Cláusula de cesión de derecho de publicación de tesis/monografía

Yo. Rolando Carlos Soto Villalta C.I. 3458625 L.P.
autor/a de la tesis titulada

Seguridad de Datos Personales en los Registros Públicos

mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de

Magister en Derecho Internacional y Justicia Constitucional

En la Universidad Andina Simón Bolívar, Sede académica La Paz.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Académica La Paz, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación a partir de la fecha de defensa de grado, pudiendo, por lo tanto, la Universidad utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en formato virtual, electrónico, digital u óptico, como usos en red local y en internet.

2. Declaro que en caso de presentarse cualquier reclamo de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.

3. En esta fecha entrego a la Secretaría Adjunta a la Secretaria General sede Académica La Paz, los tres ejemplares respectivos y sus anexos en formato impreso y digital o electrónico.

Fecha. 28-Junio-2019.

Firma: .....

UNIVERSIDAD ANDINA SIMON BOLIVAR

MAESTRIA EN DERECHO INTERNACIONAL Y JUSTICIA CONSTITUCIONAL

SEGURIDAD DE DATOS PERSONALES EN LOS REGISTROS PUBLICOS

TESIS DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE MAGISTER

Autor: Lic. Rolando Carlos Soto Villalta

Tutor de tesis: Mgr. Karina Medinaceli PhD

La Paz, junio de 2019

Dedicado:

A mi esposa Greta.

A mis padres Francisco y Nelly.

A mis hijas Estefany, Scarlet y Carla.

Quienes me brindaron su

Apoyo incondicional.

Agradezco a la Universidad Andina
Simón Bolívar por haberme formado
en su seno.

De manera muy especial al
Rector Dr. José Luis Gutiérrez Sardán
a quien conozco y admiro.

A la Mgr. Karina Medinaceli PhD, quien
desinteresadamente me oriento y guió en
la elaboración de la presente tesis

INDICE CUADROS

Dedicado:

A mi esposa Greta.

A mis padres Francisco y Nelly.

A mis hijas Estefany, Scarlet y Carla.

Quienes me brindaron su

Apoyo incondicional.

Agradezco a la Universidad Andina
Simón Bolívar por haberme formado
en su seno.

De manera muy especial al
Rector Dr. José Luis Gutiérrez Sardán
a quien conozco y admiro.

A la Mgr. Karina Medinaceli PhD, quien
desinteresadamente me oriento y guió en
la elaboración de la presente tesis

RESUMEN

Con el avance del desarrollo tecnológico el Estado cambia su rol y pasa a ser un intermediario en lo local y lo global ya que existen plataformas digitales como ser: la sociedad de la información, economía digital e Internet que hacen que cambien las relaciones entre las personas, empresas, instituciones y organizaciones. Se generan interrelaciones que están expuestas al mal manejo de datos personales. Por otro lado en todas las instituciones se van desarrollando sistemas de manejo de información y bases de datos, generando inseguridad jurídica en los ciudadanos respecto al manejo, administración de su información personal. Situación que se complica cuando los ciudadanos se encuentran registrados con datos errados en archivos o bases de datos. Hay mala información de sus datos, incluso donde se encuentran registrados sin haber proveído su información como titular.

Ante esta realidad, se plantea el objetivo de: "Proponer las bases normativas que mejoren los niveles de seguridad en el manejo de datos personales en los registros públicos, a objeto de brindar protección en su tratamiento y en el derecho a la privacidad", para lo cual se plantean cuatro objetivos específicos que son alcanzados.

Primero se analizar los elementos teóricos – históricos de la protección de datos y el derecho a la privacidad en las bases de datos públicas, así como el tratamiento y medidas de seguridad en las plataformas digitales en lo referido a las telecomunicaciones, las tecnologías de información y comunicación y la Informática. Llegándose a las conclusiones de que, el derecho a la protección de datos personales, es la profundización del derecho a la privacidad, que está referido a los datos que hacen identificable a la persona natural o jurídica, Se aplica por el Habeas Data y en Bolivia se aplica a través de la Acción de Protección a la Privacidad.

En cuanto al derecho a la Protección de Datos Personales, en Bolivia, no se encuentra explicita en su Constitución y la aplicación de medidas de seguridad de información, están relacionadas de manera directa con el Tratamiento de Datos, que tienen que contemplar principios y medidas de seguridad.

El segundo objetivo específico está relacionado con el trabajo de campo que consiste en analizar los elementos teóricos – históricos de la protección de datos y el derecho a la privacidad en las bases de datos públicas, así como el tratamiento y medidas de seguridad en las plataformas digitales en lo referido a las telecomunicaciones, las tecnologías de información y comunicación y la Informática.

Se concluye que el tratamiento de datos, ha sido normado a nivel internacional y regional en lo referido a Protección de Datos Personales. Se cuenta con normativa que le dan al responsable la responsabilidad de asegurarse de la seguridad de información en cuando a su registro, custodia y resguardo. Se cuenta con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016 y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017). Se busca la armonización.

La normativa boliviana prevé la seguridad de la información para el tratamiento de datos en registros públicos, sólo para entidades *certificadoras de firma digital.* Así mismo se deduce que la normativa existente está dirigida solo para el Desarrollo de Tecnologías de Información y Comunicación (D.S. 1793) y no contempla para sistemas de registro y custodia manual (archivos). El D.S. no tiene rango de Ley por lo que puede existir choque de competencias con la leyes propias de instituciones (SEGIP – Ley 145, y SERECI Ley 17) o leyes sectoriales (Ley del Sistema Financiero, etc).

El SERECI y el SEGIP cuentan con propias leyes que les otorgan principios y medidas de seguridad de información relacionados con el registro biométrico, y para el registro de modificaciones y documentación de respaldo el SEGIP utiliza la firma digital en sus resoluciones administrativas y el SERECI el Código QR. Ambas instituciones aplican principios y medidas de seguridad de confidencialidad, integridad y disposición.

En cuanto al análisis jurisprudencial, se cuenta con jurisprudencia que permite que los litigantes apliquen el derecho a la protección de datos ya que la garantía prevista en la Constitución y el Código Procesal no necesita norma que regule su ejercicio.

En Bolivia se cuenta con una garantía constitucional que es la "Acción de Protección de a la Privacidad", que tiene por objeto la garantía del derecho de toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental de la intimidad y privacidad personal o familiar, o a su propia Imagen, honra y reputación", regulada por la Ley del Tribunal Constitucional.

Si bien se cuenta con esta garantía constitucional la misma se encuentra con un vacío legal cuando los derechos son afectados y quieren ser accionados por los litigantes. Se hace necesario que se cuente con una política pública (norma) que establezca el derecho o el tratamiento o las medidas de seguridad a ser aplicadas.

El tercer objetivo específico está referido a comparar la normativa de seguridad de datos de Bolivia con Estándares Internaciones de Seguridad de Datos de la Red Iberoamericana de Datos Personales. Al respecto se concluye que La Normativa Boliviana contempla algunos tópicos de los Estándares Internaciones de Seguridad de Datos de la Red Iberoamericana de Datos Personales como que reconoce indirectamente los Derechos ARCO, plasmados en la Acción de Protección de Privacidad; Acceso (Conocer), Rectificación (Rectificación), Cancelación (Obtener eliminación) y Oposición (Oposición).

En cuanto a medidas de seguridad de información en Tratamiento de Datos los Estándares establecen que el responsable garantizara que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier tecnología que impliquen un tratamiento de datos cumplan por defecto y se ajusten a los principios, derecho y demás obligaciones previstas en la legislación nacional.

Por último el objetivo cuarto es elaborar las bases de un proyecto de regulación de datos personales de acuerdo a estándares normalizados y en base a la realidad nacional, Al respecto de establecer que las conclusiones del trabajo de investigación deben ser consideradas para la elaboración de una propuesta de Ley de Seguridad de Datos Personales, complementando con los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, ambos documentos deben ser considerados como bases normativas. Así la Norma legal proyectada puede mejorar los niveles de seguridad en el tratamiento de datos personales y en el derecho a la privacidad en las entidades públicas.

INDICE CUADROS

TESIS: SEGURIDAD DE DATOS EN LOS REGISTROS PUBLICOS

INDICE

CAPITULO I
PLANTEAMIENTO GENERAL DEL ESTUDIO

1.1. Introducción

El presente trabajo de investigación científica busca estudiar el tratamiento datos personales en los registros públicos de Bolivia y tiene el objetivo de proponer, como mejorar la seguridad de información a fin de dar seguridad jurídica en la protección de su tratamiento y en el derecho a la privacidad.

Se plantea la pregunta de investigación, el objetivo general, los objetivos específicos e hipótesis, identificándose dos variables: "seguridad de la información para el manejo de los datos personales en los registros públicos y protección de datos personales" y "brindar protección en el tratamiento y en el derecho a la privacidad".

La investigación a realizarse es de tipo descriptiva, el diseño de investigación que guiara la investigación es no experimental. Se usará las técnicas de estudio de casos, técnicas de investigación documental y la técnica de análisis de contenido

El uso de las técnicas de recopilación de información expuestas implica el uso de los métodos analítico-sintético e inductivo-deductivo. Se pretende utilizar técnicas cualitativas de observación directa, de la jurisprudencia existente sobre el problema de investigación. Así mismo se realizaran entrevistas estructuradas a gente entendida en Derecho constitucional, Derecho Informático y Seguridad de la información.

1.2. Planteamiento del Problema

1.2.1. Situación Problemática

El Derecho se ha fundamentado tradicionalmente en el Estado Nación, sin embargo la globalización, las normas de libre mercado y el desarrollo de las Tecnologías de Información y Comunicación, han generado un nuevo espacio donde se relacionan los seres humanos, que es el espacio o aldea global.

El Estado pasa a ser un intermediario entre lo local y lo global, surgiendo la necesidad de reconsiderar su rol, en lo referido a las plataformas digitales que existen: Sociedad de la Información, economía digital e Internet. Estas plataformas tiene la naturaleza de estar interconectadas donde la "interoperatividad" permite la realización de intercambios de información (datos), con fines económicos, personales, familiares, políticos y sociales.

Surge así la necesidad, que el marco regulatorio permita generar y reflejar la capacidad, las características y las habilidades de cada uno de los agentes (personas, empresas, asociaciones, instituciones público/privadas, etc.) en lo referido al manejo de los datos personales, dentro las: Telecomunicaciones, las Tecnologías de Información y Comunicación, y la Informática.

Hoy en día en nuestro país, las personas tienen que registrar sus datos en diferentes bases de datos con la finalidad de poder ejercer sus derechos (gracias a su identidad), para diferentes tipos de asuntos generales y particulares.

Es sabido lo tortuoso (burocrático) que resulta realizar los trámites en las instituciones, que tiene a cargo el derecho registral en una base de datos como ser el SERECI, SEGIP, MIGRACION, CNS, REJAP, DERECHOS REALES, PADRON ELECTORAL, etc. Así mismo se van creando bases de datos para fines económicos, como ser en instituciones financieras, Bancos, AFP´s, Fundaempresa, Buros de información, etc. Por otro lado, también se crean bases de datos para fines sectoriales en los Ministerios, empresas públicas, ADSIB, AGETIC, etc.

En todas estas instituciones se van desarrollando sistemas de manejo de información y bases de datos, generando inseguridad jurídica en los ciudadanos respecto al manejo, administración de su información personal. Situación que se complica cuando los ciudadanos se encuentran registrados con datos errados en

archivos o bases de datos. Hay mala información de sus datos, incluso donde se encuentran registrados sin haber proveído su información como titular.

Existen quejas de esta situación de indefensión, así como de la inexistencia de acciones tendientes a resolver los errores y falta de normativa que obligue a los que ocasionaron en daño a resarcir los perjuicios ocasionados. A esto se suma la posibilidad que terceros distintos al titular puedan acceder a su información personal para fines delictivos, afectando su derecho a la privacidad, intimidad, honra, propia imagen y dignidad[1].

El desarrollo de la tecnología hace posible que en algunos países se pueda declarar los impuestos en línea en solo tres minutos y sin tener que moverse de su casa y que también se pueda votar desde cualquier lugar. Esto es gracias a políticas en el marco de lo que se conoce como economía digital, digitalización, gobierno electrónico e interoperatidad. El derecho a la privacidad se ve implicado de forma específica en estas relaciones ya que se tratan datos personales. Estos países han regulado el tratamiento de datos personales a través de regulaciones específicas.

En Bolivia se están implementando políticas y normativas que tratan de encarar el avance tecnológico: ha implementado el "Plan de Implementación del Gobierno Electrónico y el Plan de Implementación del Software Libre y Estándares Abiertos"[2]. y posteriormente el Presidente el Estado Plurinacional de Bolivia, Don Evo Morales Ayma, ha presentado dos paquetes de acciones dentro del llamado "Plan de Desburocratización del Estado", que busca hacer más eficiente el trabajo de las instituciones públicas con ayuda de la tecnología.

[1] Constitución Política del Estado Plurinacional de Bolivia. de febrero 2009 estable en su artículo 21.2 que: "*Las bolivianas y los bolivianos tienen los siguientes derechos: a la privacidad, intimidad, honra, propia imagen y dignidad".*

[2] Gaceta Oficial de Bolivia, Decreto Supremo 3251, de fecha 12 de julio de 2017.

Es a partir de la promulgación de la Ley de Telecomunicaciones y Tecnologías de Información y Comunicación[3], que se viene construyendo el marco normativo referido a las plataformas digitales. Posteriormente, se aprueba el "Reglamento de la Ley de Telecomunicaciones y Tecnologías de Información y Comunicación".[4] Así mismo se ha creado la "Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC"[5] y se han aprobado "Lineamientos para la Implementación de Servicios de Interoperatividad en las Entidades del Sector Público"[6]. Recientemente[7] se ha planteado un proyecto de Ley que modifica la Ley del Órgano Electoral Plurinacional, que permitirá que el Servicio General de Identificación Personal (SEGIP) otorgue datos personales, contenidos en su base de datos al Servicio de Registro Cívico (SERECI) y a la AGETIC.

Estas políticas y normativas no son suficientes para otorgar seguridad jurídica a los ciudadanos sobre la administración y uso de los datos personales, afectando su derecho a la privacidad.

1.2.2. Situación Proyectada

El Estado Boliviano a través de sus instituciones se dedica al registro de datos, que permite el ejercicio de los derechos de las bolivianas y los bolivianos en lo referido a identidad, nacionalidad, ciudadanía, estado civil, derecho propietario, etc. Así mismo resultado del avance tecnológico se han creado plataformas digitales como ser la sociedad de la información, economía digital e internet que permite a sus usuarios comunicarse y realizar transacciones en línea. Para esto es necesario el registro de datos en bases de datos, mismas que requieren ser administradas y

[3] Gaceta Oficial de Bolivia, Ley 164, de fecha 8 de agosto de 2011.
[4] Gaceta Oficial de Bolivia, Decreto Supremo 1973, de fecha 13 de noviembre de 2013
[5] Gaceta Oficial de Bolivia, Decreto Supremo 2514, de fecha 9 de septiembre de 2015
[6] Presidencia del estado Plurinacional de Bolivia, Resolución Ministerial 234-17 de fecha 11 de octubre de 2017
[7] El Deber, publicación de 4-abr-18, "Claves para entender la ley que dará acceso a datos personales a una Agencia del Gobierno", www.eldeber.com.bo

custodiadas. De ello se desprende que el derecho a la intimidad y privacidad ha sido erosionado por el avance tecnológico.

Las disposiciones legales actuales no contemplan controles para los registros y acceso a los datos. Surge la necesidad de replantear el rol del Estado en el nuevo contexto de las plataformas digitales y proyectar transformaciones jurídicas institucionales que permita establecer nuevas regulaciones para el acceso a los datos, protección y su tratamiento, generando tutela del derecho a la intimidad y privacidad.

1.2.3. Formulación del Problema

El problema que guía la presente investigación se plantea de la siguiente manera:

¿De qué manera se puede mejorar el nivel de seguridad de la información, para el manejo de los datos personales en los registros públicos, a objeto de brindar protección en su tratamiento y en el derecho a la privacidad en la actual regulación de Bolivia?

1.3. Justificación

El derecho a la privacidad se ve implicado de forma específica en el tratamiento de los datos personales más aún con las plataformas digitales que son resultado del avance de las telecomunicaciones, la informática y las tecnologías de la información y comunicación. A nivel internacional existen avances en la regulación y armonización de políticas, referidas al tratamiento de los datos personales. Es el caso de la Red Iberoamericana de Datos Personales que busca vía la cooperación y coordinación armonizar en la región el marco normativo. Bolivia no se ha adherido a esta Red. Teóricamente se justifica el presente trabajo de investigación científica por el aporte a la ciencia del derecho informático, administrativo y constitucional.

En nuestro país el crecimiento y estructuración de grandes bases de datos, de procesamiento y archivo de datos de carácter personal, en registros públicos y privados ha generado dificultades a los bolivianos y bolivianas, en cuanto a: mal registro de sus datos, errores de datos, registros no autorizados por el titular y obtención de datos por terceros distintos del titular para fines delictivos entre otros. Situación que vulnerado el derecho a privacidad, intimidad, honra, propia imagen y dignidad. Socialmente se justifica porque se pretende proponer una regulación de acceso a datos.

La justificación práctica se da por la reducción de costos que representa el uso de las telecomunicaciones, las tecnologías de información y comunicación, y la Informática, en el tratamiento de datos.

Metodológicamente se justifica porque se pretende realizar una análisis comparativo entre la legislación nacional de protección de datos con los "Estándares de Protección de Datos Personales para los Estados Ibeoamericanos"[8].

El autor cuenta con 4 años de conocimientos de tratamiento de datos personales en el SERECI y el SEGIP. En esta última institución trabajó como Director Nacional de Operaciones. Así mismo cuenta con conocimientos de Economías Digital y su Regulación.

1.4. Delimitación

1.4.1. Delimitación temática

La realización de la presente investigación se hace en el marco del Derecho Informático, Derecho Administrativo, Derecho Constitucional y el Derecho Internacional en lo referido a los sistemas de protección derechos humanos como son el Sistema Universal de Protección de los Derechos Humanos (SUDH) de la

[8]Red Iberoamericana de Protección de Datos Personales, "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", aprobados en el XV encuentro en Colombia el 20 junio de 2017.

Organización de Naciones Unidas (ONU) y el Sistema Regional de Protección de Derechos Humanos, Sistema Interamericano de la Organización de Estado Americanos (OEA).

1.4.2. Delimitación espacial

La delimitación geográfica de la investigación se referirá al Estado Plurinacional de Bolivia. La investigación se realizó en el Departamento de La Paz, con alcances a nivel nacional.

1.4.3. Delimitación temporal

El presente estudio tiene como marco de referencia temporal, el periodo que comprende desde la aprobación de la nueva Constitución Política del Estado de fecha 7 de febrero de 2009, que implica un cambio de modelo de Estado, hasta el 31 de diciembre de 2017.

1.5. Objetivos

1.5.1. Objetivo general

Proponer las bases normativas que mejoren los niveles de seguridad en el manejo de datos personales en los registros públicos, a objeto de brindar protección en su tratamiento y en el derecho a la privacidad.

1.5.2. Objetivos específicos

El objetivo general será alcanzado cumpliendo los siguientes objetivos específicos:

1. Analizar los elementos teóricos – históricos de la protección de datos y el derecho a la privacidad en las bases de datos público, así como el tratamiento y medidas de seguridad en las plataformas digitales en lo referido a las telecomunicaciones, las tecnologías de información y comunicación y la Informática.

2. Evaluar los niveles de seguridad de los datos personales en los registros públicos.
3. Comparar la normativa de seguridad de datos de Bolivia con Estándares Internaciones de Seguridad de Datos de la Red Iberoamericana de Datos Personales.
4. Elaborar las bases de un proyecto de regulación de datos personales de acuerdo a estándares normalizados y en base a la realidad nacional.

1.6. Marco teórico referencial

Se presentan los principales tópicos sobre la teoría y fundamentos teóricos, de seguridad de información y tratamiento de datos personales en los registros públicos, así como el desarrollo de las tecnologías de información y como estas se presentan en la era digital.

1.6.1. Rol del Estado, derecho en la modernidad

Según Rodolfo Herrera Bravo en la Modernización del Estado a Través de la Regulación Jurídica de las Tecnologías de Información[9], "…Este nuevo contexto exige que el Estado asuma un rol innovador. En tal sentido, cabe observar cómo la modernización en los países industrializados está dirigida a consolidar un sistema económico y social que reconozca en la generación, procesamiento y distribución del conocimiento y la información, el fundamento de la productividad, el bienestar y el poder. Además, esos Estados entienden que la realización de los cambios necesarios para alcanzar dicho sistema suele apoyarse en la utilización de innovaciones tecnológicas por parte de organizaciones independientes que participan, interactúan y cooperan al interior de un país".

[9] ZARICH F., (2000, pag. 4-5)

Por lo expuesto se requiere acompañar con normativa jurídica este nuevo rol, permitiendo el avance tecnológico. Normando para que los particulares se beneficien del avance tecnológico y para que las instituciones del estado utilice el avance tecnológico en beneficio de la sociedad. Todo esto en un marco de seguridad jurídica. Para Herrera se distinguen dos niveles de acción estatal: Un estadio Subsidiarios, donde el Estado actúa como generador de condiciones que permitan el normal desenvolvimiento de los particulares, por ejemplo fijando una política educacional destinada a formar un recurso humano calificado; creando condiciones de estabilidad económica que disminuyan los riesgos de las empresas que invierten en desarrollo tecnológico; o facilitando la participación de particulares a través de políticas de fomento. Un segundo estadio de Acción estatal, que se da al interior de la Administración del Estado, que es la informatización del Estado, mediante el fomento y empleo de cambios tecnológicos, que deben permitir mejorar la gestión. Materializando el principio de simplificación y flexibilidad administrativas.

1.6.2. Sociedad de Información y Derecho

Hoy en día la humanidad, se encuentra inmersa en un cambio de paradigma, las formas tradicionales de obtener información, publicitar bienes, realizar transacciones, han sido cambiadas y superadas por el uso de medios tecnológicos que antes no existían.

Ello ha llevado a que los economistas, denominen a este nuevo paradigma como economía digital y surjan las economías colaborativas. También ha obligado a que las Administraciones públicas lo utilicen como modelo para la reforma del estado, denominado gobierno electrónico. En el campo de la educación ha generado espacios virtuales de educación donde ya no es importante la presencia física ni el

cumplimiento de horarios, esto ha ocasionado que los educadores se sientan amenazados por el computador si es que no se reestructura su misión en la escuela.

En este nuevo contexto los datos adquieren relevancia ya que la transmisión de datos permite realizar transacciones a gran velocidad gracias a la fibra óptica, Así mismo se permite el almacenamiento y procesamiento de importantes cantidades de datos en lo denominado Big Data.

1.6.3. Informática, libertades y derechos humano

El avance de la tecnología y la afirmación de los derechos del hombre en la democracia, exigen hoy nuevas reglas de derecho que, dentro del respeto de aquellos principios constitucionales, extiendan el amparo legal a situaciones que no pudieron preverse en su momento. Esas nuevas reglas deberán equilibrar los diferentes intereses jurídicos en juego. Por una parte, se trata de lograr un adecuado balance entre el derecho a controlar la propia información y el principio de la libertad de información, especialmente en cuanto esta última *se* relacione con cuestiones de interés social. Por otro lado, el derecho individual debe compadecerse con el de las instituciones democráticas para prevenir acciones que atenten contra su esencia.

El hábeas data surge con el fin de garantizar la privacidad o intimidad personal frente a los riesgos del almacenamiento, registro y utilización de datos.

"El desarrollo conceptual del derecho a la intimidad personal o "right of privacy", tiene lugar en la experiencia de los Estados Unidos y en el Reino Unido, desde finales del siglo XIX. Un punto crucial en este itinerario fue la definición del derecho a la privacidad como "theright to be letalone" es decir, el "derecho a ser dejado en soledad" (sin ser molestado o perturbado) elaborada por el Juez Cocley; este concepto

fue desarrollado por los juristas norteamericanos Warren y Grandeis, buscando proteger a la persona frente a datos o actos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado"[10].

1.6.4. Tratamiento y medidas de seguridad de datos personales

Considerando que la adopción de diversos Sistemas de Información es masiva en casi cualquier contexto, surge la necesidad de proteger la información que forma parte de dichos sistemas, pues dicha información se torna crítica e invaluable, pues concentra el día a día de la organización. La «Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y de las posesiones, es tan antigua como ella» (Manunta, 2003).

1.7. Hipótesis

La incorporación de medidas de seguridad de la información para el manejo de los datos personales en los registros públicos, permitirá la protección en su tratamiento y en el derecho a la privacidad en la actual regulación de Bolivia.

1.8. Operativización de variables

La Operacionalización de variables, de presente trabajo de investigación se representa en el siguiente cuadro.

[10]MALLMA, SOTO, JOSÉ CARLO, obtenido de www.monografias.com,lenincarlos@hotmail.com

CUADRO No. 1

OPERACIONALIZACION DE VARIABLES

VARIABLE NOMINAL	DEFINICION	INDICADOR	RESULTADO
VARIABLE INDEPENDIENTE: incorporación de medidas de seguridad de la información para el manejo de los datos personales en los registros públicos.	Todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e integridad de la misma	Revisión de normativa nacional	Verificar si la normativa boliviana prevé la seguridad de la información para el tratamiento de datos en registros públicos.
VARIABLE DEPENDIENTE: permitirá la protección en el tratamiento y en el derecho a la privacidad	Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias	Entrevistas Jurisprudencia Sentencias	Evidenciar que en el tratamiento se protegen de datos personales en lo referido al derecho a la privacidad

1.9. Tipo de estudio

La investigación a realizarse es de tipo descriptiva, ya que describe y evalúa las características del problema de investigación relacionados con el de mejorar los niveles de seguridad de la información para el manejo de datos personales en los

registros públicos, brindando protección en su tratamiento y en el derecho a la privacidad, todo esto en la actual regulación normativa de Bolivia.

Se investiga simultáneamente, las variables de seguridad de información y protección en el tratamiento de datos, haciendo un corte en el tiempo en la gestión 2017.

1.10. Diseño de la investigación

El diseño de investigación que guía la investigación es el Diseño No experimental realizando la observación del fenómeno en su ambiente natural, para conocer su comportamiento social. Es decir se procederá con entrevistas estructuradas.

Con el fin de alcanzar los objetivos de la investigación y verificar la hipótesis se utiliza las técnicas de estudio de casos, técnicas de investigación documental y la técnica de análisis de contenido. El estudio de casos es una técnica ampliamente utilizada en las investigaciones sociales debido precisamente a la complejidad de éstas, las cuales consisten en dar una descripción completa y detallada de algunos fenómenos, sin limitar la recolección de los datos al interrogatorio o a la entrevista de los sujetos, ésta técnica es válida como ilustración de una generalización (COHEN, 1984, p. 11).

Por su parte la técnica documental utiliza a los documentos como los principales instrumentos en su análisis, "los documentos son hechos o rastros de «algo» que ha pasado, de ahí que como «testimonios» que proporcionan información, datos o cifras, constituyan un tipo de material muy útil para la investigación social. Como elemento de conocimiento o fuente de información son susceptibles de ser utilizados como consulta, estudio o prueba" (ANDER,1982, p. 211).

Se puede decir 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, 1982, p. 213).

Finalmente, el análisis de contenido, es una técnica de investigación para la descripción objetiva, sistemática y cuantitativa del contenido manifiesto de la comunicación. Permite estudiar el contenido manifiesto de una comunicación, clasificando sus diferentes partes conforme a categorías establecidas por el investigador, con el fin de identificar de manera sistemática y objetiva dichas categorías dentro del mensaje; lo que interesa fundamentalmente es el estudio de las ideas, significados, temas o frases, y no las palabras o estilos con que éstas se expresan, mediante ésta técnica, se pueden hacer inferencias a partir de lo dicho, lo escrito, o bien, de materiales de expresión no lingüística. En todos los tiempos los hombres se han ocupado de la interpretación y explicación de los mensajes. En nuestro quehacer cotidiano hacemos análisis de contenido cuando resumimos y/o interpretamos lo que leemos y escuchamos (ANDER, 1982, p. 327-330).

1.11. Métodos de la Investigación

El uso de las técnicas de recopilación de información expuestas implica el uso de los métodos analítico-sintético e inductivo-deductivo. Se identificará las características e interrelación entre los elementos del problema, más la comprobación y análisis de todas las variables que intervienen en la hipótesis.

"El análisis es la separación material o mental del objeto de investigación en sus partes integrantes con el propósito de descubrir los elementos esenciales que lo conforman. Mientras que la síntesis consiste en la integración material o mental de los elementos o nexos esenciales de los objetos, con el objetivo de fijar las cualidades y rasgos principales inherentes al objeto" (RODRIGUEZ, 1984, p. 34-35).

Por otra parte, "la inducción es el método de obtención de conocimientos que conduce de lo particular a lo general, de los hechos a las causas y al descubrimiento de leyes. Mientras que la deducción es el razonamiento mental que conduce de lo general a lo particular y permite extender los conocimientos que se tienen sobre una clase determinada de fenómenos a otro cualquiera que pertenezca a esa misma clase" (RODRIGUEZ,1984, p.35-36).

El enfoque de la tesis es jurídico proyectivo en tanto que realiza una suerte de predicción sobre el futuro de un aspecto jurídico. Las predicciones surgen de premisas actualmente vigentes; asimismo, es jurídico-propositivo ya que su característica es evaluar las fallas de las normas o los sistemas, en este caso un vacío jurídico, y a partir del mismo proponer posibles soluciones.

Discute consecuencias y soluciones alternas, y llega a una conclusión crítica después de evaluar los datos investigados.

1.12. Técnicas de recojo de la Información

Se utiliza técnicas cualitativas de observación directa, de la jurisprudencia existente sobre el problema de investigación. Así mismo se realizaran entrevistas estructuradas a gente entendida en Derecho Constitucional, Derecho Informático y Seguridad de la información.

El procedimiento ha consistido en seleccionar el tema para seguidamente generar preguntas sobre el mismo que guían la recolección de información significativa al desarrollar la investigación.

Como técnicas de recojo de información, se trabajó con la entrevista estructurada para desarrollar el trabajo de campo, técnica de investigaciones cualitativas que busca profundizar el fenómeno de estudio.

La entrevista es una técnica de recopilación de información mediante una conversación profesional, con la que además de adquirir información acerca de lo que se investiga, tiene importancia desde el punto de vista educativo; los resultados a lograr en la misión dependen en gran medida del nivel de comunicación entre el investigador y los participantes en la misma.

De acuerdo al fin que se persigue con la entrevista, puede estar estructurada a través de un cuestionario previamente elaborado, que permite profundizar en el tema y obtener información del mismo.

CAPITULO II
MARCO TEORICO

2.1. Marco teórico

2.1.1. Rol del estado, derecho en la modernidad

2.1.1.1.derecho y estado nación

El derecho se ha fundamentado en gran parte con base los límites del Estado-Nación. Según Weber M. (2009, p. 83-84) afirma "hoy tenemos que decir que (a diferencia de las instituciones del pasado basadas en la fuerza) el estado es una comunidad humana que reivindica (con éxito) el monopolio del uso legítimo de la fuerza física en un territorio determinado. Obsérvese que el territorio es una de las características del estado" y continua "Una nación es una comunidad de sentimientos que se manifestaría adecuadamente en un estado propio; por tanto, una nación es una comunidad que normalmente tiende a crear un estado propio.".

Para CASTELLS M (2009, p. 43) los límites de la sociedad están dados por el estado y el territorio "Este es el supuesto implícito de la mayoría de los análisis sobre el poder, que observan las relaciones de poder dentro de un estado construido territorialmente o entre estados. Nación, estado y territorio definen los límites de la sociedad".

2.1.1.2.Génesis del Nuevo Estado

El nuevo mundo según Castell M. (1998, p. 369-370), se origina hacia finales del sesenta y mediados de los setenta, de tres procesos independientes: la revolución de la tecnología de la información; la crisis económica del capitalismo el estatismo, y el florecimiento de movimientos sociales y culturales (como el autoritarismo, la defensa de los derechos humanos, el feminismo y el ecologismo). La interacción de estos procesos y las reacciones que desencadenaron crearon una nueva estructura

social dominante, una sociedad red, una nueva economía, la economía internacional global; y una nueva cultura de la virtualidad real.

Resultado de su investigación presentada en tres volúmenes, se identifican unos rasgos decisivos de este nuevo mundo donde la tecnología de la información ha sido la herramienta indispensable para la puesta en práctica efectiva de los procesos de reestructuración socioeconómica. De importancia particular fue su papel al permitir el desarrollo de las redes interconectadas como una forma expansiva y dinámica de la organización de la actividad humana. Esta lógica de redes transforma todos los ámbitos de la vida social económica.

2.1.1.3. Derecho y aldea global

Como se mencionó, el Derecho se ha fundamentado tradicionalmente en el Estado Nación, sin embargo la globalización, las normas de libre mercado y el desarrollo de las tecnologías de información y comunicación, han generado un nuevo espacio donde se relacionan los seres humanos, ese es el espacio o aldea global.

El Estado ha pasado a ser, un intermediario entre lo local y lo global, surgiendo la necesidad de reconsiderar su rol. (CASTELLS, 2009, p. 44), citando a Ulrich Beck complementa la idea afirmando "La globalización, cuando se lleva a su conclusión lógica, significa que las ciencias sociales deben refundarse como una ciencia basada en la realidad de lo transnacional, y ello desde el punto de vista conceptual, teórico, metodológico y organizativo. Aquí se incluye el hecho de que es necesario liberar los conceptos básicos de la "sociedad moderna"- hogar, familia, clase, democracia, dominación, estado, economía, esfera pública, política, etc. de las fijaciones del nacionalismo metodológico y redefinirlos y re conceptualizarlos en un contexto del cosmopolitismo metodológico". Posteriormente CASTELLS M (2009, p. 44) continua que "la teoría clásica del poder centrada en el estado-nación o en las estructuras de gobiernos subnacionales carece de marco de referencia desde el

momento en que los elementos clave de la estructura local son locales y globales al mismo tiempo, en lugar de locales o nacionales".

Todo lo anterior nos indica que surge una nueva dimensión en la cual los seres humanos se relacionan. En efecto, con la globalización no se presenta una desaparición del Estado – Nación, sino que debemos entender que estamos en una nueva dimensión donde se presentan relaciones entre humanas. Ahora, lo que sí es cierto, es que, con el surgimiento de esta nueva dimensión, el Estado debe transformar su rol dentro del universo de las relaciones humanas.

En esa medida, debe entenderse que existen una serie de redes, locales, regionales, nacionales y globales, en distintos ámbitos, que se relacionan de forma simbiótica entre ellas, generando nuevos espacios de interacción. Y en este marco, el Estado debe **re-asumir** su rol para determinar la forma como puede generar un óptimo funcionamiento al interior de cada red y entre las mismas, para generar un beneficio común a la sociedad que se conforma a partir de ellas.

En este punto es importante recordar la naturaleza de las redes. Una red es un conjunto interconectado de nodos. Cada nodo tiene mayor o menor importancia. Según CASTELLS M. (2009, p. 45) "los nodos aumentan en importancia para la red cuando absorben más información importante y la procesan más eficientemente. La importancia relativa de un nodo no proviene de sus características especiales, sino de su capacidad para contribuir a la eficacia de la red para lograr sus objetivos, definidos por los valores e interés programados en las redes".

Nace aquí la importancia de varios principios en materia de derecho que tiene como finalidad garantizar la neutralidad de las redes y el agnosticismo tecnológico de los elementos que las compone, para que los mismos no afecten en forma negativa las relaciones que se dan entre los nodos.

Y también debemos resaltar otra realidad, en las redes, dada su naturaleza democrática y abierta, las relaciones entre los agentes han cambiado. En efecto, si bien antes las relaciones se caracterizaban por una estructura relativamente vertical, y la asimetría de información relativa entre los diferentes agentes de las cadenas de valor, lo cierto es que en la actualidad las redes permiten a los usuarios tener mayor información respecto de los bienes o servicios que adquieren.

En esa medida, elementos utilizados para reducir los costos de transacción, como la reputación que otorgaban ciertas marcas se empieza a desdibujar, y empiezan a surgir nuevas formas de mercadeo y comunicación con los usuarios. Las personas no utilizan servicios como Google o YouTube porque den cierto estatus o tenga cierta imagen, los utilizan porque son buenos en su función o en palabras de Castells, porque son nodos que procesan la información con eficacia y contribuyen al desarrollo de la red.

Esta nueva forma de relacionarse ha conllevado, a que la regulación del Estado – Nación tradicional empiece a perder relevancia y a la vez genere fallas de mercado por arbitrajes regulatorios, todo por una falta de adaptación de esta entidad a su rol en un estado globalizado caracterizado por relaciones de red.

2.1.1.4. El rol del Estado en la modernidad

Según Rodolfo Herrera Bravo en la Modernización del Estado a Través de la Regulación Jurídica de las Tecnologías de Información[11], "…Este nuevo contexto exige que el Estado asuma un rol innovador. En tal sentido, cabe observar cómo la modernización en los países industrializados está dirigida a consolidar un sistema económico y social que reconozca en la generación, procesamiento y distribución del conocimiento y la información, el fundamento de la productividad, el bienestar y el poder. Además, esos

[11] ZARICH F., (2000, pag. 4-5)

Estados entienden que la realización de los cambios necesarios para alcanzar dicho sistema suele apoyarse en la utilización de innovaciones tecnológicas por parte de organizaciones independientes que participan, interactúan y cooperan al interior de un país".

Por lo expuesto, se requiere acompañar con normativa jurídica este nuevo rol, permitiendo el avance tecnológico. Normando para que los particulares se beneficien del avance tecnológico y para que las instituciones del estado utilice el avance tecnológico en beneficio de la sociedad. Todo esto en un marco de seguridad jurídica. Para Herrera se distinguen dos niveles de acción estatal: Un estadio "subsidiarios", donde el Estado actúa como generador de condiciones que permitan el normal desenvolvimiento de los particulares, por ejemplo fijando una política educacional destinada a formar un recurso humano calificado; creando condiciones de estabilidad económica que disminuyan los riesgos de las empresas que invierten en desarrollo tecnológico; o facilitando la participación de particulares a través de políticas de fomento. Un segundo estadio de "acción estatal", que se da al interior de la Administración del Estado, que es la informatización del Estado, mediante el fomento y empleo de cambios tecnológicos, que deben permitir mejorar la gestión. Materializando el principio de simplificación y flexibilidad administrativas.

2.1.2. El derecho

La evolución del raciocinio del hombre, le dio la facultad de pensar que podía mandar o dominar a sus pares y al mismo tiempo a los demás, les dio la facultad de pensar en defenderse de quienes querían dominarlos. Se estableció así la división entre gobernantes y gobernados. Sobre este punto el filósofo griego Platón expresa la siguiente frase "Donde reina el amor y respeto, sobran la leyes", es decir si no

hubiera nacido el deseo del hombre de dominar a sus pares y si hubiera respetado los bienes de su prójimo, no hubiera habido la necesidad del derecho.

En el avance de la historia de la humanidad nos muestra que el hombre imponía su fuerza sobre sus pares. Con el transcurrir del tiempo aparecen los dioses y con ellos la divinidad de lo sagrado. Existen normas de orden religioso y reglas de orden moral que priman sobre los individuos, incluso con pena de muerte en caso de ser desacatadas. Así surge la duda de que el derecho ha nacido por la evolución del derecho natural o por la imposición de la fuerza del más fuerte sobre el más débil. Con estos antecedentes Guillermo Gil Albarracín (2007, p. 29) indica: "…ya en Roma se observa una clara distinción entre el <<jus>> que esa el derecho de los hombres y el <<fas>> que era el derecho de los Dioses".

2.1.2.1. Orígenes del derecho

Los orígenes del derecho es de naturaleza controvertida (Gil, 2007, p. 30), y sobre este tema los investigadores jurídicos se han orientado a varias posturas, entre ellas las de mayor aceptación suelen ser las siguientes:

- El Derecho nace como una relación de fuerza entre personas desiguales, sea material o psíquica.
- El Derecho nace como reparación a una ofensa física o moral que una persona infringe a otra.
- El Derecho nace para regular la indemnización debida por el incumplimiento de una palabra dada. En general para regular los negocios jurídicos entre las personas.
- El derecho nace de la necesidad de regular las relaciones que surgen entre los distintos sujetos de derecho. A medida que las relaciones interpersonales se vuelven más complejas el derecho lo va receptando.

- El derecho nace como una reacción del Estado ante la auto tutela individual (venganza privada), monopolizando o más bien, pretendiendo monopolizar el uso de la violencia como instrumento de coerción y de resolución de conflictos

Para el análisis de la protección de datos dentro del Derecho Informático, nace de la necesidad regular las relaciones de los individuos dentro de las redes y dada su complejidad en cuanto al manejo de datos, dentro de las telecomunicaciones, las tecnologías de información y comunicación y el internet, surge la necesidad que el derecho también se vaya receptando de acuerdo al avance tecnológico.

2.1.2.2. Sistemas jurídicos

Aplicando la teoría de sistemas al derecho se puede decir que un sistema jurídico es el conjunto de partes, en esta caso: normas, regulaciones, costumbres, actitudes e ideologías, que se interrelacionan sobre lo que es el derecho. Para su aplicación en la sociedad cuenta con una estructura y modalidades de funcionamiento en la aplicación e interpretación de las reglas de derecho. Está relacionado también en la forma de creación, interpretación y modificación.

Cada país tiene su sistema jurídico, y en el caso de Bolivia el sistema al que pertenece es al Sistema de Derecho Romano-Germánico. Para entenderlo y normarlo es preciso conocer los principales sistemas jurídicos, más aún cuando el rol del estado ha cambiado de ser un intermediario entre lo local y lo global, y en cuanto al tratamiento de datos y derechos de refiere a la convivencia de distintos sistemas de derecho. Según Guillermo Gil Albarracín, (2007, pag. 34 -35) en el mundo los principales sistemas son:

- *Sistema de Derecho Romano – germánico:* Se caracteriza porque la norma de derecho se elabora inicialmente, y se aplica posteriormente a los problemas que la práctica presenta.
- *Sistema Anglosajón:* La cultura inglesa nace de la fusión dc la nobleza normada con la población anglosajona, esta última, provista de sangre romana, lo cual logra la unificación del derecho a través dc las decisiones de los tribunales reales de justicia en detrimento de las costumbres locales. Para solucionar este defecto los particulares se dirigían al rey, que por medio de su «confesor–canciller» suavizaba las normas, como siglos antes lo hiciera el «pretor» romano. Este sistema se ha transmitido a las colonias inglesas en el mundo.
- *Sistemas Socialistas:* Ubicados principalmente en Europa oriental Originalmente se formaron con elementos romano-germánicos, pero después de 1917 se han transformados de acuerdo a la corriente socialista.
- *Sistemas de extracción filosófica:* Derechos como el hindú, musulmán y japonés, que sin embargo, se han ido occidentalizando hasta parecerse en mucho al romano germánico.

2.1.2.2.1. Derecho romano

Gran parte de las normas jurídicas modernas son de origen romano (GIL, 2007, p. 34), ya sea por sus raíces históricas en occidente, sea por la occidentalización que han sufrido algunos derechos de oriente. La aportación en materia jurídica de Roma al mundo ha sido principalmente en materia de derecho privado al igual que en materia técnica jurídica. En los tiempos modernos es muy útil su estudio por lo siguiente:

- *Utilidad Histórica***:** El derecho actual tiene por orígenes las costumbres y el Derecho Romano, títulos enteros del código

civil, en especial lo relacionado a las obligaciones, han sido sacados de esta fuente.

- *Modelo:* Ya que poseemos no sólo las leyes, sino las aplicaciones que los jurisconsultos romanos hicieron de estas, las cuales se distinguen por una lógica impecable, llenas de análisis y deducción, nos permiten observar la perfección en la interpretación jurídica, deseable en todo jurista moderno.
- *Auxiliar:* Ya que a excepción de Inglaterra, las legislaciones europeas han pedido prestadas más de una ley al Derecho Romano para fundamentar sus respectivos códigos, lo que hace que el resto del mundo colonizado por las potencias europeas sienten las bases de sus respectivos sistemas legales en la misma fuente.
- *Marco Teórico:* Ya que el conocimiento del Derecho Romano, es indispensable para comprender la evolución sociológica cultural del Imperio Romano.

2.1.2.2.2. Derecho continental (s.j. romano), derecho anglosajón (s.j. common law)

El desarrollo tecnológico está directamente relacionado con los países desarrollados, quienes tienen el control de la Investigación y el Desarrollo (I+D), mientras que los países de menor desarrollo tienen que adoptar o recibir la transferencia tecnológica a través de actividades como el ensamblaje o servicios auxiliares. En cuanto al derecho se hace necesario así analizar los sistemas jurídicos de los países desarrolladores de tecnología (S.J. Anglosajón) y los países receptores de tecnología en este caso los del Sistema Continental (S.J. Romano).

Los países que adoptan el sistema jurídico anglosajón o de la ley común (commonlaw) son Estados Unidos, Gran Bretaña, Irlanda, Australia y otros países

que fueron colonias de Inglaterra donde el estudio del derecho está basado en el estudio de los precedentes, es decir, de los hechos pasados. Las normas son desarrolladas por tribunales en contraposición a los creados la ley. Es un sistema general de derecho que deriva de la jurisprudencia. Lo explicado anteriormente tiene implicancia en el desarrollo de la normativa de seguridad de datos personales, que está en paripasu (con igual paso) con el desarrollo tecnológico.

Bolivia y los países de la región reconocen el sistema jurídico continental o romano, donde el estudio se basa en la lectura de las leyes. Las normas son desarrolladas por el sistema legislativo. El sistema deriva de la existencia de códigos basados en principios jurídicos de hace siglos. En el caso del desarrollo normativo de seguridad de los datos personales su desarrollo normativo es insuficiente y con retraso.

2.1.2.3.Fuentes del derecho

La mayoría de la doctrina define fuentes como el origen del Derecho. Para Jaime Moscoso (1982, pag. 243): "…Fuente, es aquella de donde surge algo; el manantial del que brota a flor de la tierra el agua. En sentido figurado se habla de fuentes del derecho, para aludir al hontanar del que nacen las normas jurídicas".

Para el constitucionalista Juan Ramos (2009, p. 44): “En el caso del Derecho Constitucional Boliviano, sus fuentes se refieren a los orígenes desde los cuales ha venido desarrollándose ésta disciplina, como un conjunto de conocimientos jurídico-científicos, referentes a la organización y estructuración del Estado. En este sentido las fuentes del Derecho Constitucional, son las mismas que para el derecho positivo en general, es decir la ley, jurisprudencia, costumbre, historia, doctrina, constitución y leyes constitucionales”

Es así que las fuentes del derecho son el «alma» del Derecho, son fundamentos e ideas que ayudan al Derecho a realizar su fin (GIL, 2007, p. 50). El conjunto de normas (en sentido amplio) que integran un sistema y que deben utilizar los órganos de aplicación para resolver los casos que se les presenten son las «fuentes del Derecho».

Tanto las leyes como la jurisprudencia constituyen razones que los órganos de aplicación, utilizan para justificar sus decisiones sobre los casos que han de resolver, ya esas razones que no son otra cosa que normas se las suele llamar fuentes del Derecho. La ley y la jurisprudencia son además fuentes del Derecho de origen deliberado y cuya fuerza vinculante varía de un sistema de Derecho a otro y según cuál sea la posición jerárquica que ocupe el órgano que la ha producido.

La mayoría de la doctrina define fuentes como el origen del Derecho. "Fuente es aquella de donde surge algo; el manantial del que brota a flor de la tierra el agua. En sentido figurado se habla de fuentes del derecho, para aludir al hontanar del que nacen las normas jurídicas"

El Derecho Occidental (en el Sistema Romano Germánico o Sistema de Derecho continental) tiende a entender como fuentes las siguientes: La constitución, las leyes, la jurisprudencia, la costumbre, los principios y la doctrina

2.1.2.3.1. La constitución

Como ley suprema del ordenamiento jurídico nacional es la fuente más importante del derecho, porque en esta se positiva el Derecho Constitucional nacional o particular, general y comparado.

2.1.2.3.2. La ley

Etimológicamente la Ley viene de latín "lex", cuyo genitivo es "legis" y su plural "leges". Pero la verdadera raíz latina se encuentra en el verbo "legere", que significa escoger, según unos, y leer, en opinión de otros. La Ley constituye un mandato y regla arbitraria de un superior, así manifiesta, Bentham.

La Ley nace del Poder Legislativo por mandato de la Constitución, ya que éste poder del Estado tiene la facultad de dictar leyes, abrogarlas, derogarlas e interpretarlas.

2.1.2.3.3. Jurisprudencia

Jurisprudencia deriva de dos vocablos latinos: Jus, Juris. Derecho y Prudencia – Pericia. Etimológicamente significa conocimiento del derecho, de la justicia y de cosas justas.

Hoy, por jurisprudencia se entiende, la doctrina sentada por el más alto tribunal de justicia de una país a través de varios fallos dictados uniformemente sobre una materia, es decir, el derecho introducido por los fallos de los tribunales mediante la aplicación de las leyes (RAMOS, 2009, p. 46). En ese entendido las sentencias del Tribunal Constitucional Plurinacional y la jurisprudencia del Tribunal Supremo de Justicia constituyen también fuentes del derecho.

2.1.2.3.4. Costumbre

En materia jurídica podemos decir que la costumbre está constituida por el uso repetitivo y tomado en cuenta por el derecho.

Para Carlos Alverto Olamo V. y Alejandro Olamo G., (2000, p. 47): “La costumbre constituye fuente autónoma del derecho objetivo, reconocido principalmente en las legislaciones del mundo occidental, a condición que no contrarié lo precéptado en la Ley”.

Así mismo (ALAMO. y ALAMO, 2000, p. 48) “la costumbre para ser fuente de derecho constitucional deberá cumplir las siguientes características: a) ser antiguas, b) uniformes, c) generales, d) exteriores, e) obligatorias”

2.1.2.3.5. La doctrina

Para Jorge Asbún (2001, pag. 21) “La etimología del término doctrina se remonta al latín “deseo” que significa enseñanza, su sentido original se encentra vinculado entonces a la formación y/o aprendizaje, sea del saber en general o de una disciplina en particular, en la actualidad se define como el conjunto de estudios y teoría sobre determinada área del conocimiento”.

La doctrina es fruto de la elaboración intelectual de los estudiosos, tratadistas, profesores y otros entendidos en materia de derecho. Es el estudio del derecho que a través de la ley se convierte en derecho positivo (RAMOS, 2009, p. 50).

2.1.2.4. Clasificación del derecho

El derecho se puede clasificar en derecho objetivo y derecho subjetivo.

El *Derecho objetivo*; es aquel que se elabora para regir los actos de los individuos, es totalmente impositivo. Se puede clasificar en Derecho Público y Derecho Privado. En el Derecho Público encontramos el Derecho Constitucional, el Administrativo, el Financiero, el Penal, el Procesal y el Tributario. En el Derecho Privado se tiene el Civil, el Mercantil, el Laboral. Así mismo el Agrario y el de

Familia (Son parte del Derecho Social o conocido de naturaleza mixta). También se encuentra el derecho internacional público o privado.

El Derecho subjetivo; es opcional, también se lo conoce como derecho facultad. Es el poder que me otorga el Derecho Objetivo para reclamar ente la autoridad competente el cumplimiento de un deber jurídico contraído por otra persona. Por eso los actos humanos, los productos de espíritu y las cosas del mundo exterior son entidades que pueden ser objeto de derecho subjetivo.

Los derechos subjetivos pueden ser absolutos o relativos, transmisibles e intransmisibles, principales y accesorios, patrimoniales y no patrimoniales. Una cosa es todo objeto material susceptible de tener un valor, un bien estado cosa y objeto inmaterial susceptible de tener valor. Las cosas pueden ser corporales e incorporables, específicas y genéricas, consumibles y no consumibles, fungibles y no fungibles, divisibles e indivisibles, simples y compuestas, principales y accesorias, partes integrantes y pertenencias, muebles y inmuebles, Es notorio el recordar que una cosa debe ser útil, debe tener existencia autónoma y apropiabiliad para ser llamadas cosas en sentido jurídico.

El derecho subjetivo puede ser considerar en dos sentidos: *1ro. Sentido Amplio:* "Es la facultad de poder hacer poseer o exigir algo conforme a la norma jurídica. *2do. Sentido Restringido*: "Es el poder exclusivo conferido a una persona para actuar en su favor la tutela jurídica (Gil, 2007, p. 57).

2.1.2.5. Derecho informático

2.1.2.5.1. Definición y objeto de estudio

*Nicolás Tato en su libro "El Derecho Informático - Aspectos Fundamentales" (2010, p.) define al Derecho Informático como: "...*el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación de sujetos en el

ámbito de la informática y sus derivaciones, especialmente en el área denominada "tecnología de la información".

Tecnología de la Información, como concepto sociológico, define a la utilización de múltiples medios para almacenar, procesar y difundir todo tipo de información; generalmente a través de computadoras y otros dispositivos electrónicos.

Para Tato, El concepto que necesariamente engloba la antedicha definición es el de "Sociedad de la Información". Tal es la denominación dada a la sociedad actual, que ha reemplazado –como sucesora- a la sociedad industrial; y en la cual la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas, convirtiéndose sin lugar a dudas en bienes intangibles altamente valorados. La "Sociedad de la Información" surge a partir del desarrollo tecnológico, en una relación dialéctica de mutua alimentación: el desarrollo tecnológico hace nacer la sociedad de la información, la cual potencia el desarrollo tecnológico, lo cual acelera el avance de la sociedad de la información.

El concepto de Derecho Informático surge, entonces, a partir de los conceptos de "Tecnología de la Información" y "Sociedad de la Información", que son antecedentes necesarios e identificadores del Derecho Informático, ya ambos conceptos son los que le otorgan un objeto de estudio propio, el cual requiere una metodología específica con categorías conceptuales propias (además de las que comparte con las otras ramas del Derecho), y cuyas fuentes tienen particularidades originadas en el vertiginoso cambio inherente al ámbito tecnológico

El objeto de estudio del Derecho Informático es propio, aunque por el momento no necesariamente exclusivo. Esto se debe a que muchos de los aspectos abarcados por el Derecho Informático son abordados hoy en día por el derecho Penal, Civil y Comercial, debido a la falta de legislación específica que ataque las diversas

problemáticas resultantes y que contemple las particularidades que la Sociedad de la Información implica. Es decir, la falta de plena autonomía en su objeto obedece más a la falta de legislación específica que a la ausencia de autonomía *per se*.

Es importante tener en cuenta que otro de los elementos que configuran el Derecho Informático como una rama autónoma es el conjunto de conceptos y categorías específicas que lo integran. La Sociedad de la Información, conjuntamente con la creación de nuevos bienes inmateriales, ha generado nuevos conceptos que los categorizan, con la particularidad de que estos conceptos son dinámicos y flexibles, pues la tecnología avanza de modo vertiginoso, y en muchos casos los bienes pueden ser copiados en cuanto a funcionalidad pero en una plataforma completamente diferente, lo cual hace muy difícil que el derecho penal o civil pueda manejarlo adecuadamente con sus categorías estáticas o analogía limitada. Sin ir más lejos, el correo electrónico tiene la misma funcionalidad que un mensaje de texto o "SMS" enviado por celular, o un mensaje enviado en una red social como "Facebook", o una leyenda escrita en una red social como "Twitter", o las múltiples plataformas que se crearán en un futuro. Es por eso que sólo a partir de la creación de categorías específicas correspondientes al Derecho Informático podrán analizarse y resolverse conflictos relacionados con la Sociedad de la Información, los cuales son cada día más frecuentes.

En consecuencia, si consideramos su particular objeto y categoría, y si sumamos a ello la importancia que revisten los bienes de la "sociedad de la información" y su específico sustrato físico o ámbito en el cual se producen los hechos, es decir, el sustrato tecnológico; concluiremos que *el Derecho Informático inevitablemente se ha convertido en una rama independiente, con un objeto propio, que aborda los temas con categorías, conceptos, y metodología de trabajo propia*.

2.1.2.5.2. Relaciones del derecho informático con las otras ramas del derecho

Al contar el derecho informático con un objeto propio de estudio en constante desarrollo relacionado con las "Tecnología de la Información" y "Sociedad de la Información", tiene un carácter multidisciplinario y es transversal a otras materias jurídicas:

- *Derecho Constitucional*.- Derecho fundamental de Acción de Privacidad
- *Derecho Internacional*.- Comercio Internacional Electrónico (E-comerce), Banca Internacional (Banca Electrónica Internacional), transferencia internacional de datos
- *Derecho Civil*.-Régimen de personas, privacidad, propiedad, obligaciones, contratos y prueba.
- *Derecho Penal*.- Delitos informáticos, ataques al derecho a la intimidad, sabotaje, fraude informático.
- *Derecho de Propiedad Intelectual***.-**Derechos de Autor, Software, patentes, marcas, nombres de dominios
- *Derecho Tributario*.- Recaudación impositiva arancelaria, documentos y firma digital
- *Derecho Comercial***.-** Defensa del consumidor, actividad comercial, registros de personerías
- *Solución de Controversias – Arbitraje*.- Jurisdicción de solución de controversias, arbitraje, mediación y conciliación electrónica,

2.1.3. Sociedad de información y derecho

Hoy en día la humanidad, se encuentra inmersa en una cambio de paradigma, las formas tradicionales de obtener información, publicitar bienes, realizar transacciones, han sido cambiadas y superadas por el uso de medios tecnológicos que antes no existían.

Ello ha llevado a que los economistas, denominen a este nuevo paradigma como economía digital y surjan las economías colaborativos. También ha obligado que las administraciones públicas lo utilicen como modelo para la reforma del estado, denominado gobierno electrónico. En el campo de la educación donde ya no es importante la presencia física ni el cumplimiento de horarios, esto ha ocasionado que los educadores se sientan amenazados por el computador si es que no se reestructura la misión de la escuela.

En este nuevo contexto los datos adquieren relevancia ya que la transmisión de datos permite realizar transacciones a gran velocidad gracias a la fibra óptica, Así mismo se permite el almacenamiento y procesamiento de importantes cantidades de datos en lo denominado Big Data.

2.1.4. Papel del derechos en la era digital

El Derecho también *se* ve afectado por estos cambios sociales, sólo que la intensidad y el grado del giro, superan ampliamente lo ocurrido.

Para el ordenamiento legal, el uso de tecnologías de la información se convierte en uno de los mayores retos que tiene que enfrentar y superar, si es que quiere cumplir con sus objetivos de establecer las reglas de convivencia social.

El Derecho tiene que tener las respuestas adecuadas para facilitar la transición del medio físico al mundo virtual, de lo contrario la convivencia social en internet sería una suerte de anarquía que puede llevar a su propio aniquilamiento. Claro está que todo ordenamiento legal surge cuando existe un grupo social, y de hecho en internet ya existen reglas de convivencia y códigos de conducta que están regulando a la mayoría de los internautas. Lo que sucede en internet es que los propios sectores,

tiene internalizadas sus normas y no la toman impuestas por terceras personas, tal como sucede con algunas comunidades campesinas respecto al derecho occidental.

El reto del Derecho es, pues, flexibilizar sus instituciones e incorporar aquellas normas surgidas dentro del Internet para que todos los actos jurídicos que se den dentro del mundo virtual tengan idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios tenga los mismos efectos legales.

Por tanto resulta de suma importancia revisar nuestros ordenamientos jurídicos y reorientarlos hacia la esfera digital tal cual lo vienen haciendo las administración es gubernamentales, empresas y personas de todo el mundo.

Ante esto nos surge la pregunta; si la actual convergencia digital de la sociedad puede originar la creación de un sistema jurídico propio o unificar los ya existentes.

2.1.5. Informática, libertades y derechos humanos

El avance tecnológico, especialmente en el área de la informática, abre nuevos cauces para progresos económicos sociales y culturales. Al mismo tiempo, empero, puede poner en peligro los derechos y las libertades de los individuos. Esta ambivalencia es una de las cuestiones fundamentales que debe resolver la sociedad moderna.

Por un lado, el manejo y almacenamiento de grandes volúmenes de información, mediante computadoras, da lugar a una nueva fuente de poder y de desigualdad entre las personas basado en el acceso a información. Por el otro, se acentúan las posibilidades de afectar el derecho a la privacidad, como

consecuencia de la divulgación a terceros de datos sobre la vida personal o familiar.

Con el avance de la informática no solo es más difícil controlar la difusión de datos personales, sino también asegurar la exactitud de aquellos que se almacenen o se transmiten para diversos fines. La propia defensa en juicio, más aún, puede ser vulnerada por el recursos a perfiles personales construidos sobre la base de informaciones contenidas en una banco e datos o resultante de una combinación de datos tomados de diferentes bancos de datos informatizados,

En síntesis, la informática debilita la capacidad de dominio de las personas sobre los datos que les conciernen. Ello es especialmente preocupante cuando se trata de las creencias religiosas o políticas, las condiciones de salud, y otros aspectos privativos de los individuos.

Carlos Correa, HikdaBatto, Susana Czar y Félix Nazar en su libro "Derecho Informático (1994, p. 241) indican que: "Diversas legislaciones, sobre todo a partir de la década pasada, establecieron mecanismos para impedir que el manejo de bancos de datos personales en poder de instituciones públicas y privadas, afecten negativamente la libertad y los derechos humanos. Suecia, Noruega, Austria, Francia y otros países, dictaron regulaciones en torno del principio fundamental de acceso del individuo a los datos que se poseen sobre él ("habeas data") y del derecho a l a rectificación o supresión, en caso de datos recogidos ilícitamente, inexactos u obsoletos. Comisiones presidenciales, integradas en algunos casos también por parlamentarios (como la Comisión de Informática y Libertades de Francia) fueron encargadas de atender y resolver los reclamos de los particulares y de controlar la constitución de bancos de datos personales públicos o privados".

Es así que el avance de la tecnología y la afirmación de los derechos del hombre en la democracia, exigen hoy nuevas reglas de derecho que, dentro del respeto de aquellos principios constitucionales, extiendan el amparo legal a situaciones que no pudieron preverse en su momento. Esas nuevas reglas deberán equilibrar los diferentes intereses jurídicos en juego. Por una parte, se trata de lograr un adecuado balance entre el derecho a controlar *la* propia información y el principio de la libertad de información, especialmente en cuanto esta última *se* relacione con cuestiones de interés social. Por otro lado, el derecho individual debe compadecerse con el de las instituciones democráticas para prevenir acciones que atenten contra su esencia.

2.1.5.1. Fundamentos del derecho protección de datos

El avance tecnológico, especialmente en el área de la informática, abre nuevos cauces para progresos económicos, sociales y culturales. Al mismo tiempo, empero, puede poner en peligro los derechos y la libertad de los individuos. Esta ambivalencia es una de las cuestiones fundamentales que debe resolver la sociedad moderna. Durante el trascurso de la última década se ha registrado una tendencia en la mayor parte de los países industrializados a proteger mediante regulaciones apropiadas los llamados datos personales.

Esta elaboración normativa que se produce paralelamente con el accionar de organismos internacionales, plasmó en la sanción de leyes cuyo objetivo es lograr una protección adecuada de los derechos y libertades fundamentales.

"En última instancia estas leyes pretenden solucionar el conflicto de intereses que se plantea entre el derecho a la vida privada que tiene todo

individuo y el derecho a la información, o la libertad de información que es la consecuencia de su ejercicio" (NOVOS, 1981, p. 9). Es decir, se procura lograr un equilibrio entre la información que necesita la sociedad para un funcionamiento democrático y el derecho del individuo a la protección de los datos que le conciernen.

Así existe una contraposición entre derechos individuales y derechos sociales. Los derechos individuales corresponden al hombre por el hecho de ser tal, y son, entre otros, el derecho a la integridad física y mental, el derecho a la imagen, el derecho al honor, al nombre, a la voz y el derecho a la vida privada. Los derechos sociales, designados genéricamente como derechos sociales, son los que corresponden al hombre por el hecho de formar parte de una comunidad organizada, y entre ellos se hallan el derecho al trabajo, a la seguridad social, a la asistencia médica, a la educación y el derecho a la información.

El conflicto entre estos dos derechos es característico de la época moderna y se acentúa en la actualidad con la aparición de las nuevas técnicas informáticas que permiten recoger información en cantidad ilimitada y difundirla a una velocidad superior a la del pensamiento humano, y la penetración cada vez más profunda de la informática en la vida social e incluso en la vida doméstica.

Mediante el uso de la informática, y en particular a través de la interconexión de ficheros, datos aparentemente inocentes se conjugan formando la historia personal de un individuo, con el consiguiente peligro de invasión de su esfera privada; inclusive una apropiada defensa enjuicio puede quedar vulnerada con el uso de datos contenidos en computadoras como medios de prueba.

Los riesgos de violación de derechos y libertades fundamentales mediante el uso de las nuevas técnicas informáticas se hacen más evidentes en el caso de las llamadas informaciones sensibles (datos sobre creencias o convicciones religiosas, opiniones políticas, origen racial, hábitos sexuales, circunstancias penales y pertenencia a sindicatos o partidos políticos, etc.) que pueden dar lugar a conductas discriminatorias por parte de quienes tienen monopolios de información.

Durante varios años las leyes de protección de datos fueron consideradas como un "lujo democrático para países ricos" por los países en desarrollo. Sin embargo, esta situación se ha ido modificando a partir de 1977[12], entre otras razones por el progresivo avance de la informática en estos países y la labor desarrollada por organizaciones internacionales.

2.1.5.2. Evolución de derecho de protección de datos

A través de los años se ha ido produciendo una evolución del concepto de protección de datos determinada por dos aspectos fundamentales: la evolución de las técnicas de información y la nueva configuración del derecho a la vida privada.

En los primeros años de aplicación de las leyes de protección de datos la discusión se centraba en la antítesis vida privada versus computadoras. En el actual estado tecnológico la protección de datos es una síntesis de los intereses individuales y sociales en juego (SIEGART, 1983, P. 16).

[12]Ley federal para la protección contra el uso ilícito de datos personales, de la República Federal Alemana, fue sancionada el 27 de enero de 1977.

2.1.5.3. Evolución de los datos personales

La sociedad de la información y el desarrollo de los sistemas de información como el big data[13] permiten un manejo rápido y eficiente de grandes volúmenes de información que facilita la concentración automática de datos referidos a las personas (constituyéndose un verdadero factor de poder). Como se analizó es hasta la década de los sesenta cuando empiezan a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos como nombre, número de documento de identidad, lugar de filiación, fecha y lugar de nacimiento, domicilio, estado civil, etc., hasta otro tipo de datos con caracteres aún más distintivos como raza, religión inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, etc.

Existen diferentes centros de recolección y acopio de datos, que ya no lo hacen con medios manuales sino con medios con apoyo de medios electrónicos, que, provocan una gran concentración, sistematización y disponibilidad instantánea de ese tipo de información para diferentes fines (registros, tramites, parroquiales, civiles, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios, laborales, identificación personal, etc). Estos datos no son vulnerables sino según la destinación de que puedan ser objeto dichas informaciones: pueden ser empleadas para fines publicitarios, comerciales, fiscales, policiales, etc., convirtiéndose de esta manera en un instrumento de operación y mercantilismo. La variedad de los supuestos posibles de indefensión frente al problema, provoca que los individuos estén a merced de un sin número de situaciones que alteren sus derechos fundamentales en sociedad provocados por discriminaciones, manipulaciones, persecuciones, presiones, asedios, etc., todo ello al margen de un control jurídico adecuado.

[13]Término que describe a cualquier cantidad voluminosa de datos estructurados, semiestructurados y no estructurados que tienen potencial de ser extraídos para obtener información.

2.1.5.4. Hábeas Data o derecho a la privacidad

El Hábeas Data surge con el fin de garantizar la privacidad o intimidad personal frente a los riesgos del almacenamiento, registro y utilización de datos.

"El desarrollo conceptual del derecho a la intimidad personal o "right of privacy", tiene lugar en la experiencia de los Estados Unidos y en el Reino Unido, desde finales del siglo XIX. Un punto crucial en este itinerario fue la definición del derecho a la privacidad como "theright to be letalone" es decir, el "derecho a ser dejado en soledad" (sin ser molestado o perturbado) elaborada por el Juez Cocley; este concepto fue desarrollado por los juristas norteamericanos Warren y Grandeis, buscando proteger a la persona frente a datos o actos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado"[14].

Como resultado del rápido desarrollo tecnológico, en los países más desarrollados Estados Unidos como en Gran Bretaña se promueven proyectos legislativos dando un nuevo giro o extensión al concepto de derecho a la privacidad se refieren a la protección de la libertad y esfera personal frente a posibles accesos del registro informatizado o difusión de datos e informaciones vinculadas a aspectos reservados o íntimos.

El Habeas Data es una de las garantías constitucionales, aunque se la denomine mitad en latín y mitad en inglés, su nombre se ha tomado parcialmente del antiguo instituto del Habeas Corpus, en el cual el primer vocablo significa "conserva o guarda tu…", y del inglés "data", sustantivo plural que significa "información o datos". En síntesis, en una traducción literal seria "conserva o guarda tus datos".

[14]MALLMA, SOTO, JOSÉ CARLO, obtenido de www.monografias.com,lenincarlos@hotmail.com

"Hábeas Data es una acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio"[15].

2.1.6. Tratamiento y medidas de seguridad, de datos personales

2.1.6.1. Seguridad con datos personales

Considerando que la adopción de diversos Sistemas de Información es masiva en casi cualquier contexto, surge la necesidad de proteger la información que forma parte de dichos sistemas, pues dicha información se torna crítica e invaluable, pues concentra el día a día de la organización. La «Seguridad es una necesidad básica. Estando interesada en la prevención de la vida y de las posesiones, es tan antigua como ella» (Manunta, 2003).

2.2. Marco referencial

2.2.1. Protección de datos y derecho a la privacidad e intimidad en las bases de datos públicos y privados

Sobre protección de datos, se revisa la investigación "La regulación para el acceso a datos en los registros públicos y privados en Bolivia" realizada por la Dra. Rosalynn María Perez Zegarra (2009), trabajo que analiza el Habeas Data. Llega entre otras a las siguientes conclusiones:

El concepto del derecho a la vida privada ha ido evolucionando con los avances tecnológicos, ya que con ellos se presentan nuevas formas de amenaza e invasión, más rápidas, más audaces y tenaces. Surge un nuevo derecho fundamental: la autodeterminación informativa, el control de los propios datos por parte de su

[15]Obtenido de:http://es.wikipedia.org/wiki/Habeas_data

titular. A la garantía de la intimidad, se le da un contenido positivo y las garantías para que el sujeto pueda hacerlo efectivo frente a terceros.

La protección al acceso de datos personales constituye una prioridad jurídica estructurada inicialmente bajo la conceptualización de un derecho fundamental denominado Habeas Data o Acción de Protección de Privacidad y/o Protección de Datos Personales, que funciona para que no se comparta la información íntima y para que esta información pueda corregirse, actualizarse o modificarse en todo momento, acción que se puede intentar solamente por su titular. En nuestro país se requiere intensificar la protección jurídica en torno a los datos personales, bajo mecanismos que van desde la protección legal en los procesos de captación, almacenamiento, sistematización y modos de compartirla, hasta los mecanismos legales para conocer datos propios y modificarlos cuando son imprecisos o erróneos. Algunos aspectos normativos actuales se relacionan con la intimidad y complementan su noción protectora, entre ellos destacan la inviolabilidad domiciliaria, inviolabilidad de las comunicaciones, el derecho a la propia imagen, etc., cada uno de ellos estructura sus propios bienes jurídicos tutelados y la forma de ejercitarlos. Las nuevas tecnologías de la información también inciden en el tema del acceso a datos personales y la protección de los mismos, principalmente en torno al tema de mantener segura la información personal sistematizada.

Es necesario que en Bolivia se legisle al respecto cuanto antes, como ya lo han hecho otros países. La salvaguarda de la información cuyo conocimiento, en principio, concierne sólo al titular, es un derecho humano. Si bien existen ciertos avances legislativos, es necesaria una legislación integral que sancione incluso la violación a este derecho fundamental. Se debe implementar en Bolivia, un mecanismo de protección jurídica en torno al acceso de los datos personales, bajo un procedimiento que asegure su ejercicio y que permita acceder a información personal de la que cada individuo es titular y que además asegure la forma jurídica para cambiarla cuando así se requiera.

2.2.2. Tratamiento de medidas de seguridad en plataformas digitales

Sobre medidas de seguridad la Dra. Karina Medinaceli en su libro publicado en la Agencia Estatal Boletín Oficial del Estado (BOE) y por la Agencia Española de Protección de Datos (AEPD), "El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano" (Medinaceli, 2016), expone el tratamiento de datos personales, este análisis es tomado en cuenta para construir un marco de referencia, para registros público privados.

2.2.2.1. Sistemas de gestión de la seguridad de la información

La norma (UNE) ISO/IEC 17799, predecesora de la actual UNE-ISO/IEC 27001, considera que la información es un activo que hay que proteger, y que puede estar en diferentes tipos de soportes. La norma citada sigue manteniendo tres principios clásicos de la seguridad (conocida como la Triada CIA por sus siglas en inglés):

Confidencialidad: el acceso a la información debe ser restringido en función de la persona que intenta acceder y de la pertinencia de dicho acceso. En otras palabras, se debe establecer quién accede a qué datos, cuándo y cómo.

Integridad: la información registrada debe ser veraz y completa, y para ello debe estar protegida contra accidentes y ataques. Si los datos no son fiables o están incompletos, no son de utilidad.

Disponibilidad: la información debe estar disponible en el momento y lugar en que sea necesaria, independientemente del momento y lugar en el que se haya generado (Blanco y Rojas, 2012).

Se entiende que la disponibilidad estaría dentro de un marco de tiempo variable según el sector y tipo de aplicación y que una situación de no disponibilidad temporal es un riesgo, generalmente mucho menor que la no disponibilidad definitiva por pérdida irreversible de la información correspondiente.

TABLA No. 2
NECESIDAD DE SEGURIDAD

Necesidad	Medidas
Confidencialidad	Definición de permisos: determinar quién puede acceder al sistema y a qué información puede acceder. Control de accesos: conocer quién accede realmente al sistema y a qué información accede. Protección del sistema: impedir accesos no autorizados.
Integridad	Protección de la información: evitar la alteración o pérdida de datos, y garantizar su recuperación en caso necesario. No repudio: impedir que un agente implicado en el tratamiento de la información niegue su participación.
Disponibilidad	Definición de los niveles de servicio correspondientes. Adaptación de los sistemas de información a los niveles de servicio. Dotación de los recursos necesarios para garantizar el nivel de servicio.

FUENTE: Rojas y Blanco, 2008

El Instituto Nacional de Tecnologías de la Comunicación de España (INTECO) señala que existen numerosos e importantes beneficios para implementar Sistemas de Seguridad de la información, como por ejemplo:

Reducción de costes: Incide directamente sobre la rentabilidad económica de una organización. No suele serlo porque lo que se ve en un principio es el coste del mismo; sin embargo, en un breve plazo, se puede observar como los diferentes mecanismos de seguridad de la información evitan varias situaciones que suponen un coste, a veces importante.

Optimizar los recursos y las inversiones en tecnología: Con medidas de seguridad de la información correcta, las decisiones se tomarán en base a información fiable sobre el estado de los sistemas de información y a los objetivos de la organización. La organización dejará de depender exclusivamente de la experiencia

o pericia del responsable de informática, o más peligroso aún, del proveedor habitual de informática a la hora de valorar las distintas opciones de compra.

Protección del negocio: La Seguridad de la información en marcha evita interrupciones en el flujo de ingresos, ya que se está asegurando de una manera eficaz la disponibilidad de los activos de información y, por lo tanto, de los servicios que la organización ofrece. Esto en cuanto a la actividad cotidiana; pero también se está preparado para recuperarse ante incidentes más o menos graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el negocio a largo plazo.

Mejora de la competitividad: Cualquier mejora en la gestión de la organización tiene consecuencias directas en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza de los clientes en el negocio, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

Cumplimiento legal y reglamentario: Cada vez son más numerosas las leyes, reglamentos y normativas que tienen implicaciones en la seguridad de la información. Gestionando de manera coordinada, la seguridad permite un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

Mantener y mejorar la imagen corporativa: Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y servicios. Debido a la exposición de cualquier organización a un fallo de seguridad que pueda acabar en la prensa, este punto puede ser un catalizador de esfuerzos, ya que nadie quiere que su marca quede asociada a un problema de seguridad o una multa por incumplimiento, por las repercusiones que acarrea (INTECO, 2010).

2.2.2.2. Protección de datos y seguridad de la información

Cuando se maneja documentación personal (tratamiento) en documentación administrativa y empresarial, es necesario tomar en cuenta las obligaciones legales vigentes. España contaba con un ordenamiento legal de tratamiento de datos personales, que está compatibilizado con la derogada Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD)[16].

La derogada Ley Orgánica de Protección de Datos (LOPD)[17] en su artículo 3, establecía las principales definiciones vinculadas con la protección de datos. En su reglamento abrogado, Real Decreto 1720/2007, de 21 de diciembre de 2007[18] (Anexo 1), se diferencian en sus artículos 80 y 81, los niveles básico, medio y alto de protección de la información personal y se establece en qué casos se aplican. Posteriormente en el Capítulo III (medidas de seguridad aplicables a ficheros y tratamientos automatizados), ilustra las medidas de seguridad que garantizan la seguridad de la información en los sistemas informáticos, que se han de aplicar según el nivel de protección (nivel básico, medio y alto de protección de la información personal) en lo que respecta a:

- Funciones y obligaciones del personal
- Registro de incidencias
- Controles de acceso
- Gestión de soportes y documentos

[16] En Europa a partir del 25 de Mayo del 2018, entra en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD). Publicado en el DOUE el pasado 4 de mayo de 2016

[17] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, Agencia Estatal Boletín Oficial del Estado, España

[18] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, Agencia Estatal Boletín Oficial del Estado, España

- Identificación y autenticación
- Copias de respaldo y recuperación
- Responsable de seguridad
- Auditoría
- Telecomunicaciones

El tratamiento de custodia física, también es contemplado con medidas de seguridad concreta para ficheros no automatizados en el Decreto Real abrogado, en su Capítulo IV, en lo relativo a:

- Criterios de archivo y de almacenamiento de la información
- Dispositivos de almacenamiento
- Custodia de los soportes
- Responsable de seguridad
- Auditoría
- Copia o reproducción
- Acceso a la documentación
- Traslado de documentación

2.3. Marco conceptual

El presente punto del Marco Teórico se busca establecer un marco conceptual, que permita establecer con claridad los diferentes conceptos que se toman en cuenta en el presente trabajo de investigación.

2.3.1. Concepto de derecho

El tratadista Marco Gerardo Monrroy Cabra, indica que etimológicamente: «Derecho deriva de la voz latina DIRECTUM, de DIRIGERE, dirigir, encauzar, y que significa lo que está conforme a la regla, a la norma. Derecho se dice en italiano

DIRITTO; en portugués, DIREITO; en rumano, DREPTU; en francés, DROIT; en inglés, RLGHT; en alemán, RECHT; en holandés REGHT». Con estos antecedentes (Gil G, 2007, pag. 48), deduce que la palabra derecho «lleva en muchas lenguas la idea de rectitud, corrección, orden, etc.».

Así mismo Guillermo Gil Albarrán (2007, p. 758) Derecho define como: "Conjunto de normas vinculado a una sociedad determinada". Menciona a otro tratadista Gustavo Radbhuch[19] el Derecho pertenece al "reino de la cultura". El Derecho es todo aquello que puede ser objeto de una apreciación de justicia o injusticia. Derecho es aquello que debiera ser derecho justo, siéndolo o no; derecho es lo que persigue por fin la justicia, aunque para serlo no necesita de ningún modo haberla alcanzado… Culmina Guillermo Gil, indicando: "Lo que determina el concepto de derecho es, precisamente, no la esencia del valor justicia, si no el substrato o esencia a la cual se refiere la justicia, llegando entonces a la conclusión de que derecho es "regulación de la sociedad o comunidad.."

2.3.1.1. Derecho a la privacidad

Según el Diccionario de la lengua española de la Real Academia Española, privacidad se define como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

Con este antecedente, Rosalynn Pérez Zegarra (2009, p. 103). Indica que "La importancia del derecho a la privacidad, donde podemos apreciar el valor de ese lugar propio, interno, no conocido por todos y que en caso de ser conocido debe ser respetado este derecho que nos protege de las injerencias de extraños y nos garantiza que en caso de que sea violentada la paz de nuestra vida privada, ese extraño responsable".

[19] Gustavo Radbruch (1878 1949)

Posteriormente define Derecho a la Privacidad indicando que “es un derecho que les corresponde por excelencia a todos los seres humanos, incluso desde su nacimiento. Todos y cada uno de nosotros nacemos con el derecho de que sea protegida por el ordenamiento jurídico esa esfera de nuestra vida que compone todos los datos y acontecimientos que conforman nuestra vida privada que están excluidos todos aquellos a quienes no hayamos autorizado a ingresar”.

2.3.1.2. Derecho a la intimidad

Según el Diccionario de la lengua española de la Real Academia Española, intimidad se define como "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia".

Guido Aguila y Elmer Capcha (2005, p. 38) definen como “Derecho que permite al individuo desarrollar su propia vida, en que todos deben guardar reserva de los detalles de la vida de los demás, con un grado mínimo de interferencia, libre de perturbación que ocasionen otros individuos o autoridades públicas. Se viola este derecho cuando un aspecto de la vida de la persona o familiar del individuo es dado a conocer sin su consentimiento. Si la persona fallece, la protección es ejercida por sus ascendientes, descendientes y por su cónyuge”.

2.3.1.3. Garantía constitucional

Para Manuel Osorio (2005, p. 453), garantía constitucional son: “Las que ofrece la Constitución, en el sentido de que se cumplirán y respetaran los derechos que ella consagra, tanto en lo que se refiere al ejercicio de los de carácter privado como al de los índole publica”.

Así mismo garantía constitucional se puede definir como: "…un proceso instituido por la misma Constitución de un Estado cuya finalidad es defender la efectiva vigencia de los derechos fundamentales que este texto reconoce o protege, haciendo efectiva la estructura jerárquica normativa establecida." (PEREZ, 2009, p. 103).

2.3.2. Profundizando el concepto de derecho informático

En el punto 2.1.2.5.1.del presente trabajo de investigación de presenta la definición y objeto de estudio del Derecho Informático. Con el objeto de definir desde el punto de vista de la ciencia del derecho se puede indicar que el derecho informático esta interrelacionado con el derecho propiamente dicho, la informática y la sociedad, así el Dr. Ariel Agramont Loza[20] indica que: "El Derecho Informático, es un producto cultural de la sociedad de la información y del conocimiento contenido en normas jurídicas , basadas en principio y valores, que estudia y regula las consecuencias jurídicas de los hechos informáticos, es multidisciplinario y transversal a otras materias jurídicas".

2.3.3. Concepto de protección de datos

La evolución de las técnicas informáticas hace necesario hablar de *sistemas de información* en lugar de ficheros y tener en cuenta las contradicciones que existen entre la vida privada y otras libertades esenciales.

La concepción del derecho a la vida privada como el derecho a ser dejado sólo, corresponde a una época caracterizada por un acentuado individualismo. En la actualidad el derecho a la vida privada ha dejado de concebirse como la libertad negativa de rechazar u oponerse, al uso de

[20]Agramont Loza Ariel: "Apuntes : "Curso Especializado en Derecho Informático y Leyes del Internet v6", Derechoteca, 2018

información sobre sí mismo, para pasar a ser la libertad positiva de supervisar el uso de la información. Ya no se trata de una libertad aristocrática como la del derecho a ser dejado solo, sino a una libertad democrática.

Según Stefano Rodota[21] "el problema no consiste en garantizar la capacidad de la vida privada, sino la trasparencia del accionar de entidades públicas y privadas. Este autor considera que la privacidad en su nueva configuración no es el derecho a ser dejado solo, ni el nuevo derecho a supervisar a quienes poseen información, sino que es fundamentalmente el derecho a no ser discriminado. Es decir que el concepto de vida privada habría quedado reducido a un núcleo central relativo a las informaciones sensibles".

Para Spiro Simitis en su artículo de Protección de Datos[22]: "la protección de datos es sólo un aspecto de la distribución de la información en una sociedad determinada: por consiguiente, carecería de significación la clasificación abstracta en información sensible o de otro tipo, ya que toda la información es relevante según el contexto y la finalidad con que sea usada".

Esta evolución del concepto de protección de datos ha determinado que la expresión "informática y vida privada" haya sido dejada de lado paulatinamente por la expresión "informática y libertades" (Correa, Batto, Czar y Nazar, 1994 p. 250).

[21] Stefano Rodotá, "Data protection. Some problems for newcomers, artículo publicado en Legislation and data protection, pag.186.
[22]Ver Spiro Simitis, "Data protection. A frew critical remarks", publicado en, Legislation and data protection, pag.171/173"

2.3.3.1 Dato de carácter personal

"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"[23]. Es toda información sobre una persona física o jurídica identificada o identificable (el interesado). Se considera identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural, personal o social.

Siguiendo esta definición, en España los datos personales se establece el tratamiento dependiendo del sector público o privado.

2.3.3.1.1. Dato personal publico

Para Miguel Angel Davara Rodríguez los datos personales públicos son: "Aquellos datos personales que son conocidos por un número cuantioso de personas, sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del datos, ni, por la calidad de datos, pueda impedir que, una vez conocido, sea libremente difundido dentro de unos límites respecto de respeto y convivencia cívicos" (DAVARA, 1993, p.50).

Siguiendo este concepto en Bolivia serían todos aquellos datos que tienen carácter registral en una base de datos sea pública o privada como ser el SERECI, SEGIP, MIGRACION, CNS, REJAP, DERECHOS REALES, PADRON ELECTORAL, ASFI, ADSIB, AGETIC, BANCOS, AFPS, etc. Estarían referidos a: nombre, apellido, fecha de nacimiento, estado civil, profesión, domicilio, teléfono,

[23] Ley Orgánica 15/1999,y Real Decreto 1720/2007, Agencia Estatal Boletín Oficial del Estado, España

números identificatorios como: cédula de identidad, pasaporte, seguros, licencia de conducir, etc. "Se trata de referencias que permiten identificar o situar a las personas individuales y su entorno cotidiano y, por lo tanto, caen en el ámbito personal de las mismas" (PERES, 2009, p. 92).

2.3.3.1.2. Dato personal sensible

El Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo, Relativo a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de Estos Datos y por el que se Deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) para el tratamiento de datos personales, estable categorías especiales («datos sensibles»), considerando uno de ellos los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas[24]. En Bolivia El derecho a la auto-identificación cultural está consagrado en el primer parágrafo del artículo 21 de la Constitución Política del Estado. Para gozar de él, es suficiente proclamar la pertenencia a una de las culturas, etnias, naciones o pueblos indígenas originarios reconocidos por la legislación boliviana, por lo que no podría considerarse un dato personal sensible sino público.

Carlos Paladella Salord (Paladella, 1998) define, "Estos datos "sensibles" o datos personales íntimos encontramos: la afinidad política y todo otro tipo de creencias o tendencias humanas episodios de naturaleza especial (violaciones, vejaciones, etc.) enfermedades padecidas, tratamientos psicológicos y otros más. Éstos revisten unas características específicas que los hacen merecedores de una

[24] Considerando 51, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la Protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la libre Circulación de estos Datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

protección más profundizada que los otros. Se trata de información relativa al fuero interno de las personas, es decir, que identifica los sentimientos, la personalidad, las creencias y pensamientos de orden privado de las personas, se trata de partes del ser que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público".

2.3.3.2 Fichero o base de datos

Fichero se define como "Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.*"*[25].

Según el Wikipedia, "Una base de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, por tanto se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos"[26].

2.3.3.3 Manejo o tratamiento de datos

Se define como "cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión,

[25] Ley Orgánica derogada 15/1999,y Real Decreto derogado 1720/2007, Agencia Estatal Boletín Oficial del Estado, España
[26] Véase: https://es.wikipedia.org/wiki/Base_de_datos, Categoría: Base de datos

así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias..”[27].

El desarrollo tecnológico y de las plataformas de información hacen que se maneje o trate datos mediante textos, imágenes, documentos, registros, listados, etc, que pueden estar afectando información concerniente a intimidad y privacidad de las personas.

2.3.4. Definición de seguridad de información

La Real Academia Española (RAE) define como seguro, algo que tiene características importantes como la de estar libre y exento de peligro, daño o riesgo.Toda vez que el activo que se está resguardando se encuentra en los sistemas de información, se puede seguir la definición de Aguilera López (2010, p. 9) que señala que la seguridad de la información «es una disciplina que se ocupa de diseñar normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable». De la misma manera, Sanz y Hualde (2000, p. 74) definen a la seguridad como «la característica de un sistema que lo hace ser capaz de proteger sus datos frente a la destrucción, interceptación o modificación no deseadas».

Por lo que se entenderá en el presente trabajo como seguridad a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e integridad de la misma. “Así mismo la seguridad debe ser una característica de los sistemas de información que almacenan datos, por lo que se hace muy necesario tenerlo en cuenta en todo el ciclo de desarrollo de los Sistemas de Información.” (MEDINACELI, 2010, p. 436).

[27] Ley Orgánica 15/1999,y Real Decreto 1720/2007, Agencia Estatal Boletín Oficial del Estado, España

2.4. Marco Histórico

El presente punto del Marco Teórico está referido a los antecedentes del problema, es decir referido a la evolución del Habeas Data. Sobre este punto la Dra. Rosalynn Pérez en su Tesis "La Regulación para el Acceso a Datos en los Registros Públicos y Privados de Bolivia" realiza un análisis de reseña histórica que se presenta a continuación.

2.4.1. Reseña histórica

El Hábeas Data surge como un proceso constitucional especializado, para la protección de ciertos derechos en relación a la libertad informática sus antecedentes genéricos básicos podemos remontarlos a los intentos por preservar esferas personales de injerencias o perturbaciones externas no deseadas, a fin de garantizar la privacidad o intimidad personal frente a los riesgos del almacenamiento, registro y utilización de datos.

"El desarrollo conceptual del derecho a la intimidad personal o "right of privacy", tiene lugar en la experiencia de los Estados Unidos y en el Reino Unido, desde finales del siglo XIX. Un punto crucial en este itinerario fue la definición del derecho a la privacidad como "the right to be let alone" es decir, el "derecho a ser dejado en soledad" (sin ser molestado o perturbado) elaborada por el Juez Cocley; este concepto fue desarrollado por los juristas norteamericanos Warren y Grandeis, buscando proteger a la persona frente a datos o actos de índole personal, que se ponen en conocimiento del público o de terceros sin el consentimiento del afectado"[28]

Tiempo después, aproximadamente desde 1960 y como reacción al vertiginoso desarrollo tecnológico que se traduce en nuevos sistemas informáticos,

[28] Véase: www.monografias.com, lenincarlos@hotmail.com, Monografía de José Carlo Mallma Soto

tanto en los Estados Unidos como en Gran Bretaña se empiezan a promover proyectos legislativos dando un nuevo giro o extensión al concepto de derecho a la privacidad se refieren a la protección de la libertad y esfera personal frente a posibles accesos del registro informatizado o difusión de datos e informaciones vinculadas a aspectos reservados o íntimos. El primer texto de protección de datos es la Datenshutz, dictada en el Parlamento del Land de Hesse en la República Federal Alemana, promulgada el 7 de octubre de 1970, esta ley dio origen a la Ley federal de 27 de febrero de 1977; en Suecia, la norma que protege los datos es del 11 de mayo de 1973; en los Estados Unidos de Norteamérica a la "*Privacy Act*" del 31 de diciembre de 1974 que protege el derecho a la intimidad; en Inglaterra a la "*Data Protection Act*" de 1984; y Ley Orgánica mayo de 1992 España, denominada "Regulación del tratamiento automatizada de datos". En el ámbito latinoamericano fue la Constitución Brasileña de 1988, la primera en abordar estos temas, pero sobre todo también la primera en "bautizar" constitucionalmente al instituto del hábeas data.

El habeas data es una de las garantías constitucionales, aunque se la denomine mitad en latín y mitad en inglés, su nombre se ha tomado parcialmente del antiguo instituto del Habeas Corpus, en el cual el primer vocablo significa “conserva o guarda tu …”, y del inglés “data”, sustantivo plural que significa “información o datos”. En síntesis, en una traducción literal seria “conserva o guarda tus datos”.

“El **habeas data** es una acción jurisdiccional, normalmente constitucional, que confirma el derecho de cualquier persona física o jurídica para solicitar y obtener la información existente sobre su persona, y de solicitar su eliminación o corrección si fuera falsa o estuviera desactualizada. Este derecho aplica a información almacenada en registros o banco de datos de todo tipo, ya sea en instituciones públicas o privadas, y en registros informáticos o no. El derecho habeas data puede cobijar también el concepto de derecho al olvido, esto es, el derecho a eliminar

información que se considera obsoleta por el transcurso del tiempo y ha perdido su utilidad"[29]

En Bolivia "Para nosotros el hábeas data es un instrumento para controlar la calidad de los datos, corregir o cancelar datos inexactos o indebidamente procesados y disponer sobre su posible transmisión. Es un derecho que asiste a toda *persona* identificada o identificable a solicitar la exhibición de los registros públicos y privados, en los cuales están incluidos sus datos personales o los de su grupo familiar, político, social, económico, etc., que impliquen discriminación". ((PEREZ R., 2009, pág. 56).

2.4.1. Reseña histórica en Bolivia del derecho a la intimidad y habeas data

Este derecho fundamental para el goce pleno de los derechos y obligaciones, se refiere básicamente a la prohibición de violar datos o archivos personales pese a su importancia no fue considerado en la primera CPE, aparece en la de 1831, Art. 160 señalando sus alcances y fijando responsabilidades a los funcionarios de correos "Es inviolable el secreto de las cartas: los empleados de la renta de correos, serán responsables de la violación de esta garantía, fuera de los casos que prescriben las leyes"(TRIGO, 2003, p. 251). Esta norma se complementaba con otra muy avanzada para la época Art. 161: "Están prohibidas las requisiciones arbitrarias y apoderamiento injusto de los papeles y correspondencia de cualquier boliviano. La Ley determinará en qué casos y con qué justificación pueda procederse a ocuparlos" (TRIGO, 2003, p. 251).

Se observa un notable avance en la constitución garantísta de 1967 aprobada por uno de los regímenes que más inculcó los derechos humanos que ratifica y amplía el derecho de inviolabilidad de correspondencia con la prohibición de interceptar conversaciones y comunicaciones privadas mediante instalación que las controle o

[29] Vease: https://es.wikipedia.org/wiki/Habeas_data, Categoría: Habeas Data

centralice en el Art. 20 “Son inviolables la correspondencia y los papeles privados, los cuales no podrán ser ocupados sino en los casos determinados por las leyes y en virtud de orden escrita y motivada de autoridad competente. No producen efecto legal los documentos privados que fueren violados o substraídos. Ni la autoridad pública, ni persona y organismo alguno podrán interceptar conversaciones y comunicaciones privadas mediante instalación que las controle o centralice” *(*TRIGO*,* 2003*,* p. 651-652).

También encontramos el Art. 6 “Todo ser humano tiene personalidad y capacidad jurídica, con arreglo a las leyes. Goza de los derechos, libertades y garantías reconocidos por esta Constitución, sin distinción de raza, sexo, idioma, religión, opinión política o de otra índole, origen condición económica o social, u otra cualquiera. La dignidad y la libertad de la persona son inviolables. Respetarlas y protegerlas es deber primordial del Estado” (TRIGO, 2003, p. 710).

Las reformas constitucionales de 2002 ratifican los alcances y garantías, amplían más aún los derechos ciudadanos, reflejados en el Art. 7 sobre todo en el inciso ”l) Al nombre, a la intimidad y privacidad personal y familiar, así como a su imagen, honra y reputación”; y “n) Acceso a la información pública” (TRIGO, 2003, p. 782).; es evidente que se sufrió un penoso retroceso en las reformas constitucionales de 2004, que eliminan de hecho los alcances del Art. 7 incisos l) y n), esta reforma incorpora el Art. 23 referido al Hábeas Data, que ordena la revelación, eliminación o rectificación de los “datos registrados por cualquier medio físico, electrónico, magnético, informático, que cursen en archivos o banco de datos públicos o privados significativamente que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen y honra, reputación reconocidos, pero no procederá para levantar el secreto de materia de prensa” (CPE, 2002, p. 11).

Al referirnos de archivos se hace referencia fundamentalmente a la evolución de los derechos constitucionales de acceso y uso de la información oficial en Bolivia de la información de los registros y documentos públicos y esto se completa con el derecho de difusión y el derecho a la intimidad, es decir el reciclaje de la información y/o la generación de nuevo conocimiento. Las reformas constitucionales de 2002 ratifican y amplían los derechos ciudadanos, el conjunto de derechos descritos en el Art. 7 incisos: "b) A la libertad de conciencia, pensamiento y religión; a emitir y a recibir libremente ideas, opiniones, creencias e informaciones por cualquier medio de difusión; los incisos l) y n)"(TRIGO, 2003, p. 781) mencionados anteriormente, tienen relación directa e indirecta con el uso, acceso y difusión de información, las nuevas concepciones introducidas en estas reformas poseen una tremenda connotación sobre todo los incisos "l" y "n", sin embargo existe un notable retroceso en las reformas constitucionales de 12 de febrero de 2004, que dejan sin efecto los avances del artículo 7 (incisos l y n), volviendo en esto al texto de 1994 reconocidas como derechos fundamentales de hombres y mujeres son resquicios que otorga el Estado para proteger y abrir sus registros, archivos públicos al uso y su protección la intimidad de la persona.

2.5. Marco jurídico

El presente punto del Marco Teórico tiene como objetivo referenciar la normativa vigente en Bolivia referida a la protección de datos personales, su tratamiento en los registros públicos y privados y el nivel de seguridad de información.

Se hará un análisis considerando la jerarquía jurídica de la Constitución Política del Estado, los tratados internacionales, las leyes y los decretos reglamentarios.

2.5.1. Constitución Política del Estado

La Constitución Política del Estado, aprobada por Referéndum Nacional el 25 de enero de 2009 y promulgada por el Presidente Evo Morales Ayma el 7 de febrero de 2009, reconoce los Derechos Civiles de derecho a la privacidad e intimidad. Así mismo estos derechos gozan de garantías jurisdiccionales y acciones de defensa, siendo una de ellas la Acción de Protección de Privacidad. Los principales artículos se exponen a continuación:

> **Artículo 21.** Las bolivianas y los bolivianos tienen los siguientes derechos: …2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad.

> **Artículo 130. I.** Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad. **II.** La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

> **Artículo 131. I.** La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional. **II.** Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. **III.** La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución. **IV.** La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin

observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.

La Constitución vigente reconoce los instrumentos internacionales de derechos humanos que se aplican de manera preferente sobre la constitución, así lo establecen los artículos 256 y 410:

Artículo 256. I. Los tratados e instrumentos internacionales en materia de derechos humanos que hayan sido firmados, ratificados o a los que se hubiera adherido el Estado, que declaren derechos más favorables a los contenidos en la Constitución, se aplicarán de manera preferente sobre ésta. **II.** Los derechos reconocidos en la Constitución serán interpretados de acuerdo a los tratados internacionales de derechos humanos cuando éstos prevean normas más favorables.

Artículo 410. I. Todas las personas, naturales y jurídicas, así como los órganos públicos, funciones públicas e instituciones, se encuentran sometidos a la presente Constitución. **II.** La Constitución es la norma suprema del ordenamiento jurídico boliviano y goza de primacía frente a cualquier otra disposición normativa. El bloque de constitucionalidad está integrado por los Tratados y Convenios internacionales en materia de Derechos Humanos y las normas de Derecho Comunitario ratificados por el país. La aplicación de las normas jurídicas se regirá por la siguiente jerarquía, de acuerdo a las competencias de las entidades territoriales: **1.** Constitución Política del Estado. **2.** Los tratados internacionales. **3.** Las leyes nacionales, los estatutos autonómicos, las cartas orgánicas y el resto de legislación departamental, municipal e indígena. **4.** Los decretos, reglamentos y demás resoluciones emanadas de los órganos ejecutivos correspondientes.

2.5.2. Instrumento internacionales – privacidad y protección de datos personales

2.5.2.1. Declaración Universal de los Derechos Humanos

La Declaración Universal de los Derechos Humanos (DUDH) es un documento declarativo adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París; en esta se recogen en sus 30 artículos los derechos humanos considerados básicos, a partir de la carta de San Francisco (26 de junio de 1945)[30]. Ratificado por el Estado Plurinacional de Bolivia.

Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

2.5.2.2. Pacto Internacional de Derechos Civiles y Políticos

Es un tratado multilateral general que reconoce derechos civiles y políticos y establece mecanismos para su protección y garantía. Fue adoptado por la Asamblea General de las Naciones Unidas, mediante Resolución 2200 A (XXI) de 16 de diciembre de 1966[31]. Fue Adoptado y abierto a la firma, ratificación y adhesión por el Estado Plurinacional de Bolivia por Ley 2119 de 11 de septiembre del año 2000.

Artículo 17. 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni ataques ilegales a su

[30] Vease: https://es.wikipedia.org/wiki/Declaraci%C3%B3n_Universal_de_los_Derechos_Humanos, Categoría: Declaración Universal de Derechos Humanos

[31] Veasehttps://es.wikipedia.org/wiki/Pacto_Internacional_de_Derechos_Civiles_y_Pol%C3%ADticos

honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques

2.5.2.3. Convención americana sobre derechos humanos

La Convención Americana sobre Derechos Humanos (también llamada Pacto de San José de Costa Rica) fue suscrita, tras la Conferencia Especializada Interamericana de Derechos Humanos, el 22 de noviembre de 1969 en la ciudad de San José en Costa Rica y entró en vigencia el 18 de julio de 1978. Es una de las bases del sistema interamericano de promoción y protección de los derechos humanos[32]. Adoptado y abierto a la firma, ratificación y adhesión por el estado plurinacional de Bolivia.

> **Artículo 11.** 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

2.5.2.4. Declaración americana de los derechos y deberes del hombre

Fue aprobada por la IX Conferencia internacional americana realizada en Bogotá en 1948, la misma que dispuso la creación de la Organización de los Estados Americanos (OEA). Históricamente, fue el primer acuerdo internacional sobre derechos humanos, anticipando la Declaración Universal de los Derechos Humanos, sancionada seis meses después. El valor jurídico de la *Declaración* ha sido

[32] Vease: https://es.wikipedia.org/wiki/Convenci%C3%B3n_Americana_sobre_Derechos_Humanos, Categoría: Convención Americana de Derechos Humanos.

muy discutido, debido a que no forma parte de la Carta de la OEA y tampoco es un tratado[33].

> **Artículo 5** - Derecho a la protección a la honra, la reputación personal y la vida privada y familiar Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

2.5.3. Código Civil y Código Penal

Si bien el Hábeas Data no está contemplado expresamente en la Constitución o en otras leyes secundarias, creemos que en Bolivia se puede aplicar recurriendo al Código Civil para el derecho a la intimidad y al Código Penal para la protección de la intimidad frente al avance tecnológico

2.5.3.1. Código Civil

El Código Civil Boliviano, Ley No. 439 de 19 de noviembre de 2013, reconoce el derecho a la intimidad.

> **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.

[33] Vease: https://es.wikipedia.org/wiki/Declaraci%C3%B3n_Americana_de_los_Derechos_y_Deberes_del_Hombre.

2.5.3.2. Código Penal

El Código Penal fue sancionado por el Decreto Ley N° 10426 de 23 de agosto de 1972, modificado según Ley N° 1768 de modificaciones al Código Penal y actualizado según Ley 2494 de 04 de agosto de 2003.

Artículo 298 (ALLANAMIENTO DEL DOMICILIO O SUS DEPENDENCIAS).- El que arbitrariamente entrare en domicilio ajeno o sus dependencias, o en un recinto habitado por otro, o en un lugar de trabajo, o permaneciere de igual manera en ellos, incurrirá en la pena de privación de libertad de tres meses a dos años y multa de treinta a cien días. Se agravará la sanción en un tercio, si el delito se cometiere de noche, o con fuerza en las cosas o violencias en las personas, o con armas, o por varias personas reunidas

Artículo 299 (POR FUNCIONARIO PÚBLICO).- El funcionario público o agente de la autoridad que, con abuso de sus funciones o sin las formalidades previstas por ley cometiere los hechos descritos en el artículo anterior, será sancionado con privación de libertad de uno a cuatro años.

Artículo. 300.- (VIOLACIÓN DE LA CORRESPONDENCIA Y PAPALES PRIVADOS).- El que indebidamente abriere una carta, un pliego cerrado o una comunicación telegráfica, radiotelegráfica o telefónica, dirigidos a otra persona, o el que, sin abrir la correspondencia, por medios técnicos se impusiere de su contenido, será sancionado con reclusión a tres meses a un año o multa de sesenta a doscientos cuarenta días. Con la misma pena será sancionado el que de igual modo se apoderare, ocultare o destruyere una carta, un pliego, un despacho u otro papel privado, aunque estén abiertos, o el que arbitrariamente desviare de su destino la correspondencia que no le pertenece. Se elevará el máximo de la sanción a dos años, cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados.

Artículo. 301.- (VIOLACIÓN DE SECRETOS EN CORRESPONDENCIA NO DESTINADA A LA PUBLICIDAD).- El que grabare las palabras de otro no destinadas al público, sin su consentimiento, o el que mediante procedimientos técnicos escuchare manifestaciones privadas que no le estén dirigidas, o el que hiciere lo mismo con papeles privados o con una correspondencia epistolar o telegráfica aunque le hubieren sido dirigidos, siempre que el hecho pueda ocasionar algún perjuicio, será sancionado con privación de libertad de tres meses a un año.

Artículo. 302.- (REVELACIÓN DE SECRETO PROFESIONAL).- El que teniendo conocimiento de secretos en virtud de su estado, ministerio, profesión, empleo, oficio, arte o comisión, los revelare sin justa causa, o los usare en beneficio propio o ajeno, si de ello se siguiere algún perjuicio, será sancionado con privación de libertad de tres meses a un año y multa de treinta a cien días.

Art. 363 bis.- (MANIPULACIÓN INFORMÁTICA).- El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Art. 363 ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).- El que sin estar autorizado se apoderare, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

2.5.3.3. Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación

La Ley 164, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación de fecha 8 de agosto de 2011, en el marco de las telecomunicaciones establece la protección de datos personales como un derecho de los usuarios y como un deber por parte del proveedor del servicio.

> **Artículo 2. (OBJETIVOS).** La presente Ley tiene por objetivos: …2. Asegurar el ejercicio del derecho al acceso universal y equitativo a los servicios de telecomunicaciones, tecnologías de información y comunicación, así como del servicio postal.

> **Artículo 26. (DEL CONTRATO). II.** Las condiciones generales del contrato deberán estar orientadas a garantizar:… 6. **La protección de los datos de las personas.**

> **Artículo 54. (DERECHOS DE LAS USUARIAS Y USUARIOS).** Las usuarias o los usuarios de los servicios de telecomunicaciones y tecnologías de información y comunicación tienen derecho a:… 9. Solicitar la exclusión, sin costo alguno, de las guías de usuarias o usuarios disponibles al público, ya sean impresas o electrónicas. Las usuarias o usuarios podrán decidir cuáles datos personales se incluyen, así como comprobarlos, corregirlos o suprimirlos. 17. Recibir protección del proveedor del servicio sobre los datos personales contra la publicidad no autorizada por la usuaria o usuario, en el marco de la Constitución Política del Estado y la presente Ley.

> **Artículo 56. (INVIOLABILIDAD Y SECRETO DE LAS COMUNICACIONES).** En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben

garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma.

Artículo 59. (OBLIGACIONES DE LOS OPERADORES Y PROVEEDORES). …**6.** Entregar en servicios de modalidad post-pago de forma oportuna, comprensible y veraz, la factura mensual desglosada de todos los cargos y servicios del cual es proveedor, en la forma y por el medio en que se garantice la privacidad de la usuaria o del usuario y facilitar los medios de pago por los servicios prestados, comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma.

…13. Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley.

Artículo 72. (ROL DEL ESTADO). I. El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales.

Artículo 84. (REGLAMENTACIÓN). El reglamento referido a firmas y certificados digitales comprenderá: …3. Las definiciones, principios y procedimientos relativos al tratamiento de los datos personales.

Artículo 89. (CORREO ELECTRÓNICO PERSONAL). A los efectos de esta Ley el correo electrónico personal se equipara a la correspondencia postal,

estando dentro del alcance de la inviolabilidad establecida en la Constitución Política del Estado. La protección del correo electrónico personal abarca su creación, transmisión, recepción y almacenamiento.

Artículo 90. (CORREO ELECTRÓNICO LABORAL). Cuando una cuenta de correo electrónico sea provista por la entidad empleadora al dependiente como medio de comunicación, en función de una relación laboral, se entenderá que la titularidad de la misma corresponde al empleador, independientemente del nombre de usuario y clave de acceso que sean necesarias para su uso, debiendo comunicarse expresamente las condiciones de uso y acceso del correo electrónico laboral a la empleada o empleado.

Artículo 91. (COMUNICACIONES COMERCIALES PUBLICITARIAS POR CORREO ELECTRÓNICO O MEDIOS ELECTRÓNICOS). Mediante reglamento se establecerán, las condiciones de las comunicaciones comerciales publicitarias realizadas por medio de correo electrónico o cualquier otro medio electrónico, sin perjuicio de la aplicación, en los casos que corresponda, de la normativa vigente en materia comercial sobre publicidad y protección a las usuarias o usuarios.

2.5.3.4. Decreto Supremo No. 1793,

El Reglamento a la Ley 164, Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación. Decreto Supremo 1793 de fecha 13 de noviembre de 2013, en protección de datos personales establece:

Artículo 3. (DEFINICIONES). Además de las definiciones técnicas establecidas en la Ley 164, para cumplimiento del presente Reglamento, se adoptan las siguientes definiciones: …IV. Respecto al tratamiento de los datos personales. a. Datos personales: A los fines del presente Reglamento, se entiende

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

ARTÍCULO 40.- (FUNCIONES DE LA AGENCIA DE REGISTRO). Las funciones de la Agencia de Registro son las siguientes:

a. La recepción de las solicitudes de emisión de certificados;

b. Comprobar la identidad y autenticación de los datos de los titulares de certificados;

c. Comprobar otros datos de los titulares de certificados que se presenten ante ella cuya verificación delegue la entidad certificadora

d. La remisión de las solicitudes aprobadas a la entidad certificadora con la que se encuentre operativamente vinculada;

e. La recepción y validación de las solicitudes de revocación de certificados; y su direccionamiento a la entidad certificadora con la que se vinculen;

f. La identificación y autenticación de los solicitantes de revocación de certificados;

g. El archivo y conservación de toda la documentación de respaldo del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por la entidad certificadora;

h. El cumplimiento de las normas y recaudos establecidos para la protección de los datos personales;

i. El cumplimiento de las disposiciones que establezca la política de certificación y el manual de procedimiento de la entidad certificadora con la que se encuentre vinculada.

ARTÍCULO 56.- (PROTECCIÓN DE DATOS PERSONALES). A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones: a. La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;

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

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

ARTÍCULO 57.- (COMUNICACIONES COMERCIALES PUBLICITARIAS). Las comunicaciones por medio de correo electrónico u otro medio de comunicación digital equivalente que tengan por finalidad la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, deberán cumplir las siguientes condiciones:

a. Deberán publicitar los servicios, caracterizando los mismos sobre la base de términos técnicos y de tecnología, incluyendo características técnicas,

económicas, comerciales, tarifas, aspectos legales, respecto de todos los servicios, así como los mecanismos de suscripción y conclusión de la suscripción a dicho tipo de servicios;

b. En los textos publicitarios que se refieran a los servicios, las condiciones y características, y promociones así como en la publicidad de acceso a contenido y aplicaciones digitales, deben utilizar redacciones de difusión que resalten las facilidades y bondades del servicio;

c. En caso de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, se deberá asegurar, además del cumplimiento de los requisitos establecidos en los incisos anteriores del presente Artículo, que sean claramente identificadas como tales y que las condiciones de acceso, y en su caso de participación, se expresen de forma clara e inequívoca, así como las autorizaciones de las autoridades competentes;

d. Deberá indicar la forma, como el destinatario puede aceptar o rechazar el envío de futuras comunicaciones del remitente, para que los usuarios puedan habilitarse o deshabilitarse en el caso de que no deseen continuar recibiendo estos mensajes o correos;

e. Deberán ser claramente identificables los remitentes y datos del mismo, indicando la persona natural o jurídica en nombre de la cual se realizan;

f. En la publicidad y acceso interactivo a los sitios web del proveedor a través de equipo terminal, el simple registro comercial de ingreso no conlleva a un enlace comercial del proveedor de difusión posterior, sino que ésta debe ser explícita y manifiestamente aceptada por suscripción;

g. Las ofertas de productos o servicios deberán proporcionar información clara, precisa y veraz concordante con sus prestaciones.

CAPITULO III
MARCO PRÁCTICO

3.1. Marco práctico

3.1.1. Análisis y diagnóstico de medidas de seguridad de información

3.1.1.1. Medidas de seguridad de información, en tratamiento de datos personales a nivel internacional

Como se mencionó en el punto 2.2.2.2 Protección de Datos y Seguridad de la Información, el Real Decreto 1720/2007 de 21 de diciembre de 2007 se diferencias del Reglamento (UE) 2016/679 en cuanto a medidas de seguridad aplicables a ficheros y tratamientos automatizados, se establecen niveles de seguridad en el tratamiento de datos de carácter personal. Establecen tres niveles: **Básicos** (todos los datos de carácter personal), **Medio** (infracciones administrativas, penales, tributarias, financieras, de seguridad social, personalidad) y **Alto** (ideología, afiliación sindicas, religión. Creencias, origen racial, salud o vida sexual, violencia de género). Como se aprecia en el Cuadro No. 3, de Principales Medidas de Seguridad de Información en Tratamiento de Datos Personales Las medidas de seguridad Reglamento (UE) 2016/679 se verifica que las medidas de seguridad de información, se aplican de manera acumulativa dependiendo del nivel de protección. Situación similar se repite en medidas de seguridad de información aplicable en ficheros (archivos físicos), Cuadro No. 4.

Cuadro No. 3

PRINCIPALES MEDIDAS DE SEGURIDAD DE INFORMACIÓN EN TRATAMIENTO DE DATOS PERSONALES.

REAL DECRETO 1720/2007	NIVEL DE PROTECCIÓN NIVEL BÁSICO	NIVEL DE PROTECCIÓN NIVEL MEDIO	NIVEL DE PROTECCIÓN NIVEL ALTO
▪ Funciones y obligaciones del personal	Art. 89	Art. 89	Art. 89
▪ Registro de incidencias	Art 90	Art. 90 Art. 100	Art. 90 Art. 100
▪ Controles de acceso		Art.99	Art.99
▪ Registro de Accesos			Art. 103
▪ Gestión de soportes y documentos		Art. 97	Art. 97
▪ Gestión de soportes y documentos	Art. 92	Art. 92	Art. 101
▪ Identificación y autenticación	Art. 93	Art. 93 Art. 98	Art. 93 Art. 98
▪ Copias de respaldo y recuperación	Art. 94	Art. 94	Art. 102
▪ Responsable de seguridad		Art. 95	Art. 95
▪ Auditoría		Art.96	Art.96
▪ Telecomunicaciones			Art. 104

FUENTE: Elaboración propia, extraído del Real Decreto 1720/2007

El tratamiento de custodia física, también es contemplado con medidas de seguridad concreta para ficheros no automatizados en el Decreto Real, en su Capítulo IV, en lo relativo a:

Cuadro No. 4

PRINCIPALES MEDIDAS DE SEGURIDAD DE INFORMACIÓN APLICABLES A LOS FICHEROS Y TRATAMIENTOS NO AUTORIZADOS (TRATAMIENTO DE CUSTODIA FÍSICA)

REAL DECRETO 1720/2007	NIVEL DE PROTECCIÓN NIVEL BÁSICO	NIVEL DE PROTECCIÓN NIVEL MEDIO	NIVEL DE PROTECCIÓN NIVEL ALTO
▪ Criterios de archivo y de almacenamiento de la información	Art. 106		Art. 111
▪ Dispositivos de almacenamiento	Art. 107		
▪ Custodia de los soportes	Art. 108		
▪ Responsable de seguridad		Art. 109	
▪ Auditoría		Art. 110	
▪ Copia o reproducción			Art. 112
▪ Acceso a la documentación			Art. 113
▪ Traslado de documentación			Art. 114

FUENTE: Elaboración propia, extraído del Real Decreto 1720/2007

Como se observa en el Real Decreto 1720/2007, se tiene una norma que en aspectos seguridad de la Información, considera todas las áreas que se deben tomar en cuenta para garantizar una adecuada seguridad de la información.

El reglamento de la Unión Europea 2016/679, reconoce la ISO 27001 que es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. Está redactada por los mejores especialistas del mundo en el tema y proporciona una

metodología para implementar la gestión de la seguridad de la información en una organización[34].

Se enfoca en que las empresas establezcan un sistema de gestión de seguridad de la información. Requiere controles para controlar la información en general (contempla la ISO 9000 en lo referido al apartado de comunicación y la ISO 25.000 administración control y calidad), Proyecta como te aseguras de que esa información: sea conservada, sea preservada, y se de a conocer a quien debe conocer esa información. El Alcance, lo definen las empresas en base a sus necesidades de las áreas organizacionales. El sistema y protocolo, los beneficios depende de la relevancia de cada organización (información persé, administrar correctamente la información que generas). Hay que evitar que la información sea pública, o sea realizar las acciones para proteger la información. Esta hecha para cualquier industria (cuidar información física y digital). Analiza la información y establece el procedimiento (protocolos).

En los requerimientos, primero se realiza el análisis de información, se ve que todo cambio este apoyado por las gerencias, las áreas deben clasificar que información es confidencial y que es públicas, el liderazgo es importante, debe haber una planeación. Toda la información es restringida, los controles son diferentes. Es importante ver cómo se va implantar y como se va clasificar. El otro tema es el soporte, inversión en la clasificación (servidores, etc), la operativa que se va controlar. Como todo sistema tiene una evaluación de desempeño (como mejora) análisis a dónde quieres llegar (todo esfuerzo requiere gasto).

ISO/IEC 27001 se divide en 11 secciones más el anexo A; las secciones 0 a 3 son introductorias (y no son obligatorias para la implementación), mientras que las

[34] Vease: https://advisera.com/27001academy/es/que-es-iso-27001/

secciones 4 a 10 son obligatorias, lo que implica que una organización debe implementar todos sus requerimientos si quiere cumplir con la norma. Los controles del Anexo A deben implementarse sólo si se determina que corresponden en la Declaración de aplicabilidad.

De acuerdo con el Anexo SL de las Directivas ISO/IEC de la Organización Internacional para la Normalización, los títulos de las secciones de ISO 27001 son los mismos que en ISO 22301:2012, en la nueva ISO 9001:2015 y en otras normas de gestión, lo que permite integrar más fácilmente estas normas.

Sección 0 – Introducción – explica el objetivo de ISO 27001 y su compatibilidad con otras normas de gestión.

Sección 1 – Alcance – explica que esta norma es aplicable a cualquier tipo de organización.

Sección 2 – Referencias normativas – hace referencia a la norma ISO/IEC 27000 como estándar en el que se proporcionan términos y definiciones.

Sección 3 – Términos y definiciones – de nuevo, hacen referencia a la norma ISO/IEC 27000.

Sección 4 – Contexto de la organización – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para comprender cuestiones externas e internas, también define las partes interesadas, sus requisitos y el alcance del SGSI.

Sección 5 – Liderazgo – esta sección es parte de la fase de Planificación del ciclo PDCA y define las responsabilidades de la dirección, el establecimiento de roles y responsabilidades y el contenido de la política de alto nivel sobre seguridad de la información.

Sección 6 – Planificación – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos para la evaluación de riesgos, el tratamiento de riesgos, la Declaración de aplicabilidad, el plan de tratamiento de riesgos y la determinación de los objetivos de seguridad de la información.

Sección 7 – Apoyo – esta sección es parte de la fase de Planificación del ciclo PDCA y define los requerimientos sobre disponibilidad de recursos, competencias, concienciación, comunicación y control de documentos y registros.

Sección 8 – Funcionamiento – esta sección es parte de la fase de Planificación del ciclo PDCA y define la implementación de la evaluación y el tratamiento de riesgos, como también los controles y demás procesos necesarios para cumplir los objetivos de seguridad de la información.

Sección 9 – Evaluación del desempeño – esta sección forma parte de la fase de Revisión del ciclo PDCA y define los requerimientos para monitoreo, medición, análisis, evaluación, auditoría interna y revisión por parte de la dirección.

Sección 10 – Mejora – esta sección forma parte de la fase de Mejora del ciclo PDCA y define los requerimientos para el tratamiento de no conformidades, correcciones, medidas correctivas y mejora continua.

Annexo A – este anexo proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones (secciones A.5 a A.18).

Para implementar la norma ISO 27001 en una empresa, se tiene que seguir estos 16 pasos:

1) Obtener el apoyo de la dirección.
2) Utilizar una metodología para gestión de proyectos
3) Definir el alcance del SGSI.
4) Redactar una política de alto nivel sobre seguridad de la información.
5) Definir la metodología de evaluación de riesgos.
6) Realizar la evaluación y el tratamiento de riesgos.
7) Redactar la Declaración de aplicabilidad,
8) Redactar el Plan de tratamiento de riesgos.
9) Definir la forma de medir la efectividad de sus controles y de su SGSI.

10) Implementar todos los controles y procedimientos necesarios.
11) Implementar programas de capacitación y concienciación.
12) Realizar todas las operaciones diarias establecidas en la documentación de su SGSI.
13) Monitorear y medir su SGSI.
14) Realizar la auditoría interna.
15) Realizar la revisión por parte de la dirección.
16) Implementar medidas correctivas.

ISO 27001 requiere que se confeccione la siguiente documentación:

- Alcance del SGSI (punto 4.3)
- Objetivos y política de seguridad de la información (puntos 5.2 y 6.2)
- Metodología de evaluación y tratamiento de riesgos (punto 6.1.2)
- Declaración de aplicabilidad (punto 6.1.3 d)
- Plan de tratamiento de riesgos (puntos 6.1.3 e y 6.2)
- Informe de evaluación de riesgos (punto 8.2)
- Definición de roles y responsabilidades de seguridad (puntos A.7.1.2 y A.13.2.4)
- Inventario de activos (punto A.8.1.1)
- Uso aceptable de los activos (punto A.8.1.3)
- Política de control de acceso (punto A.9.1.1)
- Procedimientos operativos para gestión de TI (punto A.12.1.1)
- Principios de ingeniería para sistema seguro (punto A.14.2.5)
- Política de seguridad para proveedores (punto A.15.1.1)

- Procedimiento para gestión de incidentes (punto A.16.1.5)
- Procedimientos para continuidad del negocio (punto A.17.1.2)
- Requisitos legales, normativos y contractuales (punto A.18.1.1)

Y estos son los registros obligatorios:

- Registros de capacitación, habilidades, experiencia y calificaciones (punto 7.2)
- Monitoreo y resultados de medición (punto 9.1)
- Programa de auditoría interna (punto 9.2)
- Resultados de auditorías internas (punto 9.2)
- Resultados de la revisión por parte de la dirección (punto 9.3)
- Resultados de medidas correctivas (punto 10.1)
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (puntos A.12.4.1 y A.12.4.3)

Por supuesto que una empresa puede decidir confeccionar otros documentos de seguridad adicionales si lo considera necesario.

3.1.1.2. Medidas de seguridad de información en tratamiento de datos personales en Bolivia

Ley General de Telecomunicaciones, Ley N° 164 de 28 de julio de 2011, en su Artículo 72, Parágrafo I señala textualmente, que: …"El Estado en todos sus niveles, fomentará el acceso, uso y apropiación social de las tecnologías de información y comunicación, el despliegue y uso de infraestructura, el desarrollo de contenidos y aplicaciones, la protección de las usuarias y usuarios, la seguridad informática y de redes, como mecanismos de democratización de oportunidades para

todos los sectores de la sociedad y especialmente para aquellos con menores ingresos y con necesidades especiales"...

Reglamento a la Ley Nª 164, Decreto Supremo N°1793 de fecha 13 de noviembre de 2013, en su artículo 3 (definiciones) en su acápite IV, define respecto al tratamiento de datos personales:

a. *Datos personales:* A los fines del presente Reglamento, se entiende como datos personales, a toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable;
b. *Autorización:* Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada;
c. *Tratamiento de los datos personales:* Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Así mismo en su acápite VI, define respecto a seguridad informática:

a. *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;

b. *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;
c. *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.

El artículo 4 (principios) en parágrafo II, Tratamiento de datos personales, establece: …"Los servicios de certificación digital en cuanto a tratamiento de datos personales se regirán por los siguientes principios: …d) Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravió, utilización y acceso no autorizado o fraudulento"...

Como se aprecia, este principio sólo se aplica para servicios de certificación digital. Este principio debía aplicarse para todas las acciones que implican tratamiento de datos personales.

El Articulo 8 (Plan de contingencia) menciona (textual): …"Las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad"…

Decreto Supremo 2514, de fecha 9 de septiembre de 2015, en su artículo 1 (objeto) establece: …"tiene por objeto: a) crear la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – EGETIC. b) Crear los Comités Interinstitucionales de Simplificación de Trámites"..,

El artículo 7 (funciones de la AGETIC) asigna a la AGETIC funciones y el inciso f) asigna la función: … "Establecerá los lineamientos técnicos en seguridad de información para las entidades del sector público".

En el Artículo 8 en su acápite primero establece: …"Se crea el Centro de Gestión de Incidentes Informáticos – CGII como parte de la estructura técnico operativa de la AGETIC", y el acápite II en su Inciso c) que menciona el CGII tiene

las siguiente funciones: …”b) “Establecer los lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público”…

Acápite III del Artículo 17, establece que: …“Las entidades del sector publico deberán desarrollar el Plan Institucional de Seguridad de la Información acorde a los lineamientos establecidos por el CGII”...

Acápite II del Artículo 18 señala que: …“Las entidades del sector público, en el marco de la Soberanía Tecnológica, deben designar un Responsable de Gobierno Electrónico y Tecnologías de Información y Comunicación y un Responsable de Seguridad Informática, encargados de coordinar con la AGETIC”…

3.1.1.3.Lineamientos para la elaboración de planes de seguridad de información de las entidades del sector público

El Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CTIC-EPB) y el Centro de Gestión de Incidentes Informáticos (CGII), en fecha 19 de septiembre de 2017, pone en vigencia los “Lineamientos para la elaboración de Planes de Seguridad de Información de las entidades del sector público”.

Los lineamientos, tienen como objetivo establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente.

El contenido deben ser asumidos por todas las entidades del sector público, sin perjuicio del trabajo desarrollado por aquellas que hayan asumido como parámetros rectores, normas y estándares nacionales e internacionales vigentes, o de otra naturaleza, en materia de seguridad de la información, siempre y cuando no sean

contrapuestas a los lineamientos establecidos. Señala que, las entidades o instituciones públicas que ya tengan implementado un Sistema de Gestión de Seguridad de la Información bajo normas nacionales o internacionales, podrán realizar un mapeo o cuadro de equivalencia para la verificación de concordancia con los presentes lineamientos.

El documento señala los siguientes controles de seguridad de la información:

- Seguridad de recursos humanos
- Gestión de activos de información
- Control de accesos
- Criptografía
- Seguridad física y ambiental.
- Seguridad de las operaciones
- Seguridad de las comunicaciones.
- Desarrollo, mantenimiento y adquisición de sistemas.
- Gestión de incidentes de seguridad de la información
- Plan de contingencias tecnológicas
- Cumplimiento

3.1.2. Atención Internacional en tratamiento de datos

Las respuestas normativas de los países e instituciones al tratamiento de datos personales se caracterizan, entre otras razones, por tener un enfoque internacional y ser armonizadas. Por eso, la recolección, el almacenamiento, el uso, la circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional en regulación con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia. En ese sentido, diferentes organizaciones internacionales, redes especializadas o grupos de autoridades han publicado documentos contentivos de las reglas que deben observarse en el tratamiento de datos personales, dentro de las cuales se encuentran varios principios

que evocan los grandes mensajes o propósitos que se deben materializar para lograr que los derechos de las personas no sean amenazados o vulnerados por la indebida recolección, almacenamiento, uso o circulación de dicha información.

A continuación en el **Cuadro No. 5** se resumen los principales documentos sobre tratamiento de datos personales emitidos por diferentes organizaciones.

Cuadro No. 5

PRINCIPALES ORGANIZACIONES INTERNACIONALES QUE HAN EMITIDO DOCUMENTOS SOBRE TRATAMIENTO DE DATOS PERSONALES.

Organización	Principales documentos
Red Iberoamericana de Protección de Datos (RIPD)	Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017)
Unión Europea (UE)	1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril del 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); 2. Protocolos adicionales al Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001 y 2018); 3. Carta de los Derechos Fundamentales de la Unión Europea (2000); 4. Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981)
Organización de Estados Americanos (OEA)	Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015)
Organización para la Cooperación y el Desarrollo Económicos (OCDE)	Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980)
Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (CIAPDP)	Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal – Resolución de Madrid– (2009)
Foro de Cooperación Económica Asia Pacífico (APEC)	Marco de privacidad APEC (2004) APEC Cross Border Privacy Rules (CBPR) APEC Cross Border Privacy Enforcement Arrangement (CPEA)
Organización de las Naciones Unidas (ONU)	Resolución 45/95 del 14 de diciembre de 1990. Principios rectores para la reglamentación de los ficheros computadorizados de datos personales

FUENTE: Guía GECTI para la implementación del principio de responsabilidad demostrada —*accountability*— en las transferencias internacionales de datos personales, Universidad Los Andes, Colombia 2018

3.1.2.1. Red Iberoamericana de Protección de Datos

La Red Iberoamericana de Protección de Datos (RIPD), surge con motivo del acuerdo alcanzado 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[35].

Esta iniciativa contó desde sus inicios con un apoyo político reflejado en la Declaración Final 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, conscientes del carácter de la protección de datos personales como Derecho Fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

En el XV Encuentro Iberoamericano de Protección de Datos, celebrado durante los días 20 a 22 de junio en Santiago de Chile, organizado por el Consejo para la Transparencia de Chile, junto con la Red Iberoamericana de Protección de Datos, se dieron por aprobados los Estándares Iberoamericanos de Protección de Datos. Los países de Andorra, Argentina, Chile, Colombia, Costa Rica, España, México, Perú, Portugal y Uruguay convinieron adoptar los presentes Estándares como máxima prioridad en la Comunidad Iberoamericana para que con el carácter de directrices orientadoras contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región de los países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes, favoreciendo la adopción de un marco regulatorio armonizado que ofrezca un nivel adecuado de protección de las personas físicas respecto al tratamiento de sus

[35] Vease: http://www.redipd.es/la_red/Historia/index-ides-idphp.php

datos personales y garantizando, a su vez, el desarrollo comercial y económico de la región.

Los Estándares son aplicables al tratamiento de datos personales, que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Se establece que el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

Así mismo establece los derechos del titular de los datos, los denominados Derechos ARCO, donde en todo momento el titular o su representante podrán solicitar al responsable, el Acceso, Rectificación, Cancelación, Oposición y portabilidad de los datos personales que le conciernen.

También establece el derecho a la portabilidad de los datos personales y el derecho a la limitación del tratamiento de los datos personales. El de portabilidad se entendido que, cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera. El de limitación entendido a que el titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable.

Así mismo se establecen las atribuciones y limitaciones del encargado, definidos en su alcance y formalización de la prestación de servicios. También se establece las reglas generales para la transferencia internacional de datos personales.

Un capítulo establece medidas proactivas en el tratamiento de datos personales donde se establece que la legislación nacional podrá reconocer y establecer medidas que promuevan el mejor cumplimiento de su legislación y coadyuven a fortalecer y elevar los controles de protección de datos personales implementados por el responsable. Se establece en el punto 38. Privacidad por diseño y privacidad por defecto:

“38.1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano "que le resulte aplicable.

38.2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, tratamiento de redes electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas”.

Enuncia la existencia de autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia. Establece que podrán ser órganos unipersonales o pluripersonales; actuarán con carácter imparcial e independiente en sus potestades, así

como serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna.

Por último establece un régimen de reclamaciones y sanciones, así como el derecho a la indemnización, como consecuencia de una violación de su derecho a la protección de datos personales. Y por último establece mecanismos de cooperación internacional.

Como se aprecia los Estándares Iberoamericanos de Protección de Datos no establecen medidas específicas de protección de datos pero reconoce que la legislación nacional podrá reconocer y establecer medidas en materia de tratamiento que promuevan el mejor cumplimiento de su legislación

3.1.2.2. Bolivia miembro de la Red Iberoamericana de Protección de Datos (RIPD)

En fecha 6 de abril de 2009 se suscribe Convenio de Cooperación CONV Nº 9/2009 con la Agencia Española de Cooperación Internacional para el Desarrollo – AECID, para la elaboración del Proyecto de Ley de Protección de Datos Personales en Bolivia. El proyecto no se puede concluir pese a los esfuerzos realizados en el 2009 de: enviar dos abogados de la ADSIB a una pasantía en la AEPD (Madrid) y haber contratado un especialista para iniciar el trabajo de elaboración del Proyecto de Ley (22 de junio de 2009).

En fecha 16/octubre/2009 se lleva a cabo el Seminario - Taller dirigido a las entidades del sector público boliviano. Participaron 35 entidades del sector público (Ministerios, Autoridades de Fiscalización y Control, ENTEL, SIN, Corte Nacional Electoral, Tribunal Constitucional, entre otras). Participa el Presidente del Consejo de

la Unidad Reguladora y de Control de Datos Personales de Uruguay, llegando a las siguientes conclusiones[36]:

- Desconocimiento de la Acción de Protección de Privacidad.
- No existe políticas de seguridad de la información en instituciones públicas.
- Necesidad de una Ley específica que regule la privacidad y protección de datos personales en Bolivia. Creación de una Autoridad de Control Independiente (control, fiscalización, sanción).
- Mayor difusión y socialización del tema en el sector público, privado, sociedad civil y ciudadanía.
- Mayor capacitación a los responsables del tratamiento de los datos personales en las entidades del sector público.

El proyecto no es concluido porque el inicio de trabajos estuvo dirigido por el Ministerio de Transparencia Institucional y Lucha Contra la Corrupción, que se tenía previsto que trabajaría en materia de Protección de Datos.

3.1.3. Diagnóstico de legislación en protección de datos personales

3.1.3.1. Análisis y diagnóstico internacional de avance en legislación

La legislación en cuanto al tratamiento de datos personales debido al avance tecnológico á tenido atención de gobiernos, reguladores y organizaciones. Fue poco reglamentado hasta finales del siglo pasado, pero en la última década se ha presentado una evolución a nivel mundial, con matices de estandarización regional. El avance más significativo regional se da en la Unión Europea, con el caso del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos

[36] *Vease: https://studylib.es/doc/4516176/la-accion-de-proteccion-de-privacidad-y-la*

datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Como se analizó en América Latina surge la iniciativa que es La Red Iberoamericana de Protección de Datos (RIPD).

Para PUCCINELLI, (1999) La protección de datos personales es un asunto de relevancia constitucional en el escenario latinoamericano[37]. Lo anterior se corrobora en un reporte realizado por Nelson Remolina Angarita, titulado *"Latin America and Protection of Personal Data: Facts and Figures (1985-2014)"*, en el cual se pone de presente el estado del arte de la regulación sobre datos personales en los siguientes veinte países de América La-tina: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Republica Dominicana, Uruguay y Venezuela.

En el reporte analiza las constituciones de estos países concluyendo lo siguiente:

- El 70% de los países latinoamericanos incorpora en su Constitución disposiciones explicitas referentes a aspectos relacionados con la protección de datos personales.
- El 100% de las disposiciones constitucionales consagra el derecho de acceso de la persona a conocer sus datos y el 92,85% menciona explícitamente el dato personal o la información personal.
- El 85,71% establece el derecho del titular del dato a solicitar la rectificación o la corrección de la información errónea, mientras que el 64,28% le confiere el derecho constitucional de solicitar la supresión, eliminación, destrucción o cancelación del dato.
- El 64,28% considera la actualización de la información un derecho del titular del dato personal.

[37] Cfr. Remolina, Nelson. Latin America and Protection of Personal Data: Facts and Figures (1985-2014) (March 20, 2014). Disponible en SSRN: https://ssrn.com/abstract=241209 o en http://dx.doi.org/10.2139/ssrn.241209. El texto fue inicialmente publicado por el Observatorio Ciro Angarita Barón sobre la protección de datos personales en Colombia.

– El 57,14% establece el *habeas data* y el 7,14% la acción de amparo y acción de protección de privacidad.
– El 50% consagra el derecho a conocer la finalidad del tratamiento de los datos y el 21,42% el derecho a saber el uso que se les está dando a estos.
– El 28,57% erige como derecho constitucional el exigir la confidencialidad sobre los datos personales.
– El 14,28% de las constituciones analizadas otorgan expresamente rango constitucional a la protección de los datos personales.
– Panamá (2004), Ecuador (2008) y México (2009) consagran explícitamente el derecho a la "protección" de la "información personal" y a la "protección de los datos personales".
– Republica dominicana (2010) es el único país que contiene un plexo de principios constitucionales (calidad, licitud, lealtad, seguridad y finalidad) que deben regir el tratamiento de datos personales.
– Las constituciones de Panamá y Ecuador exigen que los datos personales se recolecten con el consentimiento del titular del dato.

En cuanto a las leyes de los países del estudio, se concluyó que el 100% de ellos cuenta con normas sectoriales —sobre distintos temas, como historias clínicas y censos de la población y el 50% cuenta con normas generales.

3.1.3.2. Análisis y diagnóstico nacional de avance en legislación

En el caso de Bolivia, la Constitución Política del Estado del 2009 incorpora disposiciones de derecho a la intimidad y privacidad. La protección de datos personales no se encuentra explícita, sino que se encuentra como una Acción, referida a "conocer, objetar u obtener la eliminación o rectificación de los datos registrados…". En la CPE no se establece el Habeas Data, pero sí la Acción de Protección a la Privacidad con procedimiento previsto para la acción de Amparo Constitucional. No establece ni se refiere al derecho a conocer la finalidad del

tratamiento de datos, ni al uso que se le está dando. Tampoco hace referencia al derecho de exigir la confidencialidad de datos personales. En síntesis no se le da rango constitucional a la protección de datos personales.

La Ley de Telecomunicaciones establece la Protección de datos personales, regulando en este aspecto a operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación. El Reglamento de la Ley de Telecomunicaciones (Decreto Supremo 1793), norma el tratamiento de datos personales (recolección, almacenamiento, uso, circulación o supresión), autorización (consentimiento) de los usuarios para el tratamiento. Establece también las funciones de las Agencias de Registro y el tratamiento de datos personales en el sector público y privado en todas las actividades.

Los principios que establece en el artículo 4, acápite II Tratamiento de datos que se aplican para certificación digital son:

a. *Finalidad:* La utilización y tratamiento de los datos personales por parte de las entidades certificadoras autorizadas, deben obedecer a un propósito legítimo, el cual debe ser de conocimiento previo del titular;
b. *Veracidad:* La información sujeta a tratamiento debe ser veraz, completa, precisa, actualizada, verificable, inteligible, prohibiéndose el tratamiento de datos incompletos o que induzcan a errores;
c. *Transparencia:* Se debe garantizar el derecho del titular a obtener de la entidad certificadora autorizada, en cualquier momento y sin impedimento, información relacionada de la existencia de los datos que le conciernan;
d. *Seguridad:* Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravío, utilización y acceso no autorizado o fraudulento;

e. *Confidencialidad***:** Todas las personas involucradas y que intervengan en el tratamiento de datos personales, están obligadas a garantizar la reserva de la información, incluso hasta después de finalizado su vínculo con alguna de las actividades que comprende el tratamiento, pudiendo únicamente realizar el suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las tareas autorizadas.

Específicamente el artículo 56 de protección de datos personales establece: "A fin de garantizar los datos personales y la seguridad informática de los mismos, se adoptan las siguientes previsiones:

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

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

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

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

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

En el análisis normativo, se puede deducir que las medidas de seguridad de la información a ser adoptadas para el manejo de datos personales que permiten la protección en su tratamiento y en el derecho a la intimidad y privacidad en la actual regulación en Bolivia, es una decisión que recae en el responsable del tratamiento de datos personales, pudiendo ser este público o privado

3.1.3.3. Análisis de la protección de datos en los registros públicos

En cuanto a manejo de datos personales públicos existen dos entidades que manejan datos personales y que otorgan documentos de nacionalidad, ciudadanía, como instituciones de otorgar documentos que contienen datos primarios y son el SERECI y el SEGIP.

3.1.3.3.1. Servicio de Registro Cívico - SERECI

El artículo 208 de la Constitución Política del Estado, parágrafo III establece que: ”Es función del Tribunal Supremo Electoral organizar y administrar el Registro Civil y el Padrón Electoral”.

La Ley 018, Ley del Órgano Electoral Plurinacional (OEP) de fecha 16-jun-10, en el inc. 13 del Artículos 6 (Competencias) estable que la OEP tiene las siguientes competencias: "…Organización y administración del Servicio de Registro Cívico (SERECÍ)."

Así mismo el artículo 70 (Creación) establece: "…I. Se crea el Servicio de Registro Cívico (SERECÍ) como entidad pública bajo dependencia del Tribunal Supremo Electoral, para la organización y administración del registro de las personas naturales, en cuanto a nombres y apellidos, su estado civil, filiación, nacimiento, hechos vitales y defunción, así como el registro de electores y electoras, para el ejercicio de los derechos civiles y políticos."

El artículo 71 (Funciones) establece que el SERECI: "…tiene las siguientes funciones:

1. Establecer un sistema de registro biométrico de las personas naturales que garantice la confiabilidad, autenticidad y actualidad de los datos.
2. Registrar los nacimientos, matrimonios, divorcios, defunciones, reconocimientos y nacionalidad de las personas naturales.
3. Expedir certificados de nacimiento, matrimonio y defunción.
4. Registrar el domicilio de las personas y sus modificaciones.
5. Registrar la naturalización o adquisición de nacionalidad de las personas naturales.
6. Registrar la suspensión y la rehabilitación de ciudadanía.
7. Registrar en el Padrón Electoral a las bolivianas y bolivianos, por nacimiento o por naturalización, mayores de 18 años.
8. Registrar a las ciudadanas y ciudadanos extranjeros que tengan residencia legal en Bolivia y que cumplan las previsiones legales para el ejercicio del voto en elecciones municipales.
9. Rectificar, cambiar o complementar los datos asentados en el Registro Civil, mediante trámite administrativo gratuito.

10. Atender solicitudes fundamentadas de verificación de datos del Registro Civil y el Padrón Electoral requeridas por el Órgano Judicial o el Ministerio Público.
11. Conocer y decidir las controversias suscitadas con motivo de la inclusión, modificación y actualización de datos en el Registro Civil y Electoral.
12. Actualizar el Registro Electoral y elaborar el Padrón Electoral para cada proceso electoral, referendo o revocatoria de mandato a nivel nacional, departamental, regional y municipal.
13. Elaborar, a partir del Padrón Electoral, la lista de personas habilitadas para votar y la lista de personas inhabilitadas, para cada proceso electoral, referendo o revocatoria de mandato a nivel nacional, departamental, regional y municipal.
14. Conocer y resolver reclamaciones de los ciudadanos incluidos en la lista de personas inhabilitadas del Padrón Electoral.
15. Dictar resoluciones administrativas para la implementación y funcionamiento del Registro Cívico.
16. Otras establecidas en la Ley y su reglamentación correspondiente.

En cuanto a tratamiento de datos personales establece en su artículo 71 (Obligaciones) que: " tiene las siguientes obligaciones:

2. Respeto irrestricto del derecho a la intimidad e identidad de las personas y los demás derechos derivados de su registro.
3. Garantizar la privacidad y confidencialidad de los datos registrados de las personas.
4. Velar por la seguridad e integridad de la totalidad de la información registrada."

3.1.3.3.2. Servicio de Identidad Personal - SEGIP

La Constitución Política del Estado, en su artículo 14, determina que: "… todo ser humano tiene personalidad y capacidad jurídica con arreglo a las leyes y goza de

los derechos reconocidos por esta constitución, sin discriminación. Asimismo, las extranjeras y los extranjeros en el territorio boliviano tienen derechos y deben cumplir los deberes establecidos en la Constitución, salvo las restricciones que ésta contenga". Así mismo, el artículo 24, establece que: "… toda persona tiene derecho a la petición de manera individual o colectiva, sea oral o escrita, y a la obtención de respuesta formal y pronta. Para el ejercicio de este derecho no se exigirá más requisito que la identificación del peticionario".

Es en este marco constitucional que se establece la necesidad de la personalidad y capacidad jurídica, así como la necesidad de la identificación de las personas.

Al respecto la "Ley 145; Ley del Servicio General de Identificación Personal y Ley de Servicio General de Licencias para Conducir", de fecha 27-jun-2011 establece en su artículo 1 (objeto): "…La presente Ley tiene por objeto la creación del Servicio General de Identificación Personal y del Servicio General de Licencias para Conducir, determinando su naturaleza jurídica, principios, atribuciones y estructura organizacional".

Su artículo 2 (Creación y Naturaleza Jurídica) en su acápite I que:"…El Servicio General de Identificación Personal – SEGIP, es la única entidad pública facultada para otorgar la Cédula de Identidad – C.I., dentro y fuera del territorio nacional, crear, administrar, controlar, mantener y precautelar el Registro Único de Identificación – RUI, de las personas naturales a efecto de su Identificación y ejercicio de sus derechos en el marco de la presente Ley y la Constitución Política del Estado..",

En el **Artículo 4. (PRINCIPIOS DE LA ENTIDAD),** establece principios bajo los cuales el SEGIP, sujetará su acción en base a los siguientes principios: de

Universalidad, Confidencialidad, Unicidad, Seguridad, Calidez, Celeridad, Eficiencia, Transparencia, Obligatoriedad y Respeto a la dignidad.

De estos principios dos se refieren a la seguridad de la información que son Confidencialidad y Seguridad definiéndose en la Ley lo siguiente:

> 2. **Confidencialidad.** Es el respeto y resguardo riguroso sobre la administración y control de la información proporcionada por las bolivianas y los bolivianos, las y los extranjeros radicados en Bolivia**.**
>
> 4. **Seguridad.** Se garantiza la inviolabilidad de la identidad de las bolivianas y los bolivianos mediante mecanismos adecuados, oportunos y confiables.

Dentro de las atribuciones del SEGIP, también se establecen algunas que están referidas a la seguridad de datos personales, textual el **Artículo 5.** (ATRIBUCIONES), establece: …" El Servicio General de Identificación Personal – SEGIP, tiene las siguientes atribuciones:

a) Establecer los procedimientos para el manejo, administración y registro de los datos de identificación correspondientes a las bolivianas, los bolivianos y extranjeros radicados en Bolivia.
b) Establecer en coordinación con el Servicio de Registro Cívico – SERECI, un sistema de registro biométrico de las personas naturales que garantice la confiabilidad y autenticidad de los datos registrados de forma permanente.
c) Regular el uso, actualización, administración y almacenamiento del Registro Único de Identificación – RUI.
d) Implementar mecanismos y/o procedimientos que garanticen la privacidad, confidencialidad y seguridad de los datos registrados.

e) Registrar la información necesaria para otorgar la Cédula de Identidad – C.I., a las bolivianas, los bolivianos y extranjeros naturalizados, cumpliendo parámetros técnicos internacionales.
f) Registrar la información necesaria para otorgar la Cédula de Identidad de Extranjero – CIE, para extranjeros con residencia legal en Bolivia, en coordinación con la Dirección General de Migración, cumpliendo parámetros técnicos internacionales.
g) Rectificar, cambiar o complementar los datos asentados en el Registro Único de Identificación – RUI.
h) Promover, gestionar y suscribir Convenios con instituciones y entidades para el cumplimiento de sus atribuciones".
i) Mantener y administrar el Registro Único de Identificación – RUI, bajo parámetros de actualidad tecnológica.
j) Desarrollar los mecanismos para el registro domiciliario de las personas en todo el territorio del Estado Plurinacional de Bolivia.

En cuanto a medidas de seguridad el artículo 20 textual establece: **…"**Las medidas de seguridad, modalidad de otorgamiento, estructura y tiempo de vigencia de la Cédula de Identidad – C.I., serán establecidos mediante Decreto Supremo Reglamentario"

A la fecha el SEGIP no ha logrado gestionar un Decreto Supremo que establezca medidas de seguridad y se enmarca en el Decreto Supremo 39294[38] de fecha 03 de Octubre de 2007, que solamente establece las características de: Especificaciones Técnicas del formato la Cédula Identidad Personal, pero en cuanto a medidas de seguridad no se cuenta con el Decreto Supremo.

[38] Gaceta Oficiall

3.1.4. Aplicación del derecho a la privacidad y protección de datos personales en los registros públicos y seguridad de la información.

Con el objetivo de evidenciar que en el tratamiento se protegen de datos personales en lo referido al derecho a la privacidad es que se ha realizado entrevistas a expertos constitucionalistas en lo referido a la aplicación desde el marco legal y otro respecto a especialistas en seguridad de la información en cuanto a la aplicación.

3.1.4.1. Entrevista a constitucionalista Fernando Escobar Pacheco

1. **Breve biografía del entrevistado (datos generales y experiencia derecho constitucional, derechos humanos y derecho informático).**

Fernando Escobar Pacheco, Abogado desde 2005, con 10 años de experiencia en materia constitucional, Maestría en Derecho Internacional y Comparado en l Universidad de Lausanne en Suiza. Actualmente cursando un doctorado en Derecho en esa Universidad.

2. **¿Cree que es necesario la existencia de una norma específica (Ley, Decreto Supremo) de protección de datos personales? Explique sus fundamentos.**

Si, ya que n Bolivia no existe una Ley específica sobre protección de datos personales, como en otros países (Costa Rica, Colombia, Ecuador, Perú etc.); asimismo, aún no existen pronunciamientos específicos de los Tribunales de Justicia en Bolivia (Tribunal Constitucional y Tribunal Supremo de Justicia) que hayan desarrollado ampliamente aspectos relativos a la protección de datos personales; sin embargo, se deben considerar disposiciones de orden constitucional y legal, así como jurisprudencia constitucional general, que pueden delinear cual debería ser el contenido de una legislación en la materia;

El Art. 21. 2 de la Constitución Política del Estado, establece que todas las personas tienen los siguientes derechos: a la privacidad, intimidad, honra, honor, propia imagen y dignidad; estos derechos no son absolutos y pueden ser objeto de limitaciones, como el uso de datos personales en circunstancias específicas.

Por ejemplo en materia de los datos que genera un trabajador en su lugar de trabajo el art. 90 de la Ley General de telecomunicaciones, tecnologías de información y comunicación, establece que el correo electrónico laboral pertenece al empleador, y que las condiciones de uso y acceso deben ser comunicados al trabajador; esto es una limitación al derecho a la privacidad, aspectos de este estilo deben ser establecidos con claridad en una norma legal, considerando además que conforme al mandato del art. 109.II de la CPE solo una Ley puede limitar derechos fundamentales.

3. **¿Cree que es necesario la existencia de una entidad específica encargada de protección de datos personales? Explique los fundamentos.**

En la creación de esta Ley se debe crear una entidad específica y especializada que tenga un conocimiento técnico.

4. **La ausencia de una norma específica de protección de datos personales es un obstáculo para el ejercicio del Habeas Data o Acción de Protección de Privacidad.**

No, porque como garantía jurisdiccional prevista por la Constitución y el Código Procesal Constitucional no necesita de ninguna norma que regule su ejercicio. Sin embargo en términos sustantivos es necesario una norma que ayude a establecer cómo debe enfrentarse en términos de una política pública la protección de datos personales.

5. **¿Existen accionantes que al ser afectado su derecho a la privacidad, accionan la Acción de Protección de Privacidad o erróneamente accionan la Acción de Amparo Constitucional? De ser así cual es la razón de este desvío.**

En la jurisprudencia constitucional existe un muy bajo índice de acciones de protección de privacidad en las que se ha concedido la tutela. Señalo este aspecto porque es un indicador que nos permite mostrar que la naturaleza jurídica de esta acción constitucional no ha sido bien entendida por el mundo litigante, y por esa razón también se acude erróneamente a la acción de amparo constitucional, olvidando que esta acción constitucional es subsidiaria incluso en relación a otras acciones constitucionales, como el caso de la Acción de Protección de Privacidad.

6. **¿Cómo se puede asegurar la protección de datos personales en su tratamiento y el derecho a la intimidad y privacidad?**

Se deben considerar los siguientes aspectos:

1) La administración, acceso y control de la información deben estar limitados a propósitos estrictamente necesarios desde el punto de vista razonable, evitando cualquier tipo de intromisión en la esfera privada de la persona;

2) La persona debe brindar su consentimiento expreso y autorizar labores de administración, acceso y control de la información que produce. Uno uso de datos por más proporcional que sea que no esté consentido por la persona implica un menoscabo de su derecho a la privacidad (Ejemplo Sentencia Constitucional del Tribunal Constitucional de España 0029/2013).

7. Que principios y que aspectos debería contemplar la norma específica (Ley, Decreto Supremo) de protección de datos personales

Los principios que debe contemplar la nueva legislación, y recogiendo el último desarrollo legislativo a nivel comparado en la materia (REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)

Son el de legalidad del tratamiento y de consentimiento informado.

En efecto, consdieramos pertinente rescatar el Artículo 5 de la norma Europea mencionada, el mismo que señala:

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto

en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

8. **Favor proporcionar jurisprudencia (TCP o TSJ).**

SCP 1300/2012, 2175/2012, 0440/2016-S3, **0819/2015-S3 entre otras**

3.1.4.2. Entrevista a constitucionalista José Rodolfo Sáenz Paz

1. **Breve biografía del entrevistado (datos generales y experiencia derecho constitucional, derechos humanos y derecho informático).**

José Rodolfo Sáenz Paz, Abogado desde 2001, con 10 años de experiencia en materia constitucional, Maestría en Derecho Internacional y Justicia Constitucional en la Universidad Andina Simón Bolívar, con diplomados en Derecho Constitucional, Argumentación Jurídica, Educación Superior Maestría de Derecho Corporativo. Fue Secretario General del Tribunal Constitucional Plurinacional (2012) y Letrado de Coordinación Jurisprudencial, Letrado de la Sala Tercera. Actualmente Letrado de la Comisión de Admisión.

2. **¿Cree que es necesario la existencia de una norma específica (Ley, Decreto Supremo) de protección de datos personales? Explique sus fundamentos.**

Para contextualizar la respuesta se debe convenir que los datos personales están referidos a la información de una persona, que permite su identificación, el lugar de nacimiento, estado civil, edad, lugar, domicilio, trayectoria académica, laboral, o profesional, su estado de salud, sus características físicas, su autoidenficiación, dentro de la sociedad, su estado financiero, registro de antecedentes penales, su estado civil, sus bienes, etc.. Bajo ese marco, es necesario la respuesta a la pregunta es afirmativa, es necesaria la existencia de una norma específica que regule la protección de los datos personales, a objeto de vulnerar los derechos y garantías establecido en la Constitución, tales como, la privacidad, intimidad, honra, honor, propia imagen y dignidad .

Debe convenirse también que el solo registro de los datos personales, persé no vulnera ningún derecho, pero que estos pueden ser desconocidos, cuando la información personal registrada pueda ser mal utilizada, en perjuicio de los derechos de las personas en sus actividades públicas, privadas, comerciales, laborales, políticas, etc, por lo que a este fin si es necesaria un regulación, que establezca la finalidad con la cual se registra la información y los límites para divulgarlas, estableciendo sanciones punitivas o económicas ante su desconocimiento.

La regulación necesariamente debe ser realizada a través de una ley del nivel central del Estado, en observancia de la reserva de ley.

3. **¿Cree que es necesario la existencia de una entidad específica encargada**

de protección de datos personales? Explique los fundamentos.

No porque son varias las instituciones que manejan la información personal, el Registro Civico para el Estado Civil, el Registro de Derechos Reales para los bienes inmuebles, los Gobiernos Municipales en registro de bienes muebles vehículos, la Autoridad Supervisión Financiera sobre datos financieros, las Cajas de Salud o los Servicios de Salud, sobre registros de salud, el Órgano Electoral sobre la actividad política, Impuestos, aduana, etc; en fin determinadas entidades encargadas del registro de datos personales, que no podrían ser reunidas en una sola entidad, y por ello no seria posible una sola entidad de registro, por ello tampoco una única enitidad encargada de los datos personales.

4. **La ausencia de una norma específica de protección de datos personales es un obstáculo para el ejercicio del Habeas Data o Acción de Protección de Privacidad.**

La jurisprudencia del Tribunal en acciones habeas data actualmente acción de protección de privacidad, no muestra que la protección de los datos personales, no haya sido materializada por el vacío normativo de una norma específica de protección de datos personales, en los caso en que se concedió la tutela, fue la aplicación inmediata y directa de los postulados establecidos en el art. 109 de la Constitución.

5. **¿Existen accionantes que al ser afectado su derecho a la privacidad, accionan la Acción de Protección de Privacidad o erróneamente accionan la Acción de Amparo Constitucional? De ser así cual es la razón de este desvío.**

La Constitución Política del Estado y el Código Procesal Constitucional, delimitan el ámbito de protección de todas las acciones de tutela, en lo particular la Acción de Amparo Constitucional, y la acción de protección de privacidad si bien ambas protegen derechos subjetivos, esta última está destinada exclusivamente a la protección de los derechos a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, siendo entonces excluyente la protección de estos derechos por la acción de amparo constitucional u otra acción de tutela. Considero que la razón del desvió es un incorrecto análisis por parte de los abogados de las problemáticas que se le presentan y no se debe a un vacío jurídico o la existencia de ambigüedad o vaguedad en la norma que regula estas acciones.

6. **¿Cómo se puede asegurar la protección de datos personales en su tratamiento y el derecho a la intimidad y privacidad?**

Para asegurar la protección de los datos personales y su tratamiento, se requiere una norma legal de carácter formal que establezca los límites respecto a la difusión de dichos registro estableciendo también las sanciones y la forma en que

debe ser reparada la lesión.

7. Que principios y que aspectos debería contemplar la norma específica (Ley, Decreto Supremo) de protección de datos personales

La norma que regule la protección de datos personales, debe ser una Ley de carácter formal, en observancia del principio de reserva de ley establecido en el art. 109 de la CPE., los principios establecidos en la Constitución, en el art. 8, además de los derechos y garantías que tiene aquella dimisión de además estar catalogados como derechos son también principios.

8. Favor proporcionar jurisprudencia (TCP o TSJ).

Sentencias Tribunal Constitucional Plurinacional
1084/2016-S3
El peticionante de tutela, debe demostrar la urgencia en la protección o el estado de indefensión; no advirtiéndose la urgente necesidad de protección ni mucho menos el estado de indefensión.
…no corresponde analizar la supuesta vulneración del derecho al trabajo, por ser que rebasa el ámbito de defensa que ofrece la acción de protección de privacidad;
0192/2015-S2
Jurisprudencia precedencial reiteradora
0080/2014-S2
Protección a la privacidad, por cuanto el acto lesivo denunciado no se encuentra dentro del ámbito de protección de esta acción de defensa, como es, establecer la ilegalidad en la obtención y entrega para su ulterior publicación en un medio televisivo, de imágenes grabadas en la cámara de vigilancia de un Hotel ….
0332/2015-S1
Protección de privacidad no es posible conocer y corregir la información y aseveraciones contenidas dentro de expedientes o cuadernos de investigación que presuntamente afectaren la dignidad y privacidad de las personas, debido a que las resoluciones judiciales no constituyen bancos de datos de registro de información. Deniega la acción de Libertad.
0090/2014-S1; 0851/2013-L; 2175/2012; 1300/2012; 0239/2013-L; 0428/2016-S2; 0089/2014-S2; 1010/2015-S2; 1445/2013; 1292/2015-S3

3.1.4.3. Entrevista a Director Nacional Jurídico del SEGIP, dr. Javier Antonio Caballero Romero

1. **Breve biografía del entrevistado (datos generales y experiencia en saneamiento).**

   Abogado Javier Antonio Caballero Romero, Diplomado en Ciencias Penales UMSA-Universidad de La Habana, Diplomado en Gestión Pública Intercultural.

   Desde el año 2016 Director Nacional Jurídico del SEGIP; entre sus funciones se encuentra el de saneamiento. A la fecha se encuentra en plena implementación el Gabinete Jurídico Virtual, instrumento normativo que permite reglamentar la atribuciones, funciones y procedimiento del saneamiento y modificación de datos de identificación personal a distancia en aplicación a la normativa vigente del Servicio General de Identificación Personal.

   OTRAS ENTIDADES

   Ha prestado sus servicios profesionales en otras entidades públicas: Ministerio de Finanzas (hoy Ministerio de Economía y Finanzas Públicas), Instituto Nacional de Estadística, Servicio de Impuestos Nacionales, Superintendencia de Pensiones, Valores y Seguros, Autoridad de Fiscalización y Control Social de Pensiones (AP), Autoridad de Pensiones y Seguros (APS) como Director Legal

2. **¿El tratamiento de datos personales y medidas de seguridad de información se encuentra reguladas por alguna norma (Ley, ¿Decreto, etc)? Explicar y detallar la normativa existente.**

   La Ley N°145 e 27 de junio de 2011 define el respeto y resguardo riguroso sobre la administración y control de la información proporcionada por las bolivianas y los bolivianos, las y los extranjeros radicados en Bolivia a facultado para tal fin ha ordenado al SEGIP implementar mecanismos y/o procedimientos que garanticen la privacidad, confidencialidad y seguridad de los datos registrados, en tal sentido a facultado a la MAE del SEGIP para implementar mecanismos para el desarrollo, uso y explotación de tecnologías de información y comunicación.

   El SEGIP cuenta con un Data CENTER bajo responsabilidad de la Dirección Nacional de Tecnologías de la Información y Comunicación en la que la

Unidad de Base de Datos y la Unidad de Seguridad de la Información coordinan el resguardo de los datos con la Dirección Nacional Jurídica. Estas instalaciones se definieron bajo referencia de normas internacionales y gozan de medios de seguridad y vigilancia para proteger el Sistema de Registro Único de Identificación creado por la Ley 145, por tanto, la Entidad cuenta con Políticas de Seguridad, Planes de contingencia y procedimientos para la protección de la Información que administra la Entidad.

Para el nexo interinstitucional se ha desarrollado el Sistema de Convenio Interinstitucional, que cumple los fines que la Ley 145 de 11 de junio de 2011 define; este instrumento tiene rangos altos de seguridad con las características señaladas supra, otorgando verificación y validación de datos de identidad mediante ocho Tipos de Consulta posibles de enlazarse por aplicación web y algunos casos por servicio web. Estos, se confían según el nivel de acceso de seguridad y las atribuciones otorgadas por ley para acceder a la verificación de un dato personal.

Los Servidores Públicos que reciben usuarios de acceso a datos personales deben suscribir contratos y compromisos de confidencialidad. Son capacitados e inducidos con manuales de uso en los que se describe las normas de seguridad de la información y los criterios de búsqueda fundamentada.

Cada usuario cuenta con bitácoras o registros de consulta, estos reportes cuentan con logs que evidencian horario y fecha de consulta relacionada al usuario. Esta información o registros permiten a las áreas Jurídicas y de seguridad de la información, definir puntos de control y seguimiento que garanticen que cada consulta tiene un respaldo administrativo que demuestra el resguardo riguroso a la confidencialidad y por tanto el cumplimiento de la ley.

Por otra parte, el Reglamento a la Ley Nº 164, de 8 de agosto de 2011, para el Desarrollo de Tecnologías de Información y Comunicación, 13 de noviembre de 2013 define la seguridad de la información y regula la protección de datos, siendo estos los pilares base de la norma para promoverse a todas las entidades, incluidas entidades como ADSIB AGETIC SERECI y EL SEGIP.

3. **¿Cree que es suficiente la normativa existente de seguridad de información y tratamiento de los datos personales, o es necesaria la creación de una norma específica? Favor sustentar su respuesta.**

Las normas subsistentes en el Marco de la Ley 145 y la Ley 164, se requiere de un instrumento legal que defina la Protección de los Datos en un marco procedimental más específico y que module la especificación técnica para el almacenamiento de datos.

Por lo que, aunque el marco normativo subsistente es importante y permite una buena administración, es importante contar con el instrumento normativo especifico que considere, asimismo, al SEGIP como ente rector y protector de datos personales en Bolivia, otorgándole autoridad para definir su regulación en otras entidades.

El caso de la facultad que se otorga al Directorio del SEGIP para el tratamiento de datos biométricos es un ejemplo de su viabilidad.

4. ¿**Se han presentado casos de Acción de Protección de Privacidad o Acción de Amparo Constitucional en contra su institución? Favor mencione los casos más relevantes y si dispone, mencione la cantidad y proporcione el detalle con Número de Expediente (Tribunal Constitucional Plurinacional) o Número de Auto Supremo (Tribunal Supremo de Justicia)**

   No se han presentado casos de Acción de Protección de Privacidad o Acción de Amparo Constitucional contra el Servicio General de Identificación Personal.

3.1.4.4. Entrevista al jefe nacional de seguridad de información del SEGIP. msc. Alberto Arnez,

1. **Breve biografía del entrevistado (datos generales y experiencia en manejo de seguridad de la información).**

   Msc. Alberto Arnez -Diplomado en Seguridad de la Información “Information Security Officer”

Cargos y funciones relativas a Seguridad de la Información:

Jefe Nacional de Seguridad de la Información -SEGIP

Responsable de la implementación y actualización de las Políticas de

Seguridad y del Plan de Contingencia de la Entidad.

Administrador del monitoreo y verificación del cumplimiento de procedimientos y normas internas en aspectos relacionados a la seguridad de la información.

Elaboración y propuesta de políticas directivas y normas internas de Seguridad Informática.

Otras Entidades y Empresas:

Responsable de la disponibilidad permanente de los recursos de información y comunicaciones y seguridad de éstos.

Implementar medidas de seguridad y de normas de tecnología en cumplimiento a normas, así como informes de auditoría.

2. **¿Qué medidas de seguridad de información aplican en tratamiento de los datos personales en la entidad que trabaja? Explique en detalle.**

Todos los funcionarios de la Entidad al ingresar a la Institución firman un acuerdo de confidencialidad donde se establecen tanto sus derechos como sus deberes en función a su información personal y la Información de la Entidad.

En la Entidad se cuenta con Políticas de Seguridad, Planes de contingencia y procedimientos para la protección de la Información que administra la Entidad.

3. **¿Cómo se puede asegurar la protección de datos personales en su tratamiento desde el soporte informático?**

La seguridad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: Se debe garantizar que la información sea accesible sólo a aquellas personas con autorización de acceso a la misma.

Integridad: Se debe conservar la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Se garantizará que los usuarios autorizados tengan acceso a la información cuando lo requieran.

En este marco, la protección de los datos personales se efectúa de las siguientes maneras:

- Comunicación interna y externa encriptada.
- Acceso Restringido a recursos y determinados usuarios.
- Registros de altas, bajas y modificaciones (logs)

4. **¿Cuenta con información de inconsistencias de datos de los ciudadanos? De ser así proporcione cifras.**

   NO se puede saber si un dato de un ciudadano es inconsistente hasta que el mismo procura una renovación o reposición de su cedula; por esta razón no se puede saber con exactitud si cualquier dato de un ciudadano presenta inconsistencias o no.

3.1.4.5. Entrevista a responsable del Sistema de Registro Civil del SERECI, Lic. Windsor Joaquin Quipildor.

1. **Breve biografía del entrevistado (datos generales y experiencia en manejo de seguridad de la información).**

   Datos Generales
   Nombre: Windsor Joaquin Saire Quipildor
   Profesión: Licenciado en Informática mención Ingeniería de Sistemas
   Cargo: Responsable del Sistema de Registro Civil
   Entidad: SERECI NACIONAL dependiente del Tribunal Supremo Electoral
   Cursos: El derecho a la identidad, registro civil y estadísticas vitales, Edición #9. ORGANIZACIÓN DE LOS ESTADOS AMERICANOS – OEA gestión 2017.

   Experiencia en manejo de seguridad de información
   2016-2018 Desempeño funciones en el cargo de Responsable del Sistema de Registro Civil Tribunal Supremo Electoral - SERECI Nacional. Donde se ha implementado la primera versión del servicio web para verificación biométrica 1 a 1, para sistemas internos del Tribunal Supremo Electoral, se ha desarrollado el componente para la captura de la imagen de huella dactilar de dispositivos biométricos que dispone el TSE, para su utilización en la verificación biométrica, para el Sistema de Registro Civil Biométrico y el sistema de Cambio de Domicilio, este desarrollo permite incrementar el nivel de seguridad de acceso a los datos del SERECÍ.

   2012 a 2015 Desempeñe funciones en el cargo de Base de Datos de Registro Civil Tribunal Supremo Electoral - SERECI Nacional. Donde se ha implementado el sistema de Registro de Cambio de Domicilio Biométrico aplicando criptografía asimétrica, para la encriptación de datos para el registro y des-encriptación para el procesamiento.

   2011 Desempeñe funciones como Técnico Base de Datos del GS/OAS

GENERAL SECRETARIAT OF THE ORGANIZATION OF AMERICAN STATES, a través de este apoyo técnico de la OEA, se ha realizado para el SERECI la vinculación de la búsqueda de partidas de nacimiento, matrimonio y defunción con la base de datos de partidas digitalizadas, para lo cual se ha aplicado algoritmos de criptografía asimétrica y simétrica, para visualizar la partida digitalizada y los datos primarios del resultado de la búsqueda.

2008-2009 Desempeñe funciones como ANALISTA JUNIOR EN EL AREA DE SEGURIDAD CORPORATIVA en ENTEL S.A..

2006 Realice la implementación de módulos de sistemas de micro-finanzas aplicando criptografía simétrica, para autorización de registro de pagos en mora.
1999 forme parte del equipo de desarrollo del sistema de registro de inscripciones por internet, para la carrera de informática de la UMSA sistema SIGA, donde el Jefe de Carrera lanzó un concurso para Hackear el sistema antes mencionado, para lo cual se ha coadyuvado en la implementación de medidas de seguridad en la infraestructura informática, confinando el servidor de base de datos en una red aislada físicamente.

2. ¿Qué medidas de seguridad de información aplican en tratamiento de los datos personales en la entidad que trabaja? Explique en detalle.

Todos los servidores públicos y consultores que acceden a las Bases de Datos firman un Acuerdo de Confidencialidad.

La información sensible es encriptado para lo cual se utilizan algoritmos criptográficos simétricos como asimétricos en las Bases de Datos de Registro Civil y en las comunicaciones entre los sistemas, las mismas se encuentran en redes confinadas y de acceso restringido.

Las Partidas Digitalizadas de los libros físicos también se encuentran encriptados y solo se accede a ellos a través de aplicativos.

Para que un ciudadano pueda acceder a sus datos personales con el nuevo Sistema de Registro Civil Biométrico, se realiza una verificación biométrica dactilar, con el objeto de identificarlo, se le toma una foto del rostro, se registra su domicilio a través de un mapa geo-referenciado, después de todo esto el ciudadano recién puede acceder a sus registros de partidas de Registro Civil. Con esta medida de seguridad se garantiza que solo el ciudadano pueda acceder a sus datos personales, donde ya ni el operador pueda acceder a los registros de los ciudadanos, porque el sistema le pide la huella dactilar del ciudadano facultado para acceder a esos registros.

Para todos los documentos presentados se incorpora un QR, donde el sistema imprime un QR en todos los documentos presentados y busca el código QR en

los documentos presentados para incorporarlo como documento digital. Esta medida de seguridad evita el cambio de documentos por parte de los operadores del sistema, el objetivo de la digitalización, es permitir una valoración en un entorno virtual de los documentos presentados por los ciudadanos para la realización de un trámite y así agilizar el tiempo de duración de un trámite solicitado por un ciudadano.

Para cualquier nueva inscripción los titulares y participantes deben disponer de su respectivo registro biométrico, excepto los recién nacidos, a los cuales solo se les toma una foto del rostro junto a la madre.

Para cualquier trámite el solicitante debe disponer de su respectivo registro biométrico, el cual lo debe realizar en los SERECÍ´s departamentales.

3. **¿Cómo se puede asegurar la protección de datos personales en su tratamiento desde el soporte informático?**
   El SERECÍ para asegurar la protección de datos personales desde el soporte informático aplica algoritmos criptográficos en sus datos almacenados en bases de datos y en la comunicación de datos entre sus sistemas, actualmente con el objeto de identificar a los ciudadanos y garantizar la protección de sus datos personales aplica la verificación biométrica en sus registros. Este último permite proteger los datos personales en su tratamiento desde un soporte informático, porque para acceder a sus datos requiere que el titular realice una verificación biométrica, esto significa que el ciudadano que accede a sus registros es quien dice ser, por lo que es el único que acceder a sus registros disponibles en el SERECÍ. Esto garantiza que los operadores de los sistemas del SERECÍ no pueden acceder a datos personales de otros ciudadanos, y solo pueden acceder a sus registros, porque requieren la verificación biométrica del solicitante.
   De lo anterior con el nuevo sistema de Registro Civil Biométrico el SERECÍ garantiza la protección de los datos personales de los ciudadanos.

4. **¿Cuenta con información de inconsistencias de datos de los ciudadanos? De ser así proporcione cifras.**
   En la actualidad en la mayoría de los casos los ciudadanos realizan trámites de complementación de sus registros, y solo se permite tener solo una partida de nacimiento, por lo que si un ciudadano dispone de más de una partida el sistema bloquea los registros del ciudadano hasta que este solo tenga una sola partida vigente.

   Con respecto a los matrimonios también se realiza el control, para que el ciudadano actualice su estado de libertad, es decir si en un caso tuviera registro de dos matrimonios vigentes el sistema obliga a que el ciudadano presente sus documentos de disolución de matrimonio.

Por otra parte todos los registros biométricos deben estar asociados a una partida de nacimiento, para todos los ciudadanos bolivianos, en caso de no ser así el sistema obliga a que el ciudadano corrija sus registros.

3.1.5. Análisis Jurisprudencial

Entendiendo a la Jurisprudencia como fuente del Derecho se análisis de la Jurisprudencia del Tribunal Constitucional Plurinacional y del Tribunal Supremo de Justicia.

SENTENCIA CONSTITUCIONAL PLURINACIONAL 0819/2015-S3, 10 de agosto de 2015, señala:

"…es decir, que el **Estado no cuenta con normas adecuadas para la protección de datos de carácter personal** ni con políticas públicas claras en la materia, pese a que la era digital actual así lo demanda, donde el acceso a la información fue el puntal de su propia evolución"…

"…**La protección de datos personales se concreta jurídicamente a través de la acción de protección de privacidad, en ese sentido, cabe referirnos al derecho de autodeterminación informática** como la prerrogativa que toda persona posee frente a cualquier entidad pública o privada, por la cual nadie debe introducirse, sin autorización expresa (de él mismo o por mandato de la ley), en aspectos que no sean públicos y se refieran a su vida personal y familiar, para que pueda procesarlos y/o difundirlos como vea conveniente, independientemente de la existencia o no de daño alguno. En ese entendido, **la autodeterminación informática constituye la dimensión positiva del ejercicio del derecho fundamental a la intimidad y la privacidad, es decir que dicha dimensión positiva implica el derecho que tiene la persona de acceder a los bancos de datos públicos y privados con el fin de tener conocimiento de cuanta información se ha almacenado, hacia donde fluyó la información o datos de la misma y para que fines, por lo que, sin una autorización expresa**, tan solo el titular de ese derecho tiene la potestad de disponer la información concerniente a sus datos de carácter personal, de preservar la propia identidad informática, o lo que es igual, **de consentir, controlar, o incluso el de rectificar los datos informáticos de carácter personal"**…

SETENCIA CONSTITUCIONAL PLURINACIONAL 0440/2016-S3, 13 de abril de 2016, señala:

…"En mérito al art. 61 del Código Procesal Constitucional (CPCo), la acción de protección de privacidad puede interponerse de manera directa sin trámite administrativo previo; además, **protege el derecho a la autodeterminación informativa, el cual es activado cuando las personas que tienen a su cargo un banco de datos públicos o privados asumen una postura ilegal o indebida al no permitir el acceso, rectificación, corrección, eliminación o mantenimiento de datos.** Por consiguiente, se concluye que esta acción tutelar protege datos que son el núcleo del derecho a la privacidad o intimidad del individuo, frente a la ilegal obtención, mantenimiento y distribución de información por parte de entidades públicas o privadas, otorgando a toda persona natural o jurídica la potestad de acudir a la jurisdicción constitucional para solicitar la actualización, rectificación o supresión de la información"…

SENTENCIA CONSTITUCIONAL PLURINACIONAL 1300/2012, 19 de septiembre de 2012, señala:

III.1.Naturaleza jurídica y alcances de la acción de protección de privacidad

La acción de protección de privacidad es una garantía constitucional, que brinda a la persona una protección efectiva e idónea frente al manejo o uso ilegal e indebido de información o datos personales generados, registrados o almacenados en bancos de datos públicos y privados, que son distribuidos a través de los medios o soportes informáticos.

El art. 130.I de la CPE, sobre esta acción tutelar señala, que: "Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad", entendimiento que se encuentra plasmada en la SC 0127/2010-R de 10 de mayo.

De la misma forma, el art. 81 de la LTCP, refiere que: "La Acción de Protección de Privacidad tiene por objeto la garantía del derecho de toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental de la intimidad y privacidad

personal o familiar, o a su propia imagen, honra y reputación ".

Asimismo, el art. 21.2 de la CPE, indica que las bolivianas y los bolivianos tienen los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad.

III.2. Alcances de esta acción tutelar

Respecto a los alcances de esta acción, la SC 1738/2010-R de 25 de octubre, mencionando a la SC 0965/2004-R de 23 de junio, señaló los siguientes aspectos:

1. Conocer la información o "registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal"; asimismo, conocer los fines y objetivo de la obtención y almacenamiento; es decir, qué uso le darán a esa información.

2. Actualizar los datos existentes, este es "el derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona ".

3. Modificar o corregir la información existente en el banco de datos, cuando son incorrectos o ajenos a la verdad, en otros términos es el derecho corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona.

4. Preservar la confidencialidad de la información que si bien es correcta y obtenida legalmente, no se la puede otorgar en forma indiscriminada; esta acción se funda en el derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona.

5. Excluir la información sensible, es decir, aquella información que sólo importa al titular, como las ideas políticas, religiosas, orientación sexual, enfermedades, etc.; así la citada Sentencia Constitucional señaló que es el "Derecho de exclusión de la llamada "información sensible" relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que

potencialmente podría generar discriminación o que podría romper la privacidad del registrado. (las negrillas son nuestras)

III.3. La legitimación activa en la acción de protección de privacidad

La jurisprudencia constitucional, respecto a la legitimación activa dentro de la acción de protección de la privacidad, estableció lo siguiente: "Partiendo de los conceptos referidos, se puede inferir que el hábeas data es una garantía constitucional por lo mismo se constituye en una acción jurisdiccional de carácter tutelar que forma parte de los procesos constitucionales previstos en el sistema de control de la constitucionalidad. Es una vía procesal de carácter instrumental para la defensa de un derecho humano como es el derecho a la autodeterminación informática.

Como una acción tutelar, el hábeas data sólo se activa a través de la legitimación activa restringida, la que es reconocida a la persona afectada, que puede ser natural o jurídica. En consecuencia, no admite una activación por la vía de acción popular, es decir, no se reconoce la legitimación activa amplia."

(…) 'La legitimación activa del hábeas data recae en la persona natural o jurídica -aunque el precepto constitucional no lo determina de esa manera en forma expresa, se entiende que dentro de la protección de este recurso se puede y debe abarcar tanto a las personas físicas como a las jurídicas, de quienes también se pueden registrar datos e informaciones- respecto de la cual la entidad pública o privada haya obtenido y tenga registrados datos e informaciones que le interesen a aquella conocer, aclarar, rectificar, modificar, o eliminar, y que no haya tenido respuesta favorable por la citada entidad para lograr esos extremos'.

(…) El Hábeas data no es otra cosa que el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

(…) En virtud de él, la persona tiene derecho a que se le informe qué datos suyos y de su familia reposan en los archivos y bancos de datos privados y oficiales, no sometidos a reserva legal, a que se corrijan, se actualicen y sólo se usen para fines legítimos". Así la SC 1978/2011-R de 7 de diciembre, que hizo acopio de la ST-443/94 de la legislación colombiana.

CAPITULO IV
EVALUACION DE LA NORMATIVA BOLIVIA – ESTANDARES DE PROTECCION DE DATOS PARA LOS ESTADOS IBEROAMERICANOS

4.1. Evaluación de normativa boliviana

4.1.1. Contraste con los Estándares de Protección de Datos para los Estados Iberoamericanos

La Red Iberoamericana de Protección de Datos, ha aprobado los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" en el XV Encuentro Iberoamericano de Protección de Datos, el 20 de junio de 2017. Siendo Bolivia parte de la Red, en la presente evaluación, se toma como referencia para contrastarla con la normativa existente en la Protección de Datos Personales

En Ámbito de Aplicación subjetivo, en los estándares indica que se aplican a personas físicas y jurídicas de carácter privado, autoridades y organismos públicos. En Bolivia la Ley 164, Ley de Telecomunicaciones en el artículo 72 indica que el Estado fomentará la protección de las usuarias y los usuarios, la seguridad informática y de redes.

En cuanto a Ámbito de aplicación objetivo indica los estándares serán aplicables al tratamiento de datos personales que obren en soporte físicos, automatizados total o parcialmente o en ambos o en ambos soportes. Así mismo indica que los estándares serán aplicables al tratamiento de datos efectuado (realizado) por un responsable o encargado. El Reglamento de la Ley de Telecomunicaciones en definiciones (artículo 3) acápite IV establece se entiende como datos personales, a toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable; b. Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada; c. Tratamiento de los datos

personales: Es cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Los estándares establecen principios que los responsables deber observar cuando apliquen al tratamiento de datos personales de: legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad. El Reglamento de la Ley de Telecomunicaciones en su artículo 4 (principios) en el parágrafo II establece …"Los servicios de certificación digital en cuanto a tratamiento de datos personales se regirán por los siguientes principios: …d) Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravió, utilización y acceso no autorizado o fraudulento". La normativa Boliviana solo prevé principios a los servicios de certificación de firma digital, que dando al margen las instituciones que hacen uso en soporte físico, y el tratamiento que se pueda dar en las empresas e instituciones.

También se establecen los derechos ARCO que indica que en todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen. En el reglamento de la Ley de Telecomunicaciones en el artículo 3 (Definiciones), acápite IV (en Tratamiento de Datos), inc. b) establece que debe haber una "autorización: consentimiento previo expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una entidad certificadora autorizada". Lo contrastado nos muestra que la autorización solo se da en entidad certificadora autorizada.

Los estándares también contempla la presencia de encargado de realizar las actividades de tratamiento de datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los

términos fijados por el responsable. Al respecto la normativa boliviana no menciona el papel de encargados.

Los estándares plantean medidas proactivas en el tratamiento de datos personales, indica que: se aplicara desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Por otra parte el responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad. Al respecto la normativa boliviana cuenta con los “Lineamientos para la elaboración de Planes de Seguridad de Información de las entidades de sector público” que son de cumplimiento obligatorias pero sólo está dirigido a entidades del sector público.

CAPITULO V
CONCLUSIONES

5.1. Conclusiones

5.1.1. Nuevo rol de los estados en la era digital

Según Rodolfo Herrera, el nuevo rol innovador del Estado que permita consolidar un sistema económico y social acorde al avance tecnológico, debe ser acompañado de normativa jurídica, en dos niveles de acción estatal: Un estadio Subsidiarios, donde el Estado actúa como generador de condiciones que permitan el normal desenvolvimiento de los particulares, por ejemplo fijando una política educacional destinada a formar un recurso humano calificado; creando condiciones de estabilidad económica que disminuyan los riesgos de las empresas que invierten en desarrollo tecnológico; o facilitando la participación de particulares a través de políticas de fomento. Un segundo estadio de Acción estatal, que se da al interior de la Administración del Estado, que es la informatización del Estado, mediante el fomento y empleo de cambios tecnológicos, que deben permitir mejorar la gestión. Materializando el principio de simplificación y flexibilidad administrativas.

Para el análisis de la protección de datos dentro del derecho informático, nace de la necesidad regular las relaciones de los individuos dentro de las redes y dada su complejidad en cuanto al manejo de datos, dentro de las telecomunicaciones, las tecnologías de información y comunicación y el internet, surge la necesidad que el derecho también se vaya receptando de acuerdo al avance tecnológico.

Cada país tiene su sistema jurídico, y en el caso de Bolivia el sistema al que pertenece es al Sistema de Derecho Romano-Germánico. Que**:** «se caracteriza porque la norma de derecho se elabora inicialmente, y se aplica posteriormente a los problemas que la práctica presenta...».

El desarrollo tecnológico está directamente relacionado con los países desarrollados, quienes tienen el control de la Investigación y el Desarrollo (I+D), mientras que los países de menor desarrollo tienen que adoptar o recibir la transferencia tecnológica a través de actividades como el ensamblaje o servicios auxiliares. En cuanto al derecho. Bolivia y los países de la región reconocen el sistema jurídico continental o romano, donde el estudio se basa en la lectura de las leyes. Las normas son desarrolladas por el sistema legislativo. El sistema deriva de la existencia de códigos basados en principios jurídicos de hace siglos. En el caso del desarrollo normativo de seguridad de los datos personales su desarrollo normativo es insuficiente y con retraso.

El derecho informático tiene un objeto propio de estudio en constante desarrollo relacionado con las "Tecnología de la Información" y "Sociedad de la Información" que tiene relación directa con el Derecho Constitucional, en lo referido al Derecho fundamental de Acción de Privacidad por lo que se requiere normar la forma en que se garantizará el derecho a la privacidad,

Hoy en día la humanidad, se encuentra inmersa en nuevo paradigma denominado economía digital, donde surjan les economías colaborativas, que ha obligado que las administraciones públicas lo utilicen como modelo para la reforma del Estado, denominado Gobierno Electrónico. En este nuevo contexto los datos adquieren relevancia ya que la transmisión de datos permite realizar transacciones a gran velocidad gracias a la fibra óptica, Así mismo se permite el almacenamiento y procesamiento de importantes cantidades de datos en lo denominado Big Data.

El reto del Derecho es, pues flexibilizar sus instituciones e incorporar aquellas normas surgidas dentro del Internet para que todos los actos jurídicos que se den dentro del mundo virtual tengan idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios tenga los mismos efectos legales.

El avance tecnológico, especialmente en el área de la informática, si bien abre nuevos cauces para progresos económicos sociales y culturales. Al mismo tiempo, puede poner en peligro los derechos y las libertades de los individuos. Esta ambivalencia es una de las cuestiones fundamentales que debe resolver la sociedad moderna

La informática debilita la capacidad de dominio de las personas sobre los datos que les conciernen. Ello es especialmente preocupante cuando se trata de las creencias religiosas o políticas, las condiciones de salud, y otros aspectos privativos de los individuos.

Es así que el avance de la tecnología y la afirmación de los derechos del hombre en la democracia, exigen hoy nuevas reglas de derecho que, dentro del respeto de aquellos principios constitucionales, extiendan el amparo legal a situaciones que no pudieron preverse en su momento.

5.1.2. **Desarrollo del habeas data – acción de protección de la privacidad**

La elaboración de normativa que se produce paralelamente con el accionar de organismos internacionales, que se plasmó en la sanción de leyes cuyo objetivo es lograr una protección adecuada de los derechos y libertades fundamentales. Estas leyes pretenden solucionar el conflicto de intereses entre el derecho a la vida privada y el derecho a la información (libertad de información que es consecuencia de su ejercicio). Equilibrio entre la información que necesita la sociedad para un funcionamiento democrático y el derecho del individuo a la protección de los datos que le conciernen.

Su principal propósito fue llenar el vacío manifiesto que existía en el ordenamiento jurídico, de modo de otorgar el derecho a la privacidad de las

personas, en el ámbito del Derecho Civil, ante eventuales intromisiones ilegítimas, Así se cuentan con los principales instrumentos jurídicos:

- La Declaración Universal de Derechos Humanos de 1948.
- La Declaración Americana de los Derechos y Deberes del Hombre de 1949.
- El Pacto Internacional de Derechos Civiles y Políticos de 1966
- La Convención Americana de Derechos Humanos de 1969

Mediante el uso de la informática, y en particular a través de la interconexión de ficheros, datos aparentemente inocentes se conjugan formando la historia personal de un individuo, con el consiguiente peligro de invasión de su esfera privada; inclusive una apropiada defensa en juicio, puede quedar vulnerada con el uso de datos contenidos en computadoras como medios de prueba.

Los riesgos de violación de derechos y libertades fundamentales mediante el uso de las nuevas técnicas informáticas se hacen más evidentes en el caso de las llamadas informaciones sensibles (datos sobre creencias o convicciones religiosas, opiniones políticas, origen racial, hábitos sexuales, circunstancias penales y pertenencia a sindicatos o partidos políticos,· etc.) que pueden dar lugar a conductas discriminatorias por parte de quienes tienen monopolios de información.

La Sociedad de la información y el desarrollo de los sistemas de información como el Big Data permiten un manejo rápido y eficiente de grandes volúmenes de información que facilita la concentración automática de datos referidos a las personas (constituyéndose un verdadero factor de poder). Como se analizó es hasta la década de los sesenta cuando empiezan a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos como Nombre, número de documento de identidad, lugar de filiación, fecha y lugar de nacimiento, domicilio, estado civil, etc., hasta otro tipo de datos con caracteres aún más

distintivos como raza, religión inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, etc.

Existen diferentes centros de recolección y acopio de datos, que ya no lo hacen con medios manuales sino con medios con apoyo de medios electrónicos, que, provocan una gran concentración, sistematización y disponibilidad instantánea de ese tipo de información para diferentes fines (registros, tramites, parroquiales, civiles, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios, laborales, identificación personal, etc). Estos datos no son vulnerables sino según la destinación de que puedan ser objeto dichas informaciones: pueden ser empleadas para fines publicitarios, comerciales, fiscales, policiales, etc., convirtiéndose de esta manera en un instrumento de operación y mercantilismo. La variedad de los supuestos posibles de indefensión frente al problema, provoca que los individuos estén a merced de un sin número de situaciones que alteren sus derechos fundamentales en sociedad provocados por discriminaciones, manipulaciones, persecuciones, presiones, asedios, etc., todo ello al margen de un control jurídico adecuado.

Surge así el hábeas data, con el fin de garantizar la privacidad o intimidad personal frente a los riesgos del almacenamiento, registro y utilización de datos. Así en Bolivia la protección al acceso de datos personales constituye una prioridad jurídica estructurada inicialmente bajo la conceptualización de un derecho fundamental denominado Habeas Data hasta el año 2009 y Acción de Protección de Privacidad y/o Protección de Datos Personales a partir de la Constitución Política del Estado Plurinacional de Bolivia de 2009,

La Acción de Protección de Privacidad y/o Protección de Datos Personales, funciona para que no se comparta la información íntima y para que esta información pueda corregirse, actualizarse o modificarse en todo momento, acción que se puede intentar solamente por su titular. En nuestro país se requiere intensificar la protección

jurídica en torno a los datos personales, bajo mecanismos que van desde la protección legal en los procesos de captación, almacenamiento, sistematización y modos de compartirla, hasta los mecanismos legales para conocer datos propios y modificarlos cuando son imprecisos o erróneos. Algunos aspectos normativos actuales se relacionan con la intimidad y complementan su noción protectora, entre ellos destacan la inviolabilidad domiciliaria, inviolabilidad de las comunicaciones, el derecho a la propia imagen, etc., cada uno de ellos estructura sus propios bienes jurídicos tutelados y la forma de ejercitarlos. Las nuevas tecnologías de la información también inciden en el tema del acceso a datos personales y la protección de los mismos, principalmente en torno al tema de mantener segura la información personal sistematizada.

Es este contexto la Seguridad es una necesidad básica cuando el Estado está interesado en la prevención de la vida y de las posesiones » (Manunta, 2003).

Cuando se maneja documentación personal (tratamiento) en documentación administrativa y empresarial, es necesario tomar en cuenta las obligaciones legales vigentes, en cuanto a seguridad de la información se refiere, España cuenta con un ordenamiento legal de tratamiento de datos personales, que está compatibilizado con la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD)[39]. Este ordenamiento jurídico es tomado como base referencial en la Región en los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", emitidos por la Red Iberoamericana de Protección de Datos.

El Real Decreto 1720/2007 de 21 de diciembre de 2007, en cuanto a tratamiento de datos de carácter personal. Establecen tres niveles de seguridad:

[39] En Europa a partir del 25 de Mayo del 2018, entra en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos, RGPD). Publicado en el DOUE el pasado 4 de mayo de 2016

Básicos (todos los datos de carácter personal), Medio (infracciones administrativas, penales, tributarias, financieras, de seguridad social, personalidad) y Alto (ideología, afiliación sindicas, religión. Creencias, origen racial, salud o vida sexual, violencia de género). Las medidas de seguridad se aplican de manera acumulativa. Es una norma que en aspectos seguridad de la Información, considera todas las áreas que se deben tomar en cuenta para garantizar una adecuada seguridad de la información. Otra norma que contempla la seguridad de datos es el reglamento de la Unión Europea 2016/679, que reconoce la ISO 27001, norma internacional que describe cómo gestionar la seguridad de la información en una empresa y una organización. La norma contempla proporciona un catálogo de 114 controles (medidas de seguridad)

5.1.3. **Medidas de seguridad de información en Bolivia**

En medidas de seguridad de información y tratamiento de datos personales, la Ley General de Telecomunicaciones, Ley N° 164 de 28 de julio de 2011 (que establece el régimen general de telecomunicaciones y tecnologías de información y comunicación, del servicio postal y el sistema de regulación), en su Artículo 72, Parágrafo I señala textualmente, que: …"El Estado en todos sus niveles, fomentará la... la protección de las usuarias y usuarios, la seguridad informática y de redes…". El Reglamento a la Ley Nª 164, Decreto Supremo N°1793 de fecha 13 de noviembre de 2013, en su artículo 3 (definiciones) en su acápite IV, define respecto al tratamiento de datos personales: define datos personales "…toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable…" En Bolivia la información concerniente a una persona que la hace identificable es la información que se registra en su cédula de identidad, que como requisito requiere sus datos de nacimiento y estado civil.

Igualmente el Decreto Supremo N° 1793 que Reglamenta el acceso, uso y desarrollo de las Tecnologías de Información y Comunicación en su artículo 3 (definiciones) en su acápite IV define como Autorización al "Consentimiento previo,

expreso e informado del titular para llevar a cabo el tratamiento de datos personales por una Entidad Certificadora Autorizada". En el Reglamento refiere que es la entidad que emite el certificado digital (artículo 24). Así mismo se define Tratamiento de los datos personales: "… cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. El Reglamento por lo descrito está dirigido a entidades certificadoras de firma digital.

En cuanto a Seguridad de la Información, el Reglamento en su artículo 3 (definiciones) acápite IV define como la: "…preservación de la confidencialidad, integridad y disponibilidad de la información…" pudiendo estar involucradas otras propiedades como "…la autenticidad, responsabilidad, no repudio y confiabilidad…"

Coincidente con el punto anterior el artículo 4 (principios), en el parágrafo II, Tratamiento de datos personales, establece: …"Los servicios de certificación digital en cuanto a tratamiento de datos personales se regirán por los siguientes principios: …d) Se debe implementar los controles técnicos y administrativos que se requieran para preservar la confidencialidad, integridad, disponibilidad, autenticidad, no repudio y confiabilidad de la información, brindando seguridad a los registros, evitando su falsificación, extravió, utilización y acceso no autorizado o fraudulento"... Lo descrito confirma que el Reglamento está orientado a entidades certificadoras de firma digital.

En cuanto a Seguridad Informática, el Reglamento en su artículo 3 (definiciones) acápite IV define como: "**…**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*… ".*

El Articulo 8 del Reglamento (Plan de contingencia) norma que: "…las entidades públicas promoverán la seguridad informática para la protección de datos en sus sistemas informáticos, a través de planes de contingencia desarrollados e implementados en cada entidad…". Con Decreto Supremo 2514, de fecha 9 de septiembre de 2015, se crea la Agencia de Gobierno de Tecnologías de Información y Comunicación – AGETIC, y en este mismo decreto, artículo 7, inciso f) se la asigna la función: **…** **"**Establecerá los lineamientos técnicos en seguridad de información para las entidades del sector público".

Así los lineamientos que en el Decreto Reglamento de la Ley de Telecomunicaciones se referían sobre seguridad informática, ahora han sido cambiadas a en los lineamientos de la AGETIC a Seguridad de la Información, que tienen como objetivo "…establecer los lineamientos para que las entidades del sector público del Estado Plurinacional de Bolivia puedan elaborar e implementar sus Planes Institucionales de Seguridad de la Información, en concordancia con la normativa vigente…". Los controles contemplados son: Seguridad de recursos humanos; Gestión de activos de información; Control de accesos; Criptografía; Seguridad física y ambiental; Seguridad de las operaciones; Seguridad de las comunicaciones; Desarrollo, mantenimiento y adquisición de sistemas; Gestión de incidentes de seguridad de la información; Plan de contingencias tecnológicas; y Cumplimiento.

Por el análisis realizado podemos sintetizar que la Ley 164, Ley de Telecomunicaciones y el Decreto Supremo N° 1793 que aprueba el Reglamento para el Desarrollo de Tecnologías de Información y Comunicación, en cuanto a seguridad de información y tratamiento de datos personales están se deduce están orientados a entidades certificadoras de firma digital. Y en cuanto a seguridad informática, que se aplica a los medios tecnológicos está condicionada para garantizar la protección de datos en las entidades público privadas. Para garantizar se tenían que establecer lineamientos de seguridad informática, que hasta el 31 de diciembre de 2017 no han

sido emitidos. La AGETIC ha emitido lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público.

Luego de la revisión normativa se Verifica que la normativa boliviana prevé la seguridad de la información para el tratamiento de datos en registros públicos, sólo para entidades certificadoras de firma digital.

5.1.4. **Protección en el tratamiento de datos personales y en el derecho a la privacidad**

En el ámbito internacional el tratamiento de datos personales se caracteriza por tener un enfoque internacional y ser armonizada. Así la recolección, el almacenamiento, el uso, la circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional en regulación con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia.

En la región surge la Red Iberoamericana de Protección de Datos (RIPD), instancia que en junio del 2017, con la aprobación de los países miembros de Andorra, Argentina, Chile, Colombia, Costa Rica, España, México, Perú, Portugal y Uruguay convinieron adoptar los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" como máxima prioridad en la Comunidad Iberoamericana.

Bolivia en la gestión 2019 ha recibido asistencia técnica para de la Agencia Española de Cooperación Internacional para el Desarrollo – AECID, para la elaboración del "Proyecto de Ley de Protección de Datos Personales en Bolivia", en el marco de la cooperación de la RIPD. Como parte de una de sus actividades en el año 2009, se llevó a cabo un seminario llegándose a las siguientes conclusiones:

- Desconocimiento de la Acción de Protección de Privacidad.

- No existe políticas de seguridad de la información en instituciones públicas.
- Necesidad de una Ley específica que regule la privacidad y protección de datos personales en Bolivia. Creación de una Autoridad de Control Independiente (control, fiscalización, sanción).
- Mayor difusión y socialización del tema en el sector público, privado, sociedad civil y ciudadanía.
- Mayor capacitación a los responsables del tratamiento de los datos personales en las entidades del sector público.

Pese a los esfuerzos realizados hasta el 2010, no se pudo concretar la Ley de Protección de Datos Personales en Bolivia

5.1.5. **Tratamiento de datos personales en la legislación boliviana**

En el caso de Bolivia, la Constitución Política del Estado del 2009 incorpora disposiciones de derecho a la intimidad y privacidad. La protección de datos personales no se encuentra explícita, sino que se encuentra como una Acción, referida a "conocer, objetar u obtener la eliminación o rectificación de los datos registrados…". En la CPE no se establece el Habeas Data, pero sí la Acción de Protección a la Privacidad con procedimiento previsto para la acción de Amparo Constitucional. No establece ni se refiere al derecho a conocer la finalidad del tratamiento de datos, ni al uso que se le está dando. Tampoco hace referencia al derecho de exigir la confidencialidad de datos personales. En síntesis no se le da rango constitucional a la protección de datos personales.

La Ley de Telecomunicaciones establece la Protección de datos personales, regulando en este aspecto a operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación. El Reglamento de la Ley de Telecomunicaciones (Decreto Supremo 1793), norma el tratamiento de datos personales (recolección, almacenamiento, uso, circulación o supresión),

autorización (consentimiento) de los usuarios para el tratamiento. Establece también las funciones de las Agencias de Registro y el tratamiento de datos personales en el sector público y privado en todas las actividades.

En el análisis normativo, se puede deducir que las medidas de seguridad de la información a ser adoptadas para el manejo de datos personales que permiten la protección en su tratamiento y en el derecho a la intimidad y privacidad en la actual regulación en Bolivia, es una decisión que recae en el responsable del tratamiento de datos personales, pudiendo ser este público o privado

Como se mencionó, la Ley de Telecomunicaciones artículo 3 (definiciones) en su acápite IV, respecto al TRATAMIENTO DE DATOS PERSONALES: define datos personales "…toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable…" En Bolivia la información concerniente a una persona que la hace identificable es la información que se registra en su cédula de identidad, que como requisito requiere sus datos de nacimiento y estado civil. Con esta acotación se hace análisis la normativa del SERECI y del SEGIP para verificar en marco normativo de esta entidades estatales se aplican las medidas de tratamiento de datos, previstas en el Reglamento de la Ley de Telecomunicaciones (Decreto Supremo 1793).

5.1.5.1.**Servicio de Registro Cívico**

El artículo 208 de la Constitución Política del Estado, parágrafo III establece que: "Es función del Tribunal Supremo Electoral organizar y administrar el Registro Civil y el Padrón Electoral". Así mismo La Ley 018, Ley del Órgano Electoral Plurinacional (OEP) de fecha 16-jun.2010, en el inc. 13 del Artículos 6 (Competencias) estable que la OEP tiene las siguientes competencias: "…Organización y administración del Servicio de Registro Cívico (SERECÍ)."En ese marco el artículo 71 (Funciones) establece que el SERECI tiene funciones de registrar

nacimientos, matrimonios, divorcios, defunciones y nacionalidad. Para lo cual debe establecer un sistema de registro biométrico de personas naturales que garanticen la confiabilidad, autenticidad y actualidad de datos.

En cuanto a tratamiento de datos personales establece en su artículo 71 (Obligaciones) que: " tiene las siguientes obligaciones:

1. Respeto irrestricto del derecho a la intimidad e identidad de las personas y los demás derechos derivados de su registro.
2. Garantizar la privacidad y confidencialidad de los datos registrados de las personas.
3. Velar por la seguridad e integridad de la totalidad de la información registrada."

5.1.5.2.**Servicio de Registro Cívico - SERECI**

La Constitución Política del Estado, en su artículo 14, determina que: "… todo ser humano tiene personalidad y capacidad jurídica con arreglo a las leyes y goza de los derechos reconocidos por esta constitución, sin discriminación. Asimismo, las extranjeras y los extranjeros en el territorio boliviano tienen derechos y deben cumplir los deberes establecidos en la Constitución, salvo las restricciones que ésta contenga". Así mismo, el artículo 24, establece que: "… toda persona tiene derecho a la petición de manera individual o colectiva, sea oral o escrita, y a la obtención de respuesta formal y pronta. Para el ejercicio de este derecho no se exigirá más requisito que la identificación del peticionario". Es en este marco constitucional que se establece la necesidad de la personalidad y capacidad jurídica, así como la necesidad de la identificación de las personas.

Al respecto la "Ley 145; establece en su artículo 1, tiene por objeto la creación del Servicio General de Identificación Personal, normándola como la única entidad pública facultada para otorgar la Cédula de Identidad – C.I., dentro y fuera

del territorio nacional, crear, administrar, controlar, mantener y precautelar el Registro Único de Identificación – RUI, de las personas naturales a efecto de su Identificación y ejercicio de sus derechos.

Los principios bajo los cuales el SEGIP, sujeta su acción Son: Universalidad, Confidencialidad, Unicidad, Seguridad, Calidez, Celeridad, Eficiencia, Transparencia, Obligatoriedad y Respeto a la dignidad. Tres de estos principios son parte de los cinco que establece el D.S. 1793 de transparencia, seguridad y confidencialidad, incluyendo dos adicionales de finalidad y transparencia.

En cuanto a sus atribuciones cuenta con las siguientes relacionadas con tratamiento de datos:

a) Establecer los procedimientos para el manejo, administración y registro de los datos de identificación
b) Establecer en coordinación con el SERECI, un sistema de registro que garantice la confiabilidad y autenticidad de los datos registrados de forma permanente.
c) Regular el uso, actualización, administración y almacenamiento del Registro Único de Identificación – RUI
d) Implementar mecanismos y/o procedimientos que garanticen la privacidad, confidencialidad y seguridad de los datos registrados.

5.1.6. Opiniones de expertos constitucionalistas en tratamiento de datos en lo referido a derecho a la privacidad

En Bolivia no existe una Ley específica de protección de datos personales y es necesario considerar disposiciones de orden constitucional, legal y jurisprudencial constitucional para delinear su contenido.

También reconocen que se debe definir que se entenderá como datos personales, así como establecer la finalidad con la cual se registra, los límites para

divulgarla, así como de establecer sanciones punitivas o económicas ante su desconocimiento.

En cuanto a contemplar la creación de una entidad específica encargada de datos personales, el criterio de uno de los especialistas es que si existe la necesidad de crear una entidad específica y especializada que tenga conocimiento técnico. El otro experto considera que es difícil reunir en una sola entidad de registro, tampoco en una entidad encargada de datos personales.

Ambos expertos consideran que el no contar con una norma específica no es un obstáculo para el ejercicio del Habeas Data o Acción de Protección de Datos Personales, porque la garantía prevista en la Constitución y el Código Procesal no necesita norma que regule su ejercicio. Pero en términos sustantivos uno de los expertos considera, que és necesario una norma que ayude cómo debe enfrentarse en términos de política pública la protección de datos personales.

Consideran que existe un bajo índice de acciones de protección de privacidad en las que se ha concedido tutela porque no han sido bien encaminada por el mundo litigante (indicador de naturaleza jurídica de la Acción de Protección de Datos personales). Así mismo el error de encaminarla como Acción de Amparo Constitucional se debe también al mal accionar de los litigantes que olvidan que esta acción es subsidiaria.

En cuanto a asegurar la protección de datos personales en su tratamiento y el derecho a la intimidad y privacidad, un experto considera que se debe tomar los siguientes aspectos:

1) La administración, acceso y control de la información deben estar limitados a propósitos estrictamente necesarios desde el punto de vista razonable, evitando cualquier tipo de intromisión en la esfera privada de la persona;

2) La persona debe brindar su consentimiento expreso y autorizar labores de administración, acceso y control de la información que produce. Un uso de datos por más proporcional que sea que no esté consentido por la persona implica un menoscabo de su derecho a la privacidad

El otro experto considera que se debe establecer límites respecto a la difusión de dichos registro estableciendo también las sanciones y la forma en que debe ser reparada la lesión.

5.1.7. **Opiniones de expertos en seguridad de información y tratamiento de datos en los referido al derecho a la privacidad – SERECI y SEGIP**

En cuanto a medidas de seguridad en ambas instituciones se cuenta con un acuerdo de confidencialidad donde se establecen los deberes y obligaciones de los usuarios del sistema.

En el caso del SEGIP se cuenta con Políticas de Seguridad, planes de contingencia y procedimientos para la protección de la información.

En el caso del SERECI la información sensible es encriptado así como las Partidas digitalizadas de los libros físicos. Para que un ciudadano pueda acceder a sus datos se verifica biométricamente y dactilarmente, en el Sistema de Registro Civil Biométrico.

Para cualquier trámite o nueva inscripción, los titulares o participantes deben disponer de su respectivo registro biométrico, excepto a los recién nacidos a quienes se les toma la foto con la Madre.

También se evita el cambio de documentos con la utilización de código QR, donde el sistema imprime un código QR para los documentos presentados para incorporarlo como documento digital.

En cuanto a cómo se puede asegurar la protección de datos personales en su tratamiento desde el soporte informático, en el caso del SEGIP para garantizar las características de confidencialidad (niveles de autorización de acceso), integridad (conservar la exactitud y totalidad de la información así como los métodos de procesamiento) y disponibilidad (cuando requiera el usuario) se efectúa:

- Comunicación interna y externa encriptado.
- Acceso restringido a recursos y determinados usuarios.
- Registro de altas y najas (logs)

El SERECÍ para asegurar la protección de datos personales desde el soporte informático aplica algoritmos criptográficos en sus datos almacenados en bases de datos y en la comunicación de datos entre sus sistemas, actualmente con el objeto de identificar a los ciudadanos y garantizar la protección de sus datos personales aplica la verificación biométrica en sus registros.

En cuanto a inconsistencias que se presentan. En el SEGIP solo se podría saber en el momento de la emisión o renovación de la Cédula de identidad si existe alguna inconsistencia en algún dato. En el caso del SERECI los ciudadanos realizan el trámite de complementación de sus registros, y el sistema solo le permite tener una partida de nacimiento (si dispone más de una el sistema lo bloquea). En el caso de matrimonios se realiza el control para que el ciudadano actualiza su estado de libertad (si tiene registro de dos matrimonios el ciudadano debe presentar sus documentos de disolución). El registro biométrico debe estar asociado a una partida de nacimiento, en caso de no ser así, el ciudadano debe corregir su registro.

5.1.8. **Análisis jurisprudencial**

Sentencia constitucional 0879/201-S3, de fecha 10 de agosto de 2015 que señala: "…el Estado no cuenta con normas adecuadas para la protección de datos de carácter personal ni con políticas públicas claras en la materia". Así mismo señala que"…La protección de datos personales se concreta jurídicamente a través de la acción de protección de privacidad, en ese sentido, cabe referirnos al derecho de autodeterminación informática…" que "…constituye la dimensión positiva del ejercicio del derecho fundamental a la intimidad y la privacidad, es decir que dicha dimensión positiva implica el derecho que tiene la persona de acceder a los bancos de datos públicos y privados con el fin de tener conocimiento de cuanta información se ha almacenado, hacia donde fluyó la información o datos de la misma y para que fines, por lo que, sin una autorización expresa, tan solo el titular de ese derecho tiene la potestad de disponer la información concerniente a sus datos de carácter personal, de preservar la propia identidad informática, o lo que es igual, de consentir, controlar, o incluso el de rectificar los datos informáticos de carácter personal"… La Sentencia constitucional 0440/2016-S3, 13 de abril de 2016 que reitera el derecho a la autodeterminación informática.

La Sentencia constitucional 1300/2012, 19 de septiembre de 2012 crea jurisprudencia en cuanto a la naturaleza jurídica y alcance de la acción de protección a la privacidad : "…La acción de protección de privacidad es una garantía constitucional, que brinda a la persona una protección efectiva e idónea frente al manejo o uso ilegal e indebido de información o datos personales generados, registrados o almacenados en bancos de datos públicos y privados, que son distribuidos a través de los medios o soportes informáticos…". En cuanto al Alcance de la acción tutelar señala la SC 0965/2004-R de 23 de junio de 2004, que señalo los siguientes aspectos:

1. Conocer la información o "registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se

dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal"; asimismo, conocer los fines y objetivo de la obtención y almacenamiento; es decir, qué uso le darán a esa información.

2. Actualizar los datos existentes, este es "el derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona ".

3. Modificar o corregir la información existente en el banco de datos, cuando son incorrectos o ajenos a la verdad, en otros términos es el derecho corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona.

4. Preservar la confidencialidad de la información que si bien es correcta y obtenida legalmente, no se la puede otorgar en forma indiscriminada; esta acción se funda en el derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona.

5. Excluir la información sensible, es decir, aquella información que sólo importa al titular, como las ideas políticas, religiosas, orientación sexual, enfermedades, etc.; así la citada Sentencia Constitucional señaló que es el "Derecho de exclusión de la llamada "información sensible" relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas

religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado.

5.1.9. **Resultado de la investigación**

Resultado de la investigación se puede deducir que la normativa boliviana prevé la seguridad de la información para el tratamiento de datos en registros públicos, sólo para entidades *certificadoras de firma digital.* Así mismo se deduce que la normativa existente está dirigida solo para el Desarrollo de Tecnologías de Información y Comunicación (D.S. 1793) y no contempla para sistemas de registro y custodia manual (archivos). El D.S. no tiene rango de Ley por lo que puede existir choque de competencias con la leyes propias de instituciones (SEGIP – Ley 145, y SERECI Ley 17) o leyes sectoriales (Ley del Sistema Financiero, etc).

En cuanto al Tratamiento de Datos Personales se protege el derecho a la privacidad, se deduce que la normativa no tiene rango constitucional, sino que se cuenta con leyes sectoriales que van regulando el tratamiento de datos.

Se cuenta con una garantía constitucional que es la “Acción de Protección de a la Privacidad”, que tiene por objeto la garantía del derecho de toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental de la intimidad y privacidad personal o familiar, o a su propia Imagen, honra y reputación”, regulada por la Ley del Tribunal Constitucional.

Si bien se cuenta con esta garantía constitucional la misma se encuentra con un vacío legal cuando los derechos son afectados y quieren ser accionados por los litigantes.

Resultado del análisis internacional se deduce que existe un enfoque internacional con tendencia a ser armonizada que contempla la aplicación de medidas de seguridad de información en tratamiento de datos personales, que garantizan los derechos a la privacidad.

Las presentes conclusiones deben ser consideradas para la elaboración de una propuesta de Ley de Seguridad de Datos Personales, complementando con los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (ANEXO), ambos documentos deben ser considerados como bases normativas. La Norma legal proyectada puede mejorar los niveles de seguridad en el tratamiento de datos personales y en el derecho a la privacidad en las entidades públicas.

BIBLIOGRAFIA

ALAMO C. y ALAMO H. (2000)<<*Derecho Constitucional e Instituciones Públicas*>>. Ediciones Librería del Profesional, Colombia.

AGUILA G., CAPCHA E. (2005). <<*El ABC del Derecho Civil* >>. EGACAL Escuela de Graduados Aguila & Calderón, Editorial San Marcos, Perú.

ANDER E. (1982)<<*Técnicas de Investigación Social*>>. Editorial Humanitas, Argentina.

ASBUN J. (2001). <<*Derecho Constitucional General*>>. Ediciones UPSA, Bolivia.

CORREA C., BATTO H., CZAR S., NAZAR F. (1994). <<*Derecho Informático*>>. Ediciones DEPALMA, Argentina.

DAVARA M. (1993). <<*Derecho Informático*>>. Editorial Aranzabi, España.

CASTELL M., (1997). <<*La era de la información, economía, sociedad y cultura* >>. Alianza, España.

CASTELL M., (1999). <<*La era de la información, economía, sociedad y cultura* >>. Siglo XXI, México.

CASTELL M., (2009). <<*Comunicación y Poder*>>. Alianza, España.

CASTELL M., (1999). <<*La galaxia internet*>>. Areté, España.

COHEN B., (1985). << Introducción a la Sociología >>. Ediciones Mc. Graw Hill, México.

GARCIA G., (1973). <<*Antología de fuentes del antiguo derecho: Manual de historia del derecho español II*>>. Agesa, España.

GACETA OFICIAL DE BOLIVIA (2002) <<*Constitución Política del Estado* >>. Bolivia

GIL G., (2007). <<*Derecho Informático*>>. Megabyte S.A.C., Perú..

GUERRERO R, TATO N, PROFUMO S. (2010). <<*El Derecho Informático, Aspectos Fundamentales*>>. Recuperado de http://www.nicolastato.com.ar/esp/index.php

MEDINACELI K., (2016). <<El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano>>. Agencia Española de Protección de Datos, España.

MONTANO J., (2012). <<*Teoría utópica de las fuentes del derecho ecuatoriano*>>. Corte Constitucional para el Período de transición, Ecuador.
MOSCOSO J., (1982). <<*Introducción al derecho*>>. Editorial Juventud, Bolivia.

OSORIO M., (2005). <<*Diccionario de Ciencias Jurídicas, Políticas y Sociales*>>.Editorial Heliasta, Guatemala.

OYARTE M., (2007). <<*Fuentes del derecho constitucional: poder constituyente, derechos políticos*>>. Andrade y Asociados, Ecuador.

PERES R., (2009). <<La regulación para el acceso a datos en los registros públicos y privados en Bolivia>>. UMSA, Bolivia.

PUNACELLI O., (1999). <<El Habeas Data en Iberoamérica >>. Temis, Colombia.

RAMOS J., (2009). <<*Teoría Constitucional y Constitucionalismo Boliviano*>>. ABEC, Bolivia.

REMOLINA N, ALVARES L. (2018). << Guía GECTI para la implementación del principio de responsabilidad demostrada —*accountability*— en las transferencias internacionales de datos personales >>. Universidad Los Andes, Colombia

RODRIGUEZ F., (1984). << Introducción a la Metodología de las Investigaciones Sociales >>. Editora Política, Cuba.

SIEGART P., (1983). <<*Legislation and data protection.Proceedings of the Roma Conference on problemns relating tothedevelopmente an aplication of legislation on data protection, Council of Europa*>>, Camera del Deputati, Italia

TRIGO C., (2003). <<*Las Constituciones de Bolivia*>>. Atenea S.R.L., Bolivia.

WEBER M., (1996).<<*The Political and scientific* >>.COYOAC-N, México.

WEBER M., (2009). <<*La política como vocación* >>. Alianza Editorial, Trad. Francisco Rubio LLorente, España

PALADELLA C., (1998). <<*Datos Personales Contenidos en Base de Datos y Registros Electrónicos* >>. Recuperado de www.cenithome/BaseDatos.com.

WEBER M., (2009). <<*La política como vocación* >>. Alianza Editorial, Trad. Francisco Rubio LLorente, España

ANEXO

ESTÁNDARES DE PROTECCIÓN

DE DATOS PERSONALES

RED IBEROAMERICANA DE PROTECCION DE DATOS

ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

En el marco del XV Encuentro Iberoamericano de Protección de Datos, la Red Iberoamericana de Protección de Datos (RIPD o Red) ha aprobado y presentado oficialmente los llamados "Estándares de Protección de Datos de los Estados Iberoamericanos", dando cumplimiento así a un objetivo largamente anhelado por todas las entidades integrantes de la misma, así como a uno de los acuerdos adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada el 28 y 29 de octubre de 2016 en Colombia, relacionado con solicitar a la Red la elaboración de una propuesta para la cooperación efectiva relacionada con la protección de datos personales y privacidad.

El texto ahora aprobado trata de dar respuesta a uno de los ejes de la estrategia acordada por la RIPD en noviembre de 2016 en Montevideo, plasmada en el documento "RIPD 2020", consistente en "impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes".

En este sentido, los Estándares Iberoamericanos se constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes.

Entre los objetivos de los Estándares Iberoamericanos destacan los siguientes:

- Establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región.

- 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 económico y social de la región.

- Favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia.

Como antecedentes directos de estos Estándares, pueden citarse, por un lado, la adopción por la propia RIPD, en 2007, con ocasión del V Encuentro Iberoamericano de Protección de Datos, de las "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana", con las que se pretendió establecer un "marco armonizado" de referencia para las iniciativas regulatorias nacionales que surgieran en la región en materia de protección de datos. Y, por otro, los estándares que fueron aprobados en la Conferencia Internacional de Autoridades de Privacidad y de Protección de Datos, celebrada en Madrid en 2009, los llamados "Estándares de Madrid", que constituyeron, sin duda, un avance en la búsqueda de soluciones y disposiciones específicas "que podrían aplicarse independientemente de las diferencias que puedan existir entre los diferentes modelos existentes de protección de datos y privacidad".

En la elaboración de los Estándares Iberoamericanos también se han tomado como referencia otros instrumentos internacionales y emblemáticos en materia de protección de datos personales como son las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos; el Convenio número 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, entre otros.

El recorrido que se ha seguido para su elaboración, comprende las siguientes etapas:

- Junio, 2016: en el XIV Encuentro Iberoamericano de Protección de Datos, celebrado el 8 de junio de 2016 en Santa Marta, Colombia, se acordó la elaboración de los Estándares Iberoamericanos a cargo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en ese entonces en su calidad de presidente de la Red.

- Noviembre, 2016: en el Seminario de la RIPD en el Centro de la Cooperación Española en Montevideo, celebrado los días 8 y 9 de noviembre en Montevideo, Uruguay, el INAI presentó a los miembros presentes de la Red el anteproyecto de Estándares Iberoamericanos. En dicho seminario, se acordó que durante todo el mes de diciembre de 2016 al anteproyecto de Estándares Iberoamericanos estaría abierto para comentarios y observaciones de los miembros de la Red.

- Mayo, 2017: en el Taller de la RIPD en el Centro de la Cooperación Española en Cartagena de Indias se estudió y debatió, desde el punto de vista técnico, la versión de los Estándares Iberoamericanos que había resultado de todas las aportaciones recibidas durante el mes de diciembre de 2016. En dicho taller participaron las Autoridades miembros de la RIPD, una representación del Supervisor Europeo de Protección de Datos y de la Organización de Estados Americanos, así como, mediante videoconferencia, de la Unidad de Flujos Internacionales de la Comisión Europea.

- Junio, 2017: en el XV Encuentro Iberoamericano de Protección de Datos, celebrado del 20 al 22 de junio de 2017 en Santiago de Chile, se aprobó por unanimidad en la sesión cerrada del Encuentro la versión que resultó de los trabajos realizados durante el taller de Cartagena de Indias, siendo proclamados formalmente en la Sesión Abierta.

Con la aprobación de estos Estándares, la RIPD dispone de una herramienta esencial con la que puede afrontar con rigor el seguimiento y apoyo a los futuros desarrollos legislativos en la Región, debido a que los Estándares Iberoamericanos se caracterizan por ser un modelo normativo que:

- Responde a las necesidades y exigencias nacionales e internacionales que demanda el derecho a la protección de datos personales, en una sociedad donde las tecnologías de la información y del conocimiento cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

- Incluye las mejores prácticas nacionales e internacionales en la materia.

- Propone una serie de estándares tan flexibles que faciliten su adopción entre los Estados Iberoamericanos, sin contravenir de ninguna manera su derecho interno, de tal manera que este documento sea una realidad viva y viable en la región iberoamericana en beneficio del propio titular.

- Garantiza un nivel adecuado de protección de los datos personales en la región iberoamericana, con la finalidad de no establecer barreras a la libre circulación de éstos en los Estados Iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas.

Por otro lado, y no menos importante, los Estándares Iberoamericanos permitirán reforzar la posición de la Red en el ámbito internacional. Para ello, se van a poner en marcha iniciativas en los diversos foros internacionales (Comisión Europea, Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Organización Estados Americanos, etc.), tratando de buscar la mayor difusión posible de los mismos.

En definitiva, el trabajo desplegado por las entidades que integran la RIPD, que ha llevado finalmente a la aprobación de los citados Estándares, constituye una experiencia concreta de cooperación que, a nuestro juicio, puede ser de gran utilidad para otras organizaciones, por lo que quedan a entera disposición de todas las entidades y profesionales que puedan beneficiarse de ellos, en aras de garantizar de la forma más eficaz el posible ejercicio y tutela del derecho a la protección de datos tanto en la región iberoamericana como en un contexto internacional.

Los Estados Iberoamericanos:

(1) Considerando que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental que se encuentra reconocido con rango máximo en la mayoría de las Constituciones Políticas de los Estados Iberoamericanos, bajo la forma del derecho a la protección de datos personales o habeas data, y que en algunos casos ha sido definido jurisprudencialmente por sus Tribunales o Cortes Constitucionales;

(2) Determinando que el derecho a la protección de datos personales se ha conceptualizado en algunos países Iberoamericanos, legislativamente o jurisprudencialmente, como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana;

(3) Asumiendo que salvaguardar el derecho de las personas físicas respecto al tratamiento de sus datos personales es compatible con el objetivo de garantizar y proteger otros derechos, los cuales se reconocen como indivisibles e interdependientes unos con otros, y que requieren de una protección conforme para resguardar en su esfera más amplia a las personas físicas en contra de intrusiones ilegales o arbitrarias, incluso aquellas derivadas del tratamiento de datos personales. Lo anterior, no impide que el derecho a la protección de datos personales resulte aplicable a las personas jurídicas en cumplimiento a lo establecido en el derecho interno de los Estados Iberoamericanos;

(4) Recordando que la Red Iberoamericana de Protección de Datos surgió con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos. Iniciativa que contó desde sus inicios con un apoyo político reflejado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países Iberoamericanos, celebrada en Santa Cruz de la Sierra, Bolivia, el 14 y 15 de noviembre de 2003, conscientes del carácter de la protección de datos personales como un derecho fundamental;

(5) Teniendo en cuenta que con motivo de la Resolución adoptada en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, que tuvo lugar en Cartagena de Indias, Colombia, los días 28 y 29 de octubre de 2016, se reafirmó que la adopción, elaboración e impulso de diversos manuales, programas, iniciativas y proyectos fortalecerían la gestión e impacto de las acciones de cooperación entre los países de Iberoamérica;

(6) Asumiendo que la Red Iberoamericana de Protección de Datos se constituye en un foro permanente de intercambio de información abierto a todos los países miembros de la Comunidad Iberoamericana y que permite el involucramiento de los sectores público, privado y social, con la finalidad de promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático y global;

(7) Recordando que con motivo de la reunión celebrada en Santa Cruz de la Sierra, Bolivia, del 3 a 5 de mayo de 2006, se elaboró el documento denominado Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, el cual establece un conjunto de disposiciones que tienen por objeto contribuir a la elaboración de las iniciativas regulatorias de la protección de datos que surjan en la Comunidad Iberoamericana, constituyéndose como un referente para el desarrollo de los presentes Estándares;

(8) Teniendo en cuenta que la Unión Europea ha adoptado un nuevo marco normativo en la materia, con el objetivo de modernizar sus disposiciones y garantizar mayor solidez y coherencia en la protección efectiva del derecho fundamental a la protección de datos personales en la Unión Europea y con el fin de generar confianza en la sociedad en general y, a su vez, facilitar el desarrollo de la economía digital, tanto en su mercado interior como en sus relaciones globales; marco normativo que se posiciona como un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica;

(9) Reconociendo que existe una falta de armonización en los Estados Iberoamericanos respecto al reconocimiento, adopción, definición y desarrollo de las figuras, principios, derechos y procedimientos que dan contenido al derecho a la protección de datos personales en sus legislaciones nacionales, lo cual, sin duda, dificulta actualmente hacer frente a los nuevos retos y desafíos para la protección de este derecho derivados de la constante y vertiginosa evolución tecnológica y la globalización en diversos ámbitos;

(10) Haciendo apremiante, en el marco de una constante innovación tecnológica, la adopción de instrumentos regulatorios que garanticen, por una parte, la protección de las

personas físicas con relación al tratamiento de sus datos personales y, por la otra, el libre flujo de los datos personales que actualmente constituyen la base para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital, sobre los cuales se erigen las economías de los Estados Iberoamericanos;

(11) Acordando que para garantizar un nivel alto de protección de los derechos y libertades de las personas físicas, entre otras cuestiones, se requiere, a su vez, un nivel uniforme y elevado de protección de las personas físicas con respecto a su información personal que responda a las necesidades y exigencias actuales en un contexto global, con la finalidad de no establecer barreras a la libre circulación de los datos personales en los Estados Iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas;

(12) Aceptando que con el objetivo de ampliar y fortalecer el régimen de protección de las personas físicas respecto al tratamiento de sus datos personales, es imperioso establecer un equilibrio entre los intereses de todos los actores del sector público, privado y social y titulares involucrados, incluyendo el establecimiento de excepciones por cuestiones de interés público que sean razonables y compatibles con los derechos y libertades, para evitar incurrir en restricciones o limitaciones injustificadas o desproporcionadas que no sean acordes con los fines perseguidos en sociedades democráticas;

(13) Estando conscientes acerca de los riesgos potenciales que pueden derivarse en la esfera de las personas físicas con motivo del tratamiento de sus datos personales a gran escala efectuado por parte de organismos públicos y privados y, en particular, teniendo en cuenta la especial vulnerabilidad de las niñas, niños y adolescentes, quienes demandan de garantías adecuadas y suficientes de protección frente a usos indebidos o arbitrarios de su información personal, preservando de esta manera su interés superior, el libre desarrollo de su personalidad, su seguridad y otros valores que son objeto de máxima protección por parte de los Estados Iberoamericanos;

(14) Conviniendo que el desarrollo tecnológico facilita el tratamiento de nuevas categorías de datos personales que presentan riesgos específicos, en particular el uso inadecuado de los mimos; por lo que resulta altamente relevante lograr un consenso mínimo respecto de las categorías de datos personales considerados con el carácter de sensible o especialmente protegidos, así como de las reglas para su tratamiento, teniendo en cuenta que las consecuencias e injerencias negativas que pueden derivarse a partir del uso indebido de este tipo de datos personales pueden generar condiciones injustas o discriminatorias para las personas físicas;

(15) Admitiendo que no todos los Estados Iberoamericanos cuentan con una legislación en la materia, situación que puede provocar afectaciones en el resguardo y tratamiento de la información personal, si se considera el acelerado uso de las tecnologías de la información que facilitan y permiten una comunicación masiva de datos personales de manera inmediata y casi ilimitada;

(16) Estableciendo que las legislaciones en materia de protección de datos personales de los Estados Iberoamericanos deben adoptar los referentes contenidos en los presentes Estándares para contar con un marco regulatorio armonizado que ofrezca un nivel de protección a las personas físicas respecto al tratamiento de sus datos personales y, a su vez, garantizando el desarrollo comercial y económico de la zona;

(17) Admitiendo que actualmente las bases jurídicas que legitiman a todo organismo de carácter público o privado a tratar datos personales en su posesión son el consentimiento del titular; el cumplimiento de una disposición legal; el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente; el ejercicio de facultades propias de las autoridades públicas; el reconocimiento o defensa de los derechos del titular ante una autoridad pública competente; la ejecución de un contrato o precontrato en el que el titular sea parte; el cumplimiento de una obligación legal aplicable al responsable; la protección de intereses vitales del titular o de otra persona física; el interés legítimo del organismo público o privado, o por razones de interés público;

(18) Enfatizando la necesidad que en los Estados Iberoamericanos se traten los datos personales bajo los mismos estándares y reglas homogéneas que ofrezcan a los titulares las mismas garantías de protección, a través del establecimiento de un catálogo de principios de obligado cumplimiento que responda a los actuales estándares nacionales e internacionales en la materia, así como a las exigencias que demanda un efectivo ejercicio y respeto de este derecho fundamental;

(19) Reconociendo que con el propósito de garantizar de manera efectiva el derecho a la protección de datos personales, es preciso adoptar un marco regulatorio que reconozca a cualquier persona física, en su carácter de titular de sus datos personales, la posibilidad de ejercer, por regla general de manera gratuita y excepcionalmente con costos asociados por razones naturales de reproducción, envío, certificación u otras, los derechos de acceso, rectificación, cancelación, oposición y portabilidad, inclusive en el contexto de tratamientos de datos personales efectuados por motores o buscadores de Internet; derechos que complementan las condiciones necesarias para que los titulares ejerzan de manera plena su derecho a la autodeterminación informativa;

(20) Resaltando la importancia y el papel fundamental que desempeñan los prestadores de servicios que tratan datos personales a nombre y por cuenta del responsable, incluyendo aquéllos que prestan servicios de cómputo en la nube y otras materias, lo cual conlleva a los Estados Iberoamericanos a adoptar, en un mundo globalizado, un régimen que les permita regular este tipo de servicios con la finalidad de establecer una serie de garantías para la protección de los datos personales que con motivo de su encargo poseen y tratan, sin eximir al responsable de sus obligaciones y responsabilidades que tiene ante los titulares y las autoridades de control;

(21) Considerando que el desarrollo de las nuevas tecnologías de la información y las comunicaciones así como los servicios desarrollados en el contexto de la economía digital están contribuyendo al crecimiento continuado de los flujos transfronterizos de datos personales en el marco de una sociedad global, es ineludible la obligación de establecer una base mínima que facilite y permita a responsables y encargados, en su calidad de exportadores, la realización de transferencias internacionales de datos personales con pleno respeto a los derechos de los titulares;

(22) Teniendo en cuenta que mediante el Internet es posible acceder y recabar información disponible en cualquier país, así como llevar a cabo un tratamiento de la misma, como recabar datos de millones de personas sin estar físicamente domiciliado allí, circunstancia que no debería constituirse en un factor que impida la efectiva protección de los derechos y libertades de las personas en el ciberespacio;

(23) Reconociendo la importancia de la adopción de medidas preventivas que permitan al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia; la designación de un oficial de protección de datos personales; la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones;

(24) Admitiendo la imperiosa necesidad de que cada Estado Iberoamericano cuente con una autoridad de control independiente e imparcial en sus potestades cuyas decisiones únicamente puedan ser recurribles por el control judicial, ajena a toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales y encargada de vigilar el cumplimiento de la legislación nacional en la materia, la cual esté dotada de recursos humanos y materiales suficientes para garantizar el ejercicio de sus poderes y el desempeño efectivo de sus funciones;

(25) Reconociendo que los Estados Iberoamericanos están obligados a adoptar un régimen que garantice a los titulares una serie de mecanismos y procedimientos para presentar sus reclamaciones ante la autoridad de control cuando consideren vulnerado su derecho a la protección de datos personales, así como para ser indemnizados cuando hubieren sufrido daños y perjuicios como consecuencia de una violación de su derecho;

(26) Destacando la importancia de establecer una base mínima para la cooperación internacional entre las autoridades de control latinoamericanas y entre éstas y las de terceros países, con la finalidad de favorecer y facilitar la aplicación de la legislación en la materia y una protección efectiva de los titulares;

Han convenido en adoptar los presentes Estándares como máxima prioridad en la Comunidad Iberoamericana para que con el carácter de directrices orientadoras contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región de los países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes, favoreciendo la adopción de un marco regulatorio armonizado que ofrezca un nivel adecuado de protección de las personas físicas respecto al tratamiento de sus datos personales y garantizando, a su vez, el desarrollo comercial y económico de la región, al tenor de lo siguiente:

Capítulo I

Disposiciones generales

1. Objeto

1.1 Los presentes Estándares tienen por objeto:

a. Establecer un conjunto de principios y derechos de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.

b. 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.

c. 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.

d. 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.

e. 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.

2. Definiciones

2.1. Para los efectos de los presentes Estándares se entenderá por:

a. Anonimización: la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados.

b. 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.

c. 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.

d. 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.

e. 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.

f. 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.

g. **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.

h. **Titular:** persona física a quien le conciernen los datos personales.

i. **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.

3. Ámbito de aplicación subjetivo

3.1. Los presentes Estándares serán aplicables a las personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones.

4. Ámbito de aplicación objetivo

4.1. Los presentes Estándares serán aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

4.2. Por regla general, los presentes Estándares serán aplicables a los datos personales de personas físicas, lo cual no impide que los Estados Iberoamericanos en su legislación nacional dispongan que la información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales, en cumplimiento a lo establecido en su derecho interno.

4.3. Los Estándares no resultarán aplicables en los siguientes supuestos:

a. Cuando los datos personales estén destinados a actividades exclusivamente en el marco de la vida familiar o doméstica de una persona física, esto es, la utilización de datos personales en un entorno de amistad, parentesco o grupo personal cercano y que no tengan como propósito una divulgación o utilización comercial.

b. La información anónima, es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado.

4.4. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer categorías de datos personales a las cuales no les resulte aplicable el régimen de protección previsto en los presentes Estándares, en cumplimiento de su derecho interno.

5. Ámbito de aplicación territorial

5.1. Los Estándares serán aplicables al tratamiento de datos personales efectuado:

a. Por un responsable o encargado establecido en territorio de los Estados Iberoamericanos.

b. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados Iberoamericanos, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en los Estados Iberoamericanos.

c. Por un responsable o encargado que no esté establecido en un Estado Iberoamericano pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público.

d. Por un responsable o encargado no establecido en territorio de los Estados Iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

5.2. Para los efectos de los presentes Estándares, se entenderá por establecimiento el lugar de la administración central o principal del responsable o encargado, el cual deberá determinarse en función de criterios objetivos e implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento de datos personales que lleve a cabo, a través de modalidades estables.

5.3. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituirán, en sí mismas, un establecimiento principal y no serán considerados como criterios determinantes para la definición del establecimiento principal del responsable o encargado.

5.4. Cuando el tratamiento de datos personales lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo.

6. Excepciones generales al derecho a la protección de datos personales.

6.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá limitar el derecho a la protección de datos para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.

6.2. Las limitaciones y restricciones serán reconocidas de manera expresa en ley, con el propósito de brindar certeza suficiente a los titulares acerca de la naturaleza y alcances de la medida.

6.3. Cualquier ley que tenga como propósito limitar el derecho a la protección de datos personales contendrá, como mínimo, disposiciones relativas a:

a. La finalidad del tratamiento.

b. Las categorías de datos personales de que se trate.

c. El alcance de las limitaciones establecidas.

d. Las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas.

e. La determinación del responsable o responsables.

f. Los plazos de conservación de los datos personales.

g. Los posibles riesgos para los derechos y libertades de los titulares.

h. El derecho de los titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta.

6.4. Las leyes serán las necesarias, adecuadas y proporcionales en una sociedad democrática, y deberán respetar los derechos y las libertades fundamentales de los titulares.

7. Ponderación del derecho a la protección de datos personales

7.1. Los Estados Iberoamericanos podrán exentar, en su derecho interno, el cumplimiento de los principios y derechos previstos en los presentes Estándares, exclusivamente en la medida en que resulte necesario conciliar el derecho a la protección de datos personales con otros derechos y libertades fundamentales.

7.2. Esta exención deberá requerir de un ejercicio de ponderación con la finalidad de determinar la necesidad, idoneidad y proporcionalidad de la restricción o excepción conforme a las reglas y criterios que establezcan los Estados Iberoamericanos en su derecho interno.

8. Tratamiento de datos personales de niñas, niños y adolescentes

8.1. En el tratamiento de datos personales concernientes a niñas, niños y adolescentes, los Estados Iberoamericanos privilegiarán la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral.

8.2. Los Estados Iberoamericanos promoverán en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

9. Tratamiento de datos personales de carácter sensible

9.1. Por regla general, el responsable no podrá tratar datos personales sensibles, salvo que se presente cualquiera de los siguientes supuestos:

a. Los mismos sean estrictamente necesarios para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan su actuación.

b. Se dé cumplimiento a un mandato legal.

c. Se cuente con el consentimiento expreso y por escrito del titular.

d. Sean necesarios por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

9.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones, garantías y condiciones adicionales para asegurar el debido tratamiento de los datos personales sensibles, de conformidad con su derecho interno.

Capítulo II

Principios de protección de datos personales

10. Principios aplicables al tratamiento de datos personales

10.1. En el tratamiento de datos personales, el responsable observará los principios de legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad.

11. Principio de legitimación

11.1. Por regla general, el responsable solo podrá tratar datos personales cuando se presente alguno de los siguientes supuestos:

a. El titular otorgue su consentimiento para una o varias finalidades específicas.

b. El tratamiento sea necesario para el cumplimiento de una orden judicial, resolución o mandato fundado y motivado de autoridad pública competente.

c. El tratamiento sea necesario para el ejercicio de facultades propias de las autoridades públicas o se realice en virtud de una habilitación legal.

d. El tratamiento sea necesario para el reconocimiento o defensa de los derechos del titular ante una autoridad pública.

e. El tratamiento sea necesario para la ejecución de un contrato o precontrato en el que el titular sea parte.

f. El tratamiento sea necesario para el cumplimiento de una obligación legal aplicable al responsable.

g. El tratamiento sea necesario para proteger intereses vitales del titular o de otra persona física.

h. El tratamiento sea necesario por razones de interés público establecidas o previstas en ley.

i. El tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones.

11.2. Tratándose de este último inciso, se entenderá amparado por el interés legítimo el tratamiento de datos personales de contacto que sea imprescindible para la localización de personas físicas que prestan sus servicios al responsable, con la finalidad de mantener cualquier tipo de relación con ésta.

12. Condiciones para el consentimiento

12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

12.2. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.

13. Consentimiento para el tratamiento de datos personales de niñas, niños y adolescentes

13.1. En la obtención del consentimiento de niñas, niños y adolescentes, el responsable obtendrá la autorización del titular de la patria potestad o tutela, conforme a lo dispuesto en las reglas de representación previstas en el derecho interno de los Estados Iberoamericanos, o en su caso, solicitará directamente la autorización del menor de edad si el derecho interno de cada Estado Iberoamericano ha establecido una edad mínima para que lo pueda otorgar directamente y sin representación alguna del titular de la patria potestad o tutela.

13.2. El responsable realizará esfuerzos razonables para verificar que el consentimiento fue otorgado por el titular de la patria potestad o tutela, o bien, por el menor directamente atendiendo a su edad de acuerdo con el derecho interno de cada Estado Iberoamericano, teniendo en cuenta la tecnología disponible.

14. Principio de licitud

14.1. El responsable tratará los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado Iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas.

14.2. El tratamiento de datos personales que realicen las autoridades públicas se sujetará a las facultades o atribuciones que el derecho interno del Estado Iberoamericano de que se trate les confiera expresamente, además de lo previsto en el numeral anterior de los presentes Estándares.

15. Principio de lealtad

15.1. El responsable tratará los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.

15.2. Para los efectos de los presentes Estándares, se considerarán desleales aquellos tratamientos de datos personales que den lugar a una discriminación injusta o arbitraria contra los titulares.

16. Principio de transparencia

16.1. El responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.

16.2. El responsable proporcionará al titular, al menos, la información siguiente:

a. Su identidad y datos de contacto.

b. Las finalidades del tratamiento a que serán sometidos sus datos personales.

c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las finalidades que motivan la realización de las mismas.

d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

e. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular.

16.3. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de niñas, niños y adolescentes.

16.4. Todo responsable contará con políticas transparentes de los tratamientos de datos personales que realice.

17. Principio de finalidad

17.1. Todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.

17.2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

17.3. El tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales.

18. Principio de proporcionalidad

18.1 El responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

19. Principio de calidad

19.1. El responsable adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

19.2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

19.3. En la supresión de los datos personales, el responsable implementará métodos y técnicas orientadas a la eliminación definitiva y segura de éstos.

19.4. Los datos personales únicamente serán conservados durante el plazo necesario para el cumplimiento de las finalidades que justifiquen su tratamiento o aquéllas relacionadas con exigencias legales aplicables al responsable. No obstante, la legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer excepciones respecto al plazo de conservación de los datos personales, con pleno respeto a los derechos y garantías del titular.

20. Principio de responsabilidad

20.1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

20.2. Lo anterior, aplicará cuando los datos personales sean tratados por parte de un encargado a nombre y por cuenta del responsable, así como al momento de realizar transferencias de datos personales.

20.3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:

a. Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.

b. Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.

c. Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.

d. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

e. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

f. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

g. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

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

21. Principio de seguridad

21.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

21.2. Para la determinación de las medidas referidas en el numeral anterior, el responsable considerará los siguientes factores:

a. El riesgo para los derechos y libertades de los titulares, en particular, por el valor potencial cuantitativo y cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

b. El estado de la técnica.

c. Los costos de aplicación.

d. La naturaleza de los datos personales tratados, en especial si se trata de datos personales sensibles.

e. El alcance, contexto y las finalidades del tratamiento.

f. Las transferencias internacionales de datos personales que se realicen o pretendan realizar.

g. El número de titulares.

h. Las posibles consecuencias que se derivarían de una vulneración para los titulares.

i. Las vulneraciones previas ocurridas en el tratamiento de datos personales.

21.3. El responsable llevará a cabo una serie de acciones que garanticen el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora continua de las medidas de seguridad aplicables al tratamiento de los datos personales, de manera periódica.

22. Notificación de vulneraciones a la seguridad de los datos personales

22.1. Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna.

22.2. Lo anterior, no resultará aplicable cuando el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de la vulneración de seguridad ocurrida, o bien, que ésta no represente un riesgo para los derechos y las libertades de los titulares involucrados.

22.3. La notificación que realice el responsable a los titulares afectados estará redactada en un lenguaje claro y sencillo.

22.4. La notificación a que se refieren los numerales anteriores contendrá, al menos, la siguiente información:

a. La naturaleza del incidente.

b. Los datos personales comprometidos.

c. Las acciones correctivas realizadas de forma inmediata.

d. Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus intereses.

e. Los medios disponibles al titular para obtener mayor información al respecto.

22.5. El responsable documentará toda vulneración de seguridad de los datos personales ocurrida en cualquier fase del tratamiento, identificando, de manera enunciativa más no limitativa, la fecha en que ocurrió; el motivo de la vulneración; los hechos relacionados con ella y sus efectos y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad de control.

22.6. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá los efectos de las notificaciones de vulneraciones de seguridad que realice el responsable a la autoridad de control, en lo que se refiere a los procedimientos, forma y condiciones de su intervención, con el propósito del salvaguardar los intereses, derechos y libertades de los titulares afectados.

23. Principio de confidencialidad

23.1. El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular.

Capítulo III

Derechos del titular

24. Derechos ARCO

24.1. En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen.

24.2. El ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro.

25. Derecho de acceso

25.1. El titular tendrá el derecho de solicitar el acceso a sus datos personales que obren en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

26. Derecho de rectificación

26.1. El titular tendrá el derecho a obtener del responsable la rectificación o corrección de sus datos personales, cuando éstos resulten ser inexactos, incompletos o no se encuentren actualizados.

27. Derecho de cancelación

27.1. El titular tendrá derecho a solicitar la cancelación o supresión de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.

28. Derecho de oposición

28.1. El titular podrá oponerse al tratamiento de sus datos personales cuando:

a. Tenga una razón legítima derivada de su situación particular.

b. El tratamiento de sus datos personales tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad.

28.2 Tratándose del inciso anterior, cuando el titular se oponga al tratamiento con fines de mercadotecnia directa, sus datos personales dejarán de ser tratados para dichos fines.

29. Derecho a no ser objeto de decisiones individuales automatizadas

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

29.2. Lo dispuesto en el numeral anterior no resultará aplicable cuando el tratamiento automatizado de datos personales sea necesario para la celebración o la ejecución de un contrato entre el titular y el responsable; esté autorizado por el derecho interno de los Estados Iberoamericanos, o bien, se base en el consentimiento demostrable del titular.

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

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

30. Derecho a la portabilidad de los datos personales

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

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

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

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

31. Derecho a la limitación del tratamiento de los datos personales

31.1. El titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable.

31.2. El titular tendrá derecho a la limitación del tratamiento de sus datos personales cuando éstos sean innecesarios para el responsable, pero los necesite para formular una reclamación.

32. Ejercicio de los derechos ARCO y de portabilidad

32.1. El responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad.

32.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad, así como las causales de improcedencia al ejercicio de los mismos como podrían ser, de manera enunciativa más no limitativa:

a. Cuando el tratamiento sea necesario para el cumplimiento de un objetivo importante de interés público.

b. Cuando el tratamiento sea necesario para el ejercicio de las funciones propias de las autoridades públicas.

c. Cuando el responsable acredite tener motivos legítimos para que el tratamiento prevalezca sobre los intereses, los derechos y las libertades del titular.

d. Cuando el tratamiento sea necesario para el cumplimiento de una disposición legal.

e. Cuando los datos personales sean necesarios para el mantenimiento o cumplimiento de una relación jurídica o contractual.

32.3. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá reconocer que las personas físicas vinculadas a fallecidos o designados por éstos, ejerzan los derechos a que se refiere el presente estándar respecto a los datos personales de fallecidos que les conciernan.

32.4. La legislación nacional de los Estados Iberoamericanos aplicable en la materia reconocerá el derecho que tiene el titular de inconformarse o impugnar las respuestas otorgadas por el responsable ante una solicitud de ejercicio de los derechos aludidos en el presente numeral, o ante la falta de respuesta de éste ante la autoridad de control y, en su caso, ante instancias judiciales de conformidad con el derecho interno de cada Estado Iberoamericano.

Capítulo IV

Encargado

33. Alcance del encargado

33.1. El encargado realizará las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitará sus actuaciones a los términos fijados por el responsable.

34. Formalización de la prestación de servicios del encargado

34.1. La prestación de servicios entre el responsable y encargado se formalizará mediante la suscripción de un contrato o cualquier otro instrumento jurídico que consideren los Estados Iberoamericanos en la legislación nacional aplicable en la materia.

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

34.3. El contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

a. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.

b. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.

c. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

d. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

e. Guardar confidencialidad respecto de los datos personales tratados.

f. Suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado.

g. Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.

h. Permitir al responsable o autoridad de control inspecciones y verificaciones en sitio.

i. Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.

j. Colaborar con el responsable en todo lo relativo al cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

34.4. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el alcance, contenido, medios y demás cuestiones del tratamiento de los datos personales asumirá la calidad de responsable, conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

35. Subcontratación de servicios

35.1. El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el encargado.

35.2. El subcontratado asumirá el carácter de encargado en los términos que estipulen la legislación nacional del Estado Iberoamericano aplicable en la materia.

35.3. El encargado formalizará la prestación de servicios del subcontratado a través de un contrato o cualquier otro instrumento jurídico que determine la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

35.4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a cabo conforme a lo instruido por el encargado, asumirá la calidad de responsable conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

Capítulo V

Transferencias internacionales de datos personales

36. Reglas generales para las transferencias de datos personales

36.1. El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

a. El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de éste que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.

b. El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado Iberoamericano aplicable en la materia.

c. El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados Iberoamericanos aplicable en la materia.

d. El exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando éste sea acorde con las disposiciones previstas en la legislación nacional del Estado Iberoamericano aplicable en la materia, que está obligado a observar el exportador.

e. La autoridad de control del Estado Iberoamericano del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

36.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

Capítulo VI

Medidas proactivas en el tratamiento de datos personales

37. Reconocimiento de medidas proactivas

37.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá reconocer y establecer medidas que promuevan el mejor cumplimiento de su legislación y coadyuven a fortalecer y elevar los controles de protección de datos personales implementados por el responsable, entre las cuales podrán encontrase las que a continuación se indican en el presente Capítulo.

38. Privacidad por diseño y privacidad por defecto

38.1. El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable.

38.2. El responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable. Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos, sin la intervención del titular, a un número indeterminado de personas.

39. Oficial de protección de datos personales

39.1. El responsable designará a un oficial de protección de datos personales o figura equivalente en los casos que establezca la legislación nacional de los Estados Iberoamericanos aplicable en la materia y cuando:

a. Sea una autoridad pública.

b. Lleve a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular.

c. Realice tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, entre otros factores y de manera enunciativa más no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos.

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

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

39.4. El oficial de protección de datos personales tendrá, al menos, las siguientes funciones:

a. Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.

b. Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

c. Supervisar al interior de la organización del responsable el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

40. Mecanismos de autorregulación

40.1. El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia y establecer procedimientos de resolución de conflictos entre el responsable y titular sin perjuicio de otros mecanismos que establezca la legislación nacional de la materia aplicable, teniendo en cuenta las características específicas de los tratamientos de datos personales realizados, así como el efectivo ejercicio y respeto de los derechos del titular.

40.2. Para los efectos del numeral anterior, se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza que coadyuven a contribuir a los objetivos señalados en el presente numeral.

40.3. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá las reglas que correspondan para la validación, confirmación o reconocimiento de los mecanismos de autorregulación aludidos.

41. Evaluación de impacto a la protección de datos personales

41.1. Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales.

41.2. La legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia señalará los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de éstas, los supuestos en que resulte procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación, entre otras cuestiones.

Capítulo VII

Autoridades de control

42. Naturaleza de las autoridades de control y supervisión

42.1. En cada Estado Iberoamericano deberá existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia.

42.2 Las autoridades de control podrán ser órganos unipersonales o pluripersonales; actuarán con carácter imparcial e independiente en sus potestades, así como serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna.

42.3. El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Se nombrarán mediante un procedimiento transparente en virtud de la legislación nacional aplicable y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado Iberoamericano, conforme a las reglas del debido proceso.

42.4. La legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

42.5. Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia y su derecho interno.

42.6. Las autoridades de control deberán contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

Capítulo VIII

Reclamaciones y Sanciones

43. Régimen de reclamaciones y de imposición de sanciones

43.1. Todo titular tendrá derecho a presentar su reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

43.2. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá un régimen que permita al titular presentar una reclamación ante la autoridad de control cuando considere que el tratamiento de sus datos personales infringe la normativa nacional en la materia, así como a solicitar la tutela judicial.

43.3. La legislación nacional de los Estados Iberoamericanos aplicable en la materia establecerá un régimen que permita la adopción de medidas correctivas y sancionar las conductas que contravengan lo dispuesto en las legislaciones nacionales correspondientes, indicando, al menos, el límite máximo y los criterios objetivos para fijar las correspondientes sanciones, a partir de la naturaleza, gravedad, duración de la infracción y sus consecuencias, así como las medidas implementadas por el responsable para garantizar el cumplimiento de sus obligaciones en la materia.

Capítulo IX

Derecho de indemnización

44. Reparación del daño

44.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia reconocerá el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de su derecho a la protección de datos personales.

44.2. El derecho interno de los Estados Iberoamericanos señalará la autoridad competente para conocer de este tipo de acciones interpuestas por el titular afectado, así como los plazos, requerimientos y términos a través de los cuales será indemnizado éste, en caso de resultar procedente.

Capítulo X

Cooperación internacional

45. Establecimiento de mecanismos de cooperación internacional

45.1. Los Estados Iberoamericanos podrán adoptar mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales aplicables en la materia, los cuales podrán comprender, de manera enunciativa más no limitativa:

a. El establecimiento de mecanismos que permitan reforzar la asistencia y cooperación internacional en la aplicación de las respectivas legislaciones nacionales en la materia.

b. La asistencia entre las autoridades de control a través de la notificación y remisión de reclamaciones, la asistencia en investigaciones y el intercambio de información.

c. La adopción de mecanismos orientados al conocimiento e intercambio de mejores prácticas y experiencias en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.