UNIVERSIDAD AUTÓNOMA JUAN MISAEL SARACHO
Secretaría de Educación Continua

Departamento de Posgrado

Tesis de Maestría

“PROPUESTA DE IMPLEMENTACIÓN DE UNA LEY DE PROTECCIÓN DE DATOS PERSONALES”

RONALD RAMIRO SÁNCHEZ GONZALES

Tesis de Maestría, presentada a consideración de la Universidad Autónoma Juan Misael Saracho, como requisito para optar el título de Master en Derecho Constitucional, Procedimiento Constitucional y Derechos Humanos.

Tarija –Bolivia

Hoja de aprobación.

Tesis de Maestría

“Propuesta de implementación de una Ley de Protección de datos personales”

Postulante:

RONALD RAMIRO SÁNCHEZ GONZALES

Tribunal Calificador:

Nombres y Apellidos Tribunal

Nombres y Apellidos Tribunal

Tarija, …… de ……. de …….

Hoja de advertencia.

El Tribunal Calificador del presente trabajo de Maestría no se solidariza ni responsabiliza con la forma, términos, modos y expresiones vertidas en el mismo, siendo esta responsabilidad del autor.

ÍNDICE DE TABLAS Y FIGURAS.

Resumen

La presente investigación nace a raíz de una imperiosa necesidad de contar con una norma especial que pueda tutelar el derecho a la Protección de los datos personales; es bueno saber que, si bien la Corte Interamericana de Derechos Humanos tutela y exhorta a los Estados miembros a uniformizar los criterios de protección y poder elaborar normas especiales de protección, es el Estado boliviano como parte del sistema interamericano, que no tiene una norma específica.

Así también la investigación permitirá demostrar la necesidad de crear una norma de protección de los datos personales, con el objeto de evitar la injerencia de terceros que hagan mal uso de estos datos**;** asimismo, llegaremos a evidenciar que los instrumentos internacionales de varios Sistemas de protección de Derechos Humanos, incluso de aquellos de los cuales Bolivia no es parte, han desarrollado criterios altos de protección, por tanto la creación de una norma que regule y evite el acceso arbitrario e irrespetuoso de los datos personales, no vulnera el derecho a la libertad de pensamiento, de expresión, mucho menos el derecho al acceso de la información.

Así va a contrastar que la implementación de una Ley de Protección de Datos personales, no se encuadra en la prohibición estipulada por la censura previa estipulada en la Convención Americana sobre los Derechos Humanos.

Para sostener los juicios antes nombrados, vamos a proceder a exponer las posiciones jurisprudenciales y doctrinarias de los diferentes sistemas de protección de Derechos Humanos que se ha manifestado sobre el tema, haciendo un especial énfasis en el Sistema Interamericano seguido del Sistema Europeo.

ÍNDICE

CAPÍTULO I

INTRODUCCIÓN

1.1. Antecedentes.

Las nuevas tecnologías de la información y de las comunicaciones actúan como una incitación al crecimiento de nuestra sociedad de la información, y para no estancarnos, debemos responder garantizando el equilibrio entre el derecho a la información y el derecho a la intimidad de las personas.

Toynbee sostiene que “el progreso de una civilización consiste en un proceso de superación de obstáculos materiales que permiten que las energías de la sociedad den respuesta a incitaciones que son internas antes que externas y espirituales antes que materiales”[1]. El derecho a la intimidad es una necesidad interna y espiritual de las personas, que opera ante la adversidad del mundo civilizado de nuestro tiempo. Responder con éxito a esta incitación o fracasar en la respuesta, será un indicador del crecimiento o estancamiento de nuestra civilización.

La información siempre fue valiosa, pero las nuevas tecnologías de la información y de las comunicaciones le dan hoy una nueva dimensión, un nuevo valor que antes no tenía porque no existía la posibilidad de convertir datos parciales y dispersos, en información de masas, científicamente organizada.

Hoy el poder está en la información y el conocimiento. Por ello el sistema jurídico debe ejercer un control adecuado que garantice la seguridad jurídica que todo Estado de derecho debe tener, sin descuidar la protección de los derechos humanos a todos sus habitantes.

---

[1]Toynbee, Arnold. Estudio de la Historia . Madrid: Alianza Editorial, 1991. Pàg. 106

Con la finalidad de alcanzar el bienestar general de la población, el Estado interviene en ciertos sectores de la estructura social, se relaciona con los administrados y participa de una nueva economía basada en el conocimiento. A tales efectos, los gobiernos almacenan y clasifican datos personales, los valoran y los utilizan en su accionar político y administrativo cotidiano. Los sistemas informáticos actuales tienen una gran capacidad y velocidad de almacenamiento de datos personales. Sin embargo, junto a estos importantes avances aportados por la tecnología informática, también surgen serias amenazas para los derechos y libertades de los individuos. Estos riesgos son especialmente peligrosos en el caso de la intimidad.

La sociedad tecnológicamente desarrollada cuenta con los medios para registrar la formación escolar y universitaria, las operaciones financieras, la trayectoria profesional, los hábitos de vida, el historial clínico, las creencias religiosas, políticas o gremiales de las personas, en archivos capaces de ser cruzados en una red general de información. Las personas van dejando tras su trabajo, su ocio, o los servicios de los que se sirven, innumerables datos acerca de su personalidad. En cada ocasión en la que proporcionan su filiación, domicilio, experiencia profesional, datos bancarios o antecedentes médicos, contribuyen a engrosar los archivos automatizados de datos que van aumentando el volumen de información, en directa proporción a la disminución del grado de reserva o intimidad de sus vidas privadas.

1.2. Descripción del Problema.

Las nuevas tecnologías de la información y de las comunicaciones actúan como una incitación al crecimiento de nuestra sociedad, de la información y para no estancarnos, debemos responder garantizando el equilibrio entre el derecho a la información y el derecho a la intimidad de las personas.

El sistema jurídico boliviano debe ejercer un control adecuado que garantice la seguridad jurídica que todo Estado de derecho debe tener, sin descuidar la protección de los derechos humanos a todos sus habitantes.

1.3. Planteamiento del Problema.

¿Cómo proteger los datos personales de la injerencia realizada por terceros?

1.4. Justificación del Problema

El uso indebido de los datos personales ha dado lugar a la vulneración de la privacidad, vida privada, dignidad, honra y honor de las personas, derechos resguardados por nuestra Constitución Política del Estado y por los instrumentos internacionales emitidos por diversos Organismos de protección.

Ante esta situación nace la necesidad de implementar una norma especial que regule el acceso a los datos personales, de esta forma lograremos el ejercicio efectivo del Derecho a la Protección de los datos personales, como derecho autónomo, fundamental y progresivo, tal cual establecen los estándares de protección internacionales.

En todo caso la norma específica que regule la protección y acceso a los datos personales, debe ser sometida a un Control de Convencionalidad, requisito imperante establecido por la misma C.P.E en su art 13 núm. IV concordante con el Art. 256 de la misma norma supra legal.

1.5. Objetivos:

1.5.1 Objetivo General

- Formular una Propuesta de Ley que proteja los datos personales, de la injerencia de terceros.

1.5.2 Objetivos Específicos

- Demostrar que los instrumentos internacionales, resguardan el derecho a la protección de los datos Personales.
- Evidenciar que la normativa local, es insuficiente para la protección de los datos personales.
- Comprobar que la protección de los datos personales, no vulnera el derecho al libre acceso de la información.

1.6. Hipótesis.

Una norma específica de protección de datos personales, permitirá proteger los mismos de la injerencia y acceso arbitrario e irrespetuoso de terceros.

CAPÍTULO II

MARCO TEÓRICO

2.1. Intimidad.

Es una situación jurídica en la que se tutela el espacio individual y familiar de privacidad de la persona, conformados por experiencias pasadas, situaciones actuales, características físicas y psíquicas no ostensibles y, en general, todos aquellos datos que el individuo desea que no sean conocidos por los demás, porque de serlo, sin su consentimiento, le ocasionarían incomodidad y fastidio[2].

Ahora bien, es necesario citar los razonamientos del prestigioso profesor José Ángel Camisón Yagüe, en su artículo denominado "*Los derechos civiles y políticos en la Constitución boliviana"*, publicado por la revista Derecho del Estado Nº 28, dice:

"Derecho a la privacidad y a la intimidad. Según define la Real Academia Española de la Lengua, la privacidad es aquel ámbito de la vida que se tiene derecho a proteger de cualquier intromisión. La intimidad, por su parte, hace referencia aquella zona espiritual íntima y reservada de una persona. Ambos conceptos están, por tanto, íntimamente relacionados entre sí, por ello procede abordar su estudio conjuntamente"

"El derecho a la intimidad y derecho a la privacidad aparecen formulados por primera vez en el año 1890 por Warren y Bandeis bajo la denominación de righttoprivacy. Estos derechos surgen,

---

[2] ESPINOZA ESPINOZA, Juan "Derecho de las Personas" Lima: Editorial Grijley, 5ta Edición, 2012. Página 526, citado en: Tarrillo Monteza, Daniel. Publicidad Registral y Derecho a la Intimidad. Lima: Pontificia Universidad Católica del Perú (disponible en: http://tesis.pucp.edu.pe/repositorio/handle/123456789/5003), 2013

fundamentalmente, como una reacción frente a la aparición de los grandes medios de comunicación de masas y ciertos avances científicos como la fotografía, que multiplican exponencialmente la posibilidad y los riesgos de interferencia en la intimidad y privacidad personal. De tal forma que el dato íntimo que anteriormente sólo podía llegar a ser conocido por unos pocos, puede ser ahora potencialmente conocido por todos"

Originalmente estos derechos se configuraban de forma muy básica, pues se entendían como el derecho del individuo a estar solo y a no ser molestado. Hoy en día resulta complejo alcanzar una definición clara y unánime de su contenido, sin embargo, sí es posible establecer ciertos parámetros básicos de lo que se entiende desde el punto de vista jurídico por derecho a la intimidad y a la privacidad. Se afirma, así, que ambos derechos protegen un ámbito o reducto de la vida vedado a la entrada de los otros, es decir, que a través de ellos se reconoce una esfera personal propia, reservada y, en principio, intangible a la acción y el conocimiento de los demás y, en su caso, del Estado, con el objeto de posibilitar al individuo el mantenimiento de una mínima calidad de vida y de su dignidad personal.

No obstante, lo anterior, debemos tener en cuenta que esa esfera íntima se determina y delimita por el propio sujeto, lo que se traduce en que cada uno de los individuos será quien establezca personalmente cuál es el ámbito de su vida privada que sustrae al conocimiento público, y cuál es el ámbito íntimo que puede ser conocido públicamente. Por ello, si existe consentimiento del individuo para que los demás penetren en ese espacio propio o en una parcela del mismo, se produce entonces una renuncia voluntaria, bien parcial o bien total a su intimidad y privacidad. Intimidad y privacidad son, por tanto, derechos revocables en parte o en toda su

extensión. Es preciso matizar en este punto, que una renuncia parcial de la intimidad no constituye un título habilitante para que sobre la misma se consideren legítimas otras intrusiones en aquellos ámbitos privados que el sujeto no ha querido que fueran conocidos. (2012:81,92)

En un análisis propio puedo decir que la misma CPE en su Art. 25 último parágrafo, taxativamente prohíbe la colocación de aparatos de escucha, prohíbe la utilización de esa información dentro un proceso penal, tachando esa prueba como ilegalmente obtenida. En ese entendido queda clara la prohibición de fotografiar, filmar o reproducir la vida íntima de una persona, este accionar constituirá una violación flagrante a la privacidad, aunque no se divulgue o amplifique la información.

A criterio del suscrito, la sola obtención de la información privada sin consentimiento del titular, es también una transgresión a su derecho, aun esa información haya sido dada de plena voluntad del titular, sin el consentimiento para su divulgación constituye igual una vulneración del derecho.

Obvio también hay una exención, en el caso que las imágenes se hayan tomado en vía pública, es el caso de cámaras de seguridad de lugares de uso común como plazas y calles, así también cuando sea necesario para la averiguación de la verdad histórica de los hechos, en caso investigación penal.

2.2. Dato Personal.

Un dato contiene información que puede ser de carácter estadístico, financiero, demográfico, entre otros. Cuando se habla de datos personales, nos estamos refiriendo a datos que contienen información sobre o relativos a una persona. De esta manera, un dato personal es igual a la información sobre

una persona. Algunos ejemplos bastante conocidos son el nombre, la dirección, el teléfono, el correo electrónico y hasta el historial médico y los antecedentes penales. Estos datos nos dan información sobre una persona en particular. (Access Now ;2019)

Ahora bien, la doctrina legal profundizó este concepto y actualmente no sólo son datos personales las informaciones que identifican a una persona directamente sino también aquellas que la hacen identificable tras un análisis posterior. Esto último quiere decir que hay informaciones que indirectamente se relacionan a una persona y que de igual manera las vamos a considerar datos personales. (Access Now ;2019)

Ejemplo de esto son las imágenes de las cámaras de videovigilancia o la ubicación GPS. Toda esta información es clave y revela detalles íntimos sobre la vida personal y familiar. A nivel social, muestra tendencias que pueden permitir el estudio y de comportamientos colectivos. Por eso entender qué tipos de datos existen y cómo protegerlos es esencial para la vida democrática en un marco de creciente digitalización. (Access Now ;2019)

2.3. Tipos de datos personales.

Access Now, organización internacional de derechos humanos en internet en colaboración con InternetBolivia.org, organización boliviana dedicada a la defensa y promoción de los derechos humanos en contextos digitales, en su Guía Básica sobre Datos Personales para Bolivia (2019), (Access Now ;2019) señala:

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

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

Datos anonimizados o disociados: Existen también otros tipos de datos que, por la forma en la que son obtenidos o procesados, reciben otras denominaciones. En este grupo tenemos a los datos anónimos y anonimizados o disociados. Estos son datos que en principio permiten identificar a personas pero que gracias a mecanismos de anonimización o disociación terminan teniendo poca o nula relación con la persona que antes identificaban.

Estos procesos son utilizados por ejemplo en investigaciones científicas donde, con el fin de proteger la identidad de las personas que participaron en el estudio, se elimina de los conjuntos de datos personales la información que permita la identificación. Sin embargo, esta práctica no quita que los principios de protección de los datos personales, que veremos más adelante, deban ser aplicados, en especial el de minimización de la recolección y análisis de datos; ya que existen procedimientos técnicos para revertir la anonimización y volver a identificar a las personas, en algunos casos. Los metadatos: Estos son los llamados “datos sobre los datos”, puesto que son aquellos que se obtienen al analizar otros conjuntos de datos.

Esto incluye, por ejemplo, algunos datos de navegación en internet e información sobre comunicaciones entre personas (a qué hora se mandó un SMS, en qué ubicación GPS se tomó una foto, etc). Si bien estos datos por sí solos no identifican a una persona, un análisis conjunto de los mismos sí podría hacerlo ya que nos brinda información importante y detallada sobre una persona. Por ejemplo, las redes sociales generan registros de visitas, reacciones (likes), compras en línea, entre otros. Al analizar y estudiar estos

datos podemos conocer los gustos y preferencias de los usuarios de esas redes sociales; deducir dónde viven, trabajan, van de vacaciones y quiénes son sus familiares y amigos.

2.4. Importancia de la protección de datos personales.

En el año 2019, Access Now, organización internacional de derechos humanos en internet en colaboración con InternetBolivia.org., organización boliviana dedicada a la defensa y promoción de los derechos humanos en contextos digitales, estableció: “Como la tecnología avanza y cada vez estamos más interconectados, las leyes suelen quedar desactualizadas. La Unión Europea entendió esta situación y emitió un Reglamento General de Protección de Datos Personales (“RGPD” en adelante) que cuenta con nuevas y más sofisticadas herramientas para garantizar un uso adecuado de los datos personales más allá de los límites geográficos, porque la atención primordial está puesta en el interés y los derechos de los usuarios”

“La entrada en vigor de este reglamento en mayo de 2018 generó expectativas y dudas. De la noche a la mañana, empresas de todo el mundo pusieron sus ojos en el cumplimiento del RGPD. De la misma manera, otros Estados fuera de la Unión Europea empezaron a analizar si sus marcos normativos estaban a la altura de los desafíos que impone la tecnología actual. Inclusive aquellos países que aún no cuentan con una ley de datos personales comenzaron a dialogar con mayor seriedad sobre la necesidad de contar con una” (Access Now ;2019)

2.5. Antecedentes de vulneración en el acceso a datos personales.

La Guía Básica Protección de Datos Bolivia, ha citado una serie de antecedentes ocurridos en Latinoamérica, donde resalta que últimamente en Bolivia como parte del proceso de elecciones primarias para habilitar binomios de candidatos a presidencia y vicepresidencia se han conocido denuncias de personas que han encontrado su nombre como militantes en el padrón de un

partido político donde no militan. ¿Cómo llegó ese nombre al padrón de cada partido? (Access Now ;2019)

Argentina de infiltrados en la administración pública que tenían acceso a datos personales y que gracias a una aplicación lograron vender la información a terceros.

Brasil, donde un ente de la propia administración pública vendía bases de datos de una oficina de gobierno que contenían: nombre completo, número de identificación, fecha de nacimiento, sexo, nombre de la madre y dirección, entre otros.

Perú donde, desde el 2015 hasta el 2018 se podía descargar la foto, nombre completo, dirección, sexo, estado civil, grupo de votación y datos sobre donación de órganos sin levantar ninguna alerta en el sistema del registro nacional de identificación de ese país.

Chile se reportó una filtración de más de 14 mil datos sensibles de tarjetas de crédito y débito.

México, una empresa de telemedicina habría dejado expuestos los datos personales sobre la salud de 2.373.764 personas, un daño tan grave que la Autoridad de datos personales estaba considerando una multa de más de 1 millón de dólares estadounidenses. Adicionalmente, se han reportado casos de venta de bases de datos por parte de particulares.

Perú, un noticiero reportó la venta, en plena calle, de bases de datos de empresas telefónicas y bancos a un precio de 60 dólares estadounidenses. La falta de fiscalización hace que esto sea posible. Esta situación es aún peor en países donde ni siquiera hay ley de protección de datos que permita fiscalizar estos negocios.

2.6. Derecho a la Protección de los Datos Personales.

Como aporte personal a esta investigación es menester mencionar que los derechos fundamentales están dirigidos a dar tutela a la persona, como titular de derechos y obligaciones y no los datos personales, pues estos últimos sirven para individualizar a las personas, ahí es necesario hablar de los que los Abogados conocemos como autoderminación informativa, es decir saber cómo se está utilizando nuestra información, es más podemos tener un autocontrol de nuestros datos personales, este control se efectúa a través del consentimiento, que toda persona otorga a un tercero para que utilice sus datos personales. El Estado como sujeto de Derechos está obligado a brindar protección a los datos personales, debe cumplir el mandato constitucional de proteger la privacidad y la intimidad de las personas a esto se suma los instrumentos internacionales que tutelan también privacidad y la intimidad de las personas, en su protección multinivel.

La protección de datos personales, es un derecho fundamental relativamente nuevo, y configurado a partir de las concepciones que se tienen de la vida privada o intimidad, del derecho al honor y del derecho a la propia imagen[3].

A criterio personal la evolución de estos derechos, principalmente el de la vida privada, han planteado nuevas situaciones que serán motivo de la creación de un nuevo derecho: la protección de datos personales. El estudio de este derecho se sitúa en el campo de los derechos fundamentales, por ello es importante comprender su nueva inclusión dentro del catálogo de los mismos,

4 El derecho al honor y a la propia imagen, como la protección de datos personales, son derechos independientes entre sí, sin embargo, y como ocurre con otros derechos, se relacionan entre sí, principalmente con el derecho a la vida privada. Desde una perspectiva se podría decir que el derecho a la privacidad es el género, mientras que los otros son la especie –cada uno en su propio ámbito de aplicación–. Lo anterior, ya que la vulneración de alguno afecta directamente la vida privada de la persona. Pero hay que recordar, que en el caso particular del derecho a la protección de datos personales, comprende el control por parte de la persona de su información personal, que puede o no, ser privada.

como un derecho nuevo, ya sea como derecho a la protección de datos personales o como autodeterminación informativa.

De acuerdo con la Sentencia Nº 290/2000 del Tribunal Constitucional Español, define al derecho fundamental a la Protección de Datos Personales: “Como aquel que garantiza a la persona un poder de control y disposición sobre sus datos personales. Dicho derecho confiere a su titular un haz de facultades que son elementos esenciales del derecho de PDP, integrado por la facultad que corresponde al afectado de consentir la recogida y el uso de sus datos personales, así como a conocer los mismos. Para hacer efectivo ese contenido, es incluido también, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a esa.

La Guía Básica Protección de Datos Bolivia, ha establecido los siguientes derechos (Access Now ;2019):

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

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

Derecho a la rectificación: Este derecho fue pensado en consonancia a otro principio que es el de exactitud y del que hablaremos más adelante. Los datos que se manejen deben ser exactos, por lo tanto, se nos da la posibilidad de corregir y actualizar los datos personales que estén almacenados en bases de

datos. Por ejemplo, podríamos querer actualizar nuestro estado civil o el registro de deudas que figura en servicios de información crediticia. Derecho a revocar el consentimiento o cancelación: Como comentamos líneas arriba, una de las expresiones base de la protección de los datos personales es el consentimiento. Así como damos nuestro consentimiento para que nuestros datos sean tratados, también podemos retirar dicho consentimiento cuando el tratamiento sea excesivo, no pertinente, inadecuado, entre otros. Ello significa que el responsable del tratamiento deberá dejar de tratar nuestros datos personales.

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

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

Derecho a la portabilidad: Este es un nuevo derecho que se incluyó recientemente en el RGPD. Según este derecho, tenemos el poder movilizar nuestros datos personales de una base de datos a otra. Ello puede implicar solicitar al responsable del tratamiento una copia o el original de toda nuestra información en un formato compatible que permita trasladarla a otro proveedor de servicios. En algunos casos también puede pedirse que el responsable del tratamiento de datos haga ese traslado por nosotros. Por ejemplo, se podría

solicitar a un banco que mueva todos nuestros datos a otro banco. Así, no perderíamos historial de nuestros movimientos financieros, ni de los créditos que obtuvimos.

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

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

2.7. Principios Rectores.

Los principios son fundamentos y límites básicos que se mantienen en el tiempo. (Access Now ;2019)

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

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

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

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

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

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

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

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

CAPÍTULO III

PRIVACIDAD, VIDA PRIVADA Y DATOS PERSONALES

3.1. Vida privada y protección de datos personales

Definir el derecho a la vida privada no es una tarea fácil. De hecho, existe pleno consenso entre los tribunales internacionales de derechos humanos en el sentido de que se trata de un concepto amplio, no susceptible de definiciones exhaustivas, y cuyo contenido es más extenso que el del derecho a la privacidad (C. F. CIDH 2010). De tal forma que se reconoce que el derecho a la vida privada y la privacidad no son sinónimos, a pesar de que el primero tiene un alcance mucho mayor que, en consecuencia, comprende al segundo.

Si bien la delimitación entre ambos excede los alcances de este trabajo, nos centraremos exclusivamente en el análisis del derecho de la vida privada (en el entendido de que la privacidad es parte de la misma), en relación con el derecho a la protección de los datos personales (Gayo s.f.).

3.2. Reconocimiento en Convenios y otros Instrumentos Internacionales

El derecho a la vida privada ha sido consagrado como un derecho humano tanto en el Sistema Universal de Derechos Humanos como en los sistemas regionales (específicamente en los sistemas europeo e interamericano).

Por lo que hace al Sistema Universal, esto es, con un alcance global, la Declaración Universal de los Derechos Humanos de 1948 (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos de 1966 (artículo 17), la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares de 1990 (artículo 14) y la Convención sobre los Derechos del Niño de 1989 (artículo 16), lo contemplan prácticamente en los mismos términos. Asimismo, el derecho a la vida privada

goza de un reconocimiento expreso tanto en el ámbito interamericano, mediante el artículo 11.2 de la Convención Americana sobre Derechos Humanos (Pacto de San José), como en el ámbito europeo, por medio del Convenio para la Protección de los Derechos y Libertades Fundamentales (también llamado Convención Europea de Derechos Humanos) en su artículo 8.

Cuestión distinta ocurre por lo que hace al derecho a la protección de datos personales, toda vez que estos instrumentos internacionales carecen de una referencia expresa al mismo. De hecho, en 1980, la Asamblea Parlamentaria del Consejo de Europa recomendó al Comité de Ministros, que a la vista de la aproximación que estaban adoptando varios Estados miembros de la actual Unión Europea en cuanto a legislar en materia de protección de datos personales, estudiase la posibilidad de incluir en la Convención Europea de Derechos Humanos una referencia al mismo, idea que fue rechazada por "no ser el momento adecuado" para ello, debido a la falta de experiencia en la materia y los avances hacia la aprobación del llamado Convenio 108 que, por entonces, era un borrador muy avanzado, en cuanto al derecho a la protección de datos personales.

Otros convenios e instrumentos internacionales, fundamentalmente regionales y con un alcance limitado por estar dirigidos solo a ciertos países, contemplan expresamente el derecho a la protección de datos personales y establecen en su texto una relación estrecha con el derecho a la privacidad. Al respecto es posible mencionar las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre protección de la privacidad y flujos transfronterizos de datos, adoptadas inicialmente en 1980 y actualizadas en el 2013. De acuerdo con las mismas, estas "suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal".

Su objetivo, si bien recoge los principios que informan la protección de datos personales, consiste en adoptar estándares mínimos para garantizar la

privacidad, ello a pesar de que carece de un carácter vinculante. De tal forma que en este documento la protección de datos personales adquiere un carácter instrumental para dotar de efectividad el derecho a la privacidad.

Asimismo, el Convenio (108) del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto del tratamiento automatizado de datos de carácter personal, establece en su artículo 1° que tiene por objeto proteger "a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, respecto del tratamiento automatizado de los datos personales correspondientes a dicha persona ("protección de datos")". Se trata de un instrumento vinculante, abierto incluso a la firma o ratificación por Estados que no son parte del Consejo de Europa, siempre que se cumplan con los requisitos que el propio Convenio 108 establece.

Ahora bien, será en el marco de la Unión Europea donde el derecho a la protección de los datos personales encuentra su máximo desarrollo normativo. Acerca del particular resulta interesante mencionar la Directiva 95/46/CE, misma que establece en su Considerando 10 que "las legislaciones nacionales relativas al tratamiento de datos personales tienen por objeto garantizar el respeto de los derechos y libertades fundamentales, particularmente del derecho al respeto de la vida privada reconocido en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, así como en los principios generales del Derecho comunitario".

Si bien el 27 de abril de 2016 se adoptó el Reglamento General de Protección de Datos que substituye a la Directiva 95/46/CE, el mismo sigue en la misma línea, con una aplicación directa para evitar divergencias entre los Estados miembros de la Unión Europea.

En un paso histórico para la protección de los datos personales en su calidad de derecho al más alto nivel normativo, se recoge expresamente tanto en el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) como en la Carta de los Derechos Fundamentales de la Unión Europea. Esta última lo contempla, en su Artículo 8, de manera separada del derecho a la vida privada (previsto en el artículo 7 de la propia Carta). Es así que se establece de manera específica su autonomía, sin perjuicio de la relación que se establezca entre ambos derechos.

Es esencial decir que el artículo 8 de la citada Carta de los Derechos Fundamentales establece que el tratamiento de los datos personales tiene que realizarse conforme a unos criterios o principios que lo legitimen y que deberá existir una autoridad de control independiente que se encargue de supervisar el respeto de las normas acerca de la materia.

Así, de conformidad con lo anterior, puede decirse que el derecho a la protección de datos personales se ha desarrollado fundamentalmente en el ámbito europeo.

Se consagra por primera vez en el Convenio 108 del Consejo de Europa, seguido por la Directiva 95/46/CE de la Unión Europea, como una proyección o faceta del derecho a la vida privada. Sin embargo, desde entonces hasta la fecha, especialmente tras la adopción de la Carta de Derechos Fundamentales de la Unión Europea, este derecho adquiere vida propia, al margen del reconocimiento de que el tratamiento de datos personales que no cumpla con las condiciones de legitimidad aplicables, puede llegar a suponer una injerencia en la vida privada o la privacidad.

Este modelo europeo, también ampliamente desarrollado en el derecho interno de los países que lo conforman, ha sido una importante fuente de inspiración para diversos países del Continente Americano que, como en el caso de México, reconocen la protección de datos personales como un derecho

humano diferenciado, aunque relacionado con el derecho a la vida privada. De ahí que, como veremos, sea necesario adoptar estándares comunes que excedan el ámbito nacional o, incluso, regional.

3.3. Desarrollo de la jurisprudencia internacional.

El desarrollo jurisprudencial en los distintos sistemas internacionales de derechos humanos ha sido mucho más rico respecto del derecho a la vida privada que relativas al derecho a la protección de datos personales, no solo por su reconocimiento explícito en los instrumentos internacionales que les dan origen, sino además por su propia antigüedad.

De hecho, es valioso observar que hasta el momento la Corte Interamericana de Derechos Humanos (en adelante, CIDH) no se ha pronunciado de manera específica en ningún caso respecto del derecho a la protección de datos personales, a pesar de que un gran número de países sujetos a su jurisdicción lo contemplan dentro de su propio derecho interno con el carácter de derecho humano. De tal forma que, el desarrollo internacional de la protección de datos personales se produce a nivel regional y, fundamentalmente en Europa, a partir de la propia construcción expansiva del derecho a la vida privada hasta el reconocimiento de su propia autonomía.

3. 3.1. Criterios de la Organización de Naciones Unidas.

Con el tema de la pandemia COVID-19, que está azotando al mundo, el Sistema de Protección Universal, ha emitido una declaración conjunta sobre Protección de Datos y Privacidad en la respuesta COVID-19 de las Naciones Unidas y distintas Organizaciones del Sistema de la ONU, dicha declaración está en conformidad Principios de Protección de Datos personales y privacidad de las Naciones Unidas, así como con las recomendaciones de la Estrategia de Datos del Secretario General sobre protección de datos, privacidad y derechos humanos, documentos que en esta investigación de tesis, debemos obligatoriamente analizar.

El Grupo Encargado de la Política de Privacidad de las Naciones Unidas, ha establecido los siguientes Principios (ONU) :

TRÁMITE JUSTO Y LEGÍTIMO:

Las organizaciones del sistema de las Naciones Unidas deben procesar los datos personales de manera justa, de acuerdo con sus mandatos e instrumentos rectores y sobre la base de cualquiera de los siguientes:

(i) el consentimiento del interesado;

(ii) el interés superior del interesado, de conformidad con los mandatos de la Organización del Sistema de las Naciones Unidas en cuestión;

(iii) los mandatos e instrumentos rectores de la Organización del Sistema de las Naciones Unidas correspondiente; o

(iv) cualquier otra base legal específicamente identificada por la Organización del Sistema de las Naciones Unidas en cuestión.

PROPÓSITO ESPECIFICACIÓN:

Los datos personales deben procesarse para fines específicos, que sean consistentes con los mandatos de la Organización del Sistema de las Naciones Unidas en cuestión y tengan en cuenta el equilibrio de los derechos, libertades e intereses pertinentes. Los datos personales no deben procesarse de manera incompatible con dichos fines.

PROPORCIONALIDAD Y NECESIDAD:

El procesamiento de datos personales debe ser relevante, limitado y adecuado a lo necesario en relación con los fines especificados del procesamiento de datos personales.

RETENCIÓN:

Los datos personales solo deben conservarse durante el tiempo que sea necesario para los fines especificados.

EXACTITUD:

Los datos personales deben ser precisos y, cuando sea necesario, estar actualizados para cumplir con los fines especificados.

CONFIDENCIALIDAD:

Los datos personales deben procesarse con el debido respeto a la confidencialidad.

SEGURIDAD:

Deben implementarse procedimientos y salvaguardas organizativos, administrativos, físicos y técnicos apropiados para proteger la seguridad de los datos personales, incluso contra o contra el acceso no autorizado o accidental, daño, pérdida u otros riesgos presentados por el procesamiento de datos.

TRANSPARENCIA:

El procesamiento de datos personales debe llevarse a cabo con transparencia para los interesados, según corresponda y siempre que sea posible. Esto debe incluir, por ejemplo, el suministro de información sobre el procesamiento de sus datos personales, así como información sobre cómo solicitar el acceso, verificación, rectificación y / o eliminación de esos datos personales, en la medida en que el propósito especificado para el cual los datos personales son procesado no se frustra.

TRASLADOS:

En el desempeño de sus actividades encomendadas, una Organización del Sistema de las Naciones Unidas puede transferir datos personales a un

tercero, siempre que, dadas las circunstancias, la Organización del Sistema de las Naciones Unidas se asegure de que el tercero brinde la protección adecuada para los datos personales.

RESPONSABILIDAD:

Las organizaciones del sistema de las Naciones Unidas deben contar con políticas y mecanismos adecuados para adherirse a estos Principios.

El Secretario General de las Naciones Unidas subrayó en su informe de políticas sobre derechos humanos y COVID-19, (ONU; 2020) que: "los derechos humanos son clave para configurar la respuesta a la pandemia, tanto para la emergencia de salud pública como para el impacto más amplio en la vida y los medios de sustento de las personas. Los derechos humanos ponen a las personas en el centro del escenario. Las respuestas que son moldeadas por los derechos humanos, y que los respetan, producirán mejores resultados para vencer la pandemia, garantizar la atención médica para todos y preservar la dignidad humana"

El Grupo encargado de la Política de Privacidad de Las Naciones Unidas (ONU; 2021):

“Teniendo en cuenta los principios de protección de datos personales y privacidad de las Naciones Unidas, el informe de políticas del Secretario General de las Naciones Unidas sobre derechos humanos y COVID-19 y las pertinentes normas sobre salud y humanidad, en lo relativo a la recopilación, uso y procesamiento de datos por las Organizaciones del Sistema de las Naciones Unidas en sus operaciones se deberá, al menos”:

Velar por que esas operaciones sean legítimas, limitadas en su ámbito y tiempo y necesarias y proporcionales a los propósitos especificados y válidos en la respuesta a la pandemia de COVID-19;

Velar por que los datos se mantengan confidenciales y en seguridad durante un tiempo limitado y se destruyan o borren debidamente de conformidad con los propósitos mencionados;

Velar por que todo intercambio de datos se realice de conformidad con la legislación internacional aplicable y los principios de protección de datos y privacidad y porque este intercambio se evalúe a partir de una diligencia debida y valoraciones de riesgo adecuadas.

Vincular las medidas tomadas relativas a datos a mecanismos y procedimientos aplicables para asegurarse de que cumplen los principios y propósitos mencionados, están justificadas sobre esa base y se interrumpen en cuanto dejan de ser necesarias, y

Ofrecer transparencia para generar confianza en la aplicación de iniciativas actuales y futuras.

De los principios establecido por la ONU, es evidente que este sistema de protección de los Derechos Humanos, ha trazado una línea clara con respecto a la protección de los Datos Personales, sin embargo, países como Bolivia que integran la ONU, no cuentan en su legislación local con una Ley específica que se encargue de la protección de los Datos Personales.

Más adelante podremos apreciar que tanto la Organización de Naciones Unidas (ONU), como la Organización de Estados Americanos (OEA) a través de su Órgano principal y autónomo como es CIDH, no abordaron el tema de la Protección de los Datos Personales, en la intensidad que la Corte Europea de Derechos Humanos lo hizo.

3.2.2. Criterios de la Corte Interamericana de Derechos Humanos.

En su sentido más tradicional, la CIDH ha puesto de manifiesto que el derecho a la vida privada implica una obligación negativa para el Estado. En un primer momento, ha establecido su vínculo con la inviolabilidad del domicilio. De tal

forma que la intromisión en el domicilio familiar de las personas, sin el consentimiento de quienes lo habitan y sin autorización legal para ello, así como su propia destrucción, se consideran una violación grave, injustificada y abusiva en términos del artículo 11.2 de la Convención Americana de Derechos Humanos (Ramírez, González y Gayo 2017).

Asimismo, la Corte considera que "el ámbito de la privacidad se caracteriza por quedar exento e inmune a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad pública". Además, establece que las injerencias en la vida privada de las personas deben: (1) estar previstas en ley, (2) perseguir un fin legítimo, y (3) ser idóneas, necesarias y proporcionales. En otras palabras, los requisitos que han de cumplir los límites al derecho a la vida privada comprenden tanto el principio de proporcionalidad en términos de Alexy (compuesto por sus tres subprincipios: idoneidad, necesidad y proporcionalidad en sentido estricto), como el principio de legalidad. En caso de no cumplir con estos requisitos, las injerencias se consideran contrarias a los términos de la propia Convención.

Al respecto, este Tribunal manifiesta que, a pesar de no señalarse explícitamente en el texto de la Convención, la vida privada extiende sus alcances más allá del domicilio y la correspondencia, incorporando otros aspectos como la intervención, monitoreo, grabación y divulgación de conversaciones por vía telefónica. En ese sentido se reconoce que la fluidez informativa que existe hoy coloca al derecho a la vida privada de las personas en una situación de mayor riesgo debido a las nuevas herramientas tecnológicas y su utilización cada vez más frecuente. De ahí que el Estado deba "asumir un compromiso aún mayor, con el fin de adecuar a los tiempos actuales las formas tradicionales (C. F. CIDH 2010) de protección del derecho a la vida privada" (Ramírez, González y Gayo 2017).

Así, la Corte de manera consistente con sus resoluciones previas manifiesta que "el concepto de vida privada es un término amplio no susceptible de

definiciones exhaustivas". Sin embargo, este concepto comprende, entre otras cosas, "la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos". De tal forma que las violaciones sexuales vulneran la vida privada de las personas, toda vez que impiden "el control sobre sus decisiones más personales e íntimas y sobre las funciones corporales básicas" (C. F. CIDH 2010).

En una concepción expansiva del derecho a la vida privada y su estrecha relación con otros derechos humanos reconocidos por la Convención Americana, la Corte señala que "la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás".

La CIDH, Caso Fernández Ortega vs. México, retoma los requisitos necesarios para considerar que una injerencia en la vida privada de las personas no se considere abusiva o arbitraria, señalando que tanto la idoneidad, la necesidad, como la proporcionalidad de las medidas adoptadas implican que sean "necesarias en una sociedad democrática" (2010).

Finalmente, en una resolución histórica relativa a la prohibición general de la fecundación *in vitro* concebida como una injerencia en la vida privada de las personas, la CIDH adopta de manera expresa criterios provenientes del Tribunal Europeo de Derechos Humanos, en el sentido de que el ámbito de protección del derecho a la vida privada va más allá del derecho a la privacidad. De manera textual, la Corte ahonda en el concepto de vida privada, mediante la adopción de criterios cuyo desarrollo corresponde al ámbito europeo:

> La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo por ejemplo la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el

> derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior.
>
> La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad (Fernández Ortega vs. México 2010)

Es posible decir que este fallo de la CIDH, mismo que retoma los criterios emitidos por su homóloga europea en materia del derecho a la vida privada, permite anticipar el desarrollo armónico de este derecho en ambos sistemas internacionales de derechos humanos. No obstante, su distanciamiento, por lo menos hasta la actualidad, se produce precisamente con la incorporación del derecho a la protección de datos personales y su relación con otros derechos humanos de frontera (como la libertad de expresión).

3.2.3. Criterios de la Corte Europea de Derechos Humanos.

Por lo que hace a la persecución de un fin legítimo, el Tribunal ha analizado varios casos en los que se considera que se cumple este requisito, por ejemplo, en la adopción de medidas para garantizar la seguridad nacional y la prevención del desorden o el delito e, incluso, posteriormente, en relación con la transferencia de datos de salud de una autoridad a otra para la decisión de las autoridades respecto de la asignación de recursos públicos entre otros (Ramírez, González y Gayo 2017).

(M. S. v. Sweden 1997), el requerimiento de que la interferencia esté de acuerdo con la ley, supone, de acuerdo con el TEDH, que además de encontrar sustento en la legislación doméstica, es necesario considerar la calidad de la ley y su foreseeability, esto es, que contribuya a fortalecer el

estado de derecho. Así, la Corte establece que el requerimiento de que la medida sea "de acuerdo con la ley" supone que existe una previsión legal previa y que la ley sea accesible y suficientemente clara respecto de las circunstancias y condiciones en las que las autoridades están facultades para establecer estas interferencias, estableciendo a su vez medidas adecuadas de protección legal.

Finalmente, el requerimiento de que las interferencias sean necesarias en una sociedad democrática implica la identificación, dentro del ámbito más amplio del objetivo legítimo perseguido, de la necesidad social específica que deba abordarse, la proporcionalidad de la medida para alcanzar dicho objetivo legítimo y que existan razones relevantes y suficientes que la justifiquen en razón de otras posibles medidas.

Un paso decisivo para que el Tribunal Europeo pudiera adentrarse a campos propios del derecho a la protección de datos personales, inicialmente referido al acceso a la propia información personal que consta en archivos públicos, fue el reconocimiento de que si bien el Artículo 8 del Convenio Europeo tiene esencialmente por objeto proteger a los individuos en contra de interferencias arbitrarias por las autoridades públicas, también podría comprender obligaciones positivas del Estado inherentes al respeto efectivo de la vida privada y familiar, de tal forma que incluso la negativa para conceder acceso a la información personal del individuo debe analizarse, "por una autoridad independiente" bajo la óptica de los requerimientos que establece el Artículo 8 antes indicados, con el fin de garantizar la aplicación del principio de proporcionalidad.

Al respecto, la Corte reconoce que el Artículo 8 protege, entre otros intereses, el derecho al desarrollo personal, lo que incluye el derecho de recibir información relativa a su identidad personal, necesaria para conocer sus orígenes y entender su infancia y posterior desarrollo.

Es esencial decir que las primeras referencias explícitas a la protección de los datos personales se presentan en el contexto de información sensible que contiene datos de salud. En un primer momento, la Corte Europea se cuestiona si las medidas que se impugnan —consistentes en obtener y mantener por un periodo la confidencialidad de información médica de una pareja infectada por VIH, misma que consta en el expediente de un juicio seguido en contra de uno de ellos por delitos de carácter sexual— fueron necesarias en una sociedad democrática. Al respecto, la Corte señala que la confidencialidad de los datos de salud es un principio vital en los sistemas legales de los Estados parte del Convenio. Es crucial, señala, no solo en el sentido de respeto a la privacidad de los pacientes, sino también para preservar su confianza en la profesión médica y en los servicios de salud en general. Además, estas consideraciones cobran especial relevancia cuando se trata de la confidencialidad de información relativa a una persona infectada de VIH, toda vez que la revelación de esta información puede afectar de manera dramática su vida privada y familiar, laboral y social, exponiéndola al oprobio y el ostracismo (Rotaru v. Romania 2000).

La Corte (M.S. v. Sweden s.f.) reconoce: la transferencia de datos de salud de una autoridad a otra, sin el consentimiento del paciente y que, a su vez, ha servido para diferentes propósitos, constituye una interferencia en el derecho al respeto de la vida privada y familiar del paciente. En ese sentido, la Corte establece que las medidas adoptadas para la comunicación de la información entre autoridades se deben analizar a la luz de los requerimientos previamente establecidos.

De igual forma, bajo la idea de que el término de "vida privada" no debe ser interpretado de manera restrictiva, la Corte incluye dentro del ámbito de protección del multicitado artículo 8, el almacenamiento de datos relativos a una persona, con independencia de si los mismos son o no sensibles, lo que, de acuerdo con el propio Tribunal, es consistente con el Convenio 108 del

Consejo de Europa. Asimismo, estas consideraciones se hacen extensivas al uso de la información, lo que incluye su divulgación por parte de las autoridades, y a la carencia de medios para refutar el contenido de dicha información.

En sucesivas ocasiones, la Corte reitera las obligaciones positivas del Estado para proteger la vida privada de las personas que se derivan del párrafo 1 del artículo 8 del Convenio Europeo, lo que la lleva a considerar la posibilidad de que, incluso, la divulgación de información por parte de personas distintas a las autoridades, incluida la prensa y los medios de comunicación masiva, sea contraria a los términos de la Convención.

También dentro de este rubro, consistente en las obligaciones positivas que conlleva el citado artículo 8 del Convenio, el Tribunal reitera el deber de proporcionar a las personas "un procedimiento efectivo y accesible" para obtener el acceso a "información relevante y apropiada" de los archivos personales mantenidos por las autoridades.

De esta forma, como se puede observar, el TEDH va perfilando la inclusión del derecho a la protección de datos personales en relación con el derecho a la vida privada. Incluso, ya establece en sus decisiones esta conexión al indicar textualmente que la protección de datos de carácter personal juega un rol fundamental en el ejercicio del derecho al respeto de la vida privada y familiar consagrado en el artículo 8 de la Convención. Acerca del particular se señala que el mero hecho de que la legislación interna facilite la oportunidad de reclamar indemnizaciones por daños y perjuicios por la revelación ilegal de los datos personales, no es razón suficiente para proteger la vida privada, es necesario que los Estados firmantes de la Convención provean de una protección "real y efectiva" que excluya cualquier posibilidad de acceso no autorizado.

Lo anterior es consistente con la idea central de que el derecho a la vida privada "es un término amplio no susceptible de una definición exhaustiva, que comprende la integridad física y psicológica de una persona y puede comprender múltiples aspectos de la identidad de la persona. De ahí que desde esta perspectiva el alcance del término "dato personal" sea esencialmente amplio. De hecho, el Tribunal Europeo se ha referido a muy diversos ámbitos entre los que se incluye información relativa a una persona identificada o identificable que van desde el propio nombre, la fecha de nacimiento y el historial médico, hasta las huellas dactilares, muestras de células y elaboración de perfiles de ADN, entre otros.

En virtud de los precedentes antes mencionados, es posible observar que existe cierto consenso entre la Corte Interamericana de Derechos Humanos y el Tribunal Europeo respecto del amplísimo alcance del derecho a la vida privada, fundamentalmente en el sentido de que el derecho a vida privada comprende múltiples aspectos de la identidad de las personas y de cómo deciden relacionarse con otros seres humanos.

Sin embargo, podemos observar que el desarrollo del contenido y alcance de este derecho ha sido asimétrico, específicamente por lo que se refiere al reconocimiento explícito del derecho a la protección de datos personales. Mientras que la Corte Interamericana hasta el momento no se ha pronunciado al respecto, el Tribunal Europeo ha dado pasos significativos que permiten profundizar acerca de la noción misma del derecho a la protección de datos personales en su relación con el derecho a la vida privada.

En concreto, el Tribunal de Estrasburgo reconoce que bajo el concepto de vida privada puede quedar amparada "toda información relativa a una persona física identificada o identificable", esto es, con independencia de si se trata o no de información sensible que afecta la esfera más íntima de las personas, lo que a su vez es consistente con la amplia definición de "dato personal". De igual forma, en su jurisprudencia introduce la búsqueda de criterios

interpretativos conformes con la normatividad específica en materia de protección de datos personales, como se puede observar en sus referencias al Convenio 108 del Consejo de Europa.

No obstante, es admisible advertir que la construcción del derecho a la protección de datos personales desde la perspectiva del Tribunal Europeo de Derechos Humanos aún se encuentra bajo la égida del derecho a la vida privada. Su carácter autónomo, en el ámbito internacional de los derechos humanos, se presenta con la Carta de Derechos Fundamentales y su interpretación jurisprudencial por parte del Tribunal de Justicia de la Unión Europea.

3.2.4. Criterios del Tribunal de Justicia de La Unión Europea.

El Tribunal de Justicia de la Unión Europea toma como base de interpretación no solo la Carta de Derechos Fundamentales de la Unión Europea, misma que ya reconoce de manera explícita y autónoma el derecho a la protección de datos personales, sino también la Directiva 95/46/CE antes citada, entre otros documentos normativos que regulan la protección de datos personales en la Unión Europea.

Este Tribunal se adentra a cuestiones mucho más específicas para delinear los contornos del derecho a la protección de datos personales, que terminan por acentuar el carácter autónomo de este derecho frente al derecho a la vida privada, sin dejar de reconocer su estrecha vinculación. Entre otros asuntos, este Tribunal se ha ocupado de establecer criterios interpretativos en relación con la transferencia de datos a terceros países (no miembros de la Unión Europea), la conservación de datos relativos a comunicaciones electrónicas, la gestión de motores de búsqueda concebida como tratamiento de datos personales y los sistemas de videovigilancia operados por particulares.

En un caso relevante para la interpretación de la Carta de Derechos Fundamentales en consonancia con los criterios emitidos por el TEDH, el

TJUE (;2010) establece que "el respeto a la vida privada en lo que respecta al tratamiento de los datos personales" se aplica a toda información sobre una persona física identificada e identificable y, además, que "las limitaciones al derecho a la protección de datos personales de carácter personal que pueden establecerse legítimamente corresponden a las toleradas en el contexto del artículo 8 del CEDH". De tal forma que este órgano jurisdiccional, al referirse sobre quién puede ser titular del derecho a la protección de datos personales, reconoce que solo las personas físicas cuentan con esta facultad, pues "las personas jurídicas solo pueden acogerse a la protección de los artículos 7 y 8 de la Carta frente a dicha identificación en la medida en que en la razón social de la persona jurídica se identifique a una o varias personas físicas".

Así, esta característica presenta una importante diferencia de alcance, en el contexto europeo, del derecho a la vida privada del Convenio y el derecho a la protección de datos personales reconocido en la Carta, toda vez que el ámbito de protección del primero alcanza efectivamente a las personas morales.

No obstante, el propio Tribunal ha reconocido que tratándose de "la protección de los derechos y las libertades fundamentales de las personas físicas, en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales", no es posible separar los casos de tratamiento de datos personales en dos categorías, a saber, una categoría en la que ese tratamiento sería examinado únicamente sobre la base del artículo 8 del Convenio Europeo y su interpretación jurisprudencial y otra categoría en la que dicho tratamiento estaría sujeto a las disposiciones normativas de protección de datos personales en la Unión Europea38. De ahí que el TJUE reconozca la estrecha relación entre derechos, cuyo contenido puede ser en ocasiones coincidente.

Además, es factible considerar por lo que hace a la estrecha relación entre el derecho a la vida privada consagrado por el TEDH y la Carta de Derechos Fundamentales, que esta establece en su artículo 52, apartado 3, que en la

medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo, su sentido y alcance serán iguales a los que les confiere dicho Convenio. Esta disposición no obstará a que el Derecho de la Unión conceda una protección más extensa.

De igual forma, este Tribunal en diversas ocasiones ha tenido oportunidad de referirse al carácter independiente de las autoridades de control de los datos personales, que exige la Directiva 95/46/CE. Sobre este aspecto en particular, el Tribunal ha establecido que la garantía de independencia de las autoridades de control nacionales trata de asegurar un control eficaz y fiable del respeto de la normativa en materia de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y debe interpretarse a la luz de dicho objetivo". Todo ello implica que las autoridades de control actúen con objetividad e imparcialidad, esto es, libres de cualquier influencia externa, directa o indirecta, que pudiera poner en peligro de la tarea que les corresponde de lograr un justo equilibrio entre la libre circulación de los datos personales y el derecho a su vida privada (intimidad). Bajo estas consideraciones, el Tribunal constata que si bien la independencia funcional de las autoridades, "en el sentido de que no estén sujetas a instrucción alguna en el ejercicio de sus funciones", es una condición necesaria para garantizar el cumplimiento de sus tareas, esta independencia funcional no basta por sí sola, toda vez que es necesario que la misma también se ejerza de manera indirecta, esto es, que pueda excluir toda forma de influencia que pudiera orientar las decisiones de la autoridad, como podría ser una relación de supervisión jerárquica.

Es importante subrayar que precisamente la carencia de una autoridad de control independiente por parte de los Estados Unidos de América fue uno de los motivos que dio lugar a que el TJUE invalidara el Acuerdo de Puerto Seguro, al que nos hemos referido con anterioridad (apartados 41 y 42 de la

Sentencia), mismo que pone de manifiesto la relevancia de homologar criterios en beneficio de las personas.

Por tanto, deben quedar claras tres ideas en relación con las autoridades de control o garantes de los derechos y libertades fundamentales, en particular por lo que se refiere a la protección de datos personales. La primera es que exista y que sea independiente. La segunda, que dichas autoridades de control puedan ejercer sus competencias de manera que se proteja de manera efectiva el derecho a la protección de datos personales. Y la tercera, que la ausencia de dichas autoridades de control impide el reconocimiento del nivel adecuado de protección de un país, con independencia de otros elementos previstos para su tutela.

La sentencia del TJUE que invalidó el Acuerdo de Puerto Seguro entre la Unión Europea y los Estados Unidos de América explica que "debe entenderse la expresión ’nivel de protección adecuado’ en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta"43 y añade que "[a]unque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión"44. Si bien el territorio donde se encuentran los datos personales es un factor a considerar para determinar si un país cumple con un nivel adecuado de protección, no es el único. El nacionalismo de datos no puede llevar a perder de vista que lo importante no es dónde están los datos personales, obviando otros mecanismos, como la regulación e, incluso, las normas corporativas

vinculantes que son necesarias para facilitar la libre circulación de datos personales a nivel internacional.

3.3. Desigualdades de protección.

El reconocimiento del derecho a la protección de datos personales en los instrumentos internacionales, así como su interpretación jurisprudencial, pone de manifiesto las asimetrías que se presentan por región por lo que hace a su reconocimiento y alcance.

Como se ha podido constatar de la jurisprudencia emitida por los tribunales internacionales, el desarrollo del derecho a la protección de datos personales se ha presentado fundamentalmente en Europa, sea mediante su vínculo con el derecho a la vida privada, reconocido en el artículo 8 de la CEDH, o de manera particularizada por medio del ámbito de la Unión Europea. El hecho de que la Carta de Derechos Fundamentales, de manera consistente con el Tratado de Funcionamiento de la Unión Europea, lo reconozca de forma autónoma y con un ámbito específico de protección, obliga a todos los Estados miembros de la Unión a adecuar su legislación doméstica al más alto nivel normativo y a adoptar los criterios que determinan su interpretación y alcance.

En términos generales, la base para garantizar una protección adecuada que se materialice en el control que la persona pueda tener sobre el tratamiento de sus datos personales, se constituye mediante unos criterios de legitimación, los principios de la protección de datos, la posibilidad de ejercer derechos por parte del titular de los datos y la supervisión, misma que puede concretarse en la tutela de la persona a la que se refieren los datos personales que son objeto de tratamiento, así como la atribución y el ejercicio de potestades de investigación y sanción por parte de una autoridad de control independiente. Si bien el TEDH se ha referido a algunos de estos aspectos en contextos específicos, la normatividad de la Unión Europea, así como los criterios que se han desarrollado sobre la misma, tanto en el ámbito jurisdiccional como no

jurisdiccional (como es el caso del Grupo de trabajo del Artículo 29 o, incluso, del llamado Grupo de Berlín, además por supuesto de las propias autoridades de control nacionales en la Unión Europea), han permitido establecer los contornos del derecho a la protección de datos personales.

Se trata, entonces, de garantías que tienen que darse de manera efectiva y que, al mismo tiempo, implican un claro compromiso europeo con el derecho humano a la protección de datos personales. Estas, a su vez, presentan un carácter transversal, cuyo alcance abarca cualquier ámbito o momento, con independencia de que el titular de los datos actúe en relaciones de subordinación (frente a las autoridades públicas) o de coordinación (frente a otros particulares).

Por tanto, la ausencia total o parcial de estas garantías, tanto desde un punto de vista formal, en cuanto a su reconocimiento en la legislación o mediante mecanismos de regulación sectorial o, incluso de autorregulación, como desde una perspectiva práctica, por lo que se refiere a la efectividad de las mismas, implica la imposibilidad en el ámbito europeo de reconocer un nivel de protección adecuado para quien carezca de las mismas.

Cuestión distinta ocurre en el ámbito americano y particularmente dentro del Sistema Interamericano de Derechos Humanos. Si bien ya existe una larga tradición que ampara el derecho a la vida privada, la protección de datos personales carece aún de una construcción propia, tanto normativa como jurisprudencial, a pesar de los incipientes esfuerzos y avances de la Organización de Estados Americanos (OEA) (2015) y de la Red Iberoamericana de Protección de Datos (RIDP).

Ello también, a pesar de que varios Estados parte del Sistema han adoptado, con una clara influencia europea, el derecho a la protección de datos personales con un carácter de derecho humano autónomo, aunque interrelacionado con el derecho a la vida privada, cuyo alcance se proyecta

tanto en el reconocimiento del derecho a la autodeterminación informativa de las personas, como del habeas data. Este es precisamente el caso de Argentina, Chile, Uruguay, México y Colombia, entre otros.

En el caso concreto de Argentina y Uruguay, es admisible decir que la Comisión Europea les ha otorgado el reconocimiento como países que efectivamente establecen un nivel adecuado de protección de datos personales, lo que incluso ha llevado a Uruguay a ser el primer y único país en Latinoamérica en haber procedido a la adhesión al Convenio 108 y su Protocolo Adicional, mismos que tienen por objeto establecer las reglas generales para garantizar el respeto a la vida privada (por lo que se refiere al tratamiento automatizado de datos de carácter personal) y simultáneamente la libre circulación de la información.

3.4. Necesidad de un equilibrio global.

La ausencia de criterios internacionales uniformes acerca del derecho a la protección de datos personales no solo dificulta la relación con Europa por lo que hace a los flujos de información entre autoridades y el sector privado, sino que además acentúa las diferencias conceptuales entre los diversos sistemas de derechos humanos, cuya característica fundamental debiera residir precisamente en su "universalidad".

La falta de estándares comunes entre regiones entorpece el cumplimiento de ciertos objetivos importantes para el progreso económico y social, el desarrollo del intercambio entre países y el bienestar de los individuos, como eliminar las restricciones en la libre circulación de los datos personales, falsear la competencia económica e impedir que las administraciones cumplan los cometidos que les incumben49, así como problemas de seguridad de los datos.

Además, no debemos olvidar que la protección de la persona por lo que hace al tratamiento de sus datos personales es un instrumento necesario para

garantizar la protección de otros derechos humanos y libertades fundamentales, toda vez que redunda, a fin de cuentas, en la dignidad de la persona. Como se ha constatado en las diversas resoluciones del Tribunal Europeo (y en cierta medida en la CIDH), el tratamiento adecuado de la información personal mismo que incluye su recogida, uso, acceso, divulgación, transferencia, etc.

Resulta indispensable para garantizar la vida privada de las personas. Asimismo, se relaciona con otros derechos humanos como la igualdad y la no discriminación, toda vez que la revelación de información "sensible" puede dar lugar al aislamiento de la persona o, incluso, a tratos segregacionistas.

De ahí que el derecho a la protección de datos personales busque tutelar a las personas mediante el otorgamiento de un poder de control sobre su propia información, sujeto a ciertas restricciones susceptibles de ser valoradas bajo márgenes de apreciación que comprendan tanto los requisitos que permiten justificar una injerencia como la gravedad de la afectación respecto de otros derechos humanos.

Una cuestión adicional que es posible considerar para justificar la necesidad de generar estándares homogéneos a nivel global es el efecto que ello tendría en el fortalecimiento de la confianza en los usuarios de servicios o consumidores. La protección efectiva de la información personal, mediante el derecho sustantivo, la existencia de autoridades de control independientes, las normas procedimentales y sancionatorias, así como los mecanismos de cooperación adecuados, son la base para generar esta confianza, necesaria en todos los ámbitos, sea en las relaciones entre particulares y las Administraciones Públicas como respecto de los consumidores y proveedores de bienes y servicios que tratan datos personales.

Impulsar la confianza por medio de una protección adecuada, por tanto, depende, por una parte, de la adopción e implementación de diversas medidas

tantas normativas como institucionales y, por otra parte, de que las mismas sean efectivas, lo que pasa por evaluar a lo largo del tiempo si responden a las circunstancias actuales en cada momento.

En este sentido, asegurar y proteger los derechos humanos y las libertades fundamentales, entre los que se encuentra el derecho a la protección de datos personales, debe ser una tendencia a considerar frente a los planteamientos ocurridos hasta hace apenas unas décadas, en el sentido de que aún no era el momento adecuado para reconocer este derecho en el texto del CEDH.

3.5. Patrones comunes.

La generación de estándares comunes con un alcance global acerca de la protección de datos personales no solo es necesaria sino también posible, toda vez que sus cimientos ya han sido establecidos por el propio reconocimiento y desarrollo del derecho a la vida privada. A todo ello se añade el progresivo avance en la materia que se ha venido generando en algunos países del Continente Americano y, aunque con un alcance limitado, en el propio Sistema Interamericano de Derechos Humanos.

Ciertamente los mecanismos que permitan homologar estos estándares de protección adecuada pueden adquirir muy diversa naturaleza. No obstante, dos vías que consideramos pertinentes para tal fin, debido a su proyección y su carácter vinculante en el ámbito internacional, son, por una parte, la búsqueda de la adhesión al Convenio 108 y su Protocolo Adicional por aquellos países que, como Bolivia, aún no son parte del mismo y, por la otra, la adopción de criterios compatibles en los diversos Sistemas de Derechos Humanos. Esto último podría impulsarse con la solicitud de opiniones consultivas por parte de los países interesados o, a su vez, por los propios particulares que ven vulnerados sus derechos.

Para Ramírez, González y Gayo (2017), los elementos que resultan clave para que la protección de la persona, por lo que hace al tratamiento de sus datos personales, sea efectiva son:

(a) el establecimiento de principios y deberes que legitimen el tratamiento de los datos personales, consistentes con la evolución social y tecnológica;

(b) el reconocimiento de los derechos de los interesados y los procedimientos para garantizar su ejercicio, con el fin de que se les permita un control efectivo respecto de su información, y;

(c) la existencia de autoridades independientes de control, en el sentido de que sean ajenas a cualquier influencia externa, tanto directa como indirecta.

CAPÍTULO IV

ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

La Constitución Política del Estado Plurinacional de Bolivia, establece en su Art. 13.4, dice: *"Los tratados y convenios internacionales ratificados por la Asamblea Legislativa Plurinacional, que reconocen los derechos humanos y que prohíben su limitación en los Estados de Excepción prevalecen en el orden interno. Los derechos y deberes consagrados en esta Constitución se interpretarán de conformidad con los Tratados internacionales de derechos humanos ratificados por Bolivia*".

De la misma forma el Art. 256 núm. I y II del mismo cuerpo legal (2009), establece: "*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.*

En ese entendido toda norma, más aún una Ley, debe someterse a un Control de Convencionalidad, esto quiere decir interpretar toda norma utilizando (CIDH, CUADERNILLO DE JURISPRUDENCIA DE LA CORTE INTERAMERICANA DE DERECHOS ;2019): "la *herramienta que permite a los Estados concretar la obligación de garantía de los derechos humanos en el ámbito interno, a través de la verificación de la conformidad de las normas y prácticas nacionales, con la Convención Americana sobre Derechos Humanos (CADH) y su jurisprudencia"*

Según Claudio Nash Rojas, indica que el Control de Convencionalidad: “Debe ser practicado por la Corte Interamericana, hace control de convencionalidad en sus veredictos ella descarta normas locales, incluso constitucionales, opuestas Pacto de San José de Costa Rica. A eso se lo ha denominado "control de convencionalidad en sede internacional", para diferenciarlo del que imperativamente asigna a los jueces domésticos en "Almonacid Arellano" y los demás fallos posteriores ya mencionamos, que aluden al "control de convencionalidad en sede nacional” (2011, p. 276)

Bajo esa aclaración es necesario mencionar que la Corte Interamericana de Derechos Humanos (CIDH), en el denominado Pacto de San José de Costa Rica, ha establecido derechos a ser salvaguardados, normas que deben ser analizadas de manera detallada en esta investigación.

Es así que corresponde a esta exploración, analizar de manera detallada y profunda la posición que ha establecido la Organización de Estados Americanos (OEA) a través de su Órgano especializado como es la Corte Interamericana de Derechos Humanos (CIDH), con respecto a la protección de datos personales.

4.1. Organización de Estados Americanos (OEA) – Corte Interamericana de Derechos Humanos (CIDH).

En el Capítulo anterior se ha establecido el criterio esgrimido por la Corte Interamericana de Derechos Humanos (CIDH), corresponde ahora mencionar una serie de cronologías que este mismo Órgano ha dado a conocer con referencia al tema en cuestión.

Desde 1996, la Asamblea General de la Organización de los Estados Americanos (OEA) viene dedicando especial atención a las cuestiones vinculadas con el acceso a la información y la protección de los datos personales, por ello el 7 de junio de 1996 emitió una resolución solicitando al Comité Jurídico Interamericano (CJI) que al considerar el tema relativo al

derecho de la información, otorgue particular relevancia a los aspectos concernientes al acceso del mismo y la protección de los datos de carácter personal, incluyendo aquellos que se introduzcan vía los sistemas de correo y transmisión electrónica computarizada e iniciara un estudio de los contextos jurídicos de los Estados Miembros de la OEA en relación con estos dos temas.

Además de realizar los estudios encomendados, el CJI aprobó también resoluciones sobre la materia, en un esfuerzo por abordar la regulación de la protección de datos a través de posibles instrumentos internacionales. Estos trabajos aportaron elementos valiosos, no sólo para comprender la verdadera dimensión de esta cuestión a la luz de los efectos de las nuevas tecnologías en la expansión del manejo y el uso de la información por los particulares, sino también para apoyar a los Estados Miembros a adoptar medidas en cuanto a la armonización de las legislaciones, el fomento de la cooperación regional y la búsqueda de elementos sustanciales para un futuro instrumento regional sobre la materia.

Asimismo, la Asamblea General solicitó que el Departamento de Derecho Internacional preparase un estudio preliminar sobre la protección de datos con la finalidad de ofrecer una perspectiva general de los temas más relevantes a considerar en la elaboración de los principios y recomendaciones sobre la protección de datos. Este estudio fue presentado formalmente en la Comisión de Asuntos Jurídicos y Políticos (CAJP) del Consejo Permanente de la OEA en octubre de 2011.

En ese mismo año, la Asamblea General incluyó expresamente en el título y el contenido de sus resoluciones el tema de protección de datos personales, en consideración de la creciente importancia de la privacidad y la protección de datos personales, así como la necesidad de fomentar y proteger el flujo transfronterizo de información en las Américas y reconociendo los esfuerzos de otras entidades internacionales y regionales en el área de la protección de datos personales, como es el caso de la Organización de Cooperación y

Desarrollo Económicos (OCDE), el Foro de Cooperación Económica Asia-Pacífico (APEC), la Unión Europea y el Consejo de Europa. Finalmente, encomendó al CJI la preparación de “un documento de principios de privacidad y protección de datos personales en las Américas”.

A partir de allí, en el año 2012 el CJI adoptó y presentó 12 principios a la Asamblea General, los cuales tienen por objetivo evitar daños a las personas derivados de la obtención o del uso incorrecto o innecesario de sus datos personales:

1. Propósitos Legítimos y Justos;

2. Claridad y Consentimiento;

3. Pertinencia y Necesidad;

4. Uso Limitado y Retención;

5. Deber de Confidencialidad;

6. Protección y Seguridad;

7. Fidelidad de la Información;

8. Acceso y Corrección;

9. Información Sensible;

10. Responsabilidad;

11. Flujo Transfronterizo de Información y Responsabilidad; y

12. Publicidad de las Excepciones.

Año 2013: La Asamblea General resolvió encomendar al CJI que formule propuestas a la CAJP sobre las distintas formas de regular la protección de datos personales, incluyendo un proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales

alcanzados en la materia, mandato que fue reiterado en junio de 2014 y dentro del cual también se solicita a la Secretaría General que a través del Departamento de Derecho Internacional, continúe trabajando con organizaciones internacionales y autoridades de protección de datos personales, y que identifique los recursos humanos y económicos necesarios para avanzar en el tema.

Posteriormente, durante el 83º período ordinario de sesiones del CJI (agosto de 2013), el presidente pidió al doctor David P. Stewart que fungiera como relator del tema. El Relator realizó amplias consultas con expertos y otros actores que intervienen en la formulación de principios y prácticas pertinentes, incluso en el ámbito de la Unión Europea y otros grupos regionales, así como con representantes de instituciones gubernamentales, académicas, empresariales y no gubernamentales, además de solicitar a los Estados Miembros de la Organización que informaran sobre sus prácticas y leyes vigentes en la materia.

Año 2014: La Asamblea General de la OEA le encomendó al CJI que, antes del cuadragésimo quinto período ordinario de sesiones de la Asamblea General, "formule propuestas a la CAJP sobre las distintas formas de regular la protección de datos personales, incluyendo un proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia".

Año 2015: Sobre la base de dichas consultas, el Relator concluyó que la orientación más productiva para este proyecto en este momento sería elaborar una propuesta de Guía Legislativa para los Estados Miembros, basada en los 12 Principios adoptados anteriormente por el CJI, con algunas modificaciones menores, teniendo en cuenta los diversos conjuntos de directrices preparados en la Unión Europea, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Cooperación Económica Asia-Pacífico (APEC), etc.

El objetivo de esta Guía Legislativa es explayarse en los Principios de Privacidad y Protección de Datos Personales en las Américas adoptados en 2012, proporcionando un contexto más amplio y orientación a los Estados Miembros a fin de facilitar la elaboración de leyes nacionales. En opinión del Relator, el campo de la privacidad personal y la protección de datos sigue caracterizándose por rápidos adelantos tecnológicos, así como una evolución constante de las amenazas a la privacidad personal.

Siendo que las respuestas a estos adelantos y amenazas han sido diferentes en las distintas regiones del mundo, y que en las Américas no parece haber surgido un enfoque “regional” uniforme y coherente, el Relator estimó que la contribución más importante que puede hacer el CJI es aprovechar las experiencias y los logros de otras regiones, teniendo en cuenta al mismo tiempo la situación de nuestro propio continente, a fin de formular una propuesta marco que los Estados de las Américas puedan usar para abordar este campo crucial.

De esta forma, el tema central sigue siendo los principios fundamentales y las prácticas óptimas, teniendo en cuenta la experiencia de otros en este campo, en vez de tratar de llegar a un acuerdo sobre los detalles exactos de un texto legislativo preciso.

Lo anterior consta en el Informe sobre Privacidad y Protección de Datos Personales (CJI/doc. 474/15 rev.2) adoptado por el CJI durante su octogésimo sexto periodo de sesiones, celebrado los días 23-27 de marzo de en Rio de Janeiro, Brasil.

4.2. Convención Americana sobre Derechos Humanos (Pacto de San José).

a. Protección de la honra y de la dignidad.

Los precedentes jurisprudenciales que la **Corte Interamericana de Derechos Humanos (CIDH)** ha resuelto sobre el derecho a la protección de datos personales, han sido progresivos y conexos a la vida privada, intentando asignar su debida garantía. Por ejemplo, la CIDH ha definido que:

> *El art. 11.2 de la Convención protege la vida privada y el domicilio de injerencias arbitrarias o abusivas. Dicho artículo reconoce que existe un ámbito personal que debe estar a salvo de intromisiones por parte de extraños y que el honor personal y familiar, así como el domicilio, deben estar protegidos ante tales interferencias. La Corte considera que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública.*

Asimismo, en relación con los bienes jurídicos tutelados, la CIDH sostiene que "la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás". (Atala Riffo y niñas vs. Chile. 2012) Por tanto, la protección a la vida privada incluye una serie de factores relacionados con la dignidad humana, tales como:

> *La capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales [...] engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior.* (Artavia Murillo y otros vs. Costa Rica. 2012)

Mientras que lo más cercano a una definición adecuada se recogen en dos fallos. El primero, relacionado al manejo de bases de datos sobre personas desaparecidas, conceptualizándose como una “garantía de no repetición” que “en todo momento deberá proteger los datos personales contenidos en dichas bases de datos” (González y otras vs. México ;2009) y el segundo que hace referencia al derecho a la identidad como “el conjunto de atributos y características que permiten la individualización de la persona en sociedad” (Gelman vs. Uruguay 2011)

Si bien la tendencia moderna manifiesta que el Derecho a la Protección de datos personales, es un derecho autónomo y fundamental, en el caso de Bolivia, que sigue medianamente el criterio de la CIDH, advertimos que el derecho a la protección de Datos Personales es un derecho conexo al Derecho a la Privacidad, tal cual más adelante podremos evidenciar cuando se analice el contenido del Art. 21 de la Constitución Política del Estado boliviana, bajo ese criterio es indudable que el Estado Plurinacional de Bolivia, no considera que el derecho de protección de datos personales pueda ser considerado como derecho Fundamental, Autónomo**,** por consiguiente el Principio de Progresividad es ignorado al momento de otorgarle protección a los datos de carácter personal.

Sin embargo**,** es necesario citar las líneas esgrimidas por Murillo de la Cueva y Piñar, que manifiesta que: “ En la actualidad, el derecho a la protección de los datos de carácter personal se describe como un derecho autónomo de otros derechos, es decir, como un derecho nuevo vinculado a la necesidad de proteger la dignidad personal frente a las nuevas tecnologías” (1990, p.17), así también Antonio Troncoso, manifiesta que: “Este nuevo derecho fundamental constituye un instituto de garantía de otros derechos fundamentales, en especial del derecho a la intimidad, pero no solo de este derecho... Atribuye a su titular un haz de facultades que consiste en el poder jurídico de imponer a

terceros la realización o la omisión de determinados comportamientos". (2010, p.69)

B. Derecho de acceso a la información: libertad de pensamiento y de expresión.

La Convención Americana consagra expresamente el derecho a buscar y recibir información. En el marco de la OEA tanto los órganos políticos como por ejemplo la Asamblea General, como los órganos del Sistema Interamericano de Protección de los Derechos Humanos de la OEA, Comisión Interamericana y Corte Interamericana, han dado un amplio contenido al derecho a la libertad de pensamiento y de expresión consagrado en el artículo 13 de la Convención, a través de la descripción de sus dimensiones individual y social, de las cuales se han desprendido una serie de derechos que se encuentran protegidos en dicho artículo. (Caso López Álvarez vs Honduras ;2006)

En este sentido, desde el año 2003 la Asamblea General ha emitido cuatro resoluciones específicas sobre el acceso a la información en las que resalta su relación con el derecho a la libertad de pensamiento y de expresión18. En la última resolución de 3 de junio de 2006 la Asamblea General de la OEA instó a los Estados a que respeten y hagan respetar el acceso a la información pública a todas las personas y [a] promover la adopción de disposiciones legislativas o de otro carácter que fueran necesarias para asegurar su reconocimiento y aplicación efectiva" (Organización de Estados Americanos ;2007)

En 1997 la Comisión Interamericana de Derechos Humanos creó la Relatoría Especial para la Libertad de Expresión. En octubre de 2000 la Comisión Interamericana aprobó la Declaración de Principios sobre la Libertad de Expresión elaborada por la Relatoría Especial, cuyo Principio 4 reconoce que "[e]l acceso a la información en poder del Estado es un derecho fundamental

de los individuos. Los Estados están obligados a garantizar el ejercicio de este derecho” (Relatoria Especial ;2007).

La Comisión ha interpretado consistentemente que el artículo 13 de la Convención incluye un derecho al acceso a información en poder del Estado21. En este sentido, la Relatoría manifestó que, dado que la libertad de recibir información debe impedir que las autoridades interrumpan el flujo de información hacia los ciudadanos, la palabra buscar, lógicamente, implicaría un derecho adicional22. En este sentido, la CIDH ha resaltado que las todas las personas tienen el derecho de solicitar, entre otros, documentación e información mantenida en los archivos públicos o procesada por el Estado y, en general, cualquier tipo de información que se considera que es de fuente pública o que proviene de documentación gubernamental oficial (CIDH ;2002).

El 8 de julio de 2005 la Comisión Interamericana presentó 28. una demanda ante la Corte Interamericana en el caso Claude Reyes y otros, la cual tenía como fundamento fáctico la negativa de una institución del Estado a brindar a las víctimas toda la información que requerían sobre un proyecto de deforestación con impacto ambiental en Chile. La Comisión sostuvo que dicha negativa, así como la falta de un recurso judicial efectivo para impugnarla, generaban la responsabilidad internacional del Estado por la violación del derecho a la libertad de pensamiento y de expresión y del derecho a la protección judicial (CIDH ;2005).

Con todos estos antecedentes se afianza el derecho de acceso a la información30 como derecho humano y ciertas características y elementos que conforman un marco para la construcción de su régimen jurídico. Es importante que los Estados de la región presten particular atención a este antecedente como guía para adecuar su normativa interna en materia de acceso a la información a los estándares internacionales.

El reconocimiento del derecho de acceso a la información en poder del Estado como derecho humano implica también la necesidad de garantizarlo a través de una protección judicial adecuada, para que de forma rápida y expedita se pueda obtener su protección. En este sentido es importante resaltar que, por los hechos específicos del caso Claude Reyes, el amplio contenido del derecho de acceso a la información en poder del Estado no ha sido aún descrito de forma integral por la Corte y los hechos de casos futuros podrán ayudar a delinear su alcance.

c. Antecedentes regionales e internacionales sobre el Derecho al Acceso a la Información.

c.1. Organización de Naciones Unidas.

El artículo 19 del Pacto Internacional de Derechos Civiles y Políticos de Naciones 33. Unidas (PIDCP) adoptado por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, vigente desde 1976, cuyo texto es similar al de la Declaración Universal, establece que:

Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

La Comisión de Derechos Humanos de Naciones Unidas creó la Relatoría 34. Especial para la Libertad de Opinión e Información en marzo de 1993. Desde 1998 el Relator Especial de las Naciones Unidas sobre Libertad de Opinión y Expresión ha declarado inequívocamente que el derecho de acceso a la información en poder de las autoridades del Estado está protegido por el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos28. Posteriormente, en su informe anual de 1999 el referido Relator enfatizó el derecho de acceso como derecho en sí mismo y destacó ciertos principios que lo rigen. (CdE ;1949)

La redacción del artículo 19 del PIDCP y de la Declaración Universal permite 35. inferir que se protege igualmente el derecho de buscar y recibir información30, de forma similar a como se ha interpretado el contenido y alcance del artículo 13 de la Convención Americana.

En 1998 la Comisión Económica para Europa, una de las cinco comisiones regionales de las Naciones Unidas, adoptó la “Convención sobre el acceso a la información, la participación del público en la toma de decisiones y el acceso a la justicia en asuntos ambientales”, en el marco de la Conferencia Ministerial “Medio Ambiente para Europa”, celebrada en Aarhus, Dinamarca, instrumento conocido como el Convenio de Aarhus.

C.2. Consejo de Europa.

El derecho a la libertad de expresión se encuentra establecido en el artículo 10 39. del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, abierto para la firma por el Consejo de Europa en 1950 y vigente desde 1953. Dicho artículo no incluye expresamente el derecho de buscar información y, en lo pertinente, señala que:

> *Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. […]*

A su vez, el artículo 8 del Convenio Europeo consagra el derecho al respeto a la vida privada y familiar. El Tribunal Europeo de Derechos Humanos ha interpretado que en ciertas circunstancias dicho artículo protege aspectos relacionados con el acceso a la información de las personas. El artículo 8 establece que:

> *1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.*

> *2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el* bienestar *económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*

La Asamblea Parlamentaria del Consejo de Europa ha emitido numerosas recomendaciones y resoluciones que se relacionan con el derecho de acceso a la información y con la necesidad de que se entienda como parte del derecho a la libertad de expresión e información descrito en el artículo 10 del Convenio Europeo. El 23 de enero de 1970 emitió la Recomendación No. 582 sobre medios de comunicación masiva y derechos humanos, mediante la cual realizó recomendaciones al Comité de Ministros en materia de "derecho a la libertad de información". Al respecto, recomendó instruir al Comité de Expertos en Derechos Humanos a que considerara e hiciera recomendaciones sobre:

> *La ampliación del derecho a la libertad de información establecido en el artículo 10 de la Convención Europea de Derechos Humanos, a través de la adopción de un protocolo o de otra manera, de forma tal que se incluya la libertad de buscar información (la cual está incluida en el artículo 19.2 del Pacto Internacional de Derechos Civiles y Políticos); y debe existir el correspondiente deber de las autoridades públicas de hacer accesible la información sobre asuntos de interés público, sujeta a las limitaciones apropiadas […].*

Ese mismo día, emitió la Resolución No. 428 contentiva de una declaración sobre medios de comunicación masiva y derechos humanos, en la cual afirmó que el derecho a la libertad de expresión debe incluir el derecho de buscar información, así como que debe existir "el correspondiente deber de las autoridades públicas de hacer accesible la información sobre asuntos de

interés público dentro de los límites razonables […] (Claude Reyes y otros Vs. Chile ;2006)

Asimismo, en su Resolución N.º 854 adoptada el 1 de febrero de 1979, recomendó al Comité de Ministros “invitar a los Estados Miembros, que no lo hubieren hecho, a introducir un sistema de libertad de información”39 que incluyera el derecho a buscar y recibir información de las agencias y departamentos gubernamentales.

El 9 de abril de 1982 el Comité de Ministros adoptó una “Declaración sobre libertad de expresión e información”, en la cual expresó el objetivo de buscar una política de apertura de información en el sector público40, así como la protección del derecho de todos a buscar y recibir información e impartir dicha información, de acuerdo con las condiciones establecidas en el artículo 10 del Convenio Europeo.

El 21 de febrero de 2002 el Comité de Ministros del Consejo de Europa emitió una recomendación sobre el derecho de acceso a documentos oficiales en poder de las autoridades públicas42. En dicha recomendación el Comité, tomando en consideración los artículos 19 del PIDCP y el artículo 10 del Convenio Europeo, declaró que “los Estados miembros deben garantizar el derecho de toda persona de tener acceso, a solicitud, a los documentos oficiales en poder de las autoridades públicas. Este principio debe aplicarse sin discriminación de ninguna naturaleza, incluyendo aquella referida al origen nacional”.

C.3. Sistema Africano de Derechos Humanos.

En este Sistema, el derecho a la libertad de expresión se encuentra establecido en el artículo 9 de la Carta Africana de Derechos Humanos y de los Pueblos (en lo sucesivo “la Carta Africana”), también denominada Carta de Banjul, la cual expresa que:

1. Todo individuo tendrá derecho a recibir información.
2. Todo individuo tendrá derecho a expresar y difundir sus opiniones, siempre que respete la ley. (Organización de Estados Americanos ;2007)

En el Sistema Africano se reconoce el derecho de acceso a la información en poder del Estado como derecho contenido en el de libertad de expresión. El 23 de octubre de 2002 la Comisión Africana emitió la Declaración de Principios sobre Libertad de Expresión en África, en cuyo capítulo titulado "libertad de información" sostiene que los organismos públicos tienen información como custodios del bien común, así como afirmó que todos tienen derecho de acceder a dicha información, sujeto solamente a reglas claramente establecidas por la ley Dicho capítulo establece que:

1- Los organismos públicos tienen información no para ellos, sino como custodios del orden público y todos tienen derecho de acceso a dicha información, sujeto solo a limitaciones claramente establecidas por la ley.
2- El derecho a la información debe ser garantizado por ley, de conformidad con los siguientes principios:

- *Todos tienen derecho de acceso a la información en poder de entidades públicas;*
- *Todos tienen derecho de acceso a la información que sea necesaria para el ejercicio o la protección de todo derecho y que esté en poder de entidades privadas;*
- *Cualquier negativa de suministrar información debe estar sujeta a apelación ante una entidad y/o tribunal independiente;*

- *Se debe requerir activamente a las entidades públicas, aún en ausencia de una solicitud, que hagan pública información importante de gran interés público;*
- *Nadie puede estar sujeto a sanción por suministrar de buena fe información equivocadamente, o aquella que revele una seria amenaza a la salud, seguridad del medioambiente, salvo cuando la imposición de sanciones persiga un interés legítimo y sea necesaria en una sociedad democrática; y*
- *Las leyes de información reservada deben ser enmendadas de forma tal que sean compatibles con los principios de libertad de información.*

3- Todos tienen derecho de acceder y actualizar o corregir su información personal, sea que se encuentre en poder de entidades públicas o privadas.

c.4.Mancomunidad Británica de naciones (British Commonwealthe Of Nations)

Los cincuenta y tres Estados miembros que conforman la asociación del Commonwealth trabajaron sobre el derecho a la información desde 1980. En 1999 el Commonwealth adoptó los Principios de Libertad de Información, en los que recomendó a los Estados que reconozcan la libertad de Información como un derecho legal y justiciable, así como que se rijan por la presunción a favor del suministro de información. En el 2002 la Secretaría del Commonwealth diseñó una ley modelo sobre libertad de información, con el propósito de que los Estados se guíen por ella. (Relatoria Especial ;2007)

c.5. Caso Claude Reyes y Otros Vs. Chile Sentencia de 19 de septiembre de 2006 (Fondo, Reparaciones Y Costas)

En 1998 los Sres. Marcel Claude Reyes, Sebastián Cox Urrejola en representación de varias ONG's y fundaciones relacionadas con la protección de los derechos civiles y el medio ambiente, y el diputado Arturo Longton Guerrero solicitaron al Comité de Inversiones Extranjeras, toda la información referente a dos empresas de capital extranjero con las que el Estado chileno había firmado un contrato para que se hicieran cargo de un proyecto, denominado "Río Condor", que tenía por objeto la deforestación de una determinada región de Chile, y que podría ser perjudicial para el medio ambiente e impedir el desarrollo sostenible de ese país.

Dicha Comisión no ofreció respuesta a las solicitudes presentadas, por lo que se iniciaron acciones judiciales, al entender que la ausencia de una respuesta y de una negativa formal había supuesto un perjuicio a la causa ciudadana y había lesionado el interés público, incumpliendo las obligaciones a las que está sujeta dicha entidad estatal de acuerdo con la normativa nacional e internacional sobre la materia. Tras pasar por distintas instancias judiciales, no obtuvieron respuesta satisfactoria a su pretensión, por lo que acudieron a la Comisión Interamericana de Derechos Humanos.

La Comisión, tras llevar a cabo la oportuna instrucción de la denuncia formulada, aprobó un informe en virtud del cual concluyó que el Estado chileno había violado el derecho de acceso a la información pública de los recurrentes, previstos en los artículos 13 y 25 de la Carta Americana sobre Derechos Humanos (CADH), al haberles negado el acceso a la información que estaba en poder del Comité de Inversiones Extranjeras y al no otorgarles acceso a la justicia chilena para impugnar esa denegación. (INFORME 31/05 ;2005)

Asimismo, recomendó, en primer lugar, que se facilitase a los recurrentes la información solicitada; en segundo lugar, que se les otorgase una reparación

adecuada a todos ellos; en tercer lugar, que se adaptase el ordenamiento jurídico interno, de acuerdo con el art. 13 CADH respecto al acceso a la información; y finalmente, que se adoptasen las medidas necesarias para crear prácticas y mecanismos que garanticen a los ciudadanos un acceso efectivo a la información pública y a la información de interés colectivo. Tras concluir el plazo fijado por la Comisión para que el Estado chileno cumpliera con las recomendaciones formuladas, y, al comprobar que no se habían adoptado sus recomendaciones de forma satisfactoria, la Comisión decidió someter el caso a la jurisdicción de la Corte, al entender que se había producido una posible vulneración del art. 13 de la CADH (libertad de pensamiento y de expresión) en relación con los artículos 1 y 2 de la misma. (Vivas ;2015)

La Corte, antes de entrar a analizar si la restricción al acceso a la información por parte de las autoridades chilenas supone una vulneración del art. 13 CADH, se encarga de analizar el objeto de la controversia. En este sentido, el tribunal comienza afirmando, sin género de dudas, que la información que se había solicitado y que no se había facilitado por el Estado chileno es información que reviste interés público. A continuación, la Corte recuerda su jurisprudencia sobre la libertad de pensamiento y de expresión reconocida en el art. 13 de la Convención.

Así, resalta que, de acuerdo con su jurisprudencia, este derecho comprende “no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir informaciones e ideas de toda índole” (Caso López Álvarez vs Honduras ;2006) y establece un derecho positivo a buscar y a recibir información. No obstante, la Corte va más allá, y afirma que cuando la CADH hace referencia al derecho a buscar y a recibir informaciones está protegiendo el derecho que tiene toda persona a solicitar el acceso a la información que se encuentre bajo el control del Estado.

Ahora bien, este derecho no es absoluto, sino que se somete a los límites fijados en el propio texto convencional (Claude Reyes y otros Vs. Chile, par.76). De este modo, la Corte reconoce, por un lado, el derecho de las personas a recibir dicha información y, por otro lado, la obligación positiva del Estado a suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información, o recibir una respuesta fundamentada cuando, por algún motivo permitido por la Convención, el Estado pueda limitar el acceso la misma para ese caso en concreto.

Además, la Corte considera que la información debe ser entregada sin que sea necesario acreditar un interés directo o personal, salvo en aquellos casos en los que existan restricciones legítimas, ya que lo que se protege no es sólo la dimensión individual sino también la social. En este sentido, la Corte subraya que el acceso a la información de una determinada persona puede permitir a su vez que ésta circule en la sociedad de manera que pueda conocerla, acceder a ella y valorarla (Claude Reyes y otros Vs. Chile, par.77).

Para llegar a esta interpretación, la Corte se basa en el consenso que sobre esta materia existe en la Organización de Estados Americanos que, en diversas resoluciones ha destacado la importancia del acceso a la información pública, así como la importancia de garantizarlo (Resolución Asamblea General 2003, 2004, 2005 y 2006), y, sobre todo, en el necesario control democrático que debe existir en todo Estado. En este sentido, la Corte considera que las actuaciones del Estado deben regirse por los principios de publicidad y transparencia en la gestión pública, en virtud de los cuales que se permita a las personas que se encuentran bajo su jurisdicción ejercer el control democrático de las gestiones estatales, de manera que puedan cuestionar, indagar y considerar si se está dando un adecuado cumplimiento de las funciones públicas y, de ese modo, permitir la participación en la gestión pública, a través del control social que se puede ejercer con dicho acceso (Claude Reyes y otros Vs. Chile, par.86).

Asimismo, la Corte insiste en la idea de que el control democrático por parte de la sociedad a través de la opinión púbica fomenta la transparencia de las actividades estatales y promueve la responsabilidad de los funcionarios sobre su gestión pública, y por ello, para que las personas puedan ejercer dicho control democrático es esencial que el Estado garantice el acceso a la información de interés público que se encuentra bajo su control. (Vivas ;2015)

Por otro lado, la Corte reconoce que el derecho de acceso a la información, al igual que el derecho a la libertad de pensamiento y de expresión, admite restricciones, aunque éstas han de cumplir con una serie de requisitos para que sean legítimas.

El primero de los requisitos que se exige es que cualquier limitación a este derecho ha de ser fijada previamente por ley formal, por razones de interés general y con el propósito para el que haya sido establecida (Claude Reyes y otros Vs. Chile, par. 89). Así se asegura que no se deja al arbitrio del poder público.

El segundo requisito que exige la Corte es que la restricción establecida debe responder a un objetivo permitido por la Convención, es decir, que la limitación sea necesaria para asegurar el respeto a los derechos o a la reputación de los demás o a la protección de la seguridad nacional, el orden público o la salud o moral pública.

El tercer requisito consiste en que cualquier restricción que se imponga sea necesaria en una sociedad democrática, esto es, que esté orientada a satisfacer un interés público imperativo. Y que entre las distintas opciones que puedan darse para alcanzar dicho objetivo, debe escogerse aquella que restrinja menos el derecho protegido. Es decir, la restricción debe ser proporcional al interés que la justifica y debe ser conducente para alcanzar el logro de ese legítimo objetivo, interfiriendo en la menor medida posible en el efectivo ejercicio del derecho.

Tras aclarar los requisitos que deben concurrir para que una restricción al derecho sea legítima, el Tribunal insiste en la idea de que la regla general es la de máxima divulgación, ya que es la que se corresponde con una sociedad democrática, y que corresponde a los Estados demostrar que las limitaciones que se impongan al derecho cumplen con los requisitos antes enumerados.

Es en este punto cuando la Corte, analizando los hechos que traen causa de esta sentencia, constata que en este caso no se cumplieron dichos requisitos, ya el Estado chileno no demostró que la restricción respondiera a un objetivo previsto en la CADH, ni que fuera necesaria en una sociedad democrática, pues la autoridad encargada de responder a la solicitud de información no adoptó una resolución escrita fundamentada que pudiera permitir conocer los motivos para limitar el acceso a la información en ese caso en concreto, por lo que considera que la restricción aplicada en este caso no cumplió con los parámetros convencionales. Es más, a este respecto, la Corte indica que el establecimiento de restricciones al derecho de acceso a información bajo el control del Estado a través de la práctica de sus autoridades, sin la observancia de límites convencionales crea un campo fértil para la actuación discrecional y arbitraria del Estado en la clasificación de la información como secreta, reservada o confidencial, generándose inseguridad respecto al ejercicio de dicho derecho y las facultades del Estado para restringirlo (Claude Reyes y otros Vs. Chile, par. 98)

Bajo las circunstancias arriba descritas, la Corte acordó que el Estado chileno había vulnerado el art. 13 CADH en relación con los artículos 1.1 y 2 de la misma, en ese entendido a criterio del tesista, es evidente que la propuesta de Ley, no es contraria a Convención Americana sobre Derechos Humanos, por consiguiente, saldría victoriosa al someterse a un Control de Convencionalidad.

Mas aun si tomamos en cuenta que la misma Corte Interamericana de Derechos Humanos ha fijado requisitos, entre los cuales exige a los Estados

la creación de una norma específica, que restrinja la información en conformidad a los establecido en el Pacto de San José de Costa Rica, situación que podría ser cubierta con la confección de un proyecto de Ley que proteja los Datos Personales.

4.3. Prohibición de Censura Previa.

El Artículo 13 de la Convención prohíbe la censura previa, salvo con el exclusivo objeto de regular el acceso a espectáculos públicos para la protección moral de niños y adolescentes. En casos contenciosos, tanto la Comisión como la Corte han interpretado esta disposición en sentido estricto.

La Convención permite la imposición de restricciones sobre el derecho de libertad de expresión con el fin de proteger a la comunidad de ciertas manifestaciones ofensivas y para prevenir el ejercicio abusivo de ese derecho. El artículo 13 autoriza algunas restricciones al ejercicio de este derecho, y estipula los límites permisibles y los requisitos necesarios para poner en práctica estas limitaciones. (Francisco Martorell vs Chile 1996)

El principio estipulado en ese artículo es claro en el sentido de que la censura previa es incompatible con el pleno goce de los derechos protegidos por el mismo. La excepción es la norma contenida en el párrafo 4, que permite la censura de los "espectáculos públicos" para la protección de la moralidad de los menores.

La única restricción autorizada por el artículo 13 es la imposición de responsabilidad ulterior. Además, cualquier acción de este tipo debe estar establecida previamente por la ley y sólo puede imponerse en la medida necesaria para asegurar: a) el respeto de los derechos o la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. (Francisco Martorell vs Chile 1996)

La interdicción de la censura previa, con la excepción que prevé el párrafo 4 del artículo 13, es absoluta. Esta prohibición existe únicamente en la Convención Americana. La Convención Europea y el Pacto sobre Derechos Civiles y Políticos no contienen disposiciones similares. Constituye una indicación de la importancia asignada por quienes redactaron la Convención a la necesidad de expresar y recibir cualquier tipo de información, pensamientos, opiniones e ideas, el hecho de que no se prevea ninguna otra excepción a esta norma.

El carácter fundamental del derecho de libertad de expresión fue subrayado por la Corte cuando declaró que:

La libertad de expresión es un elemento fundamental sobre el cual se basa la existencia de una sociedad democrática. Resulta indispensable para la formación de la opinión pública. También constituye una conditio sine qua non para el desarrollo de los partidos políticos, los gremios, las sociedades científicas y culturales y, en general, de todos los que desean influir al público. En resumen, representa la forma de permitir que la comunidad, en el ejercicio de sus opciones, esté suficientemente informada. En consecuencia, puede decirse que una sociedad que no está bien informada no es verdaderamente libre. (Francisco Martorell vs Chile 1996, parr.57)

Por consiguiente es necesario hacer una análisis propio que determine la posibilidad de implementar una Ley de protección de los datos personales, sin que pueda ir en disconformidad con la Convención Americana de los Derechos Humanos, bajo esa línea debo manifestar que la norma citada en su Art. 13 numeral 2, prohíbe la Censura Previa, no así la facultad de independencia legislativa que pueda tener un Estado parte para legislar en materia internas, más al contrario como se ha demostrado líneas arriba, la CIDH, incita a que se recoja las experiencias de diferentes países del mundo para poder

confeccionar una ley que brinde tutela al derecho de la protección de los datos personales.

Debemos tomar muy en cuenta que países como Uruguay y Argentina entre otros que están en camino, se han adherido a los razonamientos manejados por el Sistema de Protección Europeo, pues sería limitativo para el Estado boliviano afirmar que en aplicación al Control de Convencionalidad se encontraría impedido de poder implementar una norma de protección de datos personales, pues no debemos olvidar que la misma Corte Interamericana de Derechos Humanos establece doce (12) principios los cuales tienen por objetivo evitar daños a las personas derivados de la obtención o del uso incorrecto o innecesario de sus datos personales.

Así también debemos manifestar que la misma CIDH, ha sentado jurisprudencia en denominada Sentencia Francisco Martorell vs Chile, en la cual estipula que: “Al reglamentar la protección de la honra y de la dignidad a que hace referencia el artículo 11 de la Convención Americana y al aplicar las disposiciones pertinentes del derecho interno sobre esa materia los Estados Parte tienen la obligación de respetar el derecho de libertad de expresión. La censura previa, cualquiera sea su forma, es contraria al régimen que garantiza el artículo 13 de la Convención” (1996, parr.74)

De lo anterior claramente podemos resaltar que la misma Convención manifiesta la facultad que tienen los Estados parte, de reglamentar la protección de la honra y la dignidad referida en el Art. 11 de la Convención y aplicar disposiciones legales internas, por lo tanto, la creación de una norma de Protección de Datos personales, no significaría encuadrarse en la prohibición de la censura previa.

La censura previa es la censura materializada en la facultad de aprobar o prohibir determinado material o expresión antes de hacerse público, en este caso insistimos que no se está haciendo ninguna prohibición previa, sino se

está proponiendo la implementación de una norma especial que precautele un derecho fundamental.

CAPÍTULO V

LA PROTECCIÓN DE DATOS PERSONALES EN LA LEGISLACIÓN COMPARADA.

5.1. Desarrollo en las Constituciones Latinoamericanas.

La Constitución de Brasil adoptó el hábeas data como un recurso para garantizar la protección de las informaciones privadas relativas a la persona. Como señala Danilo Doneda:

La información personal es, casi por reflejo vinculado a la privacidad mediante una simple ecuación básica que asocia un mayor grado de privacidad a la menor de la información personal y viceversa. Esta ecuación al momento de la terminación de todos los complejos problemas que rodean a esta relación, puede servir como un punto de partida para ilustrar cómo la protección de la información personal vino a buscar refugio en nuestro sistema legal: como una rama de la protección del derecho a la privacidad.

Es el apartado X y LXXII del artículo 5 de la Constitución que protege la información personal, en derechos como la intimidad, la vida privada etc., y el hábeas data como una garantía sobre el acceso a las informaciones relativas a la persona bajo la protección de los derechos de la inviolabilidad de la intimidad y la vida privada.

En el caso de **Colombia**, el artículo 15 de la Constitución advierte la protección de datos personales a través del derecho a la intimidad personal y buen nombre; así como también a través del derecho de conocer, actualizar y rectificar la información. Sobre esta base de libertades y demás garantías reconocidas en la Constitución, “el constituyente definió la protección de la intimidad de la persona, cuando ella es fuente de información personalísima y

cuando esa información se encuentra en los llamados bancos de datos, públicos o privados". (Tovar ;2008)

La Constitución Nacional de Paraguay no contempla un derecho específico. Su protección se precisa en el derecho a la intimidad y garantía del hábeas data consagrados en los artículos 33 y 135, respectivamente. Al respecto, la doctrina considera que el hábeas data está orientado a:

Garantizar el acceso a las informaciones y datos sobre sí misma o sobre su patrimonio que se encuentren en registros oficiales o privados de público acceso. Así mismo, toda persona está legitimada para conocer el empleo o los fines de esas informaciones y datos, así como para solicitar ante el juez competente, en caso de error o cuando se viole un derecho de la persona, su actualización, corrección o destrucción. (Norbert Losing ,2002)

La Constitución Política de Chile tampoco contempla un derecho fundamental y, además, del hábeas data desde el nivel constitucional. De tal suerte que, la protección de este derecho se considera sobre la base del derecho a la vida privada consagrado en el numeral 4 del artículo 19. Como señala Renato Jijena, urgen reformas en el ámbito constitucional para determinar un derecho de carácter autónomo, así como constitucionalizar el hábeas data y considerar una autoridad autónoma que ejerza su protección.28 Para este fin, en 2014 se presentó un proyecto de reforma constitucional29 que a la fecha se mantiene en etapa de tramitación. El texto incluye, precisamente, la modificación del numeral 4 del artículo 19 de la Constitución.

5.2. Ámbito sectorial del tratamiento de información de carácter personal.

Al no contemplarse en la **Constitución Federal de Brasil** la protección de datos personales como un derecho fundamental, su protección se desarrolla mediante leyes sectoriales como la Ley No. 929631 y Ley No. 950732 que aprueba el procedimiento del hábeas data.

En el caso de **Colombia**, la Ley 126633 desarrolla las disposiciones generales del hábeas data. Esta Ley se considera como una garantía que “refiere a la protección y respeto del derecho a la autodeterminación informativa que contiene la intimidad e idoneidad personal que surge de la información suministrada por esta, según se deduce de lo consagrado en el artículo 15 de la Carta Política”. (Tovar ;2008)

Asimismo, se destaca la Ley Estatutaria 158135 destinada a establecer disposiciones generales para la protección de datos personales. Es importante señalar que Colombia cuenta con el reconocimiento internacional de su autoridad de protección de datos personales otorgada por la “Conferencia Internacional de Comisionados de Protección de Datos y Privacidad”. (Ordoñez ;2017)

Por su parte, en **Paraguay** la Ley No. 1682/0138 se orienta a proteger y garantizar el ejercicio de los derechos fundamentales de los titulares de la información. Si bien es cierto, la jurisprudencia ha definido el contenido del derecho a la autodeterminación informativa y hábeas data; en un estudio realizado por la Corte Suprema se estima que, entre otras carencias “el nivel de protección que ofrece la legislación nacional –Ley No. 1682/2001 y Ley No. 1969/2002– es insuficiente, a efectos de que Paraguay se acredite como nación “adecuada” ante los organismos de la Unión Europea”. (Ordoñez ;2017)

En el caso de **Chile**, a partir del panorama incierto en la Constitución, la protección de este derecho se ha fortalecido sobre la garantía del hábeas data prevista en la Ley No. 1962840 sobre la protección de la vida privada.

Finalmente, en **Bolivia** la Ley No. 164 se destina a proteger las telecomunicaciones y tecnologías de la información y la comunicación. En el caso de Bolivia, en el siguiente capítulo se hará un análisis a profundidad sobre las normas concernientes a protección de datos personales que se encuentran en vigencia.

5.3. Derecho fundamental a la autodeterminación informativa, en la jurisprudencia Latinoamérica.

El Supremo Tribunal Federal de Brasil mediante resolución 103236 ha señalado que:

La Ley 9296/1996 no hizo más que establecer directrices para resolver los conflictos entre la privacidad y la obligación del Estado de hacer cumplir las leyes penales. A pesar del carácter excepcional de la medida, el artículo XII posibilita, expresamente, una vez cumplidos los requisitos constitucionales, la interceptación de las comunicaciones telefónicas. Y tal permiso existe, por el simple hecho de que los derechos y garantías constitucionales no pueden servir de manto protector a prácticas ilícitas.

Asimismo, este Tribunal mediante resolución 673707 considera que:

4. El carácter público de todo registro o base de datos que contiene información que sea o puedan ser transmitidas a terceros y que no sea de uso privativo de un organismo o entidad productora o depositaria de información es inequívoco. (art. 1, Ley No. 9507/97). 5. El registro de datos debe ser entendido en su sentido más amplio, abarcando todo lo que diga respecto al interesado, sea de modo directo o indirecto (...) 6. Para interpretación el Hábeas Data extiéndase a personas físicas y jurídicas, nacionales y extranjeras, por cuanto es garantía constitucional de los derechos individuales y colectivos.

En este contexto, Brasil contextualiza la protección de los datos personales en el derecho a la intimidad en las comunicaciones, y mediante el hábeas data como acción de control constitucional. A pesar de que el derecho a la autodeterminación informativa no tiene asignación en la Constitución, puede considerarse que “el dato positivo es que no puede afirmarse que el ordenamiento brasileño este completamente al margen de estos matices”.42

Asimismo, la Corte Constitucional de Colombia en la Sentencia de Tutela No. 175/95 expone que:

El derecho al hábeas data, consagrado en el artículo 15 de la C P, constituye un derecho fundamental claramente diferenciado del derecho a la intimidad y el buen nombre. La jurisprudencia constitucional ha delimitado el alcance del derecho al hábeas data: ¿Cuál es el núcleo esencial del hábeas data? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica.

En otro fallo, la misma Corte en la Sentencia de Inconstitucionalidad No. 336/07 señala que:

En cuanto al derecho fundamental al hábeas data o a la autodeterminación informática, en diversas oportunidades la jurisprudencia de esta Corporación se ha referido a la naturaleza fundamental de este derecho, el cual comporta un plexo de facultades tales como la de disponer de la información sobre sí mismo, la de preservar la propia identidad informática, es decir, permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás.

El desarrollo teórico y práctico en **Colombia**, para la regulación del derecho a la autodeterminación informativa, es importante ya que cuenta con la protección en el ámbito constitucional, sectorial e institucional orientado a materializar la tutela de este derecho.

Por otra parte, la **Corte Suprema de Paraguay**, mediante Acuerdo y Sentencia No. 5, sobre el derecho a la autodeterminación informativa, expone que:

El objeto de esta Institución es la persona (en su fuero íntimo, en su ámbito privado) y sus bienes (entendido como reserva y completitud), los ciudadanos debemos conocer el uso y destino dado a la información o dato sobre nuestras

personas y bienes. Esto nos permite, a través de la garantía constitucional, solicitar ante el órgano judicial competente la ACTUALIZACIÓN, LA RECTIFICACIÓN O SUPRESIÓN de aquellos, considerados erróneos o que afectaren ilegítimamente nuestros derechos. Los términos atizados por la Constitución; "INFORMACIÓN" refiera a la acción y efecto de enterar, instruir, y "DATO" a los antecedentes que permiten llegar más fácilmente a conocimiento de una cosa.

La misma resolución estima que el derecho a la protección de datos tiene la naturaleza de un derecho genérico; esto significa que constituye un plexo de derechos específicos, de los cuales se nutre y recibe su contenido. Estos derechos constituyen el derecho a conocer, el derecho a acceder a los datos o información, y el derecho de rectificar o destruir los mismos.

En el caso de **Chile**, la Corte de Apelaciones de Temuco mediante Resolución No. 61146 señala que:

En el derecho a la autodeterminación informativa se encuentra implícito en el derecho fundamental a la vida privada [...] el derecho a la autodeterminación informativa consiste en la facultad que tiene una persona de ejercer control sobre sus documentos, información o datos personales que se encuentren en registros o bancos de datos públicos o privados.

Asimismo, en otro fallo la Corte de Apelaciones de Santiago mediante Resolución No. 1849-10 expone que la protección de datos personales contemplada en la Ley 19628:

Se traduce en el control de las personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros o archivos de registro de información de carácter personal, públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos

archivos o ficheros, teniendo el derecho a actualizarlos o a solicitar mediante el recurso de hábeas data su rectificación o cancelación.

Se puede considerar que Chile, al igual que Colombia, es uno de los países que más ha avanzado en los últimos años. Así se desprende de la regulación materializada en una Ley específica y en los proyectos constitucionales que buscan reformular su protección mediante un derecho específico.

CAPÍTULO VI

PROTECCIÓN DE LOS DATOS PERSONALES EN BOLIVIA

6.1. Normativa Constitucional.

Con la Constitución Política del Estado abrogada de 1995, se regula el "Recurso de Hábeas Data" en el artículo 23, el cual, a su vez, fue modificado por la Ley N.º 2410 de 2002, de 8 de agosto, quedando de la siguiente manera:

"I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya. 1. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado. III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo. 1. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa. 2. El recurso de Habeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19º de esta Constitución"

Con la actual Constitución Política del Estado, el número 2 del artículo 21 protege los datos personales a través del derecho a la privacidad e intimidad; y complementariamente, según lo dispuesto en el artículo 130 mediante la

acción de protección de privacidad. Sobre esta base, la acción de privacidad “conocida en el mundo jurídico como hábeas data, es una acción que protege los datos personales (edad, sexo, enfermedad, pertenencia política, etc.) de cada quien, y que figuran en centros de identificación, registro electoral, registros médicos, sistemas bancarios, etc. Estos datos son de propiedad exclusiva de su titular”. (Ordoñez ;2017)

Se puede decir que Bolivia ha pasado de un estado de regulación incierto, previo a la reforma constitucional de 2009, a un sistema más ordenado. Ha llegado a considerar la regulación del tratamiento de datos personales, aunque no con una ley en específica. Sobre todo, se ha consagrado a la protección de datos personales como un derecho de carácter fundamental.

6.1.1. El derecho a la intimidad o la vida privada.

Santivañez en su artículo denominado: El derecho a la protección de la vida privada y el derecho a la libertad de información en la doctrina y en la jurisprudencia. una perspectiva en Bolivia, manifiesta: ……” que el derecho a la intimidad o la vida privada consiste en la potestad o facultad que tiene toda persona para mantener en reserva determinadas facetas de su vida y personalidad, como las referidas al ámbito en el que se desenvuelve, a su ámbito afectivo, de sus convicciones y creencias, su ámbito familiar y relacional, así como al de la manifestación de su voluntad. Se trata de un derecho personalísimo que permite sustraer a la persona de la publicidad o de otras perturbaciones a la vida privada, que sin embargo está limitado por las necesidades sociales y los intereses públicos. (J. A. Santivañez ,2009)

En la doctrina constitucional boliviana, se ha entendido que se trata de un derecho que constituye obligaciones negativas para el Estado y los particulares, lo que significa la prohibición de injerencia o intromisión de extraños en la vida íntima o vida privada de la persona titular del derecho; de lo se puede inferir que surge el derecho a la protección de la vida privada,

constituyendo una obligación positiva para el Estado, consistente en la adopción de medidas legislativas, administrativas y jurisdiccionales para establecer vías y mecanismos de protección de la vida íntima o privada de la persona. Pero también se ha entendido que abarca la dimensión positiva con relación a su titular, lo que implica el derecho de la persona a acceder a un banco de datos público o privado a objeto de conocer cuánta información sobre su vida íntima o privada se ha recogido, almacenado o distribuido, con qué finalidad y a quiénes se ha distribuido; es a partir de ello que, en la reforma constitucional de 2004, (Ley 2631) se ha creado la garantía jurisdiccional de hábeas data.

Pablo Lucas Murillo de la Cueva sostiene que “el derecho a la privacidad se caracteriza por el rechazo de toda intromisión no consentida en la vida privada, sobre todo de los medios de comunicación, haciendo prevalecer las ideas de aislamiento y autonomía, especialmente en aspectos como la vida doméstica y las relaciones sexuales”. (Murillo de la Cueva ,1990, : pp. 57-58.)

6.1.2. El derecho a la inviolabilidad de las comunicaciones.

Santivañez en su artículo denominado: “El derecho a la protección de la vida privada y el derecho a la libertad de información en la doctrina y en la jurisprudencia. una perspectiva en Bolivia”, manifiesta que: “La inviolabilidad de correspondencia es un derecho que forma parte del contenido esencial del derecho a la intimidad o vida privada de la persona. Consiste en la potestad o facultad que tiene toda persona para mantener en reserva determinadas facetas de su personalidad referida a los medios relacionales, como son las comunicaciones telefónicas, de correspondencia u otros medios de comunicación; de manera que impone la obligación negativa para el Estado y otras personas de interceptar conversaciones o comunicaciones privadas” (J. A. Santivañez ,2009).

Dada su naturaleza jurídica este derecho constituye obligaciones negativas para el Estado y los particulares, la de no invadir la esfera privada de su titular, lo que supone la prohibición de incautar o interferir la correspondencia realizada por cualquiera de las vías, así como la prohibición de interceptar conversaciones o comunicaciones privadas. Este derecho puede ser vulnerado tanto por la intercepción en sentido estricto (aprehensión física del soporte del mensaje, independientemente de que el mismo se conozca o no) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo).

José Antonio Rivera dice: “Al igual que en el caso del derecho a la inviolabilidad de domicilio, por error de sistemática constitucional, este derecho está consagrado por el art. 20 de la Constitución; empero, forma parte del contenido esencial del derecho a la intimidad o la vida privada. La citada disposición constitucional textualmente prevé lo siguiente: “Son inviolables la correspondencia (...) Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones y comunicaciones privadas mediante instalación que las controle o centralice”. Adviértase que, con relación a las conversaciones y comunicaciones privadas, la norma constitucional es absoluta, toda vez que no permite por razón alguna la intercepción, sea estatal o particular, por razón o motivo alguno. Al respecto, cabe señalar que el legislador, mediante la Ley Nº 1632 de Telecomunicaciones, estableció una limitación al ejercicio de este derecho, pues en su art. 37 previó lo siguiente: “Salvo disposición judicial en favor de autoridad competente, queda terminantemente prohibido interceptar, interferir, obstruir, alterar, desviar, utilizar, publicar o divulgar el contenido de las telecomunicaciones”; como se podrá advertir, a la prohibición de interceptar o interferir las conversaciones telefónicas se estableció una excepción consistente en restringir el derecho previa orden judicial fundamentada expedida a favor de una autoridad competente, entiéndase el Ministerio Público o la Policía Judicial, en los casos

de investigación criminal. (J. A. Santivañez ,2009). Empero, la referida disposición legal fue declarada inconstitucional por el Tribunal Constitucional, mediante su sentencia SC 004/99, de 10 de septiembre. (1999)

Cumpliendo el mandato constitucional de interpretar la misma en conformidad con los Instrumentos internacionales en materia de derechos humanos, la C.P.E ha protegido y tutelado el Derecho a la privacidad y el Derecho a la vida privada, sin embargo, el último antecedente de vulneración de este derecho en nuestro país, es el reconocimiento por parte del titular del Ministerio de Gobierno, de haber interceptado conversaciones privadas:

Gobierno admite que escuchó charlas para atrapar al ministro Characayo (fuente periódico boliviano El Deber).- Textual:

"El ministro de Gobierno, Eduardo Del Castillo, reveló ayer que Inteligencia, con su avanzada tecnología, descubrió el caso de corrupción a su excolega de Desarrollo Rural, Edwin Characayo, quien fue capturado tras recibir en El Prado (a pocas cuadras de la Plaza Murillo, centro de la ciudad de La Paz), $us 20.000 de un supuesto adelanto de una coima que alcanzaba los $us 380.000, por saneamiento del predio El triunfo II, en Santa Cruz. La autoridad afirmó que "como elementos de convicción" hay "conversaciones telefónicas entre las personas que incitaron al acto de corrupción".

El titular de Gobierno señaló que "el equipo de Inteligencia del Gobierno, y la tecnología con la que cuenta es la capacidad suficiente que necesitamos para estar pendientes de todas las personas involucradas en este tipo de actos de corrupción que atentan contra la institucionalidad de nuestro país. Tampoco permitiremos que personas y grupos irregulares atenten contra los intereses del pueblo", manifestó.

Mostró imágenes del momento en que el exministro Characayo recibió en El Prado paceño la suma de $us 20.000, luego los colocó en la mochila de su

cómplice Híper García, ahora exdirector general de Desarrollo Rural. "Tenemos varios elementos de convicción, conversaciones telefónicas entre las personas que estarían incitando a la comisión de estos delitos, pero creemos que la cabeza de esta red de corrupción ha caído".

El ministro Del Castillo sustentó con esa afirmación que el exministro era el cabecilla de esta supuesta red de corrupción. También sugirió de alguna manera que los integrantes de la investigación hubieran "intervenido" llamadas telefónicas.

Es el mismo Estado que se constituye en vulnerador de este derecho, atentando contra la privacidad y la vida privada de las personas al instalar centrales de comunicación para efectuar lo que se denomina escuchas telefónicas. El mismísimo Ministro de Gobierno se encuentra compelido a cumplir sus funciones realizando un Control de Convencionalidad, pues no solo las autoridades jurisdiccionales se encuentran obligadas a ejercer control de convencionalidad, sino también las autoridades administrativas. (Caso Gelman Vs. Uruguay 2011), en ese sentido el titular de la cartera de Gobierno debe subordinar sus funciones a los Estándares Convencionales de los cuales el Estado boliviano es parte, así también se encuentra obligado a cumplir los estipulado por el Art. Numeral III, que prohíbe taxativamente las intervenciones telefónicas.

92. ... el "control de convencionalidad" constituye "una obligación" de toda autoridad de los Estados Parte de la Convención de garantizar el respeto y garantía de los derechos humanos, dentro de las competencias y regulaciones procesales correspondientes... (Caso Gelman Vs. Uruguay 2011)

6.1.3. Acción de Protección de Privacidad.

La inclusión dentro del **Título IV de unas Garantías jurisdiccionales y de acciones**, destacando en la **Sección Segunda del Capítulo Segundo, la**

Acción de Protección de Privacidad, **artículo. 130** señala: "***I.*** *Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar 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".*

El ***artículo 131*** *establece:* ***"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 ellos se suspenda la 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 lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la Ley".*

Para Rivera Santivañez, "el hábeas data se define como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la "autodeterminación informática" (2006, p. 219).

Para Pedro Néstor Sagüés, "el Hábeas Data era una especie de acción de amparo que no necesitaba de una regulación específica y bastaba con la normatividad general de la acción de amparo y subsidiariamente la aplicación de la Ley 16986, relativa a las relaciones jurídicas entre particulares y el

Estado, y el Código procesal civil y comercial de la nación (artículos 321 y 498), cuando surgían conflictos entre los particulares. (1997, p.137-150.)

La Constitución Política del Estado en vigencia establece la protección de la privacidad

6.2. Normas Infraconstitucionales.

- Código Civil, de 6 de agosto de 1975.

Artículo 15°. - (Nulidad) Son nulas toda confesión y toda manifestación de voluntad obtenidas por procedimientos lesivos a la personalidad.

Artículo 16°. - (Derecho a la imagen) Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo.

Se comprende en la regla anterior la reproducción de la voz de una persona.

Artículo 17°. - (Derecho al honor) Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.

Artículo 18°. - (Derecho a la intimidad) Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley.

- Ley № 1488 de 14 de abril de 1993. Ley de Bancos y Entidades Financieras.

Artículo 86°. - Las operaciones bancarias en general estarán sujetas al secreto bancario. No podrán proporcionarse antecedentes relativos a dichos operaciones sino a su titular, o a la persona que lo represente legalmente.

Artículo 87°. - El secreto bancario será levantado únicamente.

Mediante orden judicial motivada, expedida por un juez competente dentro de un proceso formal y de manera expresa, por intermedio de la Superintendencia.

Para emitir los informes ordenados por los jueces a la Superintendencia en proceso judicial y en cumplimiento de las funciones que le asigna la Ley.

Para emitir los informes solicitados por la administración tributaria sobre un responsable determinado, que se encuentre en curso de una verificación impositiva y siempre que el mismo haya sido requerido formal y previamente; dichos informes serán tramitados por intermedio de la Superintendencia.

Dentro de las informaciones que intercambian las entidades bancarias y financieras entre sí, de acuerdo a reciprocidad y prácticas bancarias.

Para emitir los informes de carácter general que sean requeridos por el Banco Central de Bolivia.

- Código Penal. Modificado por la Ley Nº 1768, de 10 de Marzo de 1997 (Artículo 363 Bis Manipulación informática) y Artículo 363 ter Alteración, acceso y uso indebido de datos informáticos.).

- Ley N.º 28168, de 18 de mayo de 2005. Acceso a la Información del Poder Ejecutivo.

ARTÍCULO 19.- (PETICIÓN DE HABEAS DATA). I. Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público. II. La petición de Habeas

Data se resolverá en el plazo máximo de cinco (5) días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad jerárquica competente, adicionalmente tendrá un plazo de quince (15) días hábiles para proporcionar la información solicitada. III. La petición de Habeas Data no reemplaza ni sustituye el Recurso Constitucional establecido en el Artículo 23 de la Constitución Política del Estado. El interesado podrá acudir, alternativamente, a la vía administrativa sin que su ejercicio conlleve renuncia o pérdida de la vía judicial. El acceso a la vía judicial no estará condicionado a la previa utilización ni agotamiento de esta vía administrativa.

- Ley No 3131 de 8 de agosto de 2005. Ley del Ejercicio Profesional Médico

Artículo 3°. - (Principios). - c) En el ejercicio profesional médico, inclusive en la enseñanza de la medicina, el secreto médico es inviolable salvo las excepciones previstas en la presente Ley.

Artículo 4°. - (Definiciones). - SECRETO MÉDICO: Toda información identificada durante el acto médico sobre el estado de salud o enfermedad del paciente, su tratamiento y toda otra información de tipo personal, debe mantenerse en secreto, inclusive después de su muerte, para salvaguarda de la dignidad del paciente.

Artículo 12°. - (Deberes del Médico) Son deberes del profesional médico: k. Guardar el secreto médico, aunque haya cesado la prestación de sus servicios.

Artículo 13°. - (Derechos del Paciente) Todo paciente tiene derecho a: c) La confidencialidad; d) Secreto médico; g) Reclamar y denunciar si considera que sus derechos humanos han sido vulnerados durante la atención médica; i) Respeto a su intimidad.

- Ley Nº 018, de 16 de junio de 2010, del Órgano Electoral Plurinacional. Artículos 72 (obligaciones); 74 (Registro y actualización de datos); 76 (Padrón

Electoral); 77 (Lista de habilitados e inhabilitados), y 79 (acceso a información del Padrón Electoral).

Artículo 79°. - (Acceso a información del padrón electoral). -La información estadística del Padrón Electoral es pública. Las organizaciones políticas podrán solicitar una copia digital de la misma al Servicio de Registro Cívico. La entrega de esta información se sujetará al calendario electoral establecido por el Tribunal Supremo Electoral. Las organizaciones políticas son las únicas responsables sobre su uso.

El Servicio de Registro Cívico, proporcionará anualmente datos demográficos y de residencia de las personas naturales al Consejo de la Magistratura para el sorteo de Jueces Ciudadanos.

El Servicio de Registro Cívico, proporcionará los datos solicitados de las personas naturales, a requerimiento escrito y fundamentado del Ministerio Público, de un Juez o de un Tribunal competente. Las autoridades requirentes, bajo responsabilidad, no podrán utilizar estos datos para ninguna otra finalidad.

Las instituciones públicas podrán solicitar la verificación de identidad de personas naturales, previo cumplimiento de las condiciones y requisitos establecidos mediante Reglamento por el Tribunal Supremo Electoral.

- Ley Nº 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de la Información y Comunicación.

Artículos 54 (derechos de los usuarios); 56 (inviolabilidad y secreto de las comunicaciones); 59 (obligaciones de los operadores y proveedores); 84 (reglamentación); 89 (correo electrónico personal); 90 (correo electrónico laboral), y 91 (comunicaciones comerciales publicitarias por correo electrónico o medios electrónicos).

Artículo 12°. - (Protección de datos personales y seguridad informática). - Las y los servidores y funcionarios de las instituciones previstas en la presente Ley, utilizarán los datos personales y la información generada en la plataforma de interoperabilidad y ciudadanía digital únicamente para los fines establecidos en normativa vigente.

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

- Ley № 1080, de 11 de Julio de 2018, de Ciudadanía Digital**.**

Artículo 11°. - (Prohibiciones y sanciones) El uso indebido, suplantación, alteración, modificación o venta de credenciales, datos o información, serán sancionados conforme a normativa vigente.

Artículo 12°. - (Protección de datos personales y seguridad informática). - Las y los servidores y funcionarios de las instituciones previstas en la presente Ley, utilizarán los datos personales y la información generada en la plataforma de interoperabilidad y ciudadanía digital únicamente para los fines establecidos en normativa vigente.

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

- Decreto Supremo Nº 1793, de 13 de noviembre de 2013. Reglamento de la Ley Nº 164 para el Desarrollo de Tecnologías de Información y Comunicación.

Artículos 3 (definiciones); 4 (principios), 40 (funciones de la Agencia de Registro); 54 (derechos del titular del certificado); 56 (Protección de datos personales), y 57 (comunicaciones comerciales publicitarias).

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:

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

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;

Las personas a las que se los 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.

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

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

- Decreto Supremo № 2514, de 9 de septiembre del 2015. Creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación — AGETIC.

ARTÍCULO 19.- (INTEROPERABILIDAD, DATOS E INFORMACIÓN). - I. La AGETIC coordinará con las entidades del sector público la implementación de servicios de interoperabilidad de Gobierno Electrónico, así como los datos e información que deben estar disponibles; II. Se autoriza a las entidades públicas proporcionar a la AGETIC los datos e información que hubieran producido, recolectado o generado, por medios electrónicos o mecanismos de interoperabilidad, que ésta solicite mediante nota formal de su MAE, en el marco de la política general de Gobierno Electrónico, simplificación de trámites, transparencia, participación y control social y tecnologías de la información y comunicación; III. El ente rector de Gobierno Electrónico determinará la política general y normativa específica de interoperabilidad e intercambio de información y datos entre las entidades del sector público.

- Decreto Supremo № 3251, de 11 de julio de 2017. Plan de Implementación de Gobierno Electrónico y Plan de Implementación de Software Libre y Estándares Abiertos.

Artículo 4°. - (INTEROPERABILIDAD). - El COPLUTIC, en coordinación con la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación — AGETIC, podrá determinar la obligatoriedad por parte de las

entidades públicas para compartir información mediante interoperabilidad, en el marco de las leyes y normas vigentes, así como disposiciones específicas de sectores estratégicos.

Las entidades públicas en el plazo de dos (2) meses de haber sido notificadas con la resolución del COPLUTIC, deberán habilitar a través de la AGETIC los accesos a la información objeto de la resolución.

Las entidades públicas que no cuentan con las condiciones técnicas para proporcionar la información objeto de la resolución, podrán solicitar ante la AGETIC la ampliación del plazo establecido en el Parágrafo precedente, previa justificación técnica de la entidad.

El Ente Rector del Gobierno Electrónico y Tecnologías de Información y Comunicación establecerá los mecanismos y condiciones de acceso a los datos disponibles en el marco del presente Artículo.

Las entidades del sector público, en el marco de sus funciones y atribuciones, sin perjuicio de la aplicación de lo establecido en el presente Artículo, podrán suscribir convenios de interoperabilidad, para garantizar el intercambio de información.

6.3. Jurisprudencia Constitucional Boliviana.

- **La Sentencia Constitucional 0965/2004-R, Sucre — 23 de junio de 2004 establece la protección que brinda el Habeas Data, así como sus diversos tipos:**

Siguiendo la doctrina del Dr. José Antonio Rivera Santivañez en su obra “Jurisdicción Constitucional”, el hábeas data se define como el proceso constitucional de carácter tutelar que protege a la persona en el ejercicio de su derecho a la “autodeterminación informática”.

Es una garantía constitucional que, sin desconocer el derecho a la información, al trabajo y al comercio de las entidades públicas o privadas que mantienen

centrales de información o bancos de datos, reivindica el derecho que tiene toda persona a verificar qué información o datos fueron obtenidos y almacenados sobre ella, cuáles de ellos se difunden y con qué objeto, de manera que se corrijan o aclaren la información o datos inexactos, se impida su difusión y, en su caso, se eliminen si se tratan de datos o informaciones sensibles que lesionan su derecho a la vida privada o íntima en su núcleo esencial referido a la honra, buena imagen o el buen nombre.

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.

Acción Subsidiaria.

Tomando en cuenta sus fines y objetivos , así como la aplicación supletoria de las normas previstas por el art. 19 de la CPE, dispuesta por el art. 23 parágrafo V antes referido, se entiende que el hábeas data es una acción de carácter subsidiario, es decir, que solamente puede ser viable en el supuesto que el titular del derecho lesionado haya reclamado ante la entidad pública o privada encargada del banco de datos, la entrega de la información o datos personales obtenidos o almacenados, y en su caso, la actualización, rectificación o supresión de aquella información o datos falsos, incorrectos, o que inducen a discriminaciones, y no obtiene una respuesta positiva o favorable a su requerimiento, o sea que la entidad pública o privada no asume

inmediatamente la acción solicitada. Dicho de otro modo, el hábeas data se activa exclusivamente cuando la persona demuestra que ha acudido previamente ante la entidad pública o privada para pedir la restitución de su derecho lesionado y no ha podido lograr la reparación a dicha vulneración.

- **Sentencia Constitucional 1738/2010-R Sucre, 25 de octubre de 2010.**

Del art. 130 de la CPE, se concibe que tanto las personas naturales y jurídicas tienen acceso a los derechos a la privacidad, intimidad, honra, honor, propia imagen y dignidad reconocido en el art. 21.1 de la CPE, entre uno de esos derechos esta la intimidad, que sin duda es uno de los bienes más susceptibles de ser lesionados o puesto en peligro por el uso de las nuevas tecnologías, por lo que se hace necesario colocar un límite a la utilización de la informática y las comunicaciones ante la posibilidad de que se pueda agredir a la intimidad de los ciudadanos y con ello se pueda coartar el ejercicio de sus derechos (Conde Ortíz Concepción, “La protección de datos personales: un derecho autónomo en base a los conceptos de intimidad y privacidad”), por lo mismo este mismo autor citando a Albaladejo, señaló que la intimidad consiste en “el poder concebido a la persona sobre el conjunto de actividades que forma su círculo íntimo, poder que le permite excluir a los extraños de entrometerse en él y de darle una publicidad que no desee el interesado”, así la jurisprudencia de España en su STC 134/1999 de 15 de julio, señaló que: “El derecho a la intimidad garantiza el individuo un poder jurídico sobre la información relativa a una persona o a su familia, pudiendo imponer a terceros, sean éstos simples particulares o poderes públicos, su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida”.

Ahora bien en lo que respecta a la privacidad personal o familiar, el mismo autor citando a Ruano Albertos, señaló que es “el poder de ejercer un control sobre las informaciones que le atañen a uno, teoría que viene a considerar la intimidad como el derecho a poder participar y controlar las informaciones que

concierne a cada persona", de igual forma hace una distinción entre intimidad y privacidad, señalando que la intimidad es "el conjunto de sentimientos, pensamientos e inclinaciones más internos, como la ideología, religión o creencias, las tendencias personales que afectan a la vida sexual, problemas de salud que deseamos mantener en secreto y otras inclinaciones"; mientras que, privacidad hace referencia "al ámbito de la persona formado por su vida familiar, aficiones, bienes particulares y actividades personales".

De todo lo anterior se tiene que tanto la intimidad como la privacidad son la base fundamental para la protección de todos los datos personales de las personas, que sólo le atingen a él o a ella, por lo mismo se encuentra facultado para determinar cuándo y dentro de qué límites pueden revelarse situaciones referentes a su propia vida, entendiéndose en consecuencia de que la acción de protección de privacidad, entre otros, protege la intromisión por parte de personas particulares y/o jurídicas a la vida íntima del ser humano que le corresponde como consecuencia del reconocimiento a su dignidad, por lo que la vulneración de estos derechos afectan directamente a su imagen, honra y reputación.

- **La Sentencia del Tribunal Constitucional sobre Recurso de Hábeas Data 1972/2011 de 7 diciembre 2011-R Sucre**.

Establece que la cancelación de antecedentes en actividades de narcotráfico, debía ser a través de orden judicial.

- **Sentencia Constitucional Plurinacional 0090/2014-S1 Sucre, 24 de noviembre de 2014.**

(…) la acción de protección de privacidad, constituye un medio procesal constitucional de protección de los datos personales, dirigido a la protección efectiva, inmediata y oportuna del derecho a la autodeterminación informática, en los supuestos en que éste sea transgredido por acciones u omisiones ilegales o indebidas. En ese sentido, por intermedio de ella, toda persona

natural o jurídica, puede acudir a la jurisdicción constitucional, para demandar a los bancos de datos y archivos de entidades públicas o privadas, persiguiendo el conocimiento, actualización, rectificación o supresión de las informaciones o datos contenidos en éste, que se hubiesen obtenido, almacenado o distribuido en los mismos.

- **Sentencia Constitucional Plurinacional 0819/2015-S3 Sucre, 10 de agosto de 2015, sobre la revictimización:**

(…) Lo anterior se evidencia del informe FGE/STRIA. GRAL./1/2015, emitido por el Ministerio Público y remitido ante este Tribunal, el cual señaló:

“La Fiscalía General del Estado no cuenta con un área de informática dentro de un proceso penal que le permita identificar y neutralizar las imágenes de contenido denigrante o sexual que se encuentren circulando por internet…” (las negrillas son nuestras) (fs. 308); por lo que se puede evidenciar que al no contar con una unidad especializada, ni haber gestionado convenios nacionales e internacionales pertinentes, el Ministerio Público no puede garantizar de una manera real y concreta los derechos de las víctimas ni de cualquier otra persona que vea derechos vulnerados en internet, pese que en el mismo informe también refieren que ya son treinta y siete los casos presentados en el territorio boliviano.

Ahora bien, para este Tribunal resulta claro que dentro de todo proceso penal el rol que asume el Ministerio Público es el de garantizar la no revictimización, al respecto, cabe señalar que toda actuación de la autoridad pública debe ser desde la perspectiva del respeto y garantía de los derechos humanos. Por lo referido clasificamos las obligaciones como negativas que implican el respeto y la abstención como es la de no discriminar, y obligaciones positivas vinculadas a la adopción de medidas de prevención; asimismo, la invocación efectiva de los derechos en las ya referidas obligaciones positivas y negativas, involucra cuatro niveles: obligaciones de respetar, de proteger, de asegurar y

de promover el derecho en cuestión, en ese sentido la obligación de respetar se traduce en el deber del Estado, sus servidores públicos y la sociedad de no intromisión, obstaculización o impedir el acceso al goce de los bienes que constituyen el objeto del derecho. Las obligaciones de proteger consisten en que el Estado y sus servidores públicos garanticen que terceros no vayan a interferir, obstaculizar o impedir el goce de esos derechos. Las obligaciones de asegurar suponen cerciorar que el titular del derecho acceda a éste cuando no puede hacerlo por sí mismo; y, las obligaciones de promover se caracterizan por el deber de desarrollar condiciones para que los titulares del derecho accedan al bien, es así que el Estado, servidores públicos y sociedad deben adoptar las medidas necesarias e idóneas para satisfacer el contenido de los derechos de manera que la igualdad y el ejercicio de los derechos no sea únicamente de manera formal, sino real y material.

CAPÍTULO VII

MARCO PRÁCTICO

7.1. PROPUESTA NORMATIVA.

7.1.1. DERECHO Y LA TECNOLOGÍA.

Las modernas tecnologías de la información y las comunicaciones (TIC o ITC), a resultas de la convergencia entre las telecomunicaciones y la informática, están provocando cambios significativos en todos los ámbitos (político, económico, tecnológico, sociológico) de las sociedades contemporáneas avanzadas. En este sentido, las tecnologías de la información y las comunicaciones, en la medida que representan la transformación de los formatos actuales de las más diversas acciones sociales e individuales (en la cultura, la ciencia, la economía, las relaciones laborales, etc.) y, al mismo tiempo, un incremento de las relaciones interpersonales a distancia y del tratamiento de la información personal, plantean problemas originales y complejos que exigen una adecuada respuesta del ordenamiento jurídico, que, obviamente, no ha de pretender el establecimiento de mecanismos de represión y obstáculos para su desarrollo, sino que, por el contrario, ha de tratar de impulsarlas, mediante el establecimiento y aplicación de un marco normativo adecuado que evite "las graves consecuencias" que, como en la informática, pudieran derivar de su desarrollo incontrolado para el ejercicio de los derechos y libertades. Desde una perspectiva de carácter general, los "tres órdenes de problemas", que, tradicionalmente se vinieron detectando con la aparición del fenómeno informático, son: los problemas de orden tecnológico, consistentes "en cómo impedir el acceso incontrolado a los sistemas de proceso de datos mediante la concepción y realización de unos dispositivos físicos o lógicos que le impidan"; los de orden deontológico, que exigen "la

creación de una mentalidad responsable por parte de los profesionales y la aceptación de unos códigos de ética informática"; y, finalmente, los problemas de orden jurídico, surgidos de la necesidad de creación y establecimiento de "un marco 150 conceptual que permita sistematizar supuestos de hechos posibles y darles una solución coherente y uniforme", se han incrementado en el "mundo de las telecomunicaciones", en el que "la habitual organización de sus servicios, puede incidir con especial intensidad sobre el delicado mundo de los datos", haciendo que la protección de datos de carácter personal y del secreto de las comunicaciones sean, en la actualidad, algunos de los ámbitos jurídicos en los que las modernas tecnologías de la información y las comunicaciones despiertan un mayor interés para la doctrina. Por tal motivo, siendo el derecho un instrumento privilegiado de la construcción de este nuevo espacio, resulta evidente que la investigación jurídica debe, en primer lugar, tomar un adecuado conocimiento de los fenómenos técnicos y sociales, para, a continuación, proceder al estudio de las normas que salen al encuentro de esa nueva realidad, pese a que el propio dinamismo del cambio tecnológico impide, en muchas ocasiones, el que podamos tener "una visión completa y acabada de todos y cada uno de los problemas a que puede dar lugar". No obstante, la toma en consideración del progreso tecnológico y de los nuevos fenómenos sociales que éste provoca, nos permite afirmar, como se ha pretendido por algunos, la puesta en discusión de los fundamentos mismos del ordenamiento jurídico vigente y tampoco establecer una autonomía como disciplina jurídica de las distintas cuestiones derivadas de las tecnologías de la información y de la comunicación (como también, en su momento, sucedió, debido al auge del fenómeno informático, con el denominado "derecho informático"). Nos encontramos, consiguientemente, en este campo (como en otros, derecho de la alimentación, derecho agrario, derechos de la circulación, etc.), ante lo que la doctrina italiana ha definido como "disciplinas informativas", que, como tales, "habrán de nutrirse siempre de principios muy diversos, cualitativamente heterogéneos según corresponde a las disciplinas

matrices de la que proceden". Ciertamente, no es posible aplicar los mismos principios técnico -jurídicos, por ejemplo, a la protección de datos, a los problemas derivados de la protección jurídica del software, o a los delitos cometidos por medios informáticos, o, en el concreto sector de las telecomunicaciones, respecto de las distintas importantes funciones que en el mismo se pueden suscitar y en el que se entrecruzan diversas ramas del ordenamiento jurídico (derecho administrativo, derecho mercantil y derecho comunitario, básicamente).

Por lo tanto, sin perjuicio de reconocer que el desarrollo de las tecnologías de la información y las comunicaciones, que, como en otros muchos ámbitos, siempre ha sido más rápido que el proceso de adaptación del ordenamiento jurídico, el sustentar una autonomía de este ámbito (llámese "derecho de las tecnologías de la información y las comunicacionesǁ), "derecho informático" (o cualquier otra denominación), requiere una actualización continua y a la par del crecimiento tecnológico, esfuerzo necesario para que la legislación al respecto se mantenga en continua evolución (Gil-Delgado 2004).

7.1.2. MOTIVOS QUE INDUCEN A DESARROLLAR UNA LEGISLACIÓN DE PROTECCIÓN DE DATOS PERSONALES.

El estudio de un régimen jurídico sobre protección de datos personales en el sector de las telecomunicaciones, específicamente en el internet, debe partir de justificar la necesidad de una norma encargada de regulares pacífica y separadamente estos derechos, de los ya agotados derechos fundamentales.

El uso de internet en nuestro país ha sido tan aceptado por la sociedad en general que nuestra vida como seres de sociedad, no podría desarrollarse sin el uso de estas nuevas tecnologías. Pero no solo nosotros hemos crecido con el uso de la tecnología, sino que los administradores del Estado se permitieron facilidades laborales aplicándolas, ya sea por un sinfín de motivos, como; espacio, orden, facilidad de búsqueda o específicamente, llegando a nuestro

tema; almacenaje de datos de carácter personal sometidos a tratamiento, lo que los lleva a crear sistemas informáticos para organizarse de mejor manera. Ahora bien, estos sistemas informáticos facilitaron también a la población, ya que, por medio del internet, una persona puede tener conocimiento de ciertas actividades, noticias o procedimientos sin necesidad de apersonarse a determinada institución o ente a recabar todo aquello que se encuentra ya plasmado en páginas y sitios web, creados para ese fin, informar.

Sin embargo, tras la creación de sitios y páginas web dentro de sus bases de datos y archivos, uno percata que la seguridad de información aplicada para estos sistemas no es la correcta, provocando que los datos personales sometidos a tratamiento puedan ser de cierta manera vulnerados, dando lugar a que se pueda encontrar información que solo compete a ambas partes.

Adentrando en sí a los motivos para crear una legislación de protección de datos personales en internet, se tienen casos de vulneraciones a ciertas páginas de gobierno o relacionados con el mismo, las cuales por la calidad de seguridad aplicadas en las mismas, fueron atacadas por diferentes procedimientos, donde los hackers o piratas por el conocimiento que tienen, operaron, tal y como ocurrió el primero de mayo de la gestión del 2013, donde la Presidencia de Bolivia sufrió un ataque cibernético en su página web, su base de datos fue filtrada y pudo extraerse información sobre los datos, identidades y cargos de los funcionarios que trabajaban en el Ministerio de la Presidencia, la acción atribuida a Anonymous Bolivia yAnon_0x03, permitió al pueblo boliviano conocer que en Palacio Quemado trabajaban 208 empleados, que el Presidente Morales tenía varias secretarias, tres asistentes de despacho, un maestro de ceremonias y tres comunicadores, entre otros colaboradores, asimismo y más delicado aún, mediante sus redes sociales, los hackers publicaron también las claves y contraseñas de los correos electrónicos de ciertos ministros, lo que conllevó a una total vulneración de datos de carácter personal (http://pastebin.com/hK8gmuud).

Este ataque surgió tras que el Tribunal Constitucional Plurinacional (TCP) de Bolivia declaró constitucional la habilitación del presidente Evo Morales y del vicepresidente Álvaro García Linera a una nueva postulación en elecciones generales en 2014.

No se trata de un caso aislado, en años pasados y en este año se registraron varios ataques a páginas relacionadas con el gobierno, todas ellas concernientes a un fin específico, transmitir y dar a conocer disconformidad con estipulaciones del gobierno para con la sociedad.

Demostramos de esta manera que no solo grupos autodenominados pueden acceder y vulnerar las páginas del gobierno, sino que cualquier persona con conocimientos informáticos, podría acceder a los datos más íntimos de las personas, mediante el ingreso a la base de datos de cualquier página, valiéndose de cualquier vulnerabilidad que ésta pueda tener.

Adentrándonos a uno de los incidentes específicos, nos referiremos a la publicación de las claves de correo electrónico de ministros, con la siguiente afirmación sobre lo que la Ley de Telecomunicaciones refiere acerca del tema: 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 (Ley General de Telecomunicaciones, tecnologías de Información y Comunicación -Art. 89). Lo que pretendo dar a conocer con respecto a este Artículo, es que el contenido de un correo electrónico puede ser referente a la vida íntima y privada de las personas, quienes tenemos necesidad de comunicarnos, expresarnos y relacionarnos dentro de nuestro ámbito, ya sea social o laboral, de tal manera que el correo electrónico y su contenido concierne única y exclusivamente a ambas partes, el transmisor y el receptor, no siendo autorizados para su conocimiento el de terceras personas.

Siguiendo esta línea, el correo electrónico no queda ceñido a los mensajes de texto, sino que las comunicaciones electrónicas a través del uso de múltiples aplicaciones, posibilitan su utilización con texto, voz, sonido e imagen, datos de personas que están ligadas a los derechos fundamentales donde nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada.

7.1.3. NECESIDAD Y MECANISMOS DE PROTECCIÓN DE LOS DATOS PERSONALES EN REGISTROS PÚBLICOS.

Existe una imperativa necesidad en crear una ley que se encargue de brindar protección a los datos personales.

Ley General de Telecomunicaciones, tecnologías de Información y Comunicación Art. 89 específicamente en base de datos y archivos de sitios web administrativos públicos, que contenga una serie de artículos entendibles, cuyo fin supremo radique en respaldar de una manera minuciosa nuestros datos a momento de que estos sean solicitados para realizar el tratamiento correspondiente, asimismo esta ley permitirá a la ciudadanía recurrir al órgano competente para realizar la respectiva denuncia y seguimiento en el caso que sus datos hayan sido manipulados por medio del uso del internet.

Cabe recalcar en este punto que la norma debe ser cambiante o surgir de acuerdo a los fenómenos que se presenten en la sociedad, fenómeno tecnológico trascendente que a la vez de otorgar un sinfín de adelantos para la comodidad y facilidad del ser humano, otorga también modos mediante los cuales ponen en riesgo la privacidad de nuestra información, concerniente solo y exclusivamente a nosotros o a los relacionados en cuanto a tratamientos y procedimientos en los cuales nos vemos inmersos en las actividades llevadas a cabo cotidianamente.

7.1.3.1. MECANISMOS

7.1.3.1.1. AGENCIA DE PROTECCIÓN DE DATOS PERSONALES Y EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS PERSONALES PÚBLICOS.

La creación de una Agencia de Protección de Datos Personales, dependiente de la Autoridad de Fiscalización y Regulación de Telecomunicaciones y Transportes de Bolivia ATT, vendría a constituirse en un mecanismo indispensable para proteger los datos ingresados para tratamiento en entes públicos. Para hacer efectiva la ley cabe crear un ente cuya finalidad principal será velar por el cumplimiento de la legislación en materia de protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, oposición, rectificación o cancelación de datos, y sobre todo dirigido a su protección.

Su objetivo se centrará en garantizar el derecho a la intimidad de los ciudadanos en sus relaciones con la Administración, tutelando los derechos reconocidos en la ley. Asimismo dentro de la Agencia es necesario crear como un órgano integrado y correlacionado a la Agencia un Registro General de Protección de Datos Personales Público, que llevará un detalle de todos aquellos datos concernientes a las personas a momento de su registro, modificación o eliminación a consecuencia del tratamiento llevado a cabo por el ente público, es decir que este registro general se mantendrá actualizado en cuanto al tratamiento de los datos personales realizados por los entes públicos, lo que procurará un seguimiento en caso de cualquier tipo de vulneración efectuada.

Este registro será un mecanismo necesario e indispensable para la investigación realizada por la Agencia de Protección de Datos Personales, en el caso de existir algún incidente relacionado con este tipo de datos sujetos a tratamiento, por ejemplo:

- Tras no haber sido actualizada la información.
- Cuando existiera una modificación interna realizada por el mismo ente público a cargo del tratamiento.
- Para la reposición de información relacionada con un dato de carácter personal, en el caso de que la seguridad mínima no haya sido suficiente provocando una manipulación de ciertos datos.

No solo será un medio para llegar a la verdad ante incidentes o vulneraciones, sino que también será de gran utilidad para hacer un control o fiscalización a los administradores públicos en cuanto al cumplimiento de sus funciones, registrando, modificando, eliminando, datos personales que se encontrará a su cargo.

7.1.4. PROPUESTA DE LEY

EXPOSICIÓN DE MOTIVOS

En la actualidad, los datos personales son elementos imprescindibles para llevar acabo cualquier tipo de acto o actividad dentro de nuestra sociedad; con referencia a los actos, éstos podrían ser actos de identificación; como los datos registrados para adquirir cédulas de identidad, licencias, etc., actos financieros; aquellos datos requeridos por las entidades financieras para créditos u otro tipo de servicios; actos laborales; como aquellos datos registrados de un currículum vitae, entrevistas, o informes de desempeño; o actos judiciales; que son datos registrados por los ministerios de justicia, fiscalía o juzgados, sobre informes, antecedentes, peritajes de los procesos o casos llevados a su cargo, asimismo dentro de nuestra vida cotidiana requerimos de ciertos servicios como los médicos, para los cuales también se requiere un historial de la salud del paciente, con todos los datos referentes a la intimidad.

Todos estos datos en determinado tema específico ya señalado, son sujetos a almacenamiento, que, bajo normas de ciertas instituciones, entes, organismos, ministerios, juzgados, etc. son registrados en determinados archivos, sean éstos archivos de control, archivos de historiales médicos, archivos de carácter informativo, archivos estadísticos, archivos administrativos, etc., pero lo más trascendental de lo referido se encuentra en que el registro debe ser realizado en determinado soporte, hasta hace unos años, en papel común, empero los avances tecnológicos han hecho que el registro cambie su base material de papel a soportes electrónicos o informáticos, los cuales al tener un gran tamaño de almacenamiento, proporcionan organización y facilidades de búsqueda en los mencionados entes o instituciones, quienes al realizar su tratamiento ya no recurren a la necesidad de almacenar el soporte material del papel en extensas y desordenadas bibliotecas o archivos concentrados en ambientes físicos, de tal manera que la mayoría de los datos que se posean o surjan de cualquier competencia, función o tratamiento de dichos órganos, en la actualidad son registrados en soportes tecnológicos, específicamente en una base de datos, es decir, estos datos se almacenan en archivos lógicos de una manera tan estructurada de tal forma que permite elaborar información significativa de esta estructura de datos; dicha función se encuentra a cargo de un área determinada de informática del ente u órgano, quienes crean la forma sistemática que permite que, cualquier dato ingresado por cualquier empleado o funcionario, sea registrado y almacenado automáticamente en una determinada base de datos, los cuales se encuentran en una red, red de acceso único y exclusivo solo para la institución.

Es evidente hoy en día que la difusión de información por internet es una realidad, y que así mismo, tiene gran aceptación en la población, vale decir que la sociedad tras haberse adecuado fácilmente al avance tecnológico prefiere informarse mediante el internet y no así o en menor medida mediante

los medios cotidianos, aspecto aprovechado por entes públicos quienes para demostrar transparencia y total comunicación sobre su administración con la población, crearon sitios web sobre la base de sus propios sistemas informáticos que se encuentran publicados en Internet donde publican una serie de eventos, noticias, avances, proyectos, progresos y beneficios para la sociedad.

Sin embargo, al encontrarse esta información en Internet, están sujetos a ataques cibernéticos por hackers o piratas informáticos, los cuales se aprovechan de vulnerabilidades que pueda tener el sistema y efectuar ataques a estos sitios; ataques como denegaciones de servicio a los sitios, es decir la no disponibilidad del sistema por un periodo de tiempo, el robo de información confidencial del sistema, alteraciones indebidas realizadas a los sitios web, etc. Estos ataques informáticos se podrían disminuir, siempre y cuando, cada ente cuente con las medidas de seguridad de información adecuadas.

Los sistemas informáticos de los entes públicos contienen una cantidad considerable de datos e información referente a toda aquella actividad de la que está a cargo, asimismo contiene datos personales de los empleados y de las personas que se someten a determinado tratamiento según el caso que se maneje o que esté sometido a competencia de determinado ente.

Está claro que, esta información considerada como confidencial, no será exhibida a propósito en los sitios web por los mismos entes, sin embargo, el hacker o pirata informático puede valerse de las vulnerabilidades de estos sitios web para poder ingresar hasta los sistemas que contienen esa información y hacerse de la misma conociendo todo aquel registro señalado con determinada información que no precisamente debe ser de conocimiento del común de la población, de tal manera que tras la manipulación, puede extraerse, modificarse, eliminarse, crearse, o incluso divulgarse cualquier dato o información sin tomar en cuenta su grado de confidencialidad o intimidad, como sucedió con ciertos sitios web relacionados con el gobierno, señalado

en un subtítulo anterior, con un único fin y propósito de expresar disconformidad con el sistema de gobierno o con cualquier tipo de medida aplicada por los entes públicos para el común de la sociedad.

Nuestra legislación no puede permanecer ajena a la falta de medidas legales que exijan a las entidades públicas contar con los requisitos de seguridad de información y a su vez debe regular una protección de datos personales ante los avances tecnológicos del internet, por lo que será imprescindible exigir de manera obligatoria – mediante ley – la existencia de los controles de seguridad de información adecuados para la creación de los sitios web y seguridad máxima en los sistemas informáticos públicos, con el fin de proteger, no solo la actividad realizada por los entes públicos, sino también proteger los datos personales registrados a efecto de las funciones administrativas de los diferentes entes públicos.

El presente proyecto confiere protección jurídica a todo dato de carácter personal sujeto a registro informático en bases de datos y archivos lógicos, sean datos provenientes de tratamiento como función específica de cada institución, o sean estos de carácter informativo o referencial. Todo esto tutelado por una Agencia de Protección de Datos, quien se encargará de velar por el cumplimiento de la legislación en materia de protección de datos, y controlar su aplicación.

Esta Agencia de Protección de Datos como Ente del Derecho Público, dependiente de la Agencia de regulación y fiscalización de Transportes y Telecomunicaciones ATT tendrá plena capacidad pública para garantizar el derecho a la intimidad de los ciudadanos en sus relaciones con la Administración, tutelando los derechos reconocidos en la ley.

Este proyecto vendría a llenar un vacío legal en nuestro ordenamiento jurídico. No se trata de que no exista derecho sobre la materia, el derecho que se aplica hasta ahora es el constitucional basado en los derechos fundamentales de las

personas adquiridos por Convenios y Tratados Internacionales, no especificando que el avance tecnológico pueda afectar a nuestros derechos.

PROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES.

En conformidad y aplicación del Art. 162, de la Nueva Constitución Política del Estado Plurinacional de Bolivia, en lo referido a la iniciativa legislativa ciudadana, parágrafo I, inciso 1, me permito elevar a consideración de la Asamblea Legislativa Plurinacional, el presente Proyecto de Ley referido a **PROTECCIÓN DE DATOS PERSONALES**.

TÍTULO I

DISPOSICIONES GENERALES.

Artículo 1. Objeto. La presente Ley es de orden público, tiene por objeto garantizar y proteger, los datos personales y los derechos fundamentales de las personas físicas en internet, cuyo tratamiento surja de funciones administrativas públicas, para difundir información a la población.

Artículo 2. Ámbito de aplicación.

1. La presente Ley se aplica a todo servidor público que tenga en sus registros informáticos cualquier tipo de dato personal susceptible a tratamiento, estos serán protegidos por los cuatro órganos del Estado, en todos sus niveles, ministerios, contralorías, Fuerzas Armadas, Policía Boliviana. Asimismo, también quedan obligadas las entidades que tengan relación con el Estado Plurinacional**.** Se regirá por la presente Ley todo tratamiento de datos personales, cuando el tratamiento sea efectuado en territorio boliviano en el marco de las actividades de un establecimiento público, responsable del tratamiento.

2. El régimen de protección de los datos personales que se establece en la presente Ley no será de aplicación a las bases de datos establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley los siguientes tratamientos de datos personales: a) La base de datos regulada por la legislación de régimen electoral. b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal sobre la función estadística pública. c) Los derivados del Registro Civil y del Registro Judicial de Antecedentes Penales o Registro de Antecedentes Policiales de penados y rebeldes. d) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. Definiciones. A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos personales l: Cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

b) Archivo: Todo conjunto organizado de datos personales, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

c) Tratamiento de datos: Operaciones y procedimientos técnicos de carácter automatizado, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

d) Responsable de la base de datos, archivos o tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

e) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

f) Procedimiento de disociación: Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

h) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: Toda revelación de datos realizada a una persona distinta del interesado.

j) Fuentes accesibles al público: Aquella base de datos o archivo cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el internet como medio masivo de comunicación, datos del censo, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

Artículo 4. Calidad de los datos.

1. Los datos personales sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos personales objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos personales serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos personales registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados.

5. Los datos personales serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines con base en los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. Datos especialmente protegidos.

1. De acuerdo con lo establecido en el parágrafo 2, 3, 5 y 6 del artículo 21 de la Constitución, así como con el art. 25 parágrafos I y II, los datos protegidos serán aquellos que tengan que ver con la privacidad, intimidad, honra, honor,

propia imagen y dignidad de las personas, al igual que la libertad de pensamiento religión y culto expresados de manera pública y privada, siendo inviolables la correspondencia electrónica o papeles privados contenidos en soporte informático.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos personales que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan las bases de datos o archivos mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Quedan prohibidos la base de datos y archivos creados con la finalidad exclusiva de almacenar datos personales que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

4. Los datos personales relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en bases de datos o archivos de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

5. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos personales de los apartados 2 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se

realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 6. Datos relativos a la salud. Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos personales relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos.

Artículo 7. Seguridad de los datos.

1. Toda Institución Pública, deberá contar con un mínimo de seguridad, aplicado en todo sistema del cual dependan los registros de datos e información ingresada para su respectivo tratamiento. 2. El responsable de la base de datos o archivos, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del 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. 3. No se registrarán datos personales en base de datos que no reúnan las condiciones mínimas de seguridad con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

Artículo 8. Deber de secreto. El responsable de la base de datos o archivos y quienes intervengan en cualquier fase del tratamiento de los datos personales están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular de los datos, en su caso, con el responsable del mismo.

Artículo 9. Comunicación de datos.

1. Los datos personales objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso cuando se trate de datos recogidos de fuentes accesibles al público.

TÍTULO II

DERECHOS DE LAS PERSONAS

Artículo 10. Impugnación de valoraciones.

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. La valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 11. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos personales sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia o fotocopia, certificada o no, en forma legible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

Artículo 12. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

3. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se haya comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

Artículo 13. Tutela de los derechos.

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 14. Derecho a indemnización.

Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

TÍTULO III

ARCHIVOS Y BASE DE DATOS DE TITULARIDAD PÚBLICA

Artículo 15. Creación, modificación o supresión.

1. La creación, modificación o supresión de base de datos de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en la Gaceta Oficial del Estado.

2. Las disposiciones de creación o de modificación de base de datos deberán indicar: a) La finalidad de la creación de la base de datos o archivos y los usos previstos para el mismo. b) Las personas o colectivos sobre los que se pretenda obtener datos personales o que resulten obligados a suministrarlos. c) El procedimiento de recogida de los datos personales. d) La estructura básica de la base de datos y la descripción de los tipos de datos personales incluidos en el mismo. e) Los órganos de las Administraciones responsables de la base de datos o archivos. f) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición. g) Las medidas de seguridad con indicación del nivel alto exigible.

Artículo 16. Comunicación de datos entre Administraciones Públicas.

1. Los datos personales recogidos o elaborados por las Administraciones Públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones Públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. O de lo contrario, cuando el dato sea

necesario para la averiguación de antecedentes penales o policiales, como se señala a continuación.

Artículo 17. Base de datos de las Fuerzas y Cuerpos de Seguridad.

La recogida y tratamiento para fines policiales de datos personales por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

TÍTULO IV

AGENCIA DE PROTECCIÓN DE DATOS

Artículo 18. Naturaleza y régimen jurídico.

1. La Agencia de Protección de Datos es un Ente de Derecho público, dependiente de la Autoridad de Regulación y Fiscalización de Telecomunicación y Transportes con plena capacidad pública. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.

2. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones Públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos personales de que conozca en el desarrollo de su función.

3. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos: a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del

Estado. b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

4. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 19. El Director.

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Decreto, por un período de cuatro años.

2. Ejercerá sus funciones con plena independencia y objetividad, y no estará sujeto a instrucción alguna en el desempeño de aquéllas.

Artículo 20. Funciones.

1. Son funciones de la Agencia de Protección de Datos: a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos. b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias. c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley. d) Atender las peticiones y reclamaciones formuladas por las personas afectadas. e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos personales. f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los archivos y base de datos, cuando no se

ajuste a sus disposiciones. g) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley. h) Recabar de los responsables de la base de datos cuanta ayuda e información estime necesaria para el desempeño de sus funciones. i) Redactar una memoria anual y remitirla al Ministerio de Justicia. j) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

2. Las resoluciones de la Agencia de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos. Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

Artículo 21. El Registro General de Protección de Datos.

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.

2. Serán objeto de inscripción en el Registro General de Protección de Datos: a) Las Bases de datos de que sean titulares las Administraciones Públicas.

b) Los datos relativos a la base de datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición. 3. Por vía reglamentaria se regulará el procedimiento de inscripción de la base de datos de titularidad pública, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

4. Todo registro realizado, será referencia de cualquier modificación, alteración, eliminación, etc. que se haga de cualquier dato personal,

suponiendo que éste ha sido vulnerado, lo que establecerá la originalidad y/o fidelidad de dicho dato en las listas de registro.

5. Las listas de registro serán actualizadas cada vez que se realice alguna modificación por la entidad competente, permaneciendo así para fines de comparación con las vulnerabilidades de datos, si los hubiere.

TÍTULO V

INFRACCIONES Y SANCIONES

Artículo 22. Responsables.

1. Los responsables de los archivos y bases de datos y los encargados de los tratamientos de los mismos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando Los archivos y base de datos hayan sido violentados a causa de vulneraciones encontradas en su sistema, la administración pública que esté a cargo del tratamiento de la misma, se verá obligada a otorgar pronta solución de acuerdo a lo establecido en la presente ley.

Artículo 23. Tipos de infracciones ante la Agencia de Protección de Datos Personales:

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves: a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) Proceder a la recogida de datos personales de los propios afectados sin proporcionarles la información que señala.

3. Son infracciones graves:

a) Proceder a la recogida de datos personales sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

b) Tratar los datos personales o usarlos posteriormente con contravención de los principios y garantías establecidos en la presente Ley.

c) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

d) Mantener datos personales inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

4. Son infracciones muy graves:

a) Mantener la base de datos o archivos, locales, programas o equipos que contengan datos personales sin las debidas condiciones de seguridad, estableciendo directrices o guías de implementación de seguridad. b) La vulneración del deber de guardar secreto sobre los datos personales incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros bases de datos que contengan un conjunto de datos personales suficientes para obtener una evaluación de la personalidad del individuo. La recogida de datos en forma engañosa y fraudulenta.

c) La comunicación o cesión de los datos personales, fuera de los casos en que estén permitidas.

d) No cesar en el uso ilegítimo de los tratamientos de datos personales cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos personales que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos ha dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos personales de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre todo datos personales l y así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

Artículo 24. Infracciones.

1. El Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable de la base de datos, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

Artículo 25. Prescripción.

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 26. Procedimiento sancionador.

Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

Los procedimientos sancionadores serán tramitados por la Agencia de Protección de Datos.

Artículo 27. Potestad de inmovilización de archivo y base de datos, asimismo como a su modificación o alteración.

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos personales en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de base de datos o archivos de datos personales, la cesación en la utilización o cesión ilícita de los datos.

Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales bases y archivos a los efectos de restaurar los derechos de las personas afectadas. Esto contemplará la imposibilidad de incurrir en corrupción, para lo que se apoyará en la lista de origen existente en la Agencia de Protección de Datos Personales, Registro General de Protección de Datos.

DISPOSICIONES ADICIONALES.

Primera. **Archivos y Base de Datos preexistentes**. - Los archivos y tratamientos automatizados, deberán ser inscritos en el Registro General de Protección de Datos adecuándose a la presente Ley dentro del plazo de tres años, a contar desde su entrada en vigor.

La obligación prevista en el párrafo anterior deberá complementarse en el plazo de doce años a contar desde la publicación de la presente ley, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Segunda. Base de Datos y Registro de Población de las Administraciones Públicas.

La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

La base de datos o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones Públicas.

CAPITULO VIII

DISEÑO METODOLÓGICO

8.1. Tipificación de la investigación.

El presente trabajo de investigación se circunscribe en el campo de las Ciencias Jurídicas, el tema de investigación científica se sustenta teórica y prácticamente dentro el paradigma positivista, siendo un estudio de carácter JURÍDICA - PROYECTIVA, ya que a partir de una estrategia cuantitativa se definen un conjunto de dimensiones e indicadores que permitirán realizar un diagnóstico sobre el nivel de conocimiento que presentan los administradores de justicia del Departamento de Tarija, respecto a la NECESIDAD DE UNA LEY DE PROTECCIÓN DE DATOS PERSONALES. A partir de dichos resultados encontrados, se elaborará una propuesta Ley de protección de datos personales.

Exploratoria: porque se trata de un tema que a criterio nuestro no ha sido abordado con profundidad, es necesario efectuar un análisis más riguroso y evidenciar nuestra realidad.

Descriptivo: este proyecto describe las características y propiedades del objeto de estudio tal como se presenta en la realidad, sin que exista manipulación de las variables por parte del investigador, en este caso particular respecto a la necesidad de una Ley de protección de datos personales.

8.2. Población y muestra.

La población de estudio para fines investigativos estará constituida por, Vocales de Sala Constitucional, Abogados constitucionalistas, los mismos ascienden a un total de 16 sujetos, quienes fueron parte de la población de estudio.

Al tratarse de una población reducida se optó por trabajar con el 100% de la población de estudio, de tal manera que los resultados sean representativos y generalizables, por lo que no existe muestra alguna.

DETALLE DE LA POBLACIÓN

SUJETOS	FRECUENCIA	PORCENTAJE
Vocales de Sala Constitucional	2	100%
Abogados constitucionalistas	10	100%
Docentes del Área Constitucional	4	100%
TOTAL	**16**	**100%**

8.3. Métodos, técnicas e instrumentos.

Métodos. En el desarrollo del trabajo de investigación se utilizarán diferentes métodos, los cuales detallan a continuación:

1. Métodos teóricos. Como tal, éstos permitirán establecer las relaciones del objeto de investigación, participando en la construcción y el análisis de la elaboración del marco teórico, contextual y a la vez conceptual. Entre los métodos teóricos utilizados tenemos:

Método histórico-lógico. Este método se utilizó para realizar una revisión acerca de la trayectoria y desarrollo del fenómeno de estudio, en su devenir histórico respecto a la necesidad de una Ley de protección de datos de carácter personal.

Método analítico. El mismo que a partir de la revisión bibliográfica permitió realizar un análisis de los diferentes conceptos teóricos, permitiendo de tal manera profundizar el tema de investigación. De la misma manera, a partir

de los resultados obtenidos se realizó un análisis minucioso sobre el tema en cuestión.

Método sintético. Que se utilizó tanto en el análisis e interpretación de resultados, como también en las conclusiones a las cuales se arribaron después de haber concluido con el trabajo de investigación, de tal manera se pudo tener una visión integrada y general sobre el objeto de estudio. También permitió reflexionar acerca de la revisión bibliográfica, como sustento teórico de la investigación.

Método deductivo. El mismo que se utilizó para realizar las conclusiones a las cuales se arribaron después de llevar adelante el proceso de investigación, como resultado del análisis e interpretación de resultados y a partir de ello, se hizo generalizaciones para las poblaciones con las mismas características.

Método de la modelación. Se utilizó para diseñar la propuesta sobre la necesidad de una Ley de protección de datos personales.

2. Métodos empíricos. Los mismos permitieron revelar y explicar las características fenomenológicas del objeto de estudio y se utilizó en el proceso de acumulación de información, permitiendo de tal manera el recojo de datos, la intervención, el análisis e interpretación y la transformación de la realidad en el proceso de investigación. Entre ellos:

Método de la encuesta. El mismo que sirvió para recabar toda la información de manera directa y en poco tiempo, conociendo de tal manera la realidad de las características del fenómeno de investigación, el cual se aplicó en la etapa inicial, para realizar el diagnóstico.

Método estadístico. Se utilizó precisamente para obtener información numérica acerca del objeto de estudio, medir las variables a través de procedimientos estadísticos, tanto descriptivos como inferenciales, los cuales fueron expresados en cuadros, gráficos, frecuencias y porcentajes.

Técnicas. Para la recopilación de la toda la información necesaria para el trabajo de investigación se aplicó la siguiente técnica:

1. Encuesta estructurada. Esta técnica sirvió para conocer y valorar la opinión de cada uno de los administradores de justicia sobre la necesidad de una Ley de protección de datos personales.

Instrumentos. De acuerdo con las características del trabajo de investigación, se utilizaron los siguientes instrumentos:

-Cuestionario. Se utilizó el cuestionario con alternativa de respuestas, con preguntas cerradas, en un total de 10 preguntas, que permitieron determinar el conocimiento y opinión de los administradores de justicia respecto a la necesidad de una Ley de protección de datos de carácter personal. El mismo que se aplicó de forma individual a los sujetos participantes de la investigación.

8.4. Variables.

Variable dependiente: Injerencia de terceros a los datos personales**.**

Variable independiente: Propuesta de Ley que proteja los datos personales.

9. Resultados.

La investigación arroja como resultado la necesidad de elaborar una Ley de protección de los datos personales, más aun tomando en cuenta que en muchos Estados, la protección de los datos personales se ha convertido en un Derecho Fundamental y Autónomo, en el entendido que es importante mencionar que la normativa local existente resulta insuficiente para la protección de los datos personales, sin embargo debemos reconocer que los Sistemas de protección en el ámbito de los Derechos Humanos, la necesidad de uniformizar las legislaciones con respecto a la protección de los datos personales. En el caso del Sistema interamericano de Derechos Humanos, si

bien no se alcanzó a exhortar la autonomía del derecho, se ha determinado que es un derecho fundamental y conexo de otros derechos como el Derecho a la vida privada y a la privacidad.

Es importante recalcar que al someter nuestra propuesta Ley a un Control de Convencionalidad o mejor dicho, la propuesta versus la Convención Americana sobre los derechos humanos, en su Art. 13, llegamos a desenlace que el proyecto de Ley, no vulnera el derecho al libre acceso a la información, más al contrario esta Ley estuviera en conformidad con dicho instrumento internacional, seguiría los lineamientos de la Corte Interamericana de Derechos Humanos, establecidos en Sentencia Claude Reyes y Otros Vs. Chile, del 19 de septiembre de 2006 (Fondo, Reparaciones Y Costas).

Para el Sistema Interamericano, el derecho a la protección de datos personales es conexo y progresivo, no es autónomo y fundamental como lo es para el Tratado de Funcionamiento de la Unión Europea, el cual lo reconoce como autónomo y con ámbito específico de protección, este tratado obliga a todos los Estados miembros de la Unión a adecuar su legislación doméstica al más alto nivel normativo y a adoptar los criterios que determinan su interpretación y alcance.

10. Conclusiones y Recomendaciones.

Los instrumentos internacionales tutelan los datos personales de la intromisión de terceros, pero necesitan la elaboración de una norma especial que establezca un procedimiento a seguir, en síntesis, el aplicar el Control de Convencionalidad a casos que tengan que ver con el tema en cuestión, no será suficiente, pues cada Estado se encuentra constreñido a crear normas locales que establezcan los parámetros de protección y respeto al Derecho Fundamental de Protección de los datos personales.

La norma local existente, es insuficiente para proteger los datos personales, no es una norma específica, no establece ninguna clase de procedimiento efectivo, es más en nuestro País, el Derecho a la Protección de los datos personales no está legislado exclusivamente, hasta el momento no es ni Derecho autónomo, ni mucho menos Fundamental, por consiguiente, el Estado boliviano no sigue la línea de progresividad establecida por la Corte Interamericana de Derechos Humanos.

El Derecho a la Protección de los datos personales, no vulnera el Derecho al Acceso de la Información, pues la misma C.P.E, establece que los derechos y deberes consagrados en la Constitución se interpretarán de conformidad con los Tratados internacionales de derechos humanos ratificados por Bolivia, esto quiere decir que debemos someter la propuesta de ley a la Convención Americana sobre los derechos humanos.

De lo anterior podemos sostener que al poner al tráfico jurídico nuestra propuesta de ley para la Protección de los Datos Personales, no estaríamos ingresando a terrenos de la Censura Previa, que, de acuerdo a lo establecido por la misma CIDH, la Censura Previa es incompatible con el pleno goce de los derechos protegidos por la Convención Americana sobre los derechos humanos.

La excepción es la norma contenida en el párrafo 4, que permite la censura de los "espectáculos públicos" para la protección de la moralidad de los menores. La única restricción autorizada por el artículo 13 es la imposición de responsabilidad ulterior. Además, cualquier acción de este tipo debe estar establecida previamente por la ley y sólo puede imponerse en la medida necesaria para asegurar: a) el respeto de los derechos o la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

Por tanto, ~~la~~ queda establecido que la prohibición está dirigida a la consulta previa, no la facultad legislativa que tiene los Estados, más aún cuando la Corte Interamericana de Derechos Humanos (CIDH), ha establecido dice (12) principios rectores, ha recomendado a la Comisión Jurídica Internacional (CJI) formule propuestas a la CAJP sobre las distintas formas de regular la protección de datos personales, incluyendo un proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en cuenta los estándares internacionales alcanzados en la materia.

Por consiguiente, se recomienda que haciendo eco de las relatorías arriba descritas, donde se exhorta a que la misma CJI recoja los criterios de países americanos y otros Organismos como los europeos, para poder elaborar una norma modelo de protección, de esto podemos entender que la misma CIDH, está impulsando a que los países miembros creen normas especiales dentro de los estándares ya establecidos por el mismo Sistema interamericano.

Bibliografía.

Artavia Murillo y otros vs. Costa Rica. 257 (Corte Interamericana de Derechos Humanos, 28 de noviembre de 2012).

M.S. v. Sweden. (TEDH, s.f.).

Relatoria Especial. «Organización de Estados Americanos.» *Organización de Estados Americanos.* ;2007. http://www.cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf (último acceso: 26 de Enero de 2021).

Access Now, organización internacional de derechos humanos en. *GUÍA BÁSICA SOBRE DATOS PERSONALES PARA BOLIVIA.* 03 de abril de ;2019. https://www.accessnow.org/cms/assets/uploads/2019/03/Guia-Basica-Proteccion-de-Datos-Bolivia.pdf (último acceso: 30 de octubre de 2020).

Atala Riffo y niñas vs. Chile. . 239 (Corte Interamericana de Derechos Humanos, 24 de septiembre de 2012).

Caso López Álvarez vs Honduras. (Corte Interamericana de Derechos Humanos, 1 de Febero de ;2006).

Caso López Álvarez. Sentencia de 1 de febrero de 2006. Serie C No. 141, párr. 163. (s.f.).

CdE. «Estatuto del Consejo de Europa de 5 de mayo de 1949,.» London, ;1949.

Cfr. Informe del Relator Especial de la ONU acerca de la promoción y protección del derecho a la libertad de opinión y expresión, de 17 de abril de 2013, numeral 21. s.f.

—. *Cfr. Informe del Relator Especial de la ONU acerca de la promoción y protección del derecho a la libertad de opinión y expresión, de 17 de abril de 2013, numeral 21.* s.f.

CIDH. *CUADERNILLO DE JURISPRUDENCIA DE LA CORTE INTERAMERICANA DE DERECHOS.* Dr. Claudio Nash, ;2019.

CIDH. «Demanda.» ;2005.

CIDH. «Informe sobre Terrorismo y Derechos Humanos de 2002.» ;2002.

—. «OEA.» *OEA.* Agosto de ;2007. http://www.cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf (último acceso: 26 de Enero de 2021).

CIDH, Caso Fernández Ortega y Otros vs. México. *Rev. derecho (Valdivia) vol.30 no.1 Valdivia jun. 2017.* 2010. tps://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004#n4 (último acceso: 03 de enero de 2021).

Claude Reyes y otros Vs. Chile. (Corte Interamericana de Derechos Humanos, 19 de Septiembre de ;2006).

Comité Jurídico Interamericano, sobre Privacidad y Protección de Datos Personales. 2015.

Constitución Política del Estado Plurinacional de Bolivia. 2009.

Cueva, Murillo de la. *El derecho a la autodeterminación informativa.* España: Tecnos, 1990.

DD.HH, Comisión Interamericana de. «Informe nº 31/05.» ;2005.

Digital Rights Ireland y Seitlinger y otros. (Tribunal de Justicia de la Unión Européa, 8 de Abril de ;2014).

Fernández Ortega vs. México. (CIDH, 10 de agosto de 2010).

Garzón Valdés, Ernesto. «IFAI.» *Lo íntimo, lo privado y lo público.* Abril de 2005. http://201.144.56.20/transparencia/cuadernillo_06.pdf (último acceso: 09 de 11 de 2016).

Gayo, María Solange Maqueo Ramírez*Jimena Moreno González*Miguel Recio. *Rev. derecho (Valdivia) vol.30 no.1 Valdivia jun. 2017.* s.f. tps://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004#n4 (último acceso: 03 de enero de 2021).

Gelman vs. Uruguay. 221 (Corte Interamericana de Derechos Humanos, 24 de febrero de 2011).

González y otras vs. México. 205 (Corte Interamericana de Derechos Humanos, 16 de noviembre de ;2009).

Las Masacres de Ituango vs. Colombia. 148 (Corte Interamericana de Derechos Humanos, 1 de Julio de ;2006).

Ley Nº164. *Ley General de telecomunicaciones, tecnologías de información y comunicación.* Asamblea Legislativa Plurinacional, 2011.

López Carballo, Daniel (Coord.). *Protección de Datos y Habeas Data: Una visión desde Iberoamérica.* Madrid: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2015.

Luis Freddyur Tovar. «“Positivación y protección de los derechos humanos: aproximación colombiana”.» *Revista Criterio Jurídico, No. 2*, ;2008: 45-72.

M. S. v. Sweden. (Tribunal Europeo de DD.HH, 2 de Agosto de 1997).

NACIONES, GRUPO ENCARGADO DE LA POLÍTICA DE PRIVACIDAD DE LAS, y NACIONES UNIDAS GRUPO ENCARGADO DE LA POLÍTICA DE PRIVACIDAD . *ONU.* s.f. https://unsceb.org/principles-personal-data-protection-and-privacy-listing (último acceso: 23 de Enero de 2021).

Norbert Losing. «“La justicia constitucional en Paraguay y Uruguay”, .» *Anuario de Derecho Constitucional Latinoamericano, No. 1*, ,2002: 109-33.

Ordoñez, Luis. «La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración.» *Revista de Derecho, No. 27*, ;2017: 93-94.

Piñar Mañas, José Luis. *La Red Iberoamericana de Protección de Datos. Declaraciones y documentos.* Valencia: Tirant lo Blanch, 2006.

Ramírez, María Solange Maqueo. «Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario.» *Revista de Derecho (Valdivia)*, 2017.

Ramírez, María Solange Maqueo, Jimena Moreno González, y Miguel Recio Gayo. *Revista de Derecho Valdivia.* Junio de 2017. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-09502017000100004#nb7 (último acceso: 3 de Enero de 2021).

Remolina, Angarita. «TIC e información personal.» *Ámbito Jurídico*, 2011: 12.

Remolina, Nelson. «Aproximación constitucional de la protección de Datos Personales en Latinoamerica.» *Revista Internacional de Protección de Datos Personales*, 2012: 4-13.

Remolina-Angarita, Nelson. «¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estandar europeo?» *International Law, Revista Colombiana de Derecho Internacional*, 2010: 489-524.

Rotaru v. Romania. (TEDH, 4 de Mayo de 2000).

Sagues, Nestor Pedro. *Obligaciones internacionales y control de convencionalidad.* OPUS MAGNA, 2011.

SAGUES, Pedro Néstor. El Hábeas Data en Argentina (Orden Nacional). Ius et Praxis, Año 3, Número 1º, Facultad de ciencias jurídicas y Sociales, Universidad de Talca, Talca (Chile), p.137-150. «El Hábeas Data en Argentina (Orden Nacional).» *Ius et Praxis* (Facultad de ciencias jurídicas y Sociales, Universidad de Talca, (Chile)), 1997: 137-150.

Santivañez, Rivera. «Jurisdicción Constitucional.» En *El Habias Corpus en Bolivia*, de Dora Montenegro Caballero, 225. País, 2006.

Sentencia del Tribunal de Justicia (Gran Sala), de 9 de Volker und Markus Schecke GbR y C-93/09. (Sentencia del Tribunal de Justicia (Gran Sala), 9 de Noviembre de ;2010).

Tarrillo Monteza, Daniel. *Publicidad Registral y Derecho a la Intimidad.* Lima: Pontificia Universidad Católica del Perú (disponible en: http://tesis.pucp.edu.pe/repositorio/handle/123456789/5003), 2013.

Tellez Valdez, Julio. *Derecho Informático.* Mexico: Instituto de Investigacion Jurídicas, 1987.

Tovar, Luis Freddyur. «“Positivación y protección de los derechos humanos: aproximación colombiana”.» *Revista Criterio Jurídico, No. 2* (DYKINSON S.L), ;2008: 45-72.

Toynbee, Arnold. *Estudio de la HIstoria .* Madrid: Alianza Editorial, 1991.

Tribunal Constitucional Plurinacional de Bolivia. *Sistema de Información Constitucional Plurinacional.* s.f. http://www.tcpbolivia.bo/.

Troncoso, Antonio. *La protección de datos personales: en busca del equilibrio.* (Valencia: Tirant lo Blanch, 2010.

Vivas, Yolanda Fernández. «La influencia de la Sentencia de la Corte Interamericana de Derechos Humanos “Claude Reyes contra Chile” en la jurisprudencia del Tribunal Europeo de Derechos Humanos.» *Eunomía. Revista en Cultura de la Legalidad Nº 9*, ;2015: pp. 321-333.

y, Cfr. Informe del Relator Especial de la ONU acerca de la promoción y protección del derecho a la libertad de opinión. *Rev. derecho (Valdivia) vol.30 no.1 Valdivia jun. 2017.* junio de 2017. (último acceso: 3 de enero de 2021).

TABLAS Y FIGURAS.

TABLA Y FIGURA N.º 1

1. ¿Considera que la norma local, es insuficiente para la protección de los datos personales?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	2	100	3	75	3	30
NO	0	0	1	25	7	70
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

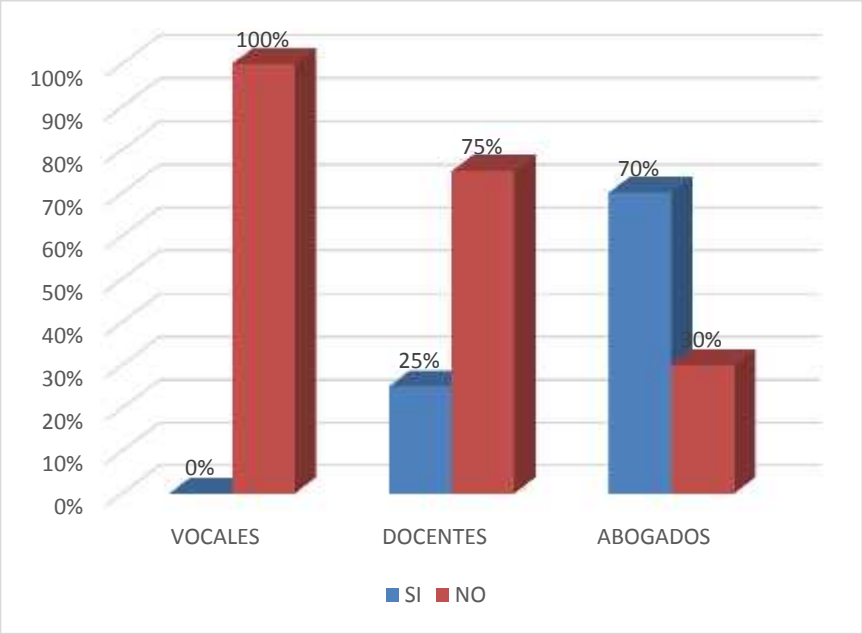


TABLA Y FIGURA N.º 2

2. ¿Considera que sea necesario implementar una norma local especifica que proteja los datos personales?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	2	100	2	50	7	100
NO	0	0	2	50	7	0
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

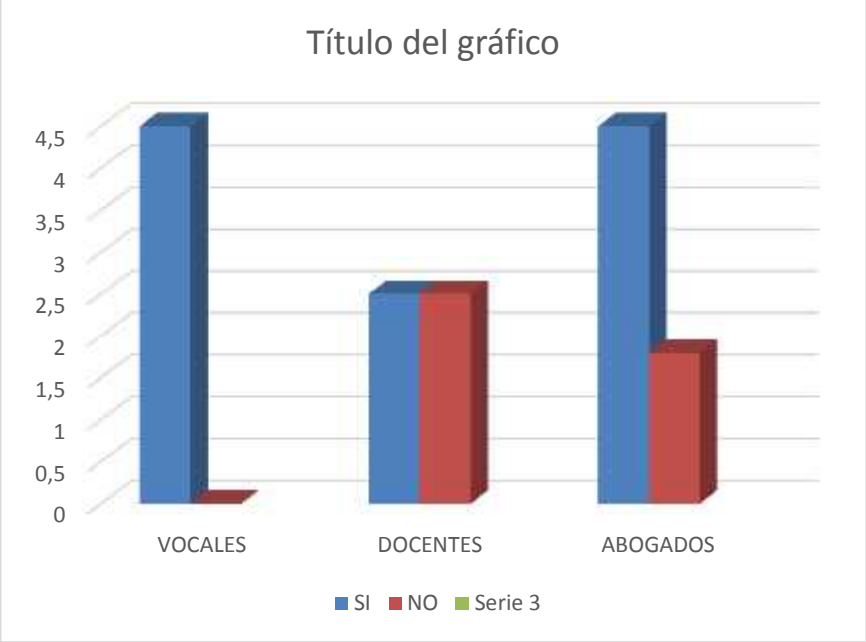


TABLA Y FIGURA N.º 3

3. ¿Los Instrumentos internacionales en materia de Derechos Humanos resguardan el Derecho a la protección de datos personales?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	2	100	4	100	8	80
NO	0	0	0	0	2	20
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

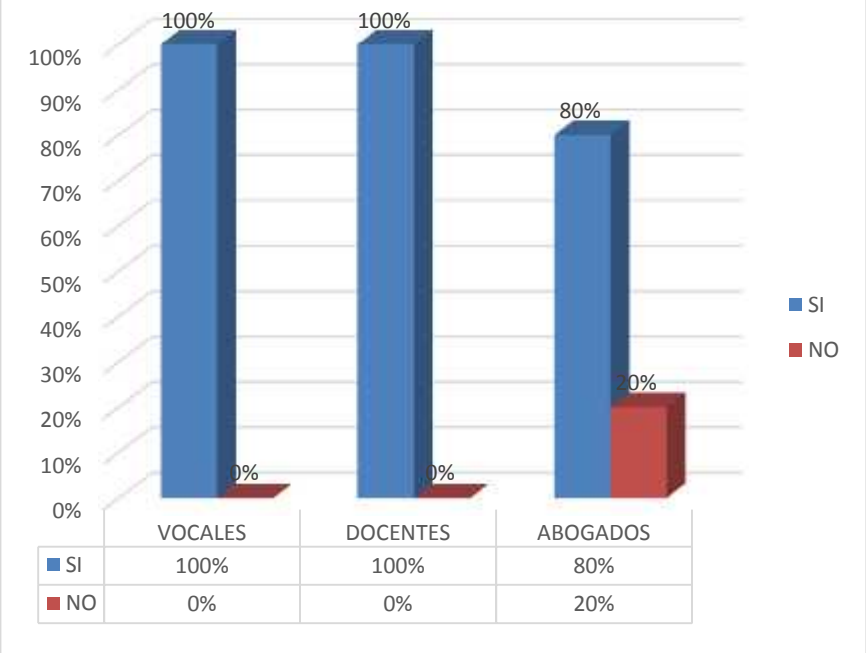


TABLA Y FIGURA N.º 4

4. ¿Son suficientes las normas Supraconstitucionales para la protección de los datos personales?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	0	0	2	50	7	100
NO	2	100	2	50	3	0
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

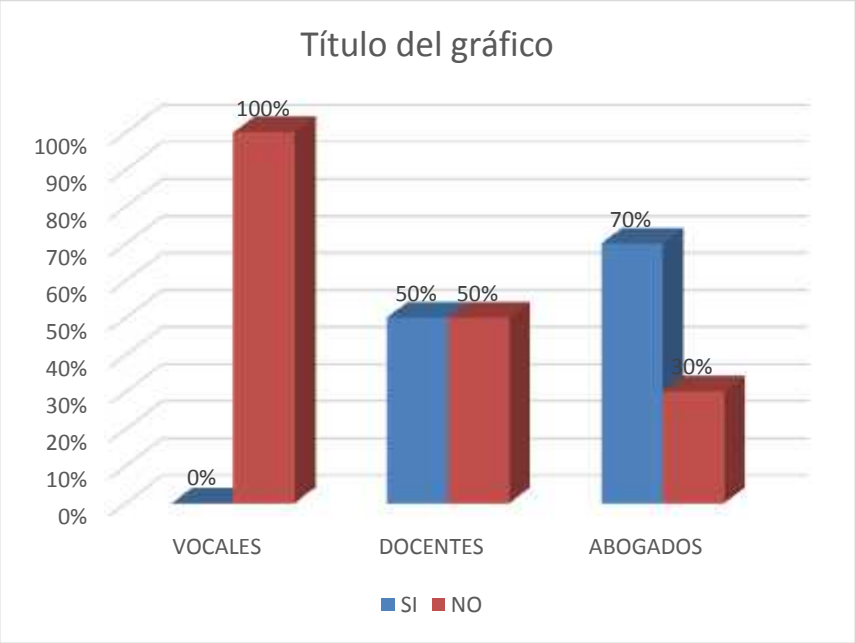


TABLA Y FIGURA N.º 5

5. ¿Es el Derecho a la protección de les datos personales un derecho autónomo en Bolivia?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	0	0	0	100	2	20
NO	2	100	4	0	8	80
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

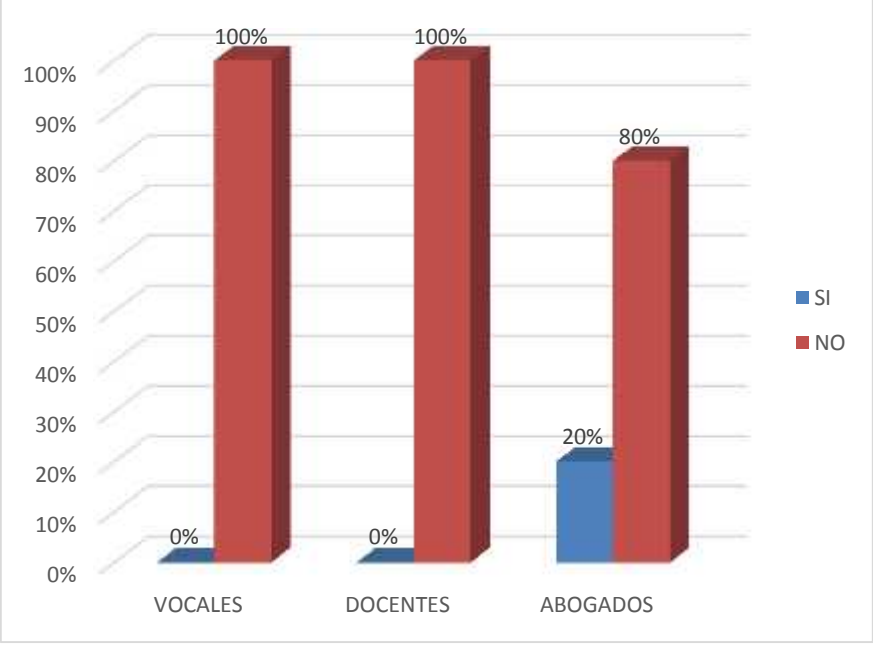


TABLA Y FIGURA N.º 6

6. ¿Considera que el necesario que el derecho a la protección de les datos personales cobre la calidad de derecho autónomo?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	2	100	3	75	7	70
NO	0	0	1	25	3	30
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

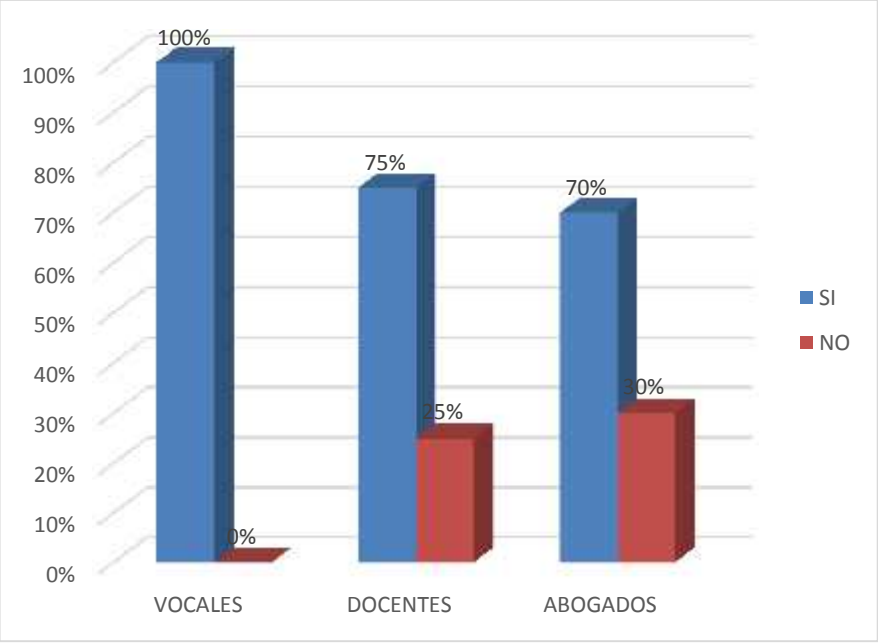


TABLA Y FIGURA N.º 7

7. ¿Es el derecho a la protección de les datos personales un derecho fundamental en Bolivia?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	0	0	0	0	0	0
NO	2	100	4	100	10	100
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

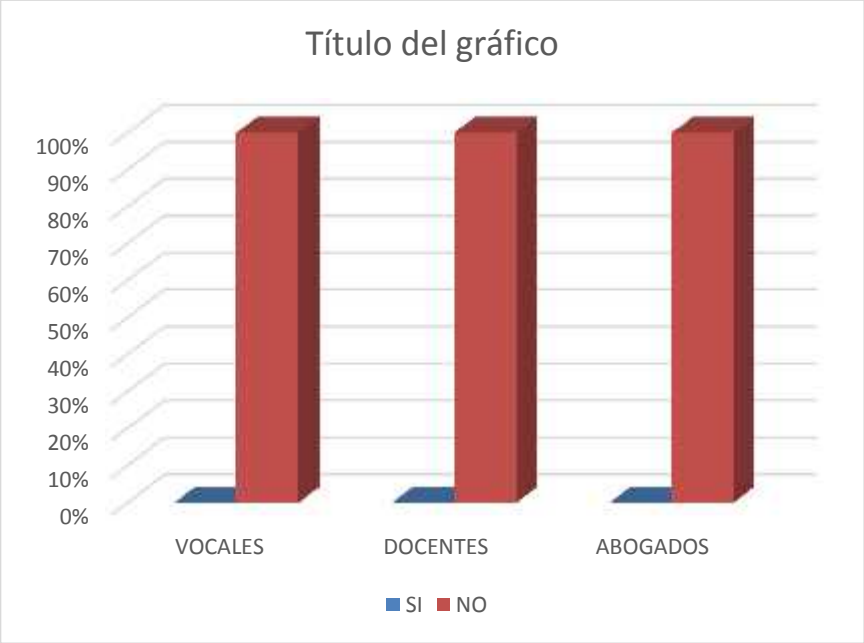


TABLA Y FIGURA N.º 8

8. ¿Considera que el necesario que el derecho a la protección de los datos personales cobre la calidad de derecho fundamental?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	20	100	3	75	3	70
NO	0	0	1	25	7	30
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

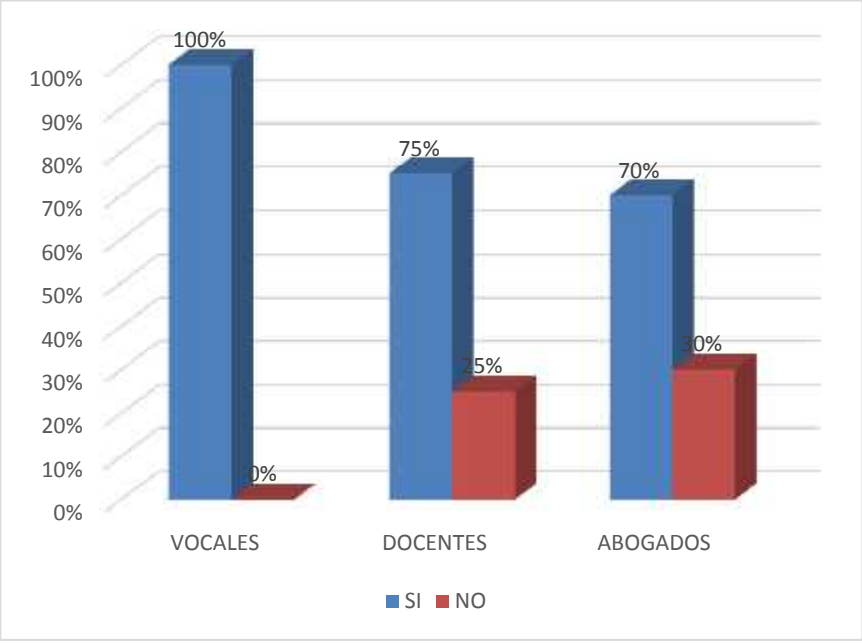


TABLA Y FIGURA N.º 9

9. ¿Es el derecho a la protección de los datos personales, es un derecho progresivo en Bolivia?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	0	100	0	0	2	20
NO	2	0	100	100	8	100
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**

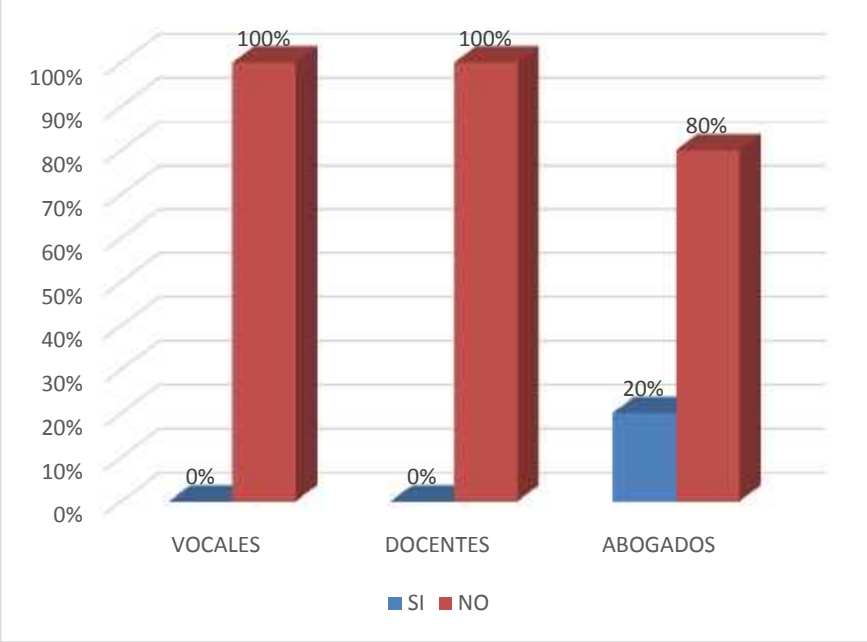
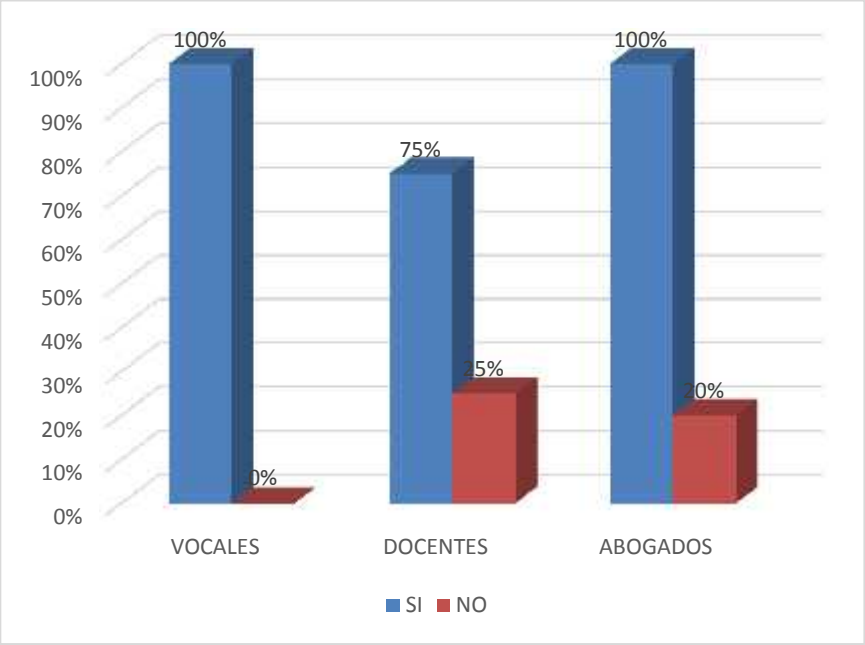


TABLA Y FIGURA N.º 10

10. ¿Considera que el necesario que el derecho a la protección de los datos personales cobre la calidad de derecho progresivo?

ALTERNATIVAS	VOCALES		DOCENTES		ABOGADOS	
	f	%	f	%	f	%
SI	2	100	3	75	8	80
NO	0	0	1	25	20	20
TOTAL	**2**	**100**	**4**	**100**	**10**	**100**



ANEXOS

CUESTIONARIO

1. ¿Considera que la norma local, es insuficiente para la protección de los datos personales?

SI o NO

2. ¿Considera que sea necesario crear una norma local especifica que proteja los datos personales?

SI o NO

3. ¿Los Instrumentos internacionales en materia de Derechos Humanos amparan el Derecho a la protección de datos personales?

SI o NO

4. ¿Son suficientes las normas Supraconstitucionales para la protección de los datos personales?

SI o NO

5. ¿Es el Derecho a la protección de les datos personales es un derecho autónomo en la legislación boliviana?

SI o NO

6. ¿Es el derecho a la protección de les datos personales un derecho fundamental en la legislación boliviana?

SI o NO

7. ¿Considera que el necesario que el derecho a la protección de los datos personales vulnera el derecho al acceso a la información?

SI o NO

8. ¿El derecho a la protección tutela el derecho a la vida privada y a la privacidad?

SI o NO

9. ¿Es el Derecho a la protección de les datos personales vulnera la libertad de pensamiento y la expresión?

SI o NO

10. ¿Considera que el necesario que el derecho a la protección de los datos personales es un derecho progresivo en la legislación boliviana?

SI o NO