de materia adopten medidas de protección pertinentes a favor de la accionante. Asimismo, exhorta al Fiscal General a que adopte la implementación de medidas de protección a la víctima, y Al Defensor del Pueblo a que haga seguimiento a esta implementación y su eficacia.

5.4.- LEGISLACIÓN COMPARADA

Red Iberoamericana de Protección de Datos Personales[7]:

Surge en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos y con el apoyo político de la **XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos** celebrada en Santa Cruz de la Sierra, Bolivia, 14 y 15 de noviembre de 2003. (RIPD, 2017)

> "(…) Se constituye como un: "(…) foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos, así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho." (RIPD, 2017)

Entre sus logros se encuentran el desarrollo de diez Encuentros, y Seminarios sobre: *"(…) protección de datos de los menores, (…) las nuevas tecnologías y su impacto sobre la privacidad; transferencias internacionales, etc."* Y, desde 2003, la promulgación de *" (…) leyes generales de protección de datos personales en Uruguay, México, Costa Rica, Perú, Nicaragua, Colombia, República Dominicana, Brasil y Panamá (…)"* (RIPD, 2017); la existencia de

[7] En adelante: RIPD

iniciativas legislativas en Chile, Ecuador y El Salvador; y el reconocimiento de la Comisión Europea de Argentina y Uruguay como países con nivel de protección adecuada (RIPD, 2017). Sin embargo, su logro principal es la creación y aprobación de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Sus objetivos y organización *"(…) están recogidos en el **Reglamento** aprobado con motivo del **VI Encuentro Iberoamericano de Protección de Datos**, celebrado en mayo de 2008, y revisado en el **XVI EIPD**, en Noviembre de 2018, en San José, Costa Rica."* (RIPD, 2017)

A la fecha, la RIPD cuenta con los siguientes países e instituciones internacionales miembros: Andorra, Argentina, Brasil, Chile, Colombia, Costa Rica, Cabo Verde, República Dominicana, Ecuador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Perú, Portugal, Paraguay, Santo Tomé y Príncipe, El Salvador, Uruguay y otras organizaciones como FIIAPP – Eurosocial, Supervisor Europeo de Protección de Datos (EDPS), Organización de Estados Americanos (OEA), y el Comité Consultivo del Convenio 108 (Consejo de Europa).

Estándares de Protección de Datos Personales[8]

Son un conjunto de directrices orientadoras para los países de la región iberoamericana que no cuentan con normativa de protección de datos personales, o para modernizar y actualizar su ordenamiento jurídico respecto a este derecho fundamental. (RIPD, 2017).

Fueron propiciados por la RIDP y aprobados en el XV Encuentro Iberoamericano de Protección de Datos del 20 al 22 de junio de 2017 en la ciudad de Santiago de Chile.

[8] En adelante: Estándares.

Estos Estándares tienen los objetivos de:

> "(…) garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región. (…) Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, así como entre los Estados Iberoamericanos, el cual responda a las necesidades y exigencias internacionales que demanda el derecho a la protección de datos personales en una sociedad en la cual las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana. (…) Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales. (…) Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento social y económico de la región. (…) Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia." (RIPD, 2017)

Reglamento Europeo de Protección de Datos Personales

Fue aprobado el 27 de abril de 2016 por el parlamento europeo y el Consejo de Europa. Reemplaza a la Directiva 95/46/CE. Es una normativa que ha servido de gran inspiración para países latinoamericanos, debido a que tiene la finalidad de establecer un marco general para los miembros de la Unión europea en cuanto al tratamiento y el flujo de datos personales.

Entre sus particularidad, plantea una serie de principios entre los que se encuentra el de extraterritorialidad, vale decir, que la protección a los

ciudadanos va mas allá de la Unión. Señala una serie de definiciones como responsable de tratamiento, encargado, delegado, etc. Del mismo modo, hace especial hincapié al modo en que se permite el tratamiento de datos personales sensibles y no sensibles. Obliga a cada Estado miembro a designar presupuesto y medidas técnicas para un órgano independiente de control, señalando a su vez la conformación del Comité Europeo de Protección de datos.

Tiene una inclinación de prevención a los daños posibles por vulneraciones en el tratamiento de datos. Debido a esto, obliga a las empresas, grupos empresariales y bancos de datos que deban tener una autorización previa por parte de la autoridad de control. Asimismo, regula Evaluaciones de impacto previas al tratamiento de datos para determinar posibles daños antes de que ocurran. Ha logrado reconocimiento internacional por sus amplias disposiciones y por su aplicación extraterritorial.

> "(…) puede obligar no solo a las empresas ubicadas en la UE que traten datos personales, sino también a las empresas ubicadas en otros países que traten información personal de ciudadanos europeos (…)". (Bojalil & Vela-Treviño, 2019)

Otorga a autoridades pertenecientes a la Unión Europea llevar a cabo investigaciones de cumplimiento, la posibilidad de evaluar que un país, territorio o sector garantice un nivel adecuado de datos personales, y otorga un estimulo financiero para países no pertenecientes a las Unión Europea para incorporar a sus legislaciones medidas de protección de datos al nivel de este reglamento.

Legislación latinoamericana

En Argentina su legislación se ha mantenido casi sin cambios desde el 2000. En 2018, se propuso un proyecto de ley para reemplazar la Ley Nº 25,326 con el fin de alinear la legislación Argentina con el Reglamento Europeo; incluyendo: nuevos conceptos como "datos genéticos", "datos biométricos" y "cómputo en la

nube"; la limitación a los titulares de datos personales únicamente a personas físicas, excluyendo a personas morales; la obligación a los organismos gubernamentales a designar a un oficial de protección de datos, en caso de que datos personales sensibles o grandes cantidades de datos estén siendo procesados; y estándares para la legalidad del tratamiento de datos personales, así también, derechos adicionales para los titulares de los datos, como el derecho a oponerse o restringir el tratamiento de sus datos personales y el derecho a la portabilidad (Bojalil & Vela-Treviño, 2019).

En Brasil por se mantuvieron diversas leyes sectoriales, hasta julio de 2018 cuando el Senado de Brasil aprobó la Ley General de Protección de Datos de Brasil, estableciendo un régimen único de protección de datos personales cuyas determinaciones incluyen la creación de una autoridad nacional de protección de datos, la obligación a empresas y organismos gubernamentales que traten datos personales a nombrar un oficial de protección de datos; y la imposición de multas de hasta el 2% de los ingresos brutos en el último año fiscal de un grupo empresarial en Brasil en caso de incumplimiento. (Bojalil & Vela-Treviño, 2019)

México aprobó el 2010 la Ley Federal Mexicana de Protección de Datos Personales en Posesión de Particulares, la cual es la base de un conglomerado de leyes referidas al tratamiento de datos personales. Las mismas otorgan derechos de acceso, rectificación, cancelación u oposición al tratamiento de datos personales a los titulares de los datos. (Bojalil & Vela-Treviño, 2019)

> "(…) Si bien las leyes mexicanas ofrecen flexibilidad y la posibilidad de autorregulación, es probable que México adopte, hasta cierto punto, disposiciones de protección de datos personales y seguridad comparables a las regulaciones europeas. Por ejemplo, México se adhirió recientemente a la Convención Europea para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal ("Convención 108") y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de

> Datos. El Convenio 108 impone obligaciones a los Estados Parte, tales como la inclusión de principios y disposiciones para el tratamiento de datos personales a su legislación local. (…)" (Bojalil & Vela-Treviño, 2019)

Perú promulgó la Ley No. 29,733 el año 2011. Sus disposiciones buscan una protección amplia y otorgan derechos a los titulares de los datos en caso de que las empresas que tratan sus datos personales no cumplan con sus obligaciones. Entre sus disposiciones están la obligación del responsable del tratamiento de datos de notificar cualquier transferencia de datos que resulte de una fusión y/o adquisición de una empresa y de registrar las transferencias internacionales de datos en un registro nacional peruano. (Bojalil & Vela-Treviño, 2019)

CAPÍTULO V

ANÁLISIS DE LOS HECHOS

6.1.- INTRODUCCIÓN

En el presente capítulo, realizaremos una interpretación de toda la bibliografía y la información que recopilamos a lo largo de este trabajo. Nuestra intención es cumplir con nuestro objetivo general el cual es: “Analizar la relación jurídica de la red social Facebook con relación al Derecho a la Protección de datos personales”. Para este cometido, en primer lugar analizaremos las Condiciones de servicio y las Políticas de datos de Facebook con relación al tratamiento de datos personales. Y finalmente, señalaremos posibles vulneraciones en cuanto al Derecho a la protección de datos personales.

6.2.- Políticas de Datos y Condiciones de Servicio

Facebook suscribe dos tipos de contratos en general. Por un lado, lo hace con los usuarios que crean perfiles en la plataforma; y por otro, con los anunciantes de publicidad, vale decir empresas externas. Estas últimas, son la fuente directa de lucro que tiene la plataforma, vale decir, de tipo comercial con carácter oneroso. Respecto a los usuarios o personas particulares, la relación contractual es a “título gratuito”, es decir, que no representa ningún costo monetario el crear un perfil y hacer uso de los servicios que ofrece la plataforma, para las personas que desean y aceptan las condiciones de creación de perfiles personales. Sin embargo, la información que cada usuario almacena y “voluntariamente” otorga a la red social, viene a ser una fuente indirecta de lucro comercial para la empresa. Las estrategias por medio de las que se administran, seleccionan, discriminan, clasifican, etc. Los datos personales de los millones de usuarios de la plataforma son la causa del éxito comercial del funcionamiento de Facebook.

Esta transacción es con base a un contrato de adhesión que suscriben los usuarios con la red social, que tiene la característica de modificarse sin la existencia de una negociación previa, limitándose a comunicar estas modificaciones al usuario. Las opciones de la persona son aceptar las modificaciones o dejar de usar la plataforma.

En cuanto al contrato o las condiciones y términos de uso que un usuario debe aceptar para crear una cuenta o perfil en Facebook, la Ley general de los derechos de las usuarias y los usuarios y de las consumidoras y consumidores establece lo siguiente:

> "Artículo 19. (CONTRATOS DE ADHESIÓN). I. El contrato de adhesión es aquél en el que las cláusulas son dispuestas unilateralmente por un proveedor de productos o servicios, normalmente mediante un formulario preimpreso, de manera que la otra parte no pueda modificarlas o negociarlas, limitándose a aceptarlas o rechazarlas en su integridad. II. Los modelos de contratos de adhesión deberán ser previamente aprobados por la autoridad que otorgue la autorización de la actividad, conforme a las disposiciones de la presente Ley y la normativa específica.
>
> Artículo 20. (EFICACIA DE LOS CONTRATOS DE ADHESIÓN). Los contratos de adhesión que no cumplan con las condiciones establecidas carecerán de eficacia jurídica total o parcial, previa determinación fundamentada por la autoridad competente.
>
> Artículo 21. (CONTENIDO DE LOS CONTRATOS DE ADHESIÓN). I. Los contratos de adhesión deben cumplir mínimamente lo siguiente: a. Contener toda la información sobre los términos, modalidades, limitaciones y cláusulas a las que se someten las usuarias y los usuarios, las consumidoras y

los consumidores al momento de contratar, así como los medios y lugares que se disponen para que se realicen los pagos. b. Estar redactados en términos claros, sencillos y comprensibles, legibles a simple vista y en idioma castellano u optativamente en otro idioma oficial del Estado que sea de conocimiento del adherente. II. El contrato de adhesión no podrá hacer remisiones a otros documentos que no se entreguen a las usuarias y los usuarios, las consumidoras y los consumidores, salvo que la remisión sea a una norma de carácter público. Artículo 22. (CLÁUSULAS ABUSIVAS EN LOS CONTRATOS). Son cláusulas abusivas aquellas que dejan a las usuarias y los usuarios, a las consumidoras y los consumidores en estado de total desventaja y desigualdad frente a los proveedores de productos o servicios. Son cláusulas abusivas las que: a. Excluyan o limiten los derechos de las usuarias y los usuarios, las consumidoras y los consumidores, así como las que impliquen renuncia o restricción a formular reclamos o denuncias. b. Establezcan a favor del proveedor, la facultad unilateral de modificar los términos del contrato de consumo o servicio, previamente suscrito.

c. Exoneren de responsabilidad al proveedor. d. Establezcan el silencio de las usuarias y los usuarios, las consumidoras y los consumidores, como aceptación de prestaciones adicionales no requeridas, pagos u otras obligaciones no estipuladas expresamente. e. Señalen que la información personal o crediticia de las consumidoras y los consumidores, será compartida con otros proveedores, salvo lo dispuesto en normativa específica. f. Otras que se establezcan en la normativa específica. III. Las cláusulas abusivas insertas en los contratos, se tendrán por no puestas y no producirán efecto legal alguno.” (Ley 453, 2013)

6.3.- Vulneraciones al Derecho a la Protección de Datos personales

Facebook promete servicios por medio del uso de los datos que cada usuario proporciona a la plataforma. El análisis de nuestros datos personales son utilizados para ofrecer experiencias personalizadas, las conexiones con personas y organizaciones, así como contenido, productos y servicios con temáticas concretas de acuerdo a la información que brinda cada usuario.

La información que recopila es: datos personales referidos a la identidad exigiendo el nombre real y permitiendo el uso de un pseudónimo. También recopila información del contenido que sus usuarios comparten, tales como: fotografías personales o publicaciones de terceros. Y por último, recopila información de mensajes privados y públicos. Por lo que es difícil tener plena seguridad de respeto hacia la intimidad de sus usuarios. Y esto se agrava debido a que expresamente, Facebook no se responsabiliza de los posibles perjuicios, bajo la consigna de que cada usuario es quien debe velar por la información que ofrece, los contactos con los que se comparte su contenido. Deja la responsabilidad plena al usuario.

Datos con protección especial: de acuerdo a su Política de Datos permite la publicación de información sobre creencias religiosas, ideologías políticas, interés o aspectos relacionados con salud, creencias filosóficas haciendo hincapié en que esta información puede estar sujeta a protecciones especiales de acuerdo a las leyes de nuestro país. Sin embargo, deja expresamente claro que la jurisdicción donde se resolverán reclamaciones es exclusivamente el Tribunal Federal del Distrito Norte de California de los Estados Unidos o en su caso en un Tribunal estatal del condado de San Mateo.

De acuerdo a su Política de Datos, utiliza la siguiente información:

- Datos personales

- Información financiera sobre transacciones con sus productos
- Información de otros usuarios relacionados con el titular, vale decir, las interacciones y comunicaciones que mantienen.
- Información de los dispositivos que se usan conociendo las características del dispositivo tales como: atributos, operaciones, identificadores, señales del dispositivo, de de la configuración, red y conexiones, datos de cookies.
- Obtiene información de empresas socios de ellos mismos, que les otorga sobre actividades fuera de Facebook. Vale decir, que extrapola la red social y se sirve de datos externos.

De la misma manera señala lo siguiente:

> "(…) estos socios nos brindan información sobre las actividades que realizas fuera de Facebook, incluidos datos sobre el dispositivo que utilizas, los sitios web que visitas, las compras que haces, los anuncios que ves y la manera en la que usas sus servicios, ya sea que tengas o no una cuenta de Facebook o hayas iniciado sesión en ella (…)" (Facebook)

El fin principal es la búsqueda de la atención, personalizando las funciones y el contenido (feed o muro) por ello la se sirven de la información brindada para proporcionar sus productos, que pueden ser la misma red social o los anuncios publicitarios que son la fuente de ingresos de la empresa.

> "(…) usamos tus conexiones, preferencias, intereses y actividades en función de los datos que recopilamos y que tú y otras personas nos proporcionan (incluidos aquellos datos con protecciones especiales que decides facilitarnos), así como la forma en la que usas nuestros Productos e interactúas con ellos, y las personas, los lugares o las cosas con los que te conectas y que te interesan, tanto dentro como fuera de nuestros Productos (…)" (Facebook)

Esta información se comparte por medio de los productos de Facebook, las personas y las cuentas con las que se tiene comunicación y en donde se almacenan estos datos. Como ya lo repetimos depende mucho del usuario, permitir o no el conocimiento público de la información personal. Sin embargo, todos los datos son utilizados por: Apps, sitios web e integraciones de terceros en sus productos o que usan sus productos, posibles propietarios nuevos de la empresa, socios externos, anunciantes, socios de medición, socios que ofrecen bienes y servicios en los productos de Facebook, vendedores y proveedores de servicios, investigadores y académicos, autoridades y solicitudes legales. (Facebook)

La desventaja de esta Red Social respecto a sus usuarios es excesivamente notoria. Considerando, además, la cantidad de usuarios que día a día se suscriben a esta plataforma, Facebook, es un depósito gigante de información. Por lo que sostenemos que es importante y urgente normar las realidades que representa.

6.4.- ¿Nuestra normativa jurídica es suficiente?

- Frente a vulneraciones tenemos completa indefensión porque no contamos ni siquiera con una normativa básica que proteja nuestro derecho de autodeterminación informativa en casos específicos. Mucho menos, contamos con un organismo que regule, autorice y resguarde el tratamiento lícito y conforme a finalidades éticas de los bancos de datos en nuestro Estado, por lo que es casi imposible poder hacer frente a irregularidades con organismos transnacionales, como es Facebook.
- No existe un órgano especializado que permita la prevención de contravenciones, en el tratamiento de los datos personales, incluso sensibles, que proporcionamos en esta red social. De ahí, que exista la posibilidad de la utilización de nuestros datos con finalidades como en el caso de Cambridge Analytica. Es insuficiente el compromiso unilateral de

Facebook de utilizar la extensa base de datos de la que es propietaria para los fines que declara en su Política de Datos y las Condiciones de Servicios.

- Nuestra normativa comercial frente a controversias, estipula que se respeta la jurisdicción que se establezca en el contrato, en este caso, la jurisdicción está en Estados Unidos. Si adoptamos que la aceptación de la condiciones de servicio como un contrato de adhesión. En casos particulares, la persona tendría que asumir la jurisdicción aceptada en las Condiciones de Servicio. Actualmente, Estados como los de la Unión Europea debido a que cuentan con un Reglamento de protección de Datos personales de donde se desprende la Autoridad de Protección de datos personales, han logrado multar a Facebook por haber cometido contravensiones en cuanto a la seguridad de los datos personales de sus habitantes.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

8.1.- CONCLUSIONES

- La Relación jurídica de Facebook con un usuario inicia y se mantiene por medio de un contrato de adhesión, por el cual la persona se obliga a aceptar que entendió y leyó todos los términos y condiciones de servicio, las cuales se encuentran en su mayoría en el idioma inglés. Este contrato tiene también una clausula que permite que Facebook pueda modificar los términos en el futuro, de manera unilateral.
- Por la dinámica en la que funciona esta Red social, el Derecho a la Privacidad Personal se encuentra en un nivel alto de vulneración. Esto se debe, a la dificultad que tiene el usuario de tener pleno control de su información personal. Estos datos interactúan rápidamente con otros usuarios de la red social, además, que es sumamente sencillo guardar información ajena por un tercero.
- Debemos agregar que las diversas aplicaciones y empresas que trabajan junto a Facebook tiene acceso a una inmensidad de datos de sus usuarios de forma muy sencilla. Por esta razón, líneas arriba, mencionamos el caso de Cambridge Analytica y la minería de datos. Afirmamos que al ser empresas con bastante poder, existe un desbalance demasiado amplio en relación a un particular que utiliza la red social, por lo que debe ser el Estado el que por medio de políticas intervenga para garantizar el respeto a la privacidad personal.
- Tenemos una ley que regula las telecomunicaciones y las tecnologías de información y comunicación, sin embargo, la misma centra su atención en la infraestructura y las viabilidades físicas y de servicio. Por lo tanto, hay una

falencia en cuanto a la regulación de software y plataformas como Facebook.

- A nivel internacional existe normativa que protege los datos personales. El caso más importante es el de la Unión Europea y su Reglamento para la protección de la privacidad que ha sido inspiración de normativa para países latinoamericanos como México, Argentina, Brasil y Perú. Con estos precedentes, consideramos de suma urgencia la necesidad de una ley de protección de datos personales, que otorgue herramientas de salvaguarda de derechos pero también genere la producción de políticas educativas para la población en general.

8.2.- RECOMENDACIONES

- El presente trabajo centró su atención en el Derecho de protección de datos personales, sin embargo, es necesario hacer un análisis de todas las aristas que implican las redes sociales, como por ejemplo: los derechos de autor y nuevas formas de tipologías delictivas.
- Si bien, Facebook hace abierta la declaración sobre los servicios que ofrece y la manera en que usa la información de sus usuarios, es evidente que esta información sigue siendo desconocida por los mismos. Teniendo en cuenta esta realidad, consideramos que es el Estado quien tiene la obligación de crear políticas que hagan una democratización de las Condiciones de uso de las Redes Sociales.
- Si bien es urgente normativa que proteja y garantice el Derecho a la Privacidad Personal, esta normativa debe hacerse con la participación de la ciudadanía y de expertos en el tema. Debido a que, es una realidad que existe mucho antes que el Derecho la regule, por lo que se necesita un conocimiento amplio del tema y desde distintas aristas, como la sociología, la psicología. Por lo que no es un trabajo únicamente jurídico, pero que necesita al Derecho para prever y sancionar vulneraciones.

CAPÍTULO VII

PROPUESTA DE PROYECTO DE LEY

ASAMBLEA LEGISLATIVA PLURINACIONAL DE BOLIVIA

LUIS ARCE CATACORA

PRESIDENTE DEL ESTADO PLURINACIONAL DE BOLIVIA

CONSIDERANDO I. Que la relación jurídica de un usuario con Facebook, o cualquier otra red social, inicia con la creación de una cuenta personal, la cual obliga a la persona a aceptar los términos y condiciones de uso sin la posibilidad de ningún tipo de discusión, entendiendo esto como una relación jurídica que se materializa en un contrato de adhesión.

CONSIDERANDO II. Que una vez que el usuario tiene acceso a los servicios que Facebook ofrece, los datos personales proporcionados no se eliminan de la plataforma a menos que la persona decida eliminar la cuenta. Facebook no solo permite interacción personal, sino otorga la posibilidad de realizar otro tipo de acciones como la venta de bienes, la promoción de negocios, etc. A través del

perfil personal o la plataforma de Marketplace o la interacción en grupos que pueden ser públicos, privados o secretos. Lo anterior, permite observar que poder ubicar la información divulgada luego de que esta ha sido compartida por medio de toda la interacción que la plataforma permite por terceros, es bastante difícil, incluso si la cuenta es eliminada.

CONSIDERANDO III. Que Facebook trabaja junto a desarrolladores y aplicaciones que pueden ser tipo test, cuestionarios o juegos, los cuales se sirven de la información del perfil personal, sus contactos, sus preferencias y sus interacciones. Esto se denomina minería de datos, que desde nuestra óptica es una grave vulneración al derecho a la protección de datos personales.

CONSIDERANDO IV. Que de acuerdo a nuestra Constitución, es competencia privativa del Nivel Central del Estado: la "(…) Codificación sustantiva y adjetiva en materia **civil**, familiar, **penal**, tributaria, laboral, **comercial**, minería y electoral. Sin embargo, el artículo 299 indica que los servicios de telecomunicaciones son competencia compartida entre el nivel central del Estado y las entidades territoriales autónomas. Así mismo, el artículo 302 manda que las políticas que garanticen la defensa de los consumidores y usuarios en el ámbito municipal representan competencias exclusivas de los gobiernos municipales autónomos, en su jurisdicción. Interpretando estos artículos, es evidente que todos los niveles de gobierno están obligados por mandato constitucional a velar por la seguridad jurídica respecto a telecomunicaciones, relaciones civiles, comerciales y la defensa de los consumidores.

CONSIDERANDO V. Que en nuestro país, no contamos con una ley de Protección de Datos Personales. Si bien, frente a la vulneración de este bien jurídico para uno y derecho subjetivo para otros, contamos con la Acción de Protección de Privacidad; existe la cláusula de las condiciones de uso de Facebook que limita la jurisdicción de resolución de reclamaciones a territorio favorable para la empresa y no así para los ciudadanos bolivianos. Dado que

como ya lo recalcamos, las redes sociales no desaparecerán es necesario crear resguardo de futuras vulneraciones al derecho a la privacidad.

A continuación, proponemos lo siguiente:

Artículo 1. (OBJETO) La presente Ley tiene el objeto de proponer la modificación del artículo 23 de la Constitución Política del Estado para agregar el Derecho a la Autodeterminación Informativa como un Derecho fundamental; la actualización de la Ley 164 o Ley General de Telecomunicaciones; y la creación de una Ley de Protección de datos personales.

Artículo 2. (MARCO LEGAL) De conformidad a lo establecido en el Artículo 411 parágrafo II, el 162 parágrafo I numeral 2, el 163 y 164 de la Constitución Política del Estado.

Artículo 3. (REFORMA CONSTITUCIONAL) El Artículo 22 de la Constitución Política del Estado especifica cada uno de los derechos que atingen a la libertad y seguridad personal. En ninguno de sus parágrafos se detalla el Derecho a la Autodeterminación Informativa que es de vital importancia para nuestros tiempos. Por lo mismo, proponemos agregar a la Constitución la autodeterminación informativa como derecho fundamental y no derivar el mismo, de los derechos a la privacidad e intimidad.

Artículo 4. (TEXTO REFORMADO DEL ARTÍCULO 23 DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO) Una vez realizado el procedimiento para el referéndum de modificación parcial de la Constitución el texto propuesto del artículo 22 es el siguiente:

Artículo 22.

La dignidad y la libertad de la persona son inviolables. Respetarlas y protegerlas es deber primordial del Estado.

I.- Se reconoce el Derecho a la Autodeterminación Informativa o Derecho de Protección de Datos Personales como derecho fundamental y autónomo.

II.- Es deber de las autoridades estatales, sin perjuicio de las propuestas de la sociedad civil, crear los medios técnicos que protejan sustancialmente el Derecho a la Protección de Datos personales.

Artículo 5. (ACTUALIZACIÓN DE LA LEY 164).

Reformulación de la Ley 164, tomando en cuenta la realidad actual y los cambios que se vienen realizando a corto, mediano y largo plazo en la vida e interacción virtual. Para este objetivo, será necesario coordinar con un equipo multidisciplinario que implique la presencia de juristas, comunicadores sociales, expertos en TICs, la ayuda de expertos en problemáticas jurídicas con empresas virtuales.

Debido a que la Ley 164 no regula la existencia de redes sociales ni mucho menos las dinámicas que representan el uso de las mismas reiteramos la urgencia de crear una comisión de trabajo que analice esta problemática.

Artículo 6. (LEY DE PROTECCIÓN DE DATOS PERSONALES)

I. Esta ley debe considerar también, la creación de políticas de educación en cuanto a los alcances de las redes sociales, Facebook en particular, sobre todo en cuanto la minería de datos. Consideramos que es en estas estrategias de clasificación y uso de información donde efectivamente se vulneran los derechos de privacidad de los usuarios.

II.- Debe contemplar la promoción del uso de medios oficiales por parte de las instituciones públicas como la Universidad, los Ministerios de Estado y demás niveles de gobierno para la difusión de comunicados o información oficial hacia

la ciudadanía. Esto debido a que Facebook es un medio oficial de difusión para muchas instituciones públicas, a tal punto que una persona no puede no tener una cuenta en dicha red social. el no estar suscrito implica la pérdida del acceso a mucha información oficial. Por lo que esta realidad, incentiva el uso de Facebook por parte de los bolivianos.

III.- Deberá crear los medios para una ingeniería comunicacional que parta del Estado, para el acceso a los términos de Las condiciones de uso de las redes sociales que utilizan los datos para fines lucrativos. Teniendo el conocimiento previo de que la mayoría de la población no lee las Condiciones de servicio ni las Políticas de Datos. Esto es importante, porque para establecer la eficacia de la prevención en cuanto al tratamiento malicioso de datos personales, los peligros de las clausulas contractuales deben llegar a la población de forma masiva y entendible, porque, la sola recomendación de leer las cláusulas no es suficiente, considerando el gran alcance que tiene Facebook para las dinámicas sociales de la población e inclusive el Estado.

IV. Puede inspirarse en el modelo base para crear normativa de protección y defensa del usuario, el cual es el Reglamento de Protección de Datos de la Unión Europea que ha sido de inspiración para países latinoamericanos vecinos, como Brasil, Argentina o Perú, en los Estándares de Protección de Datos Personales de la RIPDP, y en los proyectos elaborados por asociaciones civiles.

Artículo 7. (DISPOSICIONES ABROGATORIAS) Quedan abrogadas todas las normas legales vigentes contrarias a la Constitución Política del Estado.

BIBLIOGRAFÍA

LIBROS:

1. *ANDER-EGG, Ezequiel - 1995* — "*TÉCNICAS DE INVESTIGACIÓN SOCIAL*" *Ed. Lumen* *Buenos Aires* *Argentina*

2. *BARRAGÁN, Roxana Et. Al. - 2017* — *"GUÍA PARA LA FORMULACIÓN EJECUCIÓN DE PROYECTOS DE INVESTIGACIÓN"* *Fundación PIEB* *La Paz* *Bolivia*

3. *BOJALIL, Paulina & Et. Al. - 2017* — *"DESPUNTAN LAS REFORMAS EN MATERIA DE PROTECCIÓN DE DATOS EN AMÉRICA LATINA"* *BID* *https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/* *México*

4. *GONZÁLES, Aristeo - 2007* — *"LA PROTECCIÓN DE DATOS PERSONALES: DERECHO FUNDAMENTAL DEL SIGLO XXI. UN ESTUDIO COMPARADO"* *Boletín Mexicano de Derecho Comparado* *Distrito Federal México* *México*

5. *DELLA PORTA, Donatella; et al- 2013* — *"ENFOQUES Y METODOLOGÍAS EN LAS CIENCIAS SOCIALES: UNA PERSPECTIVA PLURALISTA"*

Ed. Akal
Santiago de Chile
Chile

6. HERNÁNDEZ, Roberto; et al.- 2004 *"METODOLOGÍA DE LA INVESTIGACIÓN"*
Ed. McGraw-Hill Interamericana
México

7. FRANGANILLO, Jorge.- 2010 *"IMPLICACIONES ÉTICAS DE LA MINERIA DE DATOS"*
Anuario ThinkEPI
España

8. MÉLICH-ORSINI, José - 1985 *"DOCTRINA GENERAL DEL CONTRATO"*
Universidad Central de Venezuela
Caracas
Venezuela

9. OSORIO, Manuel - s/a *"DICCIONARIO DE CIENCIAS JURÍDICAS, POLÍTICAS Y SOCIALES"*
Ed. Heliasta

10. RAMOS, Carlos - 2007 *"CÓMO HACER UNA TESIS DE DERECHO Y NO ENVEJECER EN EL INTENTO"*
Ed. El Búho E. I. R. L.
Lima
Perú

11. SANCHEZ, Javier - 2018 *"REDES SOCIALES: DEL DAÑO VIRTUAL A LA RESPONSABILIDAD LEGAL"*
Universidad Sergio Alboreda
Bogotá
Colombia

12. SANCHEZ, Juan & Et Al.- 2009 *"ASPECTOS LEGALES Y DOCUMENTALES DE LAS REDES SOCIALES: EL MODELO FACEBOOK"*

Ibersid

13. SALGADO, Victor - 2010 — *"NUESTROS DERECHOS EN RIESGO. INTIMIDAD, PRIVACIDAD Y HONOR EN INTERNET"*
Fundación Telefónica
Madrid
España

14. SENSO, José y DE LA ROSA, ANTONIO - 2003 — *"EL CONCEPTO DE METADATO. ALGO MAS QUE DESCRIPCIÓN DE RECURSOS ELECTRONICOS"*
Brasilia
Brasil

LEYES:

1. CONSTITUCIÓN POLÍTICA DEL ESTADO - Gaceta Oficial de Bolivia 2009 — *Bolivia*

2. Ley N° 164 - 2011 — *"LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN"*
Gaceta Oficial de Bolivia
Bolivia

3. LEY N° 1080 - 2018 — *"LEY DE CIUDADANÍA DIGITAL"*
Gaceta Oficial de Bolivia
Bolivia

4. LEY N° 453 - 2013 — *"LEY GENERAL DE LOS DERECHOS DE LAS USUARIOAS Y LOS USUARIOS Y DE LAS CONSUMIDORAS Y LOS CONSUMIDORES"*

Gaceta Oficial de Bolivia
Bolivia

5. DECRETO LEY N° 12760 - 1975 *"CÓDIGO CIVIL"*
Gaceta Oficial de Bolivia
Bolivia

6. DECRETO SUPREMO N° 1793 - 2013 *"REGLAMENTO A LA LEY N° 164"*
Gaceta Oficial de Bolivia
Bolivia

7. DECRETO SUPREMO N° 28168 - 2013 *"TRANSPARENCIA EN LA GESTIÓN PÚBLICA DEL PODER EJECUTIVO"*
Gaceta Oficial de Bolivia
Bolivia

8. SENTENCIA CONSTITUCIONAL 0819/2015-S3 - 2015 *"Repositorio del Tribunal Constitucional Plurinacional*
Bolivia

9. REGLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO - 2016 *"REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA"*
Repositorio de la Agencia Estatal Boletín Oficial del Estado
España

PÁGINAS WEB:

1. DICCIONARIO JURÍDICO - 2023 *"MÉTODO INDUCTIVO"*
Diccionario Jurídico México
http://diccionariojuridico.mx/definicion/metodo-inductivo/
México

2. BCJ - 2008 — *CENTRO DE TECNOLOGÍAS DE LA INFORMACIÓN UCAMPUS* https://www.u-cursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/bajar?id_material=163485

3. CÁRDENAS, Edna - 2009 — *"FACEBOOK, UN ESPACIO DE INTERACCIÓN VIRTUAL"* *Bibliotaca Javeriana* *https://repository.javeriana.edu.co/handle/10554/5343* *Bogotá* *Colombia*

4. DE LA PARRA, Eduardo - s/a — "*LOS DERECHOS DE LA PERSONALIDAD: TEORÍA GENERAL Y SU DISTINCIÓN CON LOS DERECHOS HUMANOS Y LAS GARANTÍAS INDIVIDUALES".* *s/E* *http://historico.juridicas.unam.mx/publica/librev/rev/jurid/cont/31/pr/pr10.pdf* *México*

5. DICCIONARIO PANHISPÁNICO DEL ESPAÑOL JURÍDICO. - *s/a* — *s/E* *https://dpej.rae.es/lema/habeas-data*

6. FACEBOOK - 2020 — *Https://Www.Facebook.Com*

7. FERNANDEZ, Pablo - 2009 — *https://www.pablofb.com/2009/03/clasificacion-de-redes-sociales/*

8. FRIGERIO, Catalina - 2018 — *"MECANISMOS DE REGULACIÓN DE DATOS PERSONALES: UNA MIRADA DESDE EL ANÁLISIS DEL DERECHO"*

Revista Chilena de Derecho y Tecnología
Chile

9. FERNANDEZ, Pablo - 2009 — *https://www.pablofb.com/2009/03/clasificacion-de-redes-sociales/*

10. GIL, Elena - 2016 — *"BIG DATA, PRIVACIDAD Y PROTECCIÓN DE DATOS"*
https://www.derechoinformatico.cl/catalogo/downloads/big_data2016.pdf
DerechoInformático.CL

11. FUCHS, Jay - 2020 — *https://blog.hubspot.com/marketing/history-facebook-adtips-slideshare*

12. LOS TIEMPOS - 2019 — *https://www.lostiempos.com/tendencias/tecnologia/20191226/alrededor-7-millones-bolivianos-usan-redes-sociales-facebook-es*

13. RAMÍREZ, R - 2021 — *"REBRANDING: DE FACEBOOK A META"*
Enlaces, La Revista de Negocios de la TEC
https://www.utec.edu.sv/media/publicaciones/flips/enlaces/enlaces61/files/file.pdf#page=8
El Salvador

14. RALLO, Artemi - 2019 — *El nuevo derecho de protección de datos*
http://repositori.uji.es/xmlui/bitstream/handle/10234/189958/rallo_2019_Eln.pdf?sequence=1&isAllowed=y

15. REAL ACADEMIA ESPAÑOLA - 2023 — *https://dle.rae.es*

16. RIPD - 2017

"ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS"
Red Iberoamericana de Protección de Datos
https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf

17. ROA, Matías - 2013

"FACEBOOK FRENTE AL DERECHO A LA VIDA Y LA PROTECCIÓN DE DATOS PERSONALES"
http://derecho.uchile.cl/centro-de-estudios-en-derecho-informatico/publicaciones/tesis
Chile

18. VERCELLI, Ariel - 2019

LA (DESPROTECCIÓN DE LOS DATOS PERSONALES): ANÁLISIS DEL CASO FACEBOOK INC. – CAMBRIDGE ANALYTICA"
http://sedici.unlp.edu.ar/handle/10915/135072
Argentina