Cláusula de cesión de derecho de publicación de tesis/monografía

Yo Martha Karen Chungara Rodriguez C.I. 4873175 L.P
autor/a de la tesis titulada

Incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela del derecho de autodeterminación informativa

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

Magister en Derecho Penal y Derecho Procesal Penal

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

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

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

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

Fecha. 25/11/2020

Firma:

UNIVERSIDAD ANDINA SIMÓN BOLIVAR

SEDE LA PAZ

MAESTRÍA EN DERECHO PENAL Y DERECHO PROCESAL PENAL

INCORPORACIÓN DE TIPOS PENALES REFERIDOS A LA PROTECCIÓN DE DATOS PERSONALES EN EL CÓDIGO PENAL DEL ESTADO PLURINACIONAL DE BOLIVIA, PARA OPTIMIZAR LA TUTELA DEL DERECHO DE AUTODETERMINACIÓN INFORMATIVA

Tesis presentada para optar el Grado Académico de Magister en Derecho Penal y Derecho Procesal Penal

ABOG. MIRTHA KAREN CHUNGARA RODRÍGUEZ

TUTOR: MSC. JORGE OMAR MOSTAJO BARRIOS

La Paz – Bolivia

2020

AGRADECIMIENTOS

Agradezco a Jehová Dios, mi guía en cada paso, mi luz y fortaleza.

A la Universidad Andina Simón Bolívar, por brindarme por intermedio de los docentes la especialización anhelada.

A mis padres Dr. Simón Chungara Cepeda y Dra. Esperanza Rodríguez Quevedo, por su incondicional apoyo, por ser el mejor ejemplo de perseverancia y por haberme inspirado la pasión por el derecho y la justicia.

A mis hijos, porque su existencia es el impulso motivador y la fuerza para poner todo mi tesón en lo que emprendo.

Al MSc. Jorge Omar Mostajo Barrios, meritorio profesional del derecho, por su orientación y guía en la elaboración del presente trabajo.

RESUMEN

Las Tecnologías de Información y Comunicación han incursionado en los más innumerables aspectos de la vida cotidiana del ser humano, con notables beneficios que facilitan la realización de operaciones comerciales, financieras, laborales, académicas y aquellas relacionadas con la administración pública. Así también, estos adelantos, posibilitan una masiva recolección y difusión de datos personales, lo cual en ocasiones es aprovechado por los delincuentes para la comisión de una amplia gama de ilícitos, en desmedro de los derechos de los titulares de estos datos y con nefastas consecuencias de orden personal y económico; fenómeno también identificado en la actual sociedad boliviana.

En ese contexto, el presente trabajo propone la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela de la autodeterminación informativa como derecho humano y fundamental, considerando que dicha norma cuenta únicamente con los Artículos 363 bis (Manipulación informática) y 363 ter (Alteración, acceso y uso indebido de datos informáticos), los cuales de acuerdo a los resultados que emanan del estudio con enfoque mixto efectuado, que comprendió el análisis doctrinal y normativo, la aplicación de la encuesta, la entrevista y el estudio de caso; son insuficientes para hacer frente a los nuevos retos que la era digital y la Sociedad de la Información plantean, en un escenario tecnológico cada vez más globalizado.

Bajo dichos parámetros, se concluyó la factibilidad de la propuesta, cuyo tenor fue reflejado en la redacción de un proyecto legislativo para incorporar al Código Penal la tutela de datos personales, datos personales sensibles y datos personales de menores de edad, configurando con ello una nueva esfera de protección, que además de los mecanismos jurídicos existentes en sede administrativa, civil y constitucional, incluya el ámbito penal y por consiguiente, derive en una optimización de la tutela del derecho de autodeterminación informativa.

Palabras clave: protección de datos personales, autodeterminación informativa, incorporación de tipos penales, tecnologías de información y comunicación.

ÍNDICE

ÍNDICE DE TABLAS

CONTENIDOS **PÁG.**

ÍNDICE DE GRÁFICOS

CONTENIDOS **PÁG.**

CAPÍTULO I
ASPECTOS GENERALES DE LA INVESTIGACIÓN

1.1 Introducción

La utilización cada vez más generalizada de las Tecnologías de Información y Comunicación (TIC)[1], el advenimiento de la red Internet[2]y su llegada exponencial a un mayor número de usuarios, son factores que incrementan el tráfico de datos; David Wall definió esta transcendental herramienta como: "(…) una red global de interconexión de redes gubernamentales, militares, empresariales y domésticas. Es una sola red, es una red de redes. Es la plataforma sobre la cual la Red Mundial opera" (Calderón, 2013, p.4).

La información "es poder", frase aún vigente en pleno siglo XXI, al ser considerada como un bien susceptible de apoderamiento y utilización, con el plus del valor patrimonial o contenido económico inherente e intrínseco que radica en su destino y utilidad. Bajo este parámetro, los datos personales cuyo contenido refleja la información de los individuos, se encuentran cada vez más expuestos, de ahí que puede afirmarse que en dicho escenario, emerge un terreno fértil para múltiples conductas ilícitas que atentan contra los mismos, con ostensible afectación al derecho de autodeterminación informativa, denominado también derecho a la protección de datos personales, entendido como la facultad del sujeto de decidir sobre el uso de su información personal: pública o privada, máxime si se trata de datos catalogados bajo el rótulo de sensibles, tales como la ideología, la religión, las creencias, la vida sexual o la salud, entre otros.

Estos atentados, no solo quebrantan el citado derecho, si no también otros vinculados, como la intimidad, la privacidad, la honra, el honor, la libertad ideológica o religiosa, la libertad sindical o el derecho a no ser discriminado, para citar sólo algunos; es decir, afectan, lesionan o ponen en peligro otros bienes jurídicos, constituyendo este un factor sustancial para su tutela.

El Estado Plurinacional de Bolivia, a raíz de los adelantos tecnológicos aplicados a los sectores estatal y privado, ha puesto en vigencia normativa que ha propiciado vehementes

[1] Las Tecnologías de Información y Comunicación, comprenden los avances reflejados en la electrónica, informática y las telecomunicaciones.

[2] Es la herramienta para tener acceso al ciberespacio, su denominación deviene de la frase: Interconnected Networks y su origen se remonta a fines de la década de los sesenta, en plena guerra fría, con la creación de una red militar de ordenadores interconectados en Estados Unidos, inicialmente se denominó ARPANET y vio la luz con cuatro ordenadores distribuidos en distintas universidades del país del norte. Su objetivo inicial fue crear un sistema de intercambio de archivos y mensajes seguro, para mantener las comunicaciones en caso de guerra ante la situación de incertidumbre y temor del momento. A partir de ello fue evolucionando, hasta que en 1991, usuarios externos tuvieron acceso a la misma, expandiéndose su utilización paulatinamente a todo el mundo.

debates y propuestas de Ley al interior de la Asamblea Legislativa Plurinacional[3], aspecto que también ha movilizado a distintos sectores y organizaciones de la sociedad civil, quienes desde la gestión 2018 se encuentran trabajando en la redacción de proyectos[4] legislativos relacionados con el rubro de la protección de datos personales y en similar sentido el Órgano Ejecutivo a través de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC)[5] (ATB Digital, 2018; Periódico Opinión, 2018), trabajó en la elaboración de otra propuesta de ley.

Si bien el derecho penal es de ultima ratio, en lo fáctico cada día es más recurrente el número de casos de vulneración a datos e información personal, muchos de los cuales fueron de conocimiento general a través de los medios de comunicación, por consiguiente; es evidente el menoscabo de derechos de los afectados, generando tal agresión y lesividad que amerita la intervención punitiva del Estado. En ese contexto, la investigación pretende generar una propuesta para la protección de la información y los datos personales desde la perspectiva del derecho penal, en función a que la actual norma sustantiva vigente del Estado Plurinacional de Bolivia, carece de una regulación específica de esta índole, siendo las normas aplicables insuficientes, generando nichos para la impunidad que alimentan el círculo de la criminalidad. Para el cumplimiento de dicho fin, el estudio esboza la tutela de datos personales contenidos en soportes físicos e informáticos con miras a una salvaguarda integral, a través de la incorporación de nuevos tipos penales en el Código Penal.

En dicho contexto, el Capítulo I, Aspectos Generales de la Investigación, parte de la identificación del escenario actual por el que atraviesa la sociedad boliviana, bajo el acelerado influjo y expansión de las Tecnologías de Información y Comunicación en las actividades cotidianas de los individuos, factor que representa un cambio de paradigma en los diferentes procesos que se llevan a cabo en la sociedad. Este fenómeno que posibilita la recolección de datos personales a escala antes insospechada, demanda el ejercicio del derecho de autodeterminación informativa, como facultad del individuo de controlar su información

[3] La Dra. Jhovanna Jordán Antonio, Diputada Nacional, mediante nota del 30 de noviembre de 2018, presentó a la Asamblea Legislativa Plurinacional el Proyecto de Ley de Protección de Datos Personales, siendo reingresado para su tratamiento en la gestión 2019.

[4] La Fundación Internet Bolivia, en mayo de 2019, presentó un Proyecto de Ley de Protección de Datos Personales a la Asamblea Legislativa Plurinacional. Así también, la Universidad Católica Boliviana San Pablo, bajo la dirección del Dr. Félix Fabian Espinoza Valencia redactó otro Proyecto de Ley sobre el tema.

[5] La Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), fue creada mediante Decreto Supremo N° 2514 de 9 de septiembre de 2015, de acuerdo a su Artículo 7, cumple las funciones de impulsar implementar y coordinar políticas, planes y estrategias de gobierno electrónico y tecnologías de información y comunicación en las entidades estatales, también trabajó en la elaboración de un proyecto de Ley de Protección de Datos Personales.

personal, y de ahí emerge la formulación del problema de investigación, como cuestionante para optimizar la tutela del citado derecho en el Estado Plurinacional de Bolivia.

Consiguientemente; la hipótesis pretende establecer si la falta de tipos penales referidos a la protección de datos personales en la norma sustantiva penal boliviana, limita la tutela del derecho precedentemente enunciado; en tanto que, el objetivo general se orienta a proponer la incorporación de nuevos ilícitos en el catálogo del Código Penal.

Los aspectos metodológicos se desarrollan en función al enfoque mixto, toda vez que posibilitaron abordar el fenómeno estudiado en su integralidad para responder apropiadamente al problema de la investigación, la hipótesis y respaldar la propuesta, en el marco de un estudio descriptivo propositivo, orientado a confluir en un proyecto legislativo. A su vez, se recurre al diseño no experimental, así como a los métodos: analítico-sintético, comparativo y dogmático jurídico, por ajustarse al tipo de investigación y coadyuvar en la formulación de la propuesta, mediante la aplicación de las técnicas de revisión documental, encuesta, entrevista y estudio de caso.

Para una apropiada comprensión de la problemática, el Capítulo II Marco Teórico, desarrolla los antecedentes teóricos y conceptuales del derecho a la protección de datos personales; consiguientemente, se aborda el tema desde la perspectiva del derecho penal, los delitos informáticos y los presupuestos a los que deben ajustarse los tipos penales cuya creación se propone.

Los resultados de la encuesta, la entrevista y el estudio de caso son presentados en el Capítulo III Marco Práctico, que analiza los datos obtenidos y los relaciona, para sintetizarlos en su respectiva conclusión. En el Capítulo IV Legislación Comparada, el estudio aborda la normativa de Argentina, Colombia y España, países que desde hace más de una década incluyeron tipos penales que sancionan la vulneración de los datos personales. A su turno, el Capítulo V Propuesta, expone los fundamentos en los que se sustenta el Proyecto de Ley de incorporación de tipos penales en el Código Penal del Estado Plurinacional de Bolivia, orientados a la protección de datos personales, datos personales sensibles y datos personales de menores de edad.

Por último, se presentan las conclusiones en relación a los objetivos general y específicos y las recomendaciones arribadas como resultado de la labor investigativa.

1.2 Planteamiento del problema

1.2.1 Situación problemática

Las Tecnologías de Información y Comunicación han irrumpido en las distintas esferas y actividades de la sociedad, siendo inexorable la utilidad que brindan para diversas finalidades y en variados aspectos, ya sea en el ámbito social, laboral, académico o económico; para citar sólo algunos, dando lugar a una conectividad e intercambio súbito de datos a escala mundial, acentuado con el advenimiento de la red Internet. En torno al descrito progreso, emerge la Sociedad de la Información, como una nueva fase del desarrollo de la humanidad, cuyo eje fundamental lo constituyen las TIC aplicadas al libre flujo de conocimientos; que de acuerdo a los postulados de la Cumbre Mundial de la Sociedad de la Información desarrollada en la ciudad de Ginebra el año 2003, deben centrarse en la persona, propendiendo a la integración y el progreso, con miras a una mejora en la calidad de vida y con pleno respeto a los principios establecidos en la Carta de Naciones Unidas y la Declaración Universal de los Derechos Humanos (Téllez, 2009, p.1).

En consecuencia, producto del vertiginoso e intrincado desarrollo tecnológico, el ser humano se encuentra en plena Era Digital, experimentando profundas transformaciones de sus hábitos, en un mundo globalizado a través de la interconexión e interacción virtual de los individuos alrededor del orbe, con efectos positivos reflejados en un incremento de la eficiencia, eficacia, innovación y optimización en las relaciones laborales, económicas, comerciales y gubernamentales. Por otra parte, estos aspectos también posibilitan que los usuarios de dichas tecnologías, proporcionen en mayor medida datos e información personal, la cual utilizada indebidamente origina riesgos potenciales y reales, que involucran desde afectaciones a la privacidad, la imagen, el honor, situaciones discriminatorias y menoscabos patrimoniales, hasta confluir en atentados contra la integridad psicológica y física, e incluso quebrantar la propia vida, llegando a configurar infracciones y delitos.

Lo anterior, genera un menoscabo de libertades y derechos fundamentales, entre los que particularmente se encuentra el derecho a la autodeterminación informativa o denominado en forma equivalente como derecho a la protección de datos personales (Murillo, 2008, p.44), cuyo carácter autónomo e independiente es fruto de la reflexión doctrinal y de la labor jurisprudencial, entendido como la facultad de toda persona para ejercer control sobre sus datos personales, no sólo los inherentes a la esfera de la intimidad y privacidad, sino cualquier tipo de dato que identifique o permita la identificación de un individuo y esté en conocimiento o tratamiento de terceros.

Consiguientemente, este derecho tiene como objetivo dotar al titular del dato, de una serie de facultades que le permitan disponer del mismo, hasta el punto de no sólo restringir su acceso y tratamiento a las personas autorizadas por él, sino también a saber en todo momento cuál será su uso y destino (Murillo, 2008, p.49).

De acuerdo al Informe Anual sobre la Delincuencia en el Internet (Internet crime report, 2018) correspondiente a la gestión 2018, emitido por el Federal Bureau of Investigation (FBI), los delitos denominados Personal Data Breach o violación de datos personales, en los Estados Unidos de Norteamérica ascienden a 50.642 casos denunciados, encontrándose en el tercer lugar de la lista de ilícitos más frecuentes después de extorsiones, generando un daño económico anual de 148.892.403 dólares americanos, monto notoriamente engrosado con relación al informe del año anterior, en el que las perdidas reportaron un total de 77.134.865 dólares americanos en el mismo rubro (Internet crime report, 2017), sin incluir los casos comprendidos dentro las cifras negras de la criminalidad informática.

Así pues, ante el surgimiento de nuevas conductas delictivas que atenten contra la información y los datos personales, es menester incorporar en la norma sustantiva penal, tipos penales especializados, actuales y vanguardistas, que se ciñan al principio de taxatividad, para hacer frente a los desafíos que involucran las TIC en la era del Big Data[6].

1.2.2 Situación proyectada

La situación proyectada, es la incorporación de tipos penales orientados a resguardar la información y los datos personales en el Código Penal; consiguientemente, en aplicación del principio de taxatividad se regularán las conductas ilícitas y las sanciones respecto a figuras hasta ahora inexistentes en la normativa vigente, bajo la premisa de mejorar la protección del derecho de autodeterminación informativa.

En ese contexto, es menester señalar que el desarrollo normativo debe concretarse en función al progreso de la sociedad, ante lo cual la actual regulación aplicable a la materia contenida en los Artículos 363 bis. (Manipulación informática) y 363 ter. (Alteración, acceso y uso indebido de datos informáticos) del Código Penal, puede resultar insuficiente, ameritando ser remozada, máxime si se considera que la tecnología avanza a pasos agigantados.

[6] El término Big Data alude al enorme crecimiento en el acceso y uso de información automatizada. Se refiere a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos.

La incorporación de nuevas figuras penales que contemplen la protección de datos personales, datos personales sensibles y datos personales de menores de edad, no sólo coadyuvará al ámbito de la prevención, sino que también ante la concreción de este tipo de ilícitos cada vez más recurrentes, el afectado podrá acudir ante las autoridades competentes para incoar la persecución penal y si corresponde, obtener una sanción en contra del autor del delito más la reparación del daño; consecuentemente, estas conductas no quedarán impunes.

El principio de legalidad, formulado por Feuerbach en las primeras décadas del Siglo XIX, que esencialmente señala: nullum crimen, nulla poena sine previa lege (no hay delito ni pena sin ley previa) conlleva un conjunto de garantías a desarrollarse en la legislación penal, entre las que se encuentran la reserva de ley, el principio de taxatividad y la prohibición de analogía.

Consiguientemente, los tipos penales cuya incorporación en la norma sustantiva penal propone el estudio, se orientan específicamente a la protección de información y datos de índole personal, para con ello optimizar la tutela del derecho de autodeterminación informativa, posibilitando la adopción de una legislación apropiada, en respuesta a los nuevos ilícitos emergentes, primordialmente como resultado de la irrupción de las TIC.

1.2.3 Formulación del problema

Dentro del presente trabajo, se establece la siguiente cuestionante:

¿En qué medida la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, optimizará la tutela del derecho de autodeterminación informativa?

1.3 Justificación del trabajo

1.3.1 Justificación teórica

La protección de datos personales, responde a las circunstancias imperantes, siendo de significativa trascendencia para la sociedad actual; no obstante, constituye una temática aun escasamente abordada desde el ámbito jurídico penal en el Estado Plurinacional de Bolivia.

Desde esta perspectiva, el aporte teórico del estudio se circunscribe al derecho penal, toda vez que partiendo del análisis doctrinal y de los resultados de la aplicación de las técnicas e

instrumentos de investigación, se generó conocimiento, consolidando un nuevo constructo teórico como fundamento para plantear soluciones tendientes a mejorar la tutela de los datos personales, a través de la emisión de una propuesta de norma orientada a la creación de tipos penales que configuren su salvaguarda, coadyuvando así a la vigencia del derecho de autodeterminación informativa y otros derechos vinculados.

1.3.2 Justificación práctica

Es menester dotar a los ciudadanos, de instrumentos normativos de protección frente a la hegemonía del desarrollo tecnológico que permite a entidades públicas, empresas privadas y personas particulares, recabar y utilizar datos personales en una progresión sin precedentes y que posibilita difundir un volumen cada vez mayor de información a escala global. Desde este enfoque, la legislación debe responder al dinamismo de la sociedad y desafíos tecnológicos, máxime si se tiene presente que otros países latinoamericanos y europeos, desde hace más de una década han desarrollado políticas y leyes en la materia, y actualmente se encuentran trabajando en adecuar las mismas a estándares internacionales, en un mundo en el que el escenario digital se muestra raudo y complejo.

Bajo dichos parámetros, el estudio brinda una solución a un problema cotidiano, que arremete y lesiona el derecho de autodeterminación informativa y derechos conexos, pero que, por la ausencia de tipos penales en la actual norma sustantiva penal, no es posible su persecución ni el establecimiento de sanciones respecto a los infractores.

1.3.3 Justificación social

A través de la incorporación de tipos penales de protección de datos personales, se beneficia a la población en general del Estado Plurinacional de Bolivia, mejorando la tutela en dicho ámbito, considerando que al presente, por el uso generalizado de las TIC, cualquier persona es proclive a ser víctima de un ilícito de esta naturaleza, con el consiguiente menoscabo de sus derechos y libertades, quedando muchas veces estas conductas en la impunidad.

A su vez, es pertinente manifestar que la ley penal debe ser precisa, es decir taxativa, a partir de ello no se entiende este principio únicamente como parte del principio de legalidad, sino como garantía integradora de un Estado Constitucional de Derecho, en el entendido de que el derecho penal marca los límites y reglas de los comportamientos de las personas para apartarse de cometer ilícitos, pero también para sancionar a los responsables. Lo anterior, posibilita la restricción de la acción punitiva estatal a los límites establecidos por la ley,

propugnando el establecimiento del orden social al permitir la identificación y determinación de las conductas más lesivas y su sanción.

1.4 Delimitación de la investigación

1.4.1 Delimitación temática

En el aspecto temático, la investigación forma parte del ámbito del Derecho Público, a su vez, dentro de esta rama se ubica dentro del Derecho Penal, relacionado con el Derecho Constitucional y el Derecho Informático.

1.4.2 Delimitación espacial

El trabajo de gabinete y el trabajo de campo se circunscriben al Departamento de La Paz, Primera Sección de la Provincia Murillo, Ciudad Nuestra Señora de La Paz, con alcance a nivel nacional puesto que el estudio propone la incorporación de tipos penales en el Código Penal del Estado Plurinacional de Bolivia.

1.4.3 Delimitación temporal

La investigación tomó como punto de partida, la puesta en vigencia de la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación Nº164 de 8 de agosto de 2011, hasta diciembre de 2019, en razón de que constituye una regulación en la que por primera vez se incluyó la noción de datos personales y por ser un periodo en que la problemática abordada cobra vigor.

1.5 Objetivos

1.5.1 Objetivo general

Proponer la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela del derecho de autodeterminación informativa.

1.5.2 Objetivos específicos

a) Caracterizar los fundamentos teóricos e históricos del derecho a la protección de datos personales.
b) Identificar las bases teóricas, doctrinales e instrumentos internacionales, que sustentan la tutela penal de los datos personales.
c) Diagnosticar la necesidad de incluir tipos penales orientados a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia.
d) Comparar la legislación penal de Argentina, Colombia y España en relación a delitos que vulneran los datos personales.
e) Diseñar la propuesta de incorporación de tipos penales referidos a la protección de los datos personales en el Código Penal del Estado Plurinacional de Bolivia.

1.6 Hipótesis

La falta de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, limita la tutela del derecho a la autodeterminación informativa.

1.6.1 Variable independiente

La falta de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia.

1.6.2 Variable dependiente

Tutela del derecho de autodeterminación informativa.

1.6.3 Operacionalización de las variables

Tabla N°1

Operacionalización de las variables

VARIABLE	DEFINICIÓN	DIMENSIÓN	INDICADOR	ESTRATEGIA
DEPENDIENTE Derecho de autodeterminación informativa	Derecho del individuo a controlar la obtención, tenencia, tratamiento, y transmisión de datos relativos a su	Datos personales	Conocimiento	Encuesta Entrevista Estudio de caso
			Frecuencia con que se proporciona	
			Frecuencia con que se comparte por medio de las TIC	
		Percepción de seguridad	Datos proporcionados a entidades públicas	

	persona, decidiendo en cuanto a los mismos, las condiciones en que dichas operaciones pueden llevarse a cabo (Serrano, 2003, p.67)		Datos proporcionados a entidades privadas	
		Vulneración de datos personales	Formas recurrentes	
INDEPENDIENTE Falta de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia	"(…) la descripción de la conducta prohibida por una norma (…) el conjunto de elementos que caracteriza a un comportamiento como contrario a la norma." (Bacigalupo, 1999, p.220)	Pertinencia	Existencia	Estudio teórico normativo Encuesta Entrevista Estudio de caso
			Incorporación	
			Datos sensibles y de menores de edad	
			Conductas	
			Dolo o culpa	
			Sanción	
		Resultados	Optimización en la tutela del derecho de autodeterminación informativa	

Fuente: elaboración propia (2019)

1.7 Enfoque de la investigación

El enfoque mixto: "(…) implica un conjunto de procesos de recolección, análisis y vinculación de datos cuantitativos y cualitativos en un mismo estudio o una serie de investigaciones para responder a un planteamiento del problema" (Hernandez, Fernández, & Baptista, 2014, p. 532), en este sentido, la investigación por sus características adoptó este enfoque, porque permitió una visión integral y más completa del fenómeno suscitado, considerando la necesidad no solo de recopilar datos cuantitativos sino también cualitativos, aspectos que luego se reflejaron en la formulación de la propuesta.

1.8 Tipo de estudio

La investigación descriptiva, consiste en describir fenómenos, situaciones, contextos y sucesos; esto es, detallar cómo son y se manifiestan. Con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es de utilidad para analizar: "¿cómo sucede?, ¿cómo es? y ¿cómo se manifiesta? un fenómeno y sus componentes. Permite detallar mediante la descripción, el fenómeno estudiado básicamente, a través de la medición de uno o más variables para llegar a conclusiones" (Criales y Torrico, 2014, p. 113).

Por su parte, el estudio propositivo se decanta por la identificación de fallas a partir de las cuales se proponen cambios y/o reformas (Witker, 2011, p. 38). En consecuencia; la investigación partió del análisis de la incidencia e implicancias del derecho a la protección de

datos personales o autodeterminación informativa y su tutela desde el ámbito del derecho penal, para desembocar en la propuesta de tipos penales a ser incluidos en el Código Penal del Estado Plurinacional de Bolivia, adscribiéndose al tipo descriptivo - propositivo.

1.9 Diseño de la investigación

Corresponde al diseño no experimental, puesto que se basó en observar: "(…) situaciones ya existentes, no provocadas intencionalmente (…) (Hernández et al., 2014, p. 152), es decir sin la manipulación intencionada de las variables, realizando la observación de los fenómenos intervinientes en su ambiente natural.

1.10 Métodos de investigación

a) Análisis - síntesis

Consiste en descomponer el todo en sus partes integrantes, para analizar cada una de ellas de forma independiente y luego proceder a su recomposición. Conforme ilustra Villabella (2015) "(…) es un recurso imprescindible cuando se estudian normas, instituciones, procedimientos, conceptos, etcétera, que necesitan descomponerse en sus estructuras para caracterizarlas" (p. 937). La investigación analizó el derecho a la protección de datos personales y su protección en el ámbito penal, desglosando conceptos, doctrina y normas relacionadas al mismo, posteriormente se dio lugar a su integración, lo cual permitió una mejor comprensión de la problemática, siendo aplicado en Marco Teórico del estudio.

b) Método comparativo

Según Tantaleán (2016, p. 19), posibilita la comparación y evaluación de la legislación con la finalidad de mejorar el ordenamiento jurídico o mostrar las bondades o defectos de alguno de los ordenamientos comparados. Permitió realizar un contraste entre las legislaciones de Bolivia, Argentina, Colombia y España, con la finalidad de vislumbrar el estado y avances regulatorios en materia de normativa penal de protección de datos personales; consiguientemente, se recurrió a este método en el acápite de Legislación Comparada y como sustento para la elaboración de la propuesta.

c) Método dogmático jurídico

Este método: "(…) se trata, en esencia, del estudio de las normas jurídicas y todo lo que tenga que ver con ellas pero siempre en sede teórica (…) estudia a las estructuras del derecho objetivo - o sea la norma jurídica y el ordenamiento normativo jurídico - un estudio dogmático se basa, esencialmente, en la legislación y la doctrina como fuentes del derecho objetivo" (Tantaleán, 2016, p.4). Con la aplicación del método dogmático jurídico se efectuó un estudio normativo desarrollado en el Marco Teórico, el cual confluyó en identificar la ausencia de tipos penales referidos a la protección de los datos personales, así como la necesidad y la pertinencia de su inclusión en el Código Penal boliviano, y en base al mismo fundamento, se sustentó la propuesta.

1.11 Técnicas de recojo de información

1.11.1 Encuesta

Al caracterizarse esta técnica por la obtención de datos de varias personas sobre un tema o problema, cuyas opiniones impersonales son de interés para la investigación (Criales y Torrico, 2014, p. 145), permitió la obtención de información para comprobar la hipótesis, así como para la elaboración y respaldo de la propuesta.

a) Universo y población

El universo lo conformaron los abogados de la ciudad de La Paz, que se desempeñan laboralmente en el ámbito del derecho penal, factor que obedece a que por este atributo tienen un mayor conocimiento sobre la problemática de la investigación. La población comprendió a profesionales registrados en el Ilustre Colegio de Abogados de La Paz con especialidad en la citada rama jurídica.

- Población (finita): 1872 (https://www.icalp.org.bo/Buscador)

b) Muestra

La muestra a la que se adscribió la investigación es la no probabilística, homogénea y por conveniencia, donde: "(…) la elección de los elementos depende de razones relacionadas con las características de la investigación", "(…) las unidades que se van a seleccionar poseen un mismo perfil o características, o bien comparten rasgos similares. Su propósito es centrarse

en el tema por investigar o resaltar situaciones, procesos o episodios en un grupo social" y están "(…) formadas por los casos disponibles a los cuales tenemos acceso" (Hernández et al., 2014, pp. 386-390). También se señala que es: "(…) un diseño de muestreo en el que se seleccionan aquellos sujetos más fácilmente accesibles, que en ocasiones pueden ser voluntarios" (Robledo, 2005, p. 6).

Bajo dichos parámetros la muestra se determinó en aplicación de la siguiente fórmula (Torrico y Pareja, 2019, p.33):

$$n = \frac{Z^2 * N * p * q}{e^2(N-1) + Z^2 * p * q}$$

$$\frac{1{,}96^2 * 1872 * 0{,}5 * 0{,}5}{0{,}05^2(1872-1) + 1{,}96^2 * 0{,}5 * 0{,}5} = \frac{1797.8688}{5.6379} = 318.8897$$

Z= valor basado en el nivel de confianza (95% Z=1,96)
P(q) = probabilidad de que ocurra (no ocurra) el suceso (0,50, por tratarse de un estudio nuevo)
N=Población =1872
e= margen de error = 0,05 (5%)

Tamaño de la muestra: 318, con un nivel de confianza de 95% y margen de error de 5%.

1.11.2 Entrevista

A través de este contacto interpersonal cuya finalidad es el acopio de testimonios orales (Witker, 2011, p.147), se obtuvo información para la constatación de la hipótesis y la redacción de la propuesta. La modalidad de la entrevista fue la semiestructurada, porque de acuerdo al problema, objetivo e hipótesis de la investigación, permitió abordar las cuestionantes preestablecidas, pero además incluir determinados puntos que en función al entrevistado y al desarrollo mismo del diálogo ameritaron mayor profundidad.

a) Universo y población

En lo que atañe a la entrevista, el universo lo conformaron profesionales abogados que por el ejercicio de su actividad se encuentran imbuidos en el área del derecho informático y/o protección de datos personales, en atención a la relación con la problemática analizada.

b) Muestra

La muestra fue no probabilística, conformada por 3 expertos, en razón de que: "(…) la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace la muestra" (Hernández et al., 2014, p.117); asimismo, Creswell (citado por Hernández et al., 2014, p. 385), subraya que en las investigaciones cualitativas los intervalos de estas muestras pueden oscilar en el rango de uno a 50 casos. En consecuencia, este tipo de muestra que en el caso particular se orientó a expertos, permitió la obtención de criterios especializados, para dar respuesta a la hipótesis formulada y como cimiento para sustentar la propuesta. Entre los entrevistados, se tomaron en cuenta los siguientes:

- Entrevistado N°1

Félix Fabian Espinoza Valencia: Licenciado en Derecho titulado de la Universidad Católica Boliviana San Pablo, Diplomado en Educación Superior – Tecnología en la Educación de la Universidad Mayor de San Andrés, Diplomado en el Nuevo Código Procesal Civil de la Universidad Mayor de San Andrés, Master en Derecho Digital y Sociedad de la Información de la Universidad de Barcelona - España. Asesor Legal de la Asamblea Legislativa Plurinacional, realizando entre otros: asesoramiento a Senadores, revisión técnica jurídica de proyectos de ley, realización de instrumentos legislativos específicos y producción de instrumentos de gestión y procedimientos legislativos; Director CEO en Buenafelegal.org, Chief Legal Counsel en Ticracia, Asesor Legal de la Fundación REDES Bolivia. Docente de Derecho Informático de la Universidad Católica Boliviana San Pablo. Miembro asociado de Internet Society Bolivia, miembro del Comité de Seguridad del Consejo de Tecnologías de Información y Comunicación del Estado (CTIC) y de la Federación Iberoamericana de Asociaciones de Derecho Informático (FIADI), así como colaborador del National Cyber Security Index (NCSI) e-Governance Academy Foundation.

Es autor de diversas publicaciones del área de ciberseguridad, ciberdelincuencia, protección de datos personales y derecho informático. Redactor del Proyecto de Ley de protección de datos personales, desde la comunidad denominada Stalkeadores de Leyes y la Universidad Católica Boliviana San Pablo. Estuvo a cargo del primer diagnóstico sobre ciber-delincuencia en Bolivia, en base a un estudio realizado en los 9 departamentos, durante la gestión 2019.

- Entrevistado N°2

Carlos Alberto Peláez Troncoso: Licenciado en Ciencias Jurídicas y Políticas titulado de la Universidad Mayor de San Simón de Cochabamba. También realizó estudios de informática a nivel técnico superior en el área de Análisis de Sistemas. Diplomado en Derecho Laboral, Diplomado en Derecho Constitucional, Diplomado en Educación Superior, Diplomado en Gestión Pública y Control Social, cursó la Especialidad Superior en Derecho Empresarial y es Magíster en Derecho Constitucional y Derechos Fundamentales. Realizó estudios en la Escuela Judicial de Republica Dominicana referentes al Derecho Internacional de los Derechos Humanos.

Asesor Jurídico de varias empresas en la ciudad de Cochabamba, donde también se desempeñó como abogado de bufete, ejerció funciones en el Tribunal Constitucional de Bolivia relacionadas con la Documentología y la Informática Jurídica, Secretario de Cámara de la Sala Penal Segunda de la Corte Suprema de Justicia, y posteriormente Abogado Asistente de la misma, Presidente de la Comisión de Derecho Informático del Ilustre Colegio de Abogados de Chuquisaca, Abogado Asistente del Equipo Técnico de Implementación del Nuevo Código de Procedimiento Penal (ETI) dependiente de la Corte Suprema de Justicia, y funcionario de enlace y coordinación entre la Corte Suprema de Justicia y la Red Iberoamericana de Documentación Judicial “IBERIUS”. Fungió como consultor externo de la Agencia de Cooperación Alemana (GTZ) en el Proyecto de Reforma Procesal Penal, Coordinador Académico del Área No Jurisdiccional del Instituto de la Judicatura de Bolivia y Docente del mismo Instituto. Docente de post grado de la Universidad Andina Simón Bolívar y del Centro de Posgrado e Investigación (CEPI) de la Universidad Mayor Real y Pontificia de San Francisco Javier de Chuquisaca, Coordinador del proceso de institucionalización del Ministerio Público, Director del Instituto de Capacitación del Ministerio Publico y posteriormente Director de la Escuela de Fiscales del Estado. Integrante del equipo de investigadores que hicieron posible la publicación de la obra denominada “La formación judicial en Bolivia perspectivas de futuro”, publicada con el auspicio del proyecto PROJURIDE – GIZ y la Oficina del Alto Comisionado de Naciones Unidad para los Derechos Humanos en Bolivia.

Asesor Legal de las Comisiones de Autonomía, de Medio Ambiente, Madre Tierra y Agua, de la de Hidrocarburos, Energía y Minería de la Asamblea Legislativa Departamental de Chuquisaca, y Abogado Sumariante de la Comisión Disciplinaria y de Ética de la misma Asamblea. Actualmente realiza actividades de consultoría a empresas privadas en la ciudad de Santa Cruz, y se desempeña como Responsable o Coordinador del Programa de Maestría

en Derecho Constitucional del Centro de Posgrado e Investigación de la Universidad San Francisco Javier de Chuquisaca.

Autor de diversos programas informáticos, bases de datos y libros electrónicos con información relacionada a la legislación, jurisprudencia y doctrina en diversas materias, como el software denominado “Pascal – Jure, “Visual Jure”, “Conociendo la nueva Constitución Política del Estado y su normativa de desarrollo”, etc., de igual manera, autor de varias publicaciones literarias como ser “Informática y Derecho”, “La Campaña de la BSA en Bolivia”, “Función y Responsabilidad del Personal de apoyo jurisdiccional”, “Derecho Registral Inmobiliario”, “Elecciones Judiciales - de la ilusión al fracaso”, “Gobierno Electrónico Judicial”, y otros, como asimismo, de numerosos artículos relacionados con la Informática Jurídica, el Derecho Notarial, el Derecho Registral y otros referidos al ámbito de la labor judicial, publicados en boletines, revistas, y periódicos.

- Entrevistado N°3

Edgar David Oliva Terán: Licenciado en Derecho titulado de la Universidad Mayor de San Simón, realizó estudios de Diplomado en Conciliación, negociación y arbitraje en la Universidad Privada Boliviana; Experto en Redes Sociales de la Universidad Privada Boliviana; Diploma Skills and Management, ESADE Facultad de Derecho de la Universidad Ramón Llull, Barcelona - España; Master en derecho de las TIC, Redes Sociales y Propiedad Intelectual, ESADE Facultad de Derecho de la Universidad Ramon Llull, Barcelona - España.

Se desempeñó como Abogado del Área de Propiedad Intelectual y Protección de datos en Cervieri Monsuarez Despacho de abogados de Propiedad Intelectual, Abogado del Área de Propiedad Intelectual en Wayar & Von Borries Abogados Despacho de Abogados Corporativos, Abogado del área de Propiedad Intelectual y Protección de Datos en Ecija law & Technology Despacho de abogados especializados en Propiedad Intelectual y Nuevas Tecnologías (Madrid - España); Abogado Interno del Área de Protección de Datos, Propiedad Intelectual, Sociedad de la Información en Defyu Technologies SL Empresa de tecnología (Barcelona- España), Abogado Jr. de Manejo de Procedimientos de Registro y fundamentación de casos en Reinicke Ostria Abogados, Asesor externo de Seguridad de la Información en Ethical Hacker Asociados, Gestor Jurídico de Derecho Mercantil en la Cámara de Comercio y Servicios de Cochabamba.

Fungió como capacitador de Derecho de Internet en Incubadora Demiun Startup (Madrid-España); expositor de Derecho Informático, de la Universidad Autónoma Gabriel René Moreno

y conferencista del Anteproyecto de Ley de Protección de Datos de la Fundación Internet Bolivia.org., es también colaborador del Observatorio Iberoamericano de Protección de Datos - OIPRODAT. Participó como Asesor legal de la Fundación Bolivia.org para la elaboración del Anteproyecto de Ley de Protección de Datos; así también en la Declaración de Riobamba: "Hacia la unificación de criterios y medidas de seguridad en protección de datos" del Observatorio Iberoamericano de Protección de Datos – OIPRODAT, presentada en la Universidad de Chimborazo (ciudad de Riobamba de la República del Ecuador - 2014), y en la Declaración de México: "Hacia la implantación de garantías para la protección de datos en los tratamientos de Big Data", a cargo del Observatorio Iberoamericano de Protección de Datos – OIPRODAT, presentada en INFOTEC (ciudad de México Distrito Federal, México-2014). Es autor de diferentes artículos y publicaciones en el ámbito del Derecho Informático, Comercio Electrónico y Protección de Datos, participó como coautor del libro: Protección de datos y habeas data: una visión desde Iberoamérica, que fue galardonado con la XVIII Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos, en la gestión 2014.

1.11.3 Estudio de caso

Para Hernández et. al (2014, p. 164) son: "(…) estudios que al utilizar los procesos de investigación cuantitativa, cualitativa o mixta analizan profundamente una unidad holística para responder al planteamiento del problema, probar hipótesis y desarrollar alguna teoría".

A través del examen de dos casos representativos del medio, referidos: el primero a la obtención y difusión de un video con contenido sexual y el segundo a la revelación del estado de salud, se ahondó en el objeto de estudio, identificando puntos relevantes para probar la hipótesis y sustentar la propuesta.

1.12 Instrumentos de investigación

1.12.1 Cuestionario

Para la concreción de la encuesta, se elaboró un cuestionario de trece preguntas, doce cerradas y una abierta (Anexo 1).

1.12.2 Guía de entrevista

Se formuló la entrevista a través de una guía base de doce preguntas (Anexo 2).

1.12.3 Matriz de estudio de caso

Se diseñó una matriz para reflejar la sistematización del análisis de los casos y posibilitar una mejor comprensión de los aspectos más relevantes relacionados con la problemática del estudio (Anexo 3).

Con relación a los instrumentos, se tomaron en cuenta las siguientes etapas:

- Etapa I (Elaboración): Se realizó la revisión del material bibliográfico para la comprensión teórica y jurídica del fenómeno motivo de investigación, considerando que el análisis teórico es relevante para sustentar el estudio y especialmente la justificación de las preguntas planteadas. Lo anterior en función a identificar las variables de la investigación, su definición operacional, la identificación de las dimensiones y sus indicadores.

- Etapa II (Validación): Para asegurar la validez de contenido del instrumento, es decir el: "(…) grado en que un instrumento refleja un dominio específico de contenido de lo que se mide" (Hernández et al., 2014, p.201), se realizó dos procedimientos: la revisión por tres jueces expertos, y el estudio piloto realizado con tres sujetos de la población de estudio.

En este procedimiento, se incluyó a profesionales en el área del Derecho a la cual responde la presente investigación, los cuales cuentan con una buena reputación en el ámbito de la comunidad jurídica, disponibilidad, motivación para participar e imparcialidad.

Respecto a los instrumentos, estos se validaron mediante formularios que incluyeron los criterios de: claridad en la redacción de la pregunta, claridad en las opciones de respuesta (únicamente para el cuestionario), inducción a respuesta, redacción adecuada a la población de estudio, contribución con el objetivo de la investigación y contribución con la evaluación del objeto de estudio. Para el estudio de caso, se incluyeron los criterios de pertinencia en la inclusión de las categorías, claridad en la redacción de las categorías, claridad en la presentación de las categorías, inducción a sesgo, contribución con el objetivo de la investigación y contribución con la evaluación del objeto de estudio. Asimismo, la validación de los instrumentos incluyó los criterios de: secuencia lógica y cantidad de ítems y sugerencias para su modificación (Anexo 4).

Se entregó a los expertos en forma individual los instrumentos construidos, al igual que los formularios de validación y posteriormente se efectuó la prueba piloto. Luego de la concreción de estos procedimientos se realizaron los ajustes respectivos, siendo los instrumentos validados por los expertos.

CAPÍTULO II
MARCO TEÓRICO

2.1 Fundamentos históricos y teóricos del derecho a la protección de datos personales o autodeterminación informativa

En el presente apartado, se identifican los conceptos, definiciones, principios y facultades que articulan el derecho a la protección de datos personales, su contextualización en las generaciones de derechos, así como sus orígenes en Europa y Latinoamérica, regiones en las que, pese a sus divergencias de orden económico, político y social, goza de reconocimiento constitucional y leyes específicas en la materia. Consiguientemente, se confluye en la caracterización del delito informático, los delitos contra los datos personales, los instrumentos de carácter internacional que contienen disposiciones sobre el tema y la legislación nacional en relación a la materia.

Finalmente, se presenta una síntesis de jurisprudencia emitida por el Tribunal Constitucional de Bolivia, respecto al reconocimiento del derecho de autodeterminación informativa como derecho fundamental. En tal sentido, este análisis conforma el sustrato teórico que respalda la investigación y constituye uno de los referentes para la formulación de la propuesta.

2.1.1 Ubicación del derecho a la protección de datos personales en las generaciones de derechos

Para realizar una aproximación al surgimiento del derecho a la protección de datos personales o autodeterminación informativa, resulta sustancial identificar su ubicación en las generaciones de derechos; es así que, tradicionalmente se identifican tres generaciones, cuyo reconocimiento atañe a un determinado momento ideológico y social, con características propias y rasgos diferenciadores de los otros derechos. La primera corresponde a aquellos propios del pensamiento liberal, vinculados a la economía capitalista y a la Declaración Universal de los Derechos del Hombre y del Ciudadano de 1789, nacen como libertades individuales, y son conocidos también como derechos civiles y políticos; entre estos, se encuentran la vida, la integridad, la dignidad, la justicia, la igualdad, la libertad, y la participación en la conformación del gobierno como elector o elegible. En esta etapa, el Estado establece las reglas que regirán las relaciones particulares y sus sanciones ante la vulneración de derechos, absteniéndose de intervenir más allá de lo indispensable (Herrán, 2003, p.13).

La segunda categoría, corresponde a los derechos sociales, económicos y culturales, y prorrumpe como resultado de la necesidad de intervención del Estado en la economía y relaciones laborales, para lograr un equilibrio ante la desigualdad y la exclusión. Emerge la noción de solidaridad y justicia social, por lo que se hace indefectible ampliar el conglomerado de derechos, es así que se incorporan los derechos relativos al bienestar económico, acceso al trabajo, seguridad social, educación y cultura, entre otros (Flores, 2015, p. 30).

La tercera generación, denominada también derechos de la solidaridad o de los pueblos, involucra los derechos a la paz, medio ambiente sano, desarrollo económico, libre determinación de los pueblos, patrimonio cultural, patrimonio común de la humanidad (Flores, 2015, p.32), tutela de los consumidores y usuarios, y protección de la persona frente a la irrupción tecnológica, en donde se sitúa al derecho a la protección de datos personales o autodeterminación informativa (Herrán, 2003, p.14), como resultado de las nuevas necesidades del hombre y a la luz de la revolución tecnológica de finales del Siglo XX e inicios del Siglo XXI, con la aparición de la denominada Sociedad de la Información (Pérez Luño, 1991, p. 208), ya no como parte del derecho a la intimidad o privacidad sino como una categoría independiente y con plena autonomía que permite a las personas determinar cómo y cuál será el tratamiento de sus datos personales.

Para algunos autores como David Vallespín Pérez, Franz Matcher, Antonio Pérez Luño, Augusto Mario Morello, Robert B. Gelman y Javier Bustamante Donas, actualmente estamos frente a una cuarta generación de derechos (Flores, 2015, p.34); en dicho sentido, a criterio de Ojeda (2015, p.60), las primeras formas de expresión del derecho de autodeterminación informativa se manifestaron en la tercera generación de derechos, pero como categoría independiente pertenece a la cuarta generación.

2.1.2 Génesis del derecho a la protección de datos personales en Europa y Latinoamérica

Con el ánimo de vislumbrar un panorama de los presupuestos sobre los que se articula la construcción del derecho a la protección de datos personales, es importante desglosar sucintamente sus orígenes para comprender su espíritu y finalidad. A estos efectos, se tomará como referente su génesis en Europa (Alemania y España) y Latinoamérica, la primera región por gozar al presente de una legislación robusta y altamente especializada, con reconocimiento a nivel global, erigiéndose en un paradigma inspirador para los distintos países del orbe y; la segunda, atendiendo a que es el territorio en el que geográficamente se sitúa el Estado Plurinacional de Bolivia, y en la cual también; aunque de disímil manera, se ha

verificado un desarrollo en la legislación de protección de datos personales, con innegable influencia del modelo europeo.

2.1.2.1 Europa

El derecho de autodeterminación informativa o protección de datos personales, goza de un reconocimiento de carácter autónomo y fundamental, contenido en el Artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (2000), diferenciado del derecho a la privacidad establecido en el Artículo 7, cuyo germen, gira en torno al desarrollo de las Tecnologías de Información y Comunicación. Frosini, (citado por Garriga, 2016, p. 92), ya en la década de los años sesenta se adelantó en afirmar que, como secuela de la civilización tecnológica, el derecho a la intimidad adquiere una nueva representación, de ser una libertad negativa de impedir la utilización de información de las personas, a una libertad positiva de ejercer el control sobre los propios datos personales que pasan a formar parte de un archivo electrónico.

a) Alemania

La Ley Fundamental para la República Federal de Alemania, aprobada el 8 de mayo de 1949 en la ciudad de Bonn y promulgada el 23 de mayo del mismo año, si bien no hace referencia expresa a la protección de datos personales, consagra en sus Artículos 1, 10 y 13, la protección de la dignidad humana, la inviolabilidad e inalienabilidad de los derechos humanos, la inviolabilidad del secreto epistolar, postal, de telecomunicaciones y de domicilio. En ese contexto, el 7 de octubre de 1970 fue promulgada la Ley no federal sobre tratamiento de datos personales (Datenshutz) en el Estado de Hesse (Land de Hesse), con el fin de brindar protección a las personas frente al tratamiento informatizado de datos efectuado por la administración pública, esta norma, aunque no gozó de carácter nacional, constituye la primera en su género (Cerda, 2003, p.57).

Más adelante, el 27 de enero de 1977, el Parlamento Federal, emitió la Ley de Protección de Datos (Bundesdatenschutzgesetz), que profundiza en el principio de legitimación para el tratamiento de datos en el ámbito público y en el privado, configurando regímenes diferenciados para ambos sectores, e incorpora la tipificación de ilícitos penales e infracciones relacionados con el tratamiento de datos (Cerda, 2003, pp. 57-58).

Si bien se contaba con normativa de protección de datos personales, el surgimiento de la autodeterminación informativa como derecho autónomo e independiente en Alemania tiene

su origen en una construcción jurisprudencial del Tribunal Constitucional Federal Alemán, que mediante Sentencia de 15 de diciembre de 1983, declaró la inconstitucionalidad de varios artículos de la Ley del Censo aprobada por el Parlamento Federal (Bundestag) el 4 de marzo de 1982 y publicada el 31 del mismo mes y año, la cual compelía a los ciudadanos a consignar en un cuestionario, un listado extenso y detallado de datos de su vida personal, imponiendo sanciones económicas para el caso de incumplimiento. Ante esta problemática, fue interpuesto un recurso de amparo constitucional, fundamentado en que dicha Ley vulneraba los preceptos constitucionales del libre desenvolvimiento de la personalidad, dignidad humana y libertad de expresión.

En consecuencia, el citado Tribunal Constitucional Federal, cimento su razonamiento en el derecho a la personalidad que bajo la influencia de la modernidad adquiere una significación particular, inicialmente configurado como el derecho que permite una libertad en el accionar para decidir la realización de determinados actos, da paso a la autodeterminación informativa como la libertad de las personas para determinar quiénes y por qué motivos pueden conocer los datos inherentes a su persona.

En lo posterior, el ya nombrado Tribunal, emitió la Sentencia de 27 de febrero de 2008, emergente de la problemática suscitada ante la reforma de la Ley de los Servicios de Inteligencia del Estado de Renania del Norte – Westfalia, que facultaba el uso secreto de un software espía (troyano) para acceder a los ordenadores de cualquier sospechoso, recabando información para su posterior análisis. En este caso, la Sentencia igualmente esgrimió su fundamento en el desarrollo de la personalidad, configurando a la autodeterminación informativa como un derecho constitucional que solo puede ser restringido en limitados casos, y si bien el Estado puede recabar ciertos datos de los ciudadanos, no puede hacerlo en investigaciones por delitos comunes, ni en la actividad de los servicios de inteligencia, requiriendo en toda ocasión la adopción de las medidas necesarias para la protección del núcleo central de la vida privada, aspecto que también alcanza a los medios tecnológicos que contienen datos personales (Murillo y Piñar, 2009, pp.100-101).

b) España

La Constitución Política Española de 1978, en su Artículo 18 numeral 4, determina: *"*La Ley limitará el uso de la informática para garantizar el honor y la libertad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".* Sobre el particular, Murillo (1990) señala que el citado artículo protege la libertad informática o de manera más precisa, la autodeterminación informativa que emana de la necesidad de las personas de: "(…) preservar

su identidad controlando la revelación y uso de datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática y de los peligros que esto supone" (p.151).

El derecho de autodeterminación informativa, configura en España una esfera de protección más amplia que la del derecho a la intimidad, facultando al individuo a controlar su información personal no necesariamente íntima, pudiendo oponerse a la recolección de datos que no solo afecten a su vida privada; erigiéndose en consecuencia, como un nuevo derecho para hacer frente a los desafíos y riesgos que acarrean la informática y las Tecnologías de Información y Comunicación (Murillo, 2008, p. 47).

En dicho contexto, el 29 de octubre de 1992, fue sancionada la Ley Orgánica N°5/1992 de 29 de octubre de 1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), con el objeto de limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de datos personales para garantizar el honor, la intimidad personal y familiar de las personas físicas. Su ámbito de aplicación, comprende primordialmente los datos que figuren en ficheros automatizados del sector público y privado, así como toda modalidad de uso posterior, incluso no automatizado de datos registrados en soporte físico susceptible de tratamiento automatizado (Artículos 1 y 2 numeral 1).

Posteriormente, la Ley Orgánica N°15/1999 de 13 de diciembre de 1999 de Protección de Datos de Carácter Personal (LOPD), abrogó a la LORTAD y en su generalidad, reiteró las disposiciones de su predecesora y de la Directiva Europea N°95/46 CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, norma comunitaria de protección de datos de la Unión Europea. Esta Ley fue objeto de un recurso de inconstitucionalidad formulado por el Defensor del Pueblo ante el Tribunal Constitucional Español, quien emitió la Sentencia N°292/2000 de 30 de noviembre de 2000, declarando inconstitucionales sus Artículos 21, numeral 1 y 24 numerales 1 y 2, bajo el fundamento de que no pueden existir comunicaciones de datos entre las Administraciones Públicas sin el consentimiento del afectado o cuando no provengan de un mandato legal. Esta Sentencia, le otorga a la autodeterminación informativa, el reconocimiento como un derecho de carácter fundamental autónomo y diferenciado respecto al derecho a la intimidad, manifestando que va más allá de aquella, ya que protege cualquier dato vinculado a la persona y no únicamente la información relacionada con lo íntimo.

Por lo hasta aquí visto, en España la evolución del derecho a la autodeterminación informativa, responde a un cauce normativo constitucional, como secuela de los crecientes avances

tecnológicos experimentados a fines del siglo pasado, particularmente en el campo de la informática, y aunado a ello, la sustancial labor del Tribunal Constitucional en la configuración de su autonomía.

2.1.2.2 Latinoamérica

En Latinoamérica el interés por establecer parámetros legales para la protección de datos personales fue más tardío, no fue sino hasta finales de los años ochenta que empieza a vislumbrarse un nuevo panorama que requería la protección que brinda este nuevo derecho.

Entre los factores para este fenómeno, se identifican la falta de cohesión a nivel regional, el incipiente desarrollo de las Tecnologías de Información y Comunicación, así como el precario acceso a las mismas experimentado durante dicho periodo; sumado a ello, el establecimiento de regímenes totalitarios de gobiernos de facto que favorecieron a un irrisorio o inexistente respeto por los derechos fundamentales (Bauzá, 2006, p.51) y que tuvieron como secuela la consolidación de sistemas democráticos tardíos.

Así la evolución del derecho de autodeterminación informativa, inspirada en normativa de Portugal y España, comenzó por incorporar en los textos constitucionales, el derecho para conocer datos y acceder a información personal cursante en registros públicos, siendo Guatemala en 1985, pionero en añadir este tipo de regulación en su Constitución (Artículo 31) y consecutivamente Nicaragua en 1987 (Artículo 26, numeral 4). Bajo este panorama, un hito trascendental, constituye la introducción de la garantía específica del habeas data en la Constitución Federal del Brasil de 1988 (Artículo 5, numeral LXXII), como instrumento para asegurar a los ciudadanos el efectivo conocimiento y rectificación de información que curse en registros o bancos de datos, a partir de lo cual otros países latinoamericanos incluyeron en sus Constituciones este instituto jurídico, tal es el caso de Colombia en 1991 (Artículo 15), Paraguay en 1992 (Artículo 135), Perú en 1993 (Artículo 2, numerales 5, 6 y 7), Argentina en 1994 (Artículo 43) y Venezuela en 1999 (Artículo 28) (Ojeda, 2015, pp. 67 y 68).

En el caso de Bolivia, se introdujo el hábeas data en la reforma constitucional efectuada mediante Ley N°2631 de 20 de febrero de 2004 (Artículo 23), y fue configurado como un recurso a interponerse ante las Cortes Superiores de Distrito o Jueces de Partido, por toda persona que crea estar indebida o ilegalmente impedida de conocer objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático en archivos o bancos de datos públicos o privados que afecten a los

derechos fundamentales a la intimidad, privacidad personal y familiar, imagen, honra y reputación.

Otro aspecto a enfatizar, lo constituye la primera legislación de protección de datos en el continente emitida por Chile en 1999, mediante Ley N°19.628 de 28 de agosto, sobre Protección a la Vida Privada, sentando así las bases para el desarrollo del derecho a la autodeterminación informativa y protección de datos personales. Un año después, el 30 de octubre de 2000, Argentina emite su Ley N°25.326 de Protección de datos de carácter personal, inspirada en normativa europea.

En Madrid el año 1997, se celebró la Conferencia Euro iberoamericana sobre protección de datos personales a la que concurrieron representantes de países latinoamericanos, en la misma se constató la falta de legislaciones en la materia acordándose el impulso por parte de los gobiernos. En ocasión del II Encuentro Iberoamericano de Protección de Datos, desarrollado del 2 al 6 de junio de 2003, en la ciudad de La Antigua (Guatemala), emerge la denominada Declaración de La Antigua, que proclamó la protección de datos personales como derecho fundamental de las personas, el respeto a la intimidad y la facultad de control y disposición sobre los mismos. A su vez, reconoció la necesidad de impulsar la adopción de medidas que garanticen un elevado nivel de protección de datos, así como la idoneidad de contar con marcos normativos nacionales que consideren los principios de protección de datos personales reconocidos en instrumentos internacionales (Declaración de La Antigua, 2003).

En este encuentro, a efectos de reforzar la colaboración entre los países iberoamericanos, se originó la Red Iberoamericana de Protección de Datos, como organismo, para la difusión de información y tratamiento de problemas, apoyo de iniciativas y desarrollo de una cultura de protección de datos. El mismo año, el 14 y 15 de noviembre, en la ciudad de Santa Cruz (Bolivia), en el marco de la XIII Cumbre Iberoamericana de Jefes de Estado y Gobierno, se suscribió la Declaración de Santa Cruz de la Sierra con la participación de representantes de 21 países, documento que en su punto 45, resaltó la protección de datos personales como derecho fundamental y la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos (Declaración de Santa Cruz de la Sierra, 2003).

Al año siguiente, se suscribió la Declaración de Cartagena de Indias, como resultado del III Encuentro Iberoamericano de Protección de Datos, desarrollado en Colombia, del 25 al 28 de mayo de 2004. Este documento, refleja conclusiones referentes a la protección de datos en el sistema financiero, transferencias internacionales de datos y privacidad en el sector de telecomunicaciones (Declaración de Cartagena, 2004).

A partir de lo anterior, la Red Iberoamericana de Protección de Datos, cuya Secretaria Permanente la ostenta la Agencia Española de Protección de Datos, realiza una labor meritoria impulsando encuentros, seminarios y actividades, consolidándose como un organismo promotor en la materia, llegando a aprobar los Estándares de Protección de Datos Personales para los Estados Iberoamericanos el año 2017, que constituyen un conjunto de directrices para la emisión de iniciativas regulatorias.

Por su parte, la Organización de Estados Americanos (OEA) desde 1996 también ha impulsado el establecimiento de mecanismos de protección respecto a los datos personales, con miras a la conformación de un marco regional, a través de estudios realizados por el Comité Jurídico Interamericano, emitió varios pronunciamientos entre los que destaca la Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas de 2012, documento que constituyó la base de la Guía Legislativa para los Estados Miembros, desglosada en el Informe N°CJI/doc. 474/15 rev.2 de 26 de marzo de 2015, basada en directrices de la Unión Europea (UE), la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Foro de Cooperación Económica Asia- Pacífico (APEC).

Recapitulando lo hasta aquí señalado, el reconocimiento del derecho a la protección de datos personales en Latinoamérica, parte de una base constitucional, con génesis en la institución del habeas data, lo cual viabilizó su desarrollo e inclusión progresiva como derecho autónomo en legislaciones específicas, siendo la tendencia actual su inclusión expresa en los textos constitucionales. Asimismo, no es menos evidente la influencia de la normativa Europea en la región, así como el rol de la Red Iberoamericana de Protección de Datos y de la Organización de Estados Americanos, en impulsar medidas conducentes al afianzamiento de sistemas jurídicos que brinden la debida garantía al citado derecho.

2.1.3 Nociones conceptuales de la protección de datos personales

En este acápite se desarrollan los conceptos y definiciones relacionados con la protección de datos personales, en el afán de posibilitar una mejor comprensión de la problemática de la investigación.

2.1.3.1 Información

Según Gallo Ruiz (citado por Ossio, 2010) la información es:

> (…) todo dato o conjunto de datos que transmiten un conocimiento en un proceso de comunicación entre un emisor y un receptor. La noción sobre la que se basa el concepto de información, dice, es el dato o conjunto de datos, ya que la información de una u otra manera está en el dato que hace perceptible el concepto. (p. 41)

En consecuencia, la información está conformada por una conjunción de datos, que sirven para construir un mensaje, el dato es la fuente primaria y base de la información, desde dicha perspectiva, su aprovechamiento racional constituye el eje del conocimiento.

2.1.3.2 Tecnologías de información y comunicación

Para Ávila (2013), constituyen el:

> (..) conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas. (pp. 222-223)

Las TIC en su conjunto, constituyen herramientas, soportes y canales que recopilan, procesan, almacenan, sintetizan, recuperan, presentan y ofrecen información de variadas formas y en diversas representaciones. Desde su surgimiento han generado notable impacto en la sociedad y al presente, en la Era Digital y del Big Data, han adquirido una connotación aún mayor por su indisoluble relación con la información y la generación de conocimientos.

2.1.3.3 Sociedad de la información

Ossio (2010), define a la Sociedad de la Información como un nuevo modelo de organización industrial, cultural y social caracterizado por el acercamiento de las personas a la información a través de las nuevas tecnologías de la comunicación; a su vez, citando a Castro el mismo autor expresa que se trata de un nuevo orden social derivado de la revolución tecnológica de finales del siglo XX y principios del Siglo XXI (p. 18). Este nuevo estadio, plantea en el ámbito jurídico cuestiones de diversa índole, que a decir de Menéndez y Gayo (2014) “(…) requieren respuestas que no pueden ni deben basarse en los tradicionales y; en muchos casos obsoletos, marcos teóricos y conceptuales hasta ahora vigentes” (p. 265), por lo cual a finales de la década de los 80, han surgido y se han desarrollado algunas disciplinas que pretenden ofrecer nuevos referentes teóricos y metodológicos para analizar y solventar los problemas

surgidos por la interacción del derecho y las nuevas tecnologías. La Sociedad de la Información conforma un nuevo peldaño en el desarrollo evolutivo de la sociedad humana, cuyo génesis radica en la utilización extendida de las TIC en las actividades cotidianas del hombre; a través de dicho uso, se genera más conocimiento y en consecuencia mayor información, en un proceso reiterativo y constante de dimensiones incuantificables. Este fenómeno conlleva beneficios incontables, pero también riesgos reales y potenciales, con la consecuente lesividad a los derechos y libertades del individuo.

2.1.3.4 Informática

Según Carrión (citado por Rincón, 2015, p. 220) la informática: "es la disciplina que estudia el fenómeno de la información y la elaboración, transmisión y utilización de la información principalmente, aunque no necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos". Bajo la citada definición, se colige que es una ciencia orientada al estudio del tratamiento de la información mediante medios automáticos, posibilitando su procesamiento automatizado a través de las TIC.

2.1.3.5 Dato

Conforme al Diccionario de la Lengua Española (Real Academia Española, 2018), la palabra dato procede del latín "datum" y significa: "antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho".

En otra acepción es: "información dispuesta de manera adecuada para su tratamiento por un ordenador". Para Davara (2008), dato es el antecedente o noticia cierta en su origen, como punto de partida para la investigación de la verdad, contenido en un documento o soporte ya sea físico o lógico con calidad de testimonio, diferenciado del concepto de información entendida como la acción de informar o dar noticia de algo (p. 46). El citado autor, expresa que cuando los datos son sometidos a: "(…) un tratamiento o adecuación a un fin, para obtener un resultado elaborado, se convierten en información. La información será el resultado y adecuado a un fin determinado" (Davara, 2008, p. 47). Por su parte Elías (citado por Ossio, 2010), expresa que dato es: "(…) una representación de una porción de la realidad expresada en términos que forman parte de un código preestablecido, de manera que pueda ser interpretado, y que está destinado a dar esa información a un receptor" (pp. 40-41). Así también Suárez (2019), señala que un dato puede ser representado por un número, una letra, un signo ortográfico, un dibujo, un gesto, o cualquier símbolo que represente una cantidad,

medida, palabra, descripción, negación o una afirmación, un señalamiento, un hecho, un valor, una situación, etc. que se percibe con los sentidos.

2.1.3.6 Dato personal

Un dato personal es cualquier información ya sea numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otra categoría concerniente a personas físicas identificadas o identificables y que posibilita revelar información sobre la misma. Bajo estos parámetros, persona identificada: "(…) es aquella cuya identidad está determinada; persona identificable, es quien cuya identidad puede determinarse ya sea directamente o indirectamente, mediante cualquier información, referida a su identidad física, fisiológica, psíquica, económica, cultural o social" (Miguel, 2016, p. 77). Gallo Ruiz (citado por Ossio, 2010) postula la siguiente definición: "(…) aquellos datos inherentes de una persona determinada, es decir cualquier dato que permita conocer las características personales, en el sentido más amplio, de alguien." (p. 44.)

Consiguientemente un dato personal es un distintivo de diversa índole y naturaleza que identifica a un individuo directa o indirectamente y que posibilita el conocimiento de las características que le otorgan singularidad.

2.1.3.7 Clasificación de los datos personales

Existen diversas clasificaciones respecto a los datos personales; no obstante, el presente estudio, de acuerdo a sus objetivos se adscribe a la sistematización atendiendo a la confidencialidad de los datos realizada por Davara (2008), esta categorización comprende:

a) **Datos privados**

Son aquellos que tienen reguladas y tasadas las situaciones o circunstancias en que la persona se ve obligada a proporcionarlos o ponerlos en conocimiento de terceros, siendo la conciencia social favorable a impedir su difusión y respetar la voluntad de secreto sobre ellos de su titular, por ejemplo: historias crediticias, datos financieros o laborales. Se subdividen en íntimos, secretos y profundos. Los **íntimos**, son aquellos datos cuya difusión el individuo protege frente a cualquiera, pero que, de acuerdo con un fin determinado, está obligado por mandato legal a proporcionar periódica o regularmente, en cumplimiento de sus obligaciones cívicas, como los datos tributarios, de seguridad social, datos sobre infracciones administrativas o penales y cualquier otro dato que referencie el estilo de vida de la persona.

Por su parte, los datos **secretos,** son los que no están obligados a ser proporcionados a nadie, salvo en casos excepcionales, expresamente tasados y regulados en las leyes, la doctrina los ha denominado también como datos sensibles. Estos a su vez pueden ser profundos y reservados, que constituyen aquellos que, bajo ningún concepto, está obligado el titular a darlos a conocer a terceros, si no es así su voluntad.

- **Datos sensibles**

Los datos sensibles por su complejidad e incidencia en el ámbito privado de las personas, poseen una mayor potencialidad discriminatoria, por tanto, son objeto de un régimen peculiar.

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, emitidos por la Red Iberoamericana de Protección de Datos el año 2017, en su numeral 2.1 inciso d) concordante con el Artículo 9, numeral 1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos - RGPD), agrupan en esta índole de datos a aquellos que revelan: ideología, afiliación sindical, religión y creencias, origen racial, salud, vida y orientación sexual, datos genéticos y biométricos; que sólo se permite sean recabados cuando, por razones de interés general, así lo disponga una Ley o el afectado lo consienta expresamente.

Denominados también especialmente protegidos, su sensibilidad se determina en torno al daño que puede causar a una persona la revelación de esta información (Miguel, 2016, p. 121). Así en los hechos, no tiene parangón la revelación del número telefónico de una persona, con la publicidad de su historial médico, máxime si el individuo padece de una patología que podría dar lugar a su exclusión social.

- **Ideología**

El Diccionario de la Lengua Española, le asigna a la ideología la acepción de: “conjunto de ideas fundamentales que caracteriza el pensamiento de una persona, colectividad o época, de un movimiento cultural, religioso o político, etc.” (Real Academia Española, 2018). Así también, para Baechler (1978) la ideología: “(…) es el conjunto de representaciones que acompañan a las acciones que, en una sociedad determinada, tiende a la conquista o a la conservación del poder” (p.24). La ideología, tiene su núcleo en las ideas fundamentales del individuo, afirmaciones y creencias que develan su punto de vista y postura adoptada en

diversas facetas de su vida, ya sea de naturaleza política, de género, social u otra, vinculadas a la intimidad de la persona y que en consecuencia la caracterizan.

- **Afiliación sindical**

En el ámbito del derecho laboral, es la incorporación de trabajadores remunerados a un sindicato, que entre otros, le otorga la capacidad de negociar las condiciones laborales frente a su empleador o empresa. Su salvaguarda como dato protegido se encuentra relacionada con el ejercicio de la libertad sindical, considerada como: "(…) un conjunto de poderes individuales y colectivos que aseguran la independencia de sus respectivos titulares en orden a la fundación, organización, administración y gobierno y actividad externa (actividad sindical) de las asociaciones profesionales de trabajadores" (Recalde, 2015, p. 104). Los empleadores no deben acopiar datos personales sobre la afiliación a una organización de trabajadores o sobre sus actividades sindicales, salvo si la legislación o los convenios colectivos así lo estipulan o autorizan (Oficina Internacional del Trabajo, 1997, p.3), en consideración de que el tratamiento de dichos datos entraña riesgos importantes para los derechos y libertades de los trabajadores, por ello es sustancial recalcar que estos datos deben ser tratados para la finalidad que ameritó su otorgamiento y bajo el consentimiento de su titular.

- **Religión y creencias**

Para Del Picó (2018), la religión se puede definir como: "(…) un complejo espiritual completo, constituido por un sistema de creencias, ritos, formas de organización y normas éticas, por medio de los cuales los miembros de una sociedad o comunidad se vinculan al ser divino o sobrehumano, procurando encontrar un sentido último y trascendente a la existencia" (p. 45).

Son datos relativos al conjunto de dogmas y convicciones religiosas profesados por un individuo. Comprenden también las creencias religiosas o políticas sin necesidad de que el individuo profese una determinada religión o esté afiliado a un partido. Este elenco de datos por su naturaleza intrínseca a la esfera más íntima del ser humano también amerita una protección especial, dado su potencial discriminatorio.

- **Origen racial o étnico**

Son datos relativos a la pertenencia del individuo a una raza o etnia. La acepción raza se refiere a las características físicas, como la estructura ósea o el color de ojos y pelo.

La etnia; por su parte, hace referencia a factores culturales como la nacionalidad y el lenguaje (Martínez, 2015, p.70). Según refieren Torres-Parodi y Bolis (2007, p. 414) si bien se reconoció que la humanidad es una unidad indivisible, tiempo después se aceptó la existencia de identidades diversas, y que las diferencias entre los seres humanos son producto de formas de vida, creencias y cosmovisiones que dan lugar a comportamientos diversos y se manifiestan en maneras de vestir, lenguajes, rituales, terapias, alimentación y formas de organización social diferentes. Como resultado de esta evolución, se reconoce dentro del conglomerado de grupos étnicos/raciales no solo a los pueblos indígenas, sino a otros grupos como los afrodescendientes, los migrantes, los pueblos rom, los desplazados y los refugiados, que tienen acervos culturales propios.

Por lo señalado, el uso de los términos origen racial o étnico, no involucran la aceptación de teorías que traten de determinar la existencia de razas humanas separadas, sino que desde la perspectiva de la protección de datos personales, se da preeminencia a la salvaguarda de este tipo de información, ya que su recolección y tratamiento puede dar lugar a un grave menoscabo de derechos de sus titulares.

- **Salud**

Para Medinaceli (2017), siguiendo un concepto amplio y expansivo, los datos relativos a la salud son todos aquellos relacionados con:

> (…) el cuerpo humano, como la sexualidad, la raza, el código genético, los antecedentes familiares, los hábitos de vida, de alimentación y consumo; los datos antropométricos como peso, talla y edad; las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; las informaciones relativas al abuso de alcohol o al consumo de drogas; los datos meramente administrativos de los centros sanitarios; y los aspectos económicos relacionados con la prestación de la asistencia sanitaria. En definitiva lo que se pretende es abarcar todos los datos que de alguna forma se refieran a la salud tanto de individuos con buena salud, enfermos o fallecidos. (pp. 178-179)

En consecuencia, estos datos involucran información concerniente a la salud de un individuo, tanto física como psicológica, ya sea del pasado, presente e incluso previsible al futuro y que no únicamente comprende enfermedades, dolencias o padecimientos, sino aquella información que indique un buen estado de salud. Cursan en la historia clínica de los pacientes, en los archivos o bases de datos físicos o automatizados de establecimientos sanitarios públicos y privados. A su vez, la historia clínica está sometida a las limitaciones en cuanto al acceso, comunicación y cesión de los datos (Pinedo, 2013). Por consiguiente, el

tratamiento de los datos de salud de los individuos, para ser integrados en el historial clínico, no implica un procesamiento que se pueda llevar a cabo libremente; sino bajo los parámetros de confidencialidad, proporcionalidad y finalidad.

- **Vida y orientación sexual**

Constituyen datos relativos a las costumbres y orientación sexual de un individuo. No tiene dicha consideración el dato de indicación del sexo en cuanto a género (femenino o masculino), al que corresponde un nivel básico de seguridad, pero sí la condición de preferencias sexuales, como por ejemplo la homosexualidad, así también los hábitos de la vida sexual. La importancia de asignar una especial protección a este tipo de datos obedece a que su acceso y difusión puede afectar a la persona en el ejercicio de otros derechos fundamentales como la intimidad personal y familiar, la dignidad y el libre desarrollo de la personalidad (Tejero, 2010, p. 616).

- **Datos genéticos**

El Reglamento General de Protección de Datos, en su Artículo 4, numeral 13, define los datos genéticos como aquellos: "(…) relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona". En el proceso de recolección y tratamiento de este tipo de datos, debe observarse el respeto a la dignidad humana, la privacidad y otros derechos fundamentales, bajo la adopción de medidas de confidencialidad, puesto que están asociados a una persona identificada o identificable.

Un manejo inapropiado de este tipo de información puede converger en la estigmatización de un individuo, familia, un grupo o una comunidad.

- **Datos biométricos**

De acuerdo al Artículo 4 numeral 14, del Reglamento General de Protección de Datos, los datos biométricos son obtenidos: "(…) a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos". Entre estos datos se encuentran los datos estáticos como: la huella digital, el iris, reconocimiento facial, geometría y líneas de la mano, reconocimiento palmar, patrón de venas, termogramas faciales y composición química del olor corporal. Así también los

dinámicos, como: la voz, dinámica del teclado, escritura manuscrita y reconocimiento de firma escrita, gestos y movimientos corporales.

La utilización de sistemas biométricos brinda grandes ventajas en procesos automatizados, por ejemplo: el reconocimiento de huellas dactilares en investigaciones policiales al permitir la identificación certera de un individuo; y es que en la Era Digital es cada vez más común autenticarse con estos sistemas, cuya tecnología se utiliza cotidianamente para desbloquear un smartphone, en el registro para los comicios subnacionales o nacionales, al consignar la llegada y salida del trabajo o en operaciones bancarias; entre otros, con repercusiones jurídicas en el ámbito de la privacidad y la seguridad digital, por el hecho de que utilizada esta información de manera inapropiada, genera el menoscabo de derechos fundamentales y puede desencadenar en ilícitos. En síntesis, los datos personales sensibles cobran una especial significación y son objeto de una protección reforzada en relación con los datos personales comunes u ordinarios, en atención a que no sólo forman parte de la esfera más íntima de la persona, sino que adquieren basamento en la dignidad del ser humano y contribuyen al desarrollo de su identidad.

b) Datos públicos

Son conocidos por un número cuantioso de personas, sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato, ni por la calidad del dato pueda impedir que, una vez conocido, sea libremente difundido dentro de unos límites de respeto y de convivencia cívicos (Davara, 2008, p. 53), entre estos se encuentran el nombre, el estado civil, la ocupación y la profesión. Por su naturaleza, pueden estar contenidos, en registros públicos, documentos públicos, gacetas y boletines oficiales o en diversas fuentes de acceso público para fines específicamente determinados, usualmente de consulta; sin embargo, si bien es cierto que es un dato de amplia circulación, ello no significa que sean utilizados para fines distintos de los que ameritaron su recolección o uso inicial.

2.1.3.8 Titular de los datos personales

El titular de los datos personales es el individuo a quien se refieren dichos datos, es quien detenta la propiedad sobre los mismos y tiene la potestad para decidir qué entidades los tratan y con qué fines, así como su confidencialidad (Miguel, 2016, p. 23).

2.1.3.9 Base de datos

Es un conjunto organizado de datos de carácter personal, que permite el acceso con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de creación, almacenamiento, organización y acceso (Miguel, 2016, p.81). Por consiguiente, los datos pueden encontrarse contenidos en soporte informático o en soportes tradicionales como el papel, es decir pueden ser: automatizados (base de datos, hoja de cálculo, documento de texto, la grabación de cámaras de videovigilancia), no automatizados (listado en papel de clientes, proveedores, etc., nóminas, curriculum vitae) e incluso mixtos (facturas, presupuestos y nóminas).

2.1.3.10 Tratamiento de datos personales

Miguel (2016), define el tratamiento de datos personales como: "(…) cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resultaren de comunicaciones, consultas, interconexiones y transferencias." (p. 91). Es decir, el tratamiento de datos involucra una variedad o conjunto de operaciones, en relación a los datos personales, no necesariamente automatizados, que van desde la recolección inicial y pueden atravesar por varias fases, hasta su eliminación.

a) Protección especial

Los datos sensibles ameritan una protección especial en lo concerniente a su tratamiento, para recabar datos relativos a la ideología, afiliación sindical, religión o creencias debe obtenerse el consentimiento expreso y por escrito, informándole al titular de su derecho a no prestarlo (Miguel, 2016, p. 80). Se exceptúan de este aspecto las bases de datos administradas por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos de sus asociados o miembros. No obstante, la cesión precisará siempre del consentimiento del titular del dato.

Respecto a los datos personales referentes a la salud, origen racial, vida y orientación sexual, estos solo pueden ser recolectados, tratados y cedidos cuando el interesado lo conscienta expresamente o cuando por razones de interés general lo disponga la Ley (Miguel, 2016, p. 80). Unicamente como excepción, no será necesario el consentimiento al tratarse de

prevención o diagnóstico médico, prestación de asistencia sanitaria o tratamientos médicos, gestión de servicios sanitarios, para salvaguardar el interés vital del titular o de otra persona y siempre que se realice por un profesional medico sujeto a secreto profesional, o personas sujetas a obligaciones equivalentes al secreto.

En concordancia, el numeral 9.1. de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, determina que por regla general, no podrá efectuarse el tratamiento de datos personales sensibles, salvo la concurrencia de cualquiera de las siguientes causales:

> a. Cuando sea estrictamente necesario para el ejercicio y cumplimiento de las atribuciones y obligaciones expresamente previstas en las normas que regulan la actuación del responsable del tratamiento.
> b. En cumplimiento de un mandato legal.
> c. Cuando se cuente con el consentimiento expreso y por escrito del titular.
> d. Por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros.

Las medidas aplicables a los datos de esta naturaleza tienen su asidero en la influencia que para la intimidad adquieren los mismos, ya que la información que reflejan utilizada inadecuadamente además de lesionar el derecho a la autodeterminación informativa, genera afectación a otros derechos fundamentales.

b) Encargado del tratamiento

Es la entidad que trata datos personales por cuenta del responsable de la base de datos, brindando un servicio a éste, para lo cual necesita acceder a los datos de carácter personal (Miguel, 2016, p. 95). Constituye la persona física o jurídica que materialmente efectúa las operaciones con los datos personales, un tercero externo a quien el responsable delega el tratamiento, ya sea a través de una relación contractual, convenio u otro instrumento jurídico análogo.

c) Responsable del tratamiento

Para Miguel (2016), es: “(…) la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realice materialmente” (p.81), es quien resuelve o define

sobre el tratamiento de los datos; determina las razones del tratamiento, el por qué y cómo, en otras palabras, dispone qué procedimientos se van a efectuar con los datos personales, si se conservarán, serán cedidos o eliminados.

2.1.4 Definición y objeto del derecho a la protección de datos personales o autodeterminación informativa

Balaguer (2016), define el derecho a la protección de datos como: "(…) el derecho de los ciudadanos frente a terceros de una utilización indebida de sus datos personales (…) es el derecho al flujo de información que concierne a cada persona (…)" (p. 188), la citada autora asiente que esta prerrogativa engloba todos los datos de la persona, que no pueden ser empleados con fines distintos para los que fueron obtenidos, por lo cual impone a terceros el deber de abstenerse de utilizarlos o difundirlos.

Este derecho, guarda una relación con la intimidad y la vida privada de las personas, no obstante, es más amplio, puesto que: "(…) no se refiere solamente a la protección de los datos íntimos de las personas, sino en principio a cualquier tipo de dato de cuya difusión quiera ser salvaguardada la persona" (Balaguer, 2016, p. 193).

Conforme señala Murillo (citado por Cerda, 2003, p.54), el derecho a la autodeterminación informativa, si bien se erige sobre la base del derecho a la intimidad, empero no se ciñe únicamente al amparo de la persona, frente al tratamiento de datos personales de naturaleza privada, si no que abarca una protección más amplia que alcanza todo tipo de dato. Por su parte, Serrano (2003), lo define como: "(…) el derecho del individuo a controlar la obtención, tenencia, tratamiento, y transmisión de datos relativos a su persona, decidiendo en cuanto a los mismos, las condiciones en que dichas operaciones pueden llevarse a cabo" (p. 67).

El objeto del derecho analizado no se reduce exclusivamente a la protección de datos íntimos, puesto que además comprende a datos públicos, ya que áun siendo estos accesibles a cualquiera, no escapan al poder de disposición del afectado (Garriga, 2004, p. 36). En consecuencia, a la luz de las posturas analizadas, el derecho humano y fundamental de autodeterminación informativa o derecho a la protección de datos personales, permite al individuo decidir el destino de sus datos de carácter personal en general, ejerciendo un control sobre los mismos, no solo los íntimos o privados, sino datos de cualquier naturaleza, y en las diversas fases del procesamiento que van desde su recolección, tratamiento, cesión, hasta su eliminación, evitando que sean utilizados para finalidades distintas a las que motivaron su otorgamiento.

2.1.4.1 Principios para el tratamiento de datos personales

El derecho a la protección de datos personales, tiene su cimiento en principios que a modo de declaraciones programáticas lo inspiran, sustentan y caracterizan como disciplina autónoma, entre éstos se destacan los siguientes:

a) Licitud: los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, en su numeral 14, refieren que el tratamiento de datos personales, observará el estricto apego a la normativa aplicable establecida en el derecho interno, el derecho internacional, y los derechos y libertades de las personas. Los datos de carácter personal, no deben ser recogidos y procesados por medios desleales o ilegales, y su tratamiento debe ceñirse a las disposiciones normativas vigentes.

b) Información: los interesados a los que se soliciten datos personales deberán ser informados de modo previo, expreso, preciso e inequívoco de:

- La existencia de una base de datos a la cual se van a incorporar los datos, o el tratamiento de los datos suministrados.
- La identidad y dirección del responsable de la base de datos o del tratamiento, o en su caso de su representante.
- Cuál es la finalidad de los datos recogidos.
- Los destinatarios de la información.
- El carácter obligatorio o voluntario de aportar los datos solicitados.
- Las consecuencias de la obtención de los datos o de la negativa a proporcionarlos.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. (Miguel, 2016, p. 108)

c) Consentimiento: se encuentra estrechamente vinculado con el principio de información, puesto que solo luego de haber sido informado el interesado de los detalles del tratamiento de sus datos personales, podrá decidir si otorga o no su consentimiento, el cual debe ser libre, específico, informado e inequívoco y de carácter expreso o tácito (Miguel, 2016, p. 113). El consentimiento debe ser previo e informado, siendo el titular de los datos, el único que puede autorizar su tratamiento encontrándose entre sus facultades incluso revocarlo, por tanto, se erige como la piedra angular a partir de la cual se construye el sistema de protección de datos personales.

Existen excepciones al consentimiento en los casos en que se recojan datos personales para el ejercicio de la administración pública en el ámbito de sus competencias, en el marco de relaciones contractuales, laborales o administrativas y cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado; asimismo, si los datos figuran en fuentes accesibles al público y su tratamiento es necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o de un tercero a quien se comuniquen los datos, siempre que con ello no se vulneren los derechos y libertades fundamentales del interesado.

d) Calidad: establece los límites que tiene una organización para el tratamiento de datos de carácter personal en su recogida, uso, actualización, almacenamiento y cancelación (Miguel, 2016, p. 104). Los datos recogidos deben ser adecuados y pertinentes en relación con el ámbito y finalidad para la que fueron recolectados. Este principio comprende:

- El principio de exactitud, que involucra que los datos deben ser precisos y actualizados.
- El principio de finalidad, por el cual los datos deben ser tratados para los fines que fueron obtenidos.
- El principio de lealtad, que implica que los datos personales solo podrán ser recogidos por medios legales sin que sea posible emplear medios o procedimientos fraudulentos o ilícitos. (Menéndez y Gayo, 2014, p. 285)

e) Responsabilidad: los responsables del tratamiento de datos personales deben adoptar las medidas adecuadas para el correcto tratamiento de los datos personales, aspecto que incluye dotarse de mecanismos específicos que evidencien lo anterior, pudiendo recurrir a: “(…) estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines” (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numeral 20.1).

f) Seguridad: los datos personales se encuentran expuestos a riesgos provenientes tanto de la acción humana como de circunstancias naturales o accidentes fortuitos, por lo cual se hace necesaria la incorporación de medidas de índole administrativo, físico y técnico que garanticen la confidencialidad, integridad y disponibilidad de los datos personales; asimismo, la mejora continua de las medidas de seguridad.

Los daños, perdidas, alteraciones, destrucción, acceso y todo uso ilícito no autorizado de los datos personales, aun de manera accidental, debe notificarse al titular de los datos (Miguel, 2016, p 124).

g) Comunicación: en los casos de cesión de datos personales a terceros, es necesaria la autorización o consentimiento del titular. Solo si la transferencia opera en virtud de un mandato legal no será exigible el mismo. Asimismo, el tercero a quien se comuniquen los datos debe cumplir las mismas obligaciones que el cedente y las disposiciones legales aplicables (Menéndez y Gayo, 2014, p. 288).

2.1.4.2 Derechos que engloba la autodeterminación informativa

La autodeterminación informativa encierra en su núcleo otros derechos, cuyo ejercicio permite al individuo un control de sus datos personales y el poder de disposición sobre los mismos, son de carácter personalísimo y conferidos exclusivamente al titular del dato. Inicialmente fueron reconocidos como tales los derechos de Acceso, Rectificación, Cancelación y Oposición bajo la denominación del acrónimo ARCO; sin embargo, con el devenir del tiempo, como secuela de la evolución tecnológica y las necesidades que de ella emergen, fueron sumándose al elenco, los derechos de indemnización, portabilidad y olvido.

a) Acceso: es la facultad para solicitar y obtener gratuitamente información de los datos de carácter personal sometidos a tratamiento, su origen, así como las comunicaciones realizadas o que se prevén hacer de los mismos (Menéndez y Gayo, 2014, p. 293). En otras palabras, es el derecho que tiene el titular de los datos de acceder a su propia información, cursante en una base de datos ya sea en archivos tradicionales (papel) o en archivos digitales; así también, a la forma en que fueron recopilados los datos, las razones que motivaron el acopio y a recibir el aviso de privacidad al que está sujeto el tratamiento.

b) Rectificación: es el derecho que le asiste al titular para poder realizar alguna modificación en los datos cuando éstos sean inexactos, incompletos (Menéndez y Gayo, 2014, p. 293) o incluso falsos, no significa borrar o destruir físicamente la información, sino la sustitución de datos por otros actuales y correctos. En definitiva, a través de la corrección se garantiza que el dato sea fidedigno.

c) Cancelación: es la facultad del titular de los datos para que éstos sean dados de baja de la base de datos, ya sea en parte o de manera completa, es decir la supresión de los mismos.

La cancelación no es procedente cuando los datos deban ser conservados por mandato legal o de conformidad a las relaciones contractuales establecidas entre el responsable del tratamiento y el interesado (Menéndez y Gayo, 2014, p. 293).

d) Oposición: esta prerrogativa, le asiste al individuo para objetar el tratamiento de sus datos personales “si fueron obtenidos fraudulentamente o sin su consentimiento” (Ibarra, 2013, p. 128), o cuando medien motivos legítimos y fundados, relacionados a situaciones concretas y siempre que la ley no disponga lo contrario.

e) Indemnización: el titular que ha sufrido daños o perjuicios en sus bienes o derechos, como resultado del tratamiento de sus datos personales, tiene derecho a una indemnización (Miguel, 2016, p. 40). Los daños y perjuicios se traducen en afectación tanto moral como patrimonial, originan una responsabilidad civil de las personas o instituciones que generaron el detrimento, siendo viable la petición de indemnización ante las autoridades competentes.

f) Portabilidad de datos: es el derecho del individuo a recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, para que pueden ser transferidos de un responsable del tratamiento a otro, ya sea por intervención del propio interesado o solicitando al responsable que efectúe la transferencia. En dicho sentido, Villarino (2018, p. 119), reconoce una doble vertiente del derecho: la obtención de la copia de los datos y la transferencia de los mismos de un sistema de tratamiento electrónico a otro. Como ejemplo, en virtud del Decreto Supremo N° 3404 de 29 de noviembre de 2017, en Bolivia es posible la portabilidad numérica que permite al usuario conservar su número telefónico cuando opta por cambiar de compañía de servicios de telefonía móvil, disposición vigente a partir del 1 de octubre de 2018.

g) Olvido: encierra la facultad del titular de borrar, bloquear o suprimir información personal que se considera obsoleta por el transcurso del tiempo o porque afecta al libre desarrollo de alguno de sus derechos fundamentales (Miguel, 2016, p.65). Es un derecho: “(…) ligado al arrepentimiento y a borrar de la memoria colectiva digital ciertos datos personales y está ligado al autocontrol de los propios datos personales” (Alvarez, 2015, p. 67). Conocido también como el derecho de cancelación de datos personales en Internet, su campo de acción lo constituye exclusivamente el entorno online, a saber, los diversos motores de búsqueda existentes. Un caso paradigmático y simbólico es el de Google vs. España, dentro del cual el Tribunal de Justicia de la Unión Europea emitió la Sentencia de 13 de mayo de 2014, obligando a Google

Inc. y Google España a cumplir con las normas de protección de datos[7], disponiendo la eliminación en el buscador Google de enlaces conducentes a páginas en las cuales figuraba información personal desactualizada del ciudadano español Mario Costeja.

2.1.5 Importancia de la información y los datos personales

Respecto a la importancia de los datos de carácter personal, Ibarra (2013), sostiene que esta radica en : "(…) el valor de la información dentro de la sociedad globalizada en la que casi todo se está volviendo un proceso automatizado; el plus de las actividades es el conocimiento completo y exacto sobre las cosas o las personas" (p.103). En concordancia, Téllez (2009) expresa que la información es un: "(…) bien susceptible de apoderamiento con un innegable valor patrimonial o contenido económico inherente o intrínseco, que radica en su destino y utilidad" (p. 69).

Sagües (citado en Ossio, 2010, p.35), afirma que con el auge de los sistemas computarizados, se genera un poder informático de dimensiones insospechadas, que puede ser económico, ya que la información se compra y se vende, viajando de un lugar a otro sin que el interesado lo sepa; o puede ser también político ya que conocer minuciosamente la vida de los demás permite regular, controlar y vigilar su comportamiento. Para Davara (2008), la información es un bien que no se agota con su consumo, que se enriquece con el uso, y ello permite su expansión, atribuyendo este fenómeno en gran medida, al desarrollo alcanzado en los sistemas de telecomunicación, que permiten que una misma información sea accesible a un número mayor de usuarios (p. 25). Palazzi (citado en Martínez, 2013), le da a los datos

[7] En 1997 el ciudadano español Mario Costeja incurrió en deudas relacionadas con la seguridad social, en consecuencia, el Ministerio de Trabajo y Asuntos Sociales de España ordenó el embargo de sus bienes, publicando su remate en el periódico: La Vanguardia. A raíz de ello, cuando un usuario introducía el nombre de Costeja en el motor de búsqueda de Google obtenía como resultado vínculos hacia dos páginas del periódico La Vanguardia en las que cursaba el anuncio de la subasta, figurando Costeja como deudor y con el estado civil de casado; no obstante de haber saldado la deuda y haberse divorciado. En el año 2010, Costeja presentó un reclamo ante la Agencia Española de Protección de Datos (AEPD) en contra del periódico La Vanguardia, Google Inc., y Google España, solicitando que el citado medio de prensa elimine o modifique la publicación, o que se utilicen las herramientas facilitadas por los motores de búsqueda para proteger dichos datos; asimismo, pidió exigir a Google España o Google Inc. la eliminación u ocultamiento de sus datos personales, argumentando que el embargo había concluido hace años y carecía de relevancia actual. La AEPD desestimó el reclamo en contra del periódico La Vanguardia, pues consideró que la publicación tenía una justificación legal al haber sido ordenada por el Estado; empero, aceptó el reclamo en contra de Google al considerar que los motores de búsqueda son responsables del tratamiento de datos personales y están sometidos a la normativa en materia de protección de datos, particularmente a la entonces vigente Directiva N°95/46/CE. Google España y Google Inc. apelaron la decisión ante la Audiencia Nacional, la cual a su vez suspendió el procedimiento y pidió una interpretación del Tribunal de Justicia de la Unión Europea acerca de los Artículos 2 incisos b) y d); 4 apartado 1 incisos a) y c); 12 inciso b), y 14 párrafo primero inciso a), de la Directiva N°95/46/CE y del Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea. La citada Corte, falló determinando que de acuerdo al Artículo 2 incisos b) y d) de la citada Directiva, las actividades que realizan los motores de búsqueda constituyen tratamiento de datos personales, y por lo tanto son responsables del mismo; y que los derechos que otorga la ya nombrada Directiva en sus Artículos 12 inciso b) y 14 párrafo primero inciso a) para solicitar la supresión y bloqueo de datos personales, así como la oposición para el tratamiento de esos datos, incluye el derecho a que el interesado pueda impedir a los buscadores de Internet la indexación de la información referida a su persona publicada en páginas web de terceros.

personales una connotación de mercancía con un valor especial, manifestando que los titulares de los mismos, suelen desconocer que estos son objeto de intercambio (p. 159).

Por su parte, Arocena (2012), señala que la información ha adquirido un altísimo valor económico, llegando a constituir: “un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etcétera) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales” (p. 851).

En la Sociedad de la Información, los datos personales de los individuos son más vulnerables, siendo accesibles y encontrándose a disposición de personas naturales, empresas privadas y entidades estatales. La administración pública recopila datos de los ciudadanos para el cumplimiento de sus fines específicos y en la esfera privada, las empresas solicitan diversos datos personales, tal como acontece en las instituciones bancarias, operadores de telefonía y entes que se dedican al comercio o negocios. Los sitios en Internet como Google, aplicaciones y redes sociales[8] como Facebook, Twitter, Instagram, WhatsApp y numerosas páginas web, para hacer efectiva la suscripción a las mismas, solicitan datos personales básicos como el nombre y apellidos, número de teléfono, e-mail, país de residencia y dirección; entre otros, y a su vez piden el acceso a otros datos personales como la ubicación, contactos y fotografías.

En muchos casos, estos sitios contienen cookies que se instalan en los navegadores de los usuarios con la finalidad de hacer un seguimiento online, las cuales pueden ser activadas remotamente y acceder a fotografías, videos y otros datos personales. Los datos recopilados, develan preferencias, patrones de comportamiento comercial y social, y son aprovechados para fines mercantiles; empero, también son empleados para fines delictivos ya que reflejan transacciones financieras, condición económica y relaciones interpersonales. Los individuos a través de las TIC comparten con asidua frecuencia su información personal y también la de terceros, de quienes usualmente no se recaba su consentimiento o autorización. A su vez, en el marco de operaciones financieras y comerciales se comparte una incuantificable cantidad de datos personales, dejando un rastro y huella digital de improbable borrado.

De acuerdo a lo expuesto y a las posturas asumidas al unísono por los citados autores, no cabe duda de la trascendencia que en la actualidad han cobrado la información y los datos personales, máxime si se considera que estos últimos son componentes e insumos de la

[8] Las redes sociales son servicios que se prestan a través de internet y que posibilitan a los usuarios crear un perfil púbico, donde plasman datos personales e información, contando con herramientas que permiten interactuar con el resto de usuarios.

primera y hacen posible su existencia, ostentando un innegable valor que trasciende a la esfera económica, pero que además coloca en una situación de vulnerabilidad y riesgo a los individuos, ya que pueden ser utilizados para fines distintos, ocasionando daños y perjuicios por su acceso y/o utilización no autorizada, menoscabando la esfera más íntima de sus titulares, por ejemplo si se trata de datos catalogados como sensibles.

Delitos como el robo o suplantación de identidad, estafas informáticas, secuestros, acoso, grooming, sexting, abuso sexual y pornografía, son consumados a través del uso de datos personales. En consecuencia, en plena Era Digital, la protección de datos es una prioridad para el Estado, ya que su vulneración lleva aparejada la transgresión de otros derechos fundamentales, y como corolario: "(…) el menoscabo de la dignidad humana que puede provocar una erosión que afecta un elemento vital en la persistencia de la sociedad: la confianza" (Ibarra, 2013, 90).

2.2 Delitos informáticos que atentan contra la información y los datos

2.2.1 Posturas sobre la existencia de los delitos informáticos

Existen posiciones duales respecto a la existencia como tal de los delitos informáticos, mientras que para unos autores constituyen únicamente las tradicionales figuras delictivas cometidas a través de medios informáticos atentando contra los clásicos bienes jurídicos; para otros, conforman auténticos ilícitos que por sus singulares características ameritan una regulación específica. Dentro de la primera corriente, Nava Garcés (citado en Martínez, 2013, p.153), dilucida que este tipo de delito no lo es per se, pues el carácter esencial para el derecho penal es la conducta, y en la mayoría de los denominados delitos informáticos, no se está frente a conductas típicas distintas en esencia. Así las cosas, las herramientas informáticas y el procesamiento de datos son un factor criminógeno para la comisión de estos delitos.

De similar modo, Martínez (2013), infiere que la lesión o puesta en peligro de un bien jurídico es independiente del medio con que se cometa, ilustrando al efecto que en todos los casos un homicidio atentará contra la vida, sea que se utilice veneno, una pistola o una navaja, mientras en el caso de los delitos informáticos: "(…) no existe coincidencia en una conducta desplegada bajo una misma estructura" y que: "(…) en la mayoría de los casos no se trata de delitos cuya única forma de ejecución sea a través de este medio comisivo. Un fraude puede llevarse a cabo sin necesidad de un ordenador, lo mismo que un atentado contra la intimidad" (p. 153).

Autores como Davara (2008) y Téllez (2009), aunque afirman que no es fácil conceptualizar estos ilícitos, reconocen el impacto de las TIC en su comisión y la necesidad de utilizar la expresión: “delitos informáticos” englobando a esta nueva especie de criminalidad en la que se emplea la informática[9] o telemática[10] como instrumento o como fin en sí mismo. Es menester traer a colación que actualmente no solo se habla de informática para referirse a la utilización de herramientas tecnológicas, sino de sistemas de información o Tecnologías de Información y Comunicación (Davara, 2008, p.23), siendo tal su incidencia en diversos ámbitos que incluso ha operado la incorporación de una nueva rama a las ciencias jurídicas denominada: Derecho de las Tecnologías de la Información y Comunicación[11].

Romeo Casabona (citado en Acurio, 2017) debate sobre la estructuración de un nuevo bien jurídico denominado la información, el cual comporta un valor, ya sea económico, de empresa o ideal, que es relevante y digno de tutela jurídico penal; pero además señala que la locución “delito informático” tiene la ventaja de su plasticidad, al relacionarlo con la tecnología sobre o través de la que actúa, ya que en puridad no puede hablarse de un delito informático especifico, sino de una pluralidad, encontrándose como nota común su vinculación a los computadores, en los cuales ni el bien jurídico agredido ni la forma de comisión es siempre el mismo (p.52).

En particular, el estudio considera que en plena Era Digital es innegable la existencia de los delitos informáticos, ya sea que, en efecto algunos se encuadren en tipos penales tradicionales; o que producto de las TIC hayan emergido nuevas formas delictivas que configuran nuevas posibilidades de delinquir, entonces ya no solo se está frente a la informática como medio sino como objeto y/o finalidad del ilícito. Adicionalmente, señalar que, con el advenimiento de la Sociedad de la Información, los procesos sociales han experimentado cambios y el Derecho Penal también debe ajustarse a estos avances para brindar una tutela efectiva de los derechos y libertades de los individuos.

2.2.2 Delito informático

Pérez Luño (1996), lo define como: “aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan el funcionamiento de los sistemas informáticos” (p.70). Por su parte, Davara (2008) señala: “la realización de una acción que,

[9] Davara, define a la informática como la ciencia del tratamiento automático de la información.
[10] Según Davara, la telemática es considerada como una simbiosis entre la informática y las comunicaciones, y hace referencia al diálogo a distancia de equipos informáticos.
[11] El Derecho de las Tecnologías de la Información y Comunicación (Derecho TIC) se ha asentado paulatinamente como una rama más de la ciencia jurídica. Así lo atestigua la aparición de asignaturas sobre la materia en los estudios de pre y postgrado de universidades, sobre todo en el contexto europeo.

reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" (pp. 358-359).

El Convenio de Ciberdelincuencia del Consejo de Europa de 23 de noviembre del 2001 llevado a cabo en Budapest, en su preámbulo alude a los delitos informáticos como: "(…) actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, redes y datos". Por otro lado, Calderón (2013), presenta una definición de los delitos informáticos, vinculada a la conectividad de los sistemas informáticos a través de las TIC y manifiesta que son:

> (…) aquellas conductas ilícitas de acuerdo con la ley penal cometidas en contra o con la ayuda de los sistemas informáticos que pueden ser perpetradas de un lado del planeta a otro, con efectos globales o locales. Esta definición reconoce el alcance de los delitos informáticos y el papel que desempeña el sistema informático en su perpetración. (p. 3)

El citado autor, esgrime dos elementos que forman parte de la estructura de este tipo de delitos: el ciberespacio y el Internet, el primero como el lugar donde algunos delitos informáticos pueden ser cometidos, prevenidos y detectados, entendido como la información a nivel mundial interconectada digitalmente y la infraestructura de las comunicaciones, y el segundo; la red Internet como herramienta para tener acceso al ciberespacio (red mundial World Wide Web), compuesta por los enlaces intercontinentales entre los países de Europa, Asia, América, África y Oceanía, motivo por el cual el ciberespacio carece de fronteras; y constituye la principal peculiaridad que le da a los delitos informáticos su carácter de delincuencia transnacional (p. 4).

A su turno, la Organización de Naciones Unidas (2017) en el documento: "Deliberaciones de la primera reunión del Grupo de expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético", refiere:

> Esa tipología incluía la consideración de nuevos tipos de delitos, cuya comisión solo era posible gracias a las nuevas tecnologías; el uso de tecnologías para cometer delitos ya tipificados o análogos, a veces de nuevas maneras; y el hecho de que los grupos delictivos organizados, los grupos terroristas u otros también utilizaran con frecuencia las tecnologías para facilitar la comisión de delitos, evitar la detección u ocultar pruebas o el producto del delito. (p.4)

Habiendo analizado las definiciones precedentes, el delito informático es una conducta (acción u omisión) pasible de ser sancionada por el derecho penal, que se efectiviza mediante

el uso de las Tecnologías de Información y Comunicación[12] (entendiendo que estas engloban las telecomunicaciones, informática, programas, dispositivos digitales, computadores e Internet) ya sea como medio o como fin, lesionando la información y otros bienes jurídicos relacionados, según sea el caso en su: titularidad, integridad, seguridad, confidencialidad o disponibilidad.

2.2.3 Ciberdelito

La delincuencia cibernética se distingue de la delincuencia informática en que esta última se perpetra en sistemas informáticos en los que la redes, de ser utilizadas, tienen una relevancia limitada o secundaria para las características de la conducta delictiva, la ciberdelincuencia, por su parte:

> (…) gira en torno a redes telemáticas o electrónicas (abiertas, cerradas o de acceso restringido), siendo en estos casos los sistemas informáticos más instrumentales o secundarios para la comisión del delito. Además, todo lo que es cibernético o telemático es también, al mismo tiempo, informático, mientras que no ocurre lo mismo en sentido inverso, siendo por tanto mucho más omnicomprensiva esta nueva categoría. (Barrio, 2017, pp. 28-29)

Es así que esta nueva generación de delitos vinculados a las TIC, se caracteriza primordialmente por la utilización de Internet, a través de la conexión de redes electrónicas en el ámbito transnacional del denominado Ciberespacio, posibilitando que desde cualquier parte del orbe se comentan delitos vulnerando bienes jurídicos como el patrimonio, la intimidad, la libertad e indemnidad sexual, la información y los datos personales; entre otros.

En ocasiones, los términos de delito informático y ciberdelito son utilizados como sinónimos, empero, debe considerarse las precisiones señaladas de las que emerge su distinción. Así también, es evidente que no existe en la actualidad un consenso sobre una definición universal del delito informático, por lo que otras corrientes doctrinales proponen que es más acertado hablar de una criminalidad informática, entendida como todo tipo de conductas criminógenas de carácter informático o cibernético, dirigidas a generar daño en un sistema, obtener un beneficio ilegal, sustraer información, bloquear sistemas y otras actividades delictivas, con fines motivados en un rédito económico, venganza o por mera diversión.

[12] Las TIC, permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de información en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética.

2.2.4 Características de los delitos informáticos

Este tipo de delitos presentan rasgos específicos para su consumación y develamiento, puesto que en muchos casos se desarrollan en el Ciberespacio es decir, en un entorno virtual y omnímodo a través del uso de las TIC. Sobre el particular, Téllez (2009, p. 188), postula las siguientes características respecto a los delitos informáticos:

1. Son consideradas conductas de cuello blanco, debido a que solo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas.
2. Son acciones ocupacionales, realizadas en muchos casos cuando el sujeto trabaja.
3. Son acciones de oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4. Provocan considerables pérdidas económicas.
5. Brindan posibilidades de tiempo y espacio, pueden cometerse en milésimas de segundo y sin necesidad de la presencia física.
6. Son muchos los casos y pocas las denuncias, debido a la ausencia de regulación jurídica.
7. Su comprobación es dificultosa por el factor técnico.
8. En su mayoría son dolosos o intencionales; no obstante, también los hay culposos o imprudenciales.
9. Ofrecen facilidades a los menores de edad para su comisión.
10. Son tendientes a proliferar, por lo que requieren una urgente regulación internacional.

Los delitos informáticos y los ciberdelitos se cometen actualmente en cualquier parte del mundo, basta con tener acceso a un dispositivo que posibilite navegar por el universo virtual, para perpetrar y consumar una amplia gama de ilícitos en cuestión de segundos y sin estar presentes físicamente en el lugar de los hechos; estos factores, sumado a que son conductas que por su vinculación con las TIC están en constante evolución, dificultan individualizar a los autores y dar con su paradero. Así también, presentan grandes obstáculos para su comprobación, caracterizándose además por la facilidad para encubrir los hechos delictivos.

Por consiguiente, la información es cada vez más propensa a ser vulnerada, generando afectación a las esferas económica y personal del individuo, cuyo daño en la mayoría de los casos es irreparable e incuantificable. Bajo dicho razonamiento, cualquier información enviada por medios electrónicos puede ser alcanzada por un ciberdelincuente, siendo estos hechos

cada vez más comunes y recurrentes, dichos factores ameritan la emisión de medidas regulatorias y leyes penales que posibiliten su persecución y su sanción, con el fin de aminorar la creciente brecha de la impunidad.

2.2.5 Clasificación de los delitos informáticos

Existen diversas clasificaciones relativas a los delitos informáticos, siendo disímiles los criterios para su catalogación, en razón de que algunos autores realizan una sistematización en función del bien jurídico protegido y en otros casos se sigue un patrón técnico. En el primer caso, Palazzi (citado en Martínez, 2013, p. 159), los clasifica de la siguiente manera:

1. Contra el patrimonio
2. Contra la intimidad
3. Contra la seguridad pública y las comunicaciones
4. Falsificaciones informáticas
5. Contenidos ilegales en Internet

Para Baón (citado en Cuervo, 1999), se distinguen dos grandes grupos de delitos en el ámbito de la criminalidad informática:

a) Delitos que recaen sobre objetivos pertenecientes al mundo de la informática, tales como:

- relativos a la destrucción o sustracción de programas o de material
- relativos a la alteración, destrucción o reproducción de datos almacenados
- referidos a la utilización indebida de ordenadores

b) Conductas que encuadran en delitos más tradicionales, en contra de:

- la intimidad
- la propiedad
- la propiedad industrial o intelectual
- la fe pública
- el buen funcionamiento de la administración
- la seguridad exterior e interior del Estado

De la Mata (2007), postula una clasificación en función a las agresiones desde el ámbito interno y externo respecto a la utilización autorizada del sistema, ya sea que se orienten contra

los intereses del gestor del sistema, contra intereses ajenos, o cometidos por el propio usuario o en su contra; en ese contexto, identifica los siguientes grupos de infracciones:

1) El que abarca lo que es la delincuencia que tiene por objeto el ataque a los sistemas informáticos en sí mismos considerados, con repercusión o no en el desarrollo de la actividad que permiten los mismos.
2) El que se refiere a la delincuencia que tiene por objeto los datos con los que se trabaja informáticamente, ya tengan carácter personal, ya carácter empresarial, desarrollada mediante la utilización de contextos digitales, que es al que en sentido más estricto se reserva por algún autor la caracterización de Derecho Penal informático por tratarse de agresiones contra y a través de sistemas informáticos. Como a menudo se señala, en realidad el resto de grupos no abarcan sino delitos tradicionales cometidos contra nuevos objetos materiales o a través de nuevas modalidades de conducta nucleados unos y otras en torno al hecho informático o cibernético.
3) El que engloba todas las conductas que se sirven de los sistemas informáticos para facilitar la actuación delictiva, ya sea de un tercero contra el titular o el beneficiario del sistema, ya sea de éste contra un tercero, que favorecen nuevas formas de ataque a bienes tradicionales o al menos facilitan la extensión de la lesividad, la peligrosidad o la proliferación de los ataques a tales bienes.
4) Finalmente, el que comprende lo que es la delincuencia que pretende únicamente atentar contra los derechos derivados de los procesos de innovación informática o de gestión de determinados derechos digitales. (pp. 45-46)

En síntesis, los autores agrupan en su generalidad a los delitos informáticos en aquellas conductas que a través de las Tecnologías de Información y Comunicación quebrantan bienes jurídicos tradicionales, en este caso las herramientas informáticas y tecnológicas vienen a constituirse en un medio. Por otra parte, se distinguen aquellas conductas que atentan específicamente contra sistemas o medios informáticos lesionando nuevos bienes jurídicos, primordialmente la información cuyo contenido lo componen datos personales, empresariales o gubernamentales, entre otros. No obstante, en ambos supuestos, la información resulta quebrantada, porque obtenida ilícitamente es utilizada para perpetrar delitos o porque el solo hecho de su obtención ilegal constituye una vulneración de los derechos y libertades de los individuos.

2.2.6 La necesidad de crear tipos penales respecto a los delitos informáticos y en particular orientados a la protección de datos personales

Latinoamérica es una región caracterizada por una rápida expansión de los usuarios de las TIC y particularmente de la red Internet, es así que el estudio denominado Monitoreo de la

Agenda Digital para América Latina y el Caribe eLAC2018, a cargo de la Comisión Económica para América Latina y el Caribe (CEPAL) que data de la gestión 2018, sostiene que en materia de acceso a infraestructura, la región presenta importantes adelantos, identificando que la penetración de usuarios a Internet, corresponde al 56% en 2016, en tanto que el crecimiento de redes móviles de cuarta generación (4G) en 2017, ha alcanzado al 70% de la población, previéndose que para el 2020 llegue al 84%. Respecto a la expansión de los teléfonos inteligentes se espera que para el final de la década, alcance al 70%, es decir por encima del promedio mundial que oscila en el 66%.

En contraste a dicho incremento, los individuos no conocen a fondo estas innovaciones tecnológicas ni sus implicancias, entre cuyas consecuencias se encuentra la fluctuación masiva en el tráfico de datos personales, datos sensibles y recursos que se transfieren. Es por esto que urgen las medidas de regulación y vigilancia a dichos medios, pues son el terreno fértil para una multiplicidad de ilícitos, ya sea como medio comisivo, o como el fin mismo de un ataque.

De ahí que Nava (2013), postula que el primer paso uniforme que debe darse en cada país de América Latina incluya normativa básica en función a las siguientes directrices:

1. Auténtica protección de datos.
2. Inhibición de la usurpación de identidad.
3. Catálogo de delitos informáticos.
4. Actualización de las normas de propiedad intelectual.
5. Responsabilidad de los proveedores de servicio de Internet.
6. Prácticas inhibitorias del bullying y el ciberacoso. (p. 179)

El citado autor además añade:

> La era digital ha llegado y los operadores de la ley no pueden mantener viejas prácticas que hagan imposible la aplicación de un real estado de Derecho.
> El delito electrónico será el delito por antonomasia en el siglo que comenzamos. Si no se realiza un cuerpo legal básico que atienda a sus rasgos primigenios, no habrá sino un panorama de impunidad como el que ha imperado sobre la materia en los últimos diez años. (Nava, 2013, p.179)

En relación a dicha problemática Téllez (2009), plantea varios aspectos a ser considerados por el legislador:

> a) Regulación de la información, ya que la información como un bien requiere un tratamiento jurídico en función de su innegable carácter económico.
> b) Protección de datos personales, es decir, el atentado a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas.
> c) Regulación jurídica de internet, con el favorecimiento o restricción de los portales en internet.
> d) Propiedad intelectual e informática, con los temas referentes a protección de los programas de cómputo y regulación de nombres dominio, ambos derivados de las acciones de "piratería" o "ciberocupación".
> e) Delitos informáticos, es decir, la comisión de actos ilícitos en los que se tengan a las computadoras como instrumentos o fin. (pp. 14 -15)

Razonando con afinidad a lo señalado, Ossio (2010) fundamenta que merced a los cambios que se suscitan en la Sociedad de la Información, con motivo de la aplicación de las TIC, se hace necesario contar con nomas especializadas, a efectos de prevenir o resolver conflictos, a las cuales denomina: "Legislación Informática (…) como un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática" (pp. 30-31) y dentro de ello el nombrado autor le da especial preeminencia a la protección de datos personales.

El impacto de las TIC en la sociedad, amerita como reflejo un tratamiento en la órbita jurídica penal, ya no bastan las disposiciones existentes o su adaptación a los nuevos requerimientos de los fenómenos sociales, sino que es menester crear una nueva regulación en base a las trasformaciones imperantes. La necesidad de tipificar delitos inherentes a la información y los datos personales, se evidencia, en que, si estas conductas no se encuentran reguladas en la norma sustantiva penal, será improbable su persecución y la imposición de sanciones para los infractores, lo anterior en aplicación del principio de legalidad; propiciando además dicho vacío jurídico, la comisión de otros ilícitos y el consecuente quebrantamiento de otros bienes jurídicos.

La autodeterminación informativa, constituye un derecho humano que ostenta una relevancia que emana de los modernos desafíos tecnológicos y de la necesidad de salvaguardar al individuo en lo que concierne a sus datos personales, puesto que, dejando de lado el concepto de intimidad negativa, posibilita avanzar hacia una fase activa del proceso de circulación de la información personal, viabilizando al interesado ejercer un control sobre la preservación de su libertad informática, de ahí la trascendencia de incorporar mecanismos que coadyuven a optimizar su tutela en la esfera del derecho penal.

2.2.7 Elementos del tipo penal que surgen del delito informático aplicados a los delitos contra los datos personales

Si bien los atentados contra la información y los datos personales no se materializan únicamente con el uso de las TIC, no es menos evidente que gracias a estas, las agresiones potenciales y reales son más habituales, incrementándose su lesividad.

Para Palazzi (citado por Martínez, 2013, p.159) la información, al ser tratada como una mercancía, adquiere un valor especial, se comercia con los datos personales, y comúnmente los titulares de los datos desconocen que los mismos son objeto de intercambio. El nombrado autor, afirma que es posible una mayor afectación a la intimidad con la existencia de nuevos medios tecnológicos que permiten acceder a zonas que antes eran inaccesibles, señalando al efecto:

> Con una simple conexión a Internet cualquiera puede saber si su vecino fue inhabilitado por el Banco Central para operar en cuenta corriente bancaria, o mediante un satélite es posible fotografiar cualquier superficie de la tierra, o por medio de un scanner térmico podemos detectar que sucede dentro de un hogar. Todo esto nos lleva a ampliar el concepto tradicional del ámbito protegido por la intimidad. Así en lo referente a la informática, se habla de protección de datos y de un nuevo espacio que se debe proteger: el ciberespacio (Palazzi citado por Martínez, 2013, p.162).

Es menester precisar que la criminalidad informática engloba a los delitos contra los datos de carácter personal (Romeo Casabona, 2007, p. 653; Riascos, 2012, p. 398); por consiguiente, bajo este parámetro se analizarán los elementos del tipo penal de los delitos informáticos, aplicados a los delitos contra los datos personales, en una relación de genero a especie, que permitirá vislumbrar un panorama más certero de los presupuestos en los que se articula su construcción.

a) Tipo penal y tipicidad

Según Zaffaroni (1895) el tipo penal constituye un: "(…) instrumento legal, lógicamente necesario y de naturaleza predominantemente descriptiva; que tiene por función la individualización de conductas humanas penalmente relevantes; por estar penalmente prohibidas" (p. 371), sustentando este razonamiento, el tipo pertenece a la ley, como fórmula orientada a individualizar las conductas que la normativa penal prohíbe; necesario para la averiguación de la delictuosidad de una conducta y que por ende es eminentemente descriptivo.

Por su parte, Bacigalupo (1999), expresa: "(…) es la descripción de la conducta prohibida por una norma (…) la descripción de la acción que infringe la norma (…) el conjunto de elementos que caracteriza a un comportamiento como contrario a la norma" (p.220). Así también, Jescheck (1993), refiere: "(…) descripción objetiva del comportamiento prohibido" (p. 221).

Para Muñoz y García (2010) el tipo penal es: "(…) la descripción de la conducta prohibida que lleva a cabo el legislador en el supuesto de hecho de una norma penal" (p. 252) y tiene una triple función:

a) Función seleccionadora de los comportamientos penalmente relevantes.
b) Función de garantía, que implica que únicamente los comportamientos subsumibles en el tipo pueden ser objeto de sanción penal.
c) Función motivadora general, a través de la descripción de los comportamientos en el tipo penal, el legislador indica a los ciudadanos qué comportamientos están prohibidos, para que éstos se abstengan de realizar la conducta prohibida.

Por consiguiente, el comportamiento debe ser definido en todas sus características y elementos para no conducir a ambigüedades; así también su grado de precisión debe excluir la posibilidad de aplicación a conductas que no están acogidas por su texto.

Sobre la tipicidad Muñoz y García (2010), señalan: "(…) la adecuación de un hecho cometido a la descripción que de ese hecho se hace en la ley penal. Por imperativo del principio de legalidad, en su vertiente del nullum crimen sine lege, sólo los hechos tipificados en la ley penal como delitos pueden ser considerados como tales" (p.204). En similar sentido, Nava (2018), puntualiza: "(…) es el proceso mediante el cual podemos adecuar la conducta al tipo" (pp.109-110). En síntesis, la conducta humana (acción u omisión) debe encuadrarse a la descripción del tipo penal para ser considerada como ilícito, a través de un proceso intelectivo que permita su identificación en el plano real, en contraste con lo determinado en la esfera legal.

b) Tipo común y tipo especial

En los tipos comunes, no se establece una cualificación o caracterización específica del sujeto activo, puede englobar a cualquier persona; por su parte, en los tipos especiales o denominados propios se requiere una específica cualificación del agente, por su relación con el bien jurídico, ya que deben cumplir el deber de garantía (Bacigalupo, 1999, p. 244).

Respecto a los delitos informáticos, y en particular aquellos relacionados con los datos personales, la legislación comparada ha optado por instaurar tipos comunes y especiales impropios, en los últimos se incluye a los servidores públicos, los responsables de las bases de datos y los encargados del tratamiento, en atención a que estos se encuentran en una posición singular que emana de condiciones personales, ya que les es exigido mayor responsabilidad y un nivel alto de moralidad y compromiso, debiendo cumplir deberes de protección de los bienes jurídicos bajo su cuidado.

c) Tipo básico y tipo agravado

El tipo agravado, presupone la concurrencia de los elementos exigidos por el tipo básico, es decir se aplica sólo si se realizan los requisitos previstos en dicho tipo y agrega algún elemento o circunstancia particular que le hace aparecer como un hecho de mayor gravedad y que justifica la elevación de la pena asignada al comportamiento (Mata, 2003, p. 118). El tipo básico contiene una descripción genérica del hecho punible, mientras que el tipo agravado como una subespecie del tipo derivado, se obtiene añadiéndole al tipo básico elementos específicos para agravar la pena, como una conducta especial del autor, así también pueden surgir de una relación preexistente entre al autor y su víctima, o en función al momento de la conducta o del uso de determinados medios comisivos; en todos los casos representan un riesgo mayor para el bien tutelado.

Los delitos informáticos y en particular los delitos contra los datos personales, en principio son figuras que podrían ser perpetradas por cualquier sujeto activo; sin embargo, en ocasiones son consumadas por servidores públicos, los encargados del tratamiento o los responsables de las bases de datos, en función de que éstos pueden aprovecharse de los beneficios, ventajas o facilidades que les brinda dicha posición, por lo cual se incluyen estos factores como agravante. Así también, legislaciones como la de España, elevan la pena cuando los hechos afectan a datos personales sensibles que revelen la ideología, religión, creencias, salud, origen racial o vida sexual.

d) Tipicidad objetiva

- **Sujeto activo**

Es la persona que: "(…) realiza la acción prohibida u omite la acción esperada (…) en algunos casos la ley exige determinadas cualidades para ser sujeto activo (…) sólo puede serlo aquella persona que, además de realizar la acción típica, tenga cualidades exigidas por el tipo (…)"

(Muñoz y García, 2010, p. 259), por ejemplo en el caso de los delitos cometidos por funcionarios públicos.

Sutherland (citado por Téllez, 2009), en 1943 introduce por primera vez el término de delitos de cuello blanco, catalogando dentro de este grupo a los delitos informáticos, en los cuales el sujeto activo a criterio del nombrado tratadista es una persona con un determinado: "(…) status socioeconómico y su comisión no puede explicarse por pobreza, ni por mala habitación, no por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional" (p. 189). Viega (2003, pp. 14-15) postula que los sujetos activos de estos delitos poseen importantes conocimientos de informática, y ocupan lugares estratégicos en su trabajo, con acceso a información de carácter sensible (delitos ocupacionales) y poseen cierto estatus socioeconómico, aduce además que las opiniones en torno a su nivel educacional, están divididas, ya que para unos la formación a nivel informático no es indicativo, mientras que para otros sí.

Por su parte, Huerta y Líbano (citados por Acurio, 2017), reconocen que muchos delitos informáticos se cometen desde dentro del sistema, por personas que habitualmente lo operan y que tienen autorizado los accesos (Insiders); no obstante, las tendencias modernas apuntan al mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones, ganando cada día más terreno el delito informático a distancia (Outsiders) (p.64), en un entorno digital de virtualidad. Lara (citado por Acurio, 2017, p.65), expresa que si bien tradicionalmente este tipo de ilícitos se encuadra en los llamados delitos de cuello blanco, actualmente toda vez que el mundo de la computación es cada día más común y corriente, debido a la facilidad que presentan los modernos sistemas y programas, ya no es imperativo poseer una eximia instrucción, pudiendo un lego en la materia ubicarse como sujeto activo de un delito informático.

La expansión de las Tecnologías de Información y Comunicación, cada vez más al alcance de la población y su irrupción en diversas áreas del quehacer cotidiano, obliga a que se adquieran mayores conocimientos informáticos a nivel empírico y/o teórico, por lo que el sujeto activo, no necesariamente se identifica hoy en día como un perito o especialista con notable instrucción y amplios estudios académicos en la materia, tampoco como una persona con un alto nivel económico, condiciones que actualmente ya no son indispensables. Es así que esta delincuencia ha adoptado diversas especialidades y denominaciones[13], de acuerdo a la

[13] Entre los tipos de delincuentes informáticos, que gozan de un mayor o menor grado de conocimientos de las TIC están los denominados: hacker (con conocimientos en seguridad y con la capacidad de detectar errores o fallos en sistemas informáticos y crear su propio software para ingresar a los sistemas); cracker (con capacidades de romper sistemas de seguridad y software); phreaker (con conocimientos amplios tanto en teléfonos modulares como en teléfonos móviles, redes públicas y coorporativas); lammers (su conocimiento es inferior ya que utilizan las herramientas creadas por los expertos, como programas y herramientas

actividad desplegada que exige mayor o menor grado de conocimientos informáticos y de las TIC, los cuales al margen de una formación técnica o profesional, pueden obtenerse a través de la práctica y experiencia; agrupándose básicamente en: estafas informáticas (phishing, carding, fraude al CEO, fraude a RRHH), los delitos informáticos de daños (sabotaje, ransomware), las defraudaciones de telecomunicaciones, delitos contra la propiedad intelectual, y los ciberdelitos contra la intimidad y los datos personales (sexting, pornovenganza, revelación de datos, procesamientos ilícitos o no autorizados de datos).

En los delitos informáticos el sujeto activo puede ser cualquier persona, y también comprender a sujetos específicos como funcionarios públicos o encargados del tratamiento y responsables de las bases de datos. En ambos casos, deben poseer un determinado nivel de conocimientos de las TIC, para de esta manera ingresar de forma intrusiva a la información o contenido protegido, vulnerando sistemas de seguridad. Así también, puede fungir como sujeto activo un individuo que tenga acceso a dichos sistemas, pero utiliza la información en ellos contenida, para fines distintos, o realiza un procesamiento que no le es facultado y/o autorizado.

Para Posada (2017, pp.90-91) en estos comportamientos punibles, es necesario enlazar el empleo de los dispositivos o sistemas con una persona natural a través de su identidad digital, ya que el ciberespacio es mucho más que un medio o un instrumento, es una verdadera realidad simulada en la cual los ciberdelincuentes se amparan en el anonimato a través de modernas técnicas de encriptación, cifrado y por el uso de espacios como la Web profunda (Deep Web).

En el caso de los datos personales, el sujeto activo puede ser determinado o indeterminado (cualificado o no cualificado) (Suárez, 2019, p. 21) un servidor público, el responsable del tratamiento, el responsable de la base de datos; o cualquier persona que vulnere datos personales, contenidos en ficheros, archivos, bases de datos, medios semejantes o cualquier otro medio, mediante el acceso o tratamientos indebidos o no autorizados, o que efectúe procesamientos para fines distintos a los que fueron recolectados, ya sea que cursen en soporte digital o en otros soportes emergentes de las TIC, e incluso en soportes catalogados como tradicionales.

---

de intrusión informática, cibervandalismo o propagación de software malicioso para luego ejecutarlo como simple usuario); bucaneros (se dedican a la venta de productos crakeados, usualmente carecen de conocimientos informáticos); gurú (dotado de un alto grado de conocimientos, entrena a los hackers); newbie (se denominan así a los novatos con poca experiencia) y trashing (con conocimientos en obtención de información secreta o privada que se logra por la revisión no autorizada del historial de navegación y archivos que almacenan cookies o a partir de la recuperación de archivos, documentos, directorios e incluso contraseñas que el usuario ha enviado a la papelera de reciclaje de su equipo).

- **Sujeto pasivo**

Es el titular del bien jurídico lesionado, quien puede diferir del sujeto perjudicado, el cual puede eventualmente, ser un tercero (Acurio, 2017, p. 62). Constituye aquel sobre el que recae la acción u omisión que realiza el sujeto activo, en otros términos, el sujeto pasivo es la víctima del delito, para el caso de los delitos informáticos puede estar conformado por personas particulares, entidades públicas y privadas que usan sistemas automatizados de información, generalmente conectados a la red Internet.

El sujeto pasivo, posee la información en formato digital y/o almacenada en un medio informático, ya sean datos, programas, documentos electrónicos, dinero electrónico, u otros, y se encuentra en contacto directo con las Tecnologías de Información y Comunicación. Acurio (2017, p. 88) advierte frente a esta problemática varios factores que confluyen en una cifra negra de criminalidad informática, entre estos identifica los innumerables delitos que no son descubiertos o denunciados, aunado a ello, la falta de leyes de protección a las víctimas y la carencia de preparación de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado.

En el caso de los delitos contra los datos personales, el sujeto pasivo es el titular de los mismos. Sobre el particular, cabe señalar que existen dos corrientes doctrinales, la primera es la adoptada en una parte de los países europeos, por la cual solo las personas naturales son susceptibles de ser titulares de datos de carácter personal excluyéndose a las personas jurídicas o de existencia ideal. Por su parte, la vertiente latinoamericana asigna además esta calidad a los entes colectivos de naturaleza pública o privada, en todo cuanto fuere pertinente.

Para Riascos (2012), la titularidad evoca un claro derecho de propiedad inmaterial sobre el dato, que engloba a su vez los derechos de acceso, conocimiento, actualización, rectificación y eliminación de datos personales recabados en bancos, registros, bases o ficheros de datos o informaciones personales, sean de índole público o privado.

- **Bien jurídico protegido**

Para Muñoz y García (2010), bien jurídico es: “(…) el valor que la ley quiere proteger de las conductas que puedan dañarlo. Este valor es una cualidad positiva que el legislador atribuye a determinados intereses (…) algo que crea la ley y no algo preexistente a ella misma (…)” (p.261).

En este sentido, se empezará por dilucidar respecto a cuál es el bien jurídico protegido dentro de los delitos informáticos, respecto al que doctrinalmente, han emergido dos posturas. Sobre el particular Acurio (2017) señala:

> (…) la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales (tradición europea continental), con una reinterpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. (p. 89)

El mismo autor refiere que la Sociedad de la Información, hace necesaria la incorporación de valores inmateriales y de la información misma como bienes jurídicos dignos de protección, señalando a su vez que la libertad informática es un bien jurídico, dentro de lo cual la información está considerada en diferentes representaciones que abarcan desde un valor económico, un valor intrínseco de la persona, su fluidez y tráfico jurídico, y los sistemas que la procesan o automatizan, equiparándose a los bienes jurídicos protegidos tradicionales, como: el patrimonio (fraudes informáticos); reserva, intimidad y confidencialidad de los datos (agresiones a la intimidad, especialmente en el caso de los bancos de datos); seguridad o fiabilidad del tráfico jurídico y probatorio (falsificaciones de datos o documentos probatorios vía medios informáticos) y la propiedad (sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático). Acurio (2017, p.91) concluye que al afectar diversidad de intereses colectivos los delitos informáticos son pluriofensivos.

En similar sentido, Blossier y Calderón (2003), expresan que este tipo de ilícitos:

> (…) es una violación mixta de valores jurídicos que en algunos casos compromete tanto al patrimonio como la libertad de las personas o el sistema informático y la protección de datos, no sólo se vulneran valores de carácter económico sino de carácter tan valioso y personal como la intimidad, lo que hace imposible negar su existencia. (p.24)

Es así que el uso inapropiado de la informática puede afectar a bienes jurídicos patrimoniales y no patrimoniales, e igualmente a derechos fundamentales y libertades constitucionales, como la intimidad, la privacidad, el derecho a la autodeterminación informativa y otros vinculados.

Otra corriente de la que es partidario Carrión (2001) afirma que la información es el bien jurídico que se pretende proteger en los delitos informáticos, ya que su ataque supone una agresión a las relaciones socio-económico-culturales, emergentes de la interacción humana

en todos sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnología, etc.) (sp). Así también, Rincón (2015), señala: “Pensar en la creación de tipos penales exige un nuevo bien jurídico tutelado: la información y el dato; la discusión no podía reducirse a que son simplemente las mismas conductas ya tipificadas que se realizaban a través de otros medios” (p. 216).

Para Reyna (citado por Castro, 2002, parr. 5-7), la información almacenada, procesada y transmitida mediante los sistemas de tratamiento automatizado, encierra un valor, un interés tanto particular como social, cualitativamente distinto, dotado de autonomía y objeto de tráfico, entendida como un proceso que engloba almacenamiento, tratamiento y transmisión, y estimado como un bien jurídico.

Por su parte, Posada (2017, p. 76), expresa: “(…) se intuye ya la necesidad y la importancia de proteger la seguridad de la información como un bien jurídico de naturaleza intermedia, que a su turno permita tutelar otros derechos constitucionales y bienes jurídicos como el patrimonio económico, la intimidad personal y la autodeterminación informática”. En correspondencia, Suárez (2019, p.20), asevera que al: “(…) dársele expresa tutela al bien jurídico de la información y los datos, basta que cada uno de los comportamientos típicos individuales constituya la superación de las medidas de seguridad informática para que se los tenga como una verdadera puesta en peligro abstracto de aquel bien jurídico supraindividual”.

Estas vertientes postulan que los delitos informáticos no solo lesionan bienes jurídicos individuales, ya que la ejecución de los hechos punibles produce efectos sobre el individuo y la sociedad como titulares de la información y los datos (interpretación dual), ocasionando la perdida de la confianza de los ciudadanos en los sistemas informáticos, redes de sistemas electrónicos, telemáticos y medios semejantes. Ahora bien, con relación a la protección de datos personales, para Anarte (2002), el ejercicio de este derecho: “(…) garantiza la salvaguarda y el ejercicio de otros derechos, como la dignidad que constituye un valor jurídico primordial, y en última instancia el libre desarrollo de la personalidad” (p. 235); en consecuencia, es posible afirmar que se le adscribe la categoría de bien jurídico merecedor de tutela penal.

Murillo y Piñar (2009) afianzan la existencia de un bien jurídico autónomo denominado autodeterminación informativa, que consiste en asegurar a las personas el control de su información y datos propios para protegerla de:

> (…) perjuicios derivados del uso por terceros, públicos o privados, de ese material. Las ilimitadas posibilidades que ofrece la tecnología de captar, acopiar, asociar, recuperar en tiempo real y conservar indefinidamente datos personales, así como de obtener ulterior información personal mediante su tratamiento, junto a la necesidad creciente de los mismos en todo tipo de relaciones, han hecho imprescindible garantizar a los individuos instrumentos jurídicos que hagan posible ese control. (p. 18)

Gonzales Rus (2007), se opone a la creación de nuevos bienes jurídicos que ameriten una protección jurídico penal como consecuencia del desarrollo tecnológico, planteando que esta problemática puede resolverse complementando las figuras de delito ya disponibles, es decir en vez de incorporar bienes jurídicos informáticos "nuevos" y crear delitos específicos dirigidos a la protección de los mismos, se debería abordar la punición de los llamados "delitos informáticos" desde las modalidades delictivas ya existentes; y solo frente a una verdadera "laguna" de punición se justifica la incorporación de un nuevo bien jurídico; no obstante, el citado autor identifica que el derecho a la protección de datos personales con relación a la libertad informática es el: "(…) único bien genuinamente informático que ha consolidado como derecho fundamental la generalización de los medios y procedimientos informáticos y telemáticos y que encuentra tutela en el Código Penal" (p.28), dotado de significación propia y autónoma de otros bienes jurídicos con los que se relaciona; por ende, susceptible y necesitado de protección penal.

Por su parte, Romeo Casabona (2002), señala: "(…) los datos de carácter personal constituyen otro de los bienes jurídicos protegidos en estos delitos" (p. 526), reconociendo su actual rango de derecho fundamental que amerita tutela penal. Se debe destacar que el bien jurídico cumple funciones de gran relevancia para el derecho penal, ya que la afectación del mismo permite fundamentar la sanción de las conductas que lo lesionan o ponen en peligro y constituye un requisito para el ejercicio del ius puniendi. La importancia y el grado de afectación del bien jurídico, constituyen criterios para el establecimiento de penas proporcionales. A su vez, el bien jurídico permite determinar el injusto específico de cada delito, sistematizar los tipos penales que componen la Parte Especial del Código Penal y orientar la interpretación de los comportamientos que ellos reprimen.

De lo anterior se colige la trascendencia de precisar cuál es el bien jurídico protegido por un determinado delito, que para el presente estudio y con sustento en las posiciones doctrinales señaladas lo conforman tanto la información como los datos (la información es en sí misma un conjunto organizado de datos y los datos sometidos a procesamiento originan a la información) cuya relevancia es incluso supraindividual, siendo que dentro de esta categoría se incluye el dato personal. Los ilícitos contra estos bienes jurídicos, transgreden el derecho

fundamental y autónomo de autodeterminación informativa, sin dejar de lado el carácter pluriofensivo de los mismos que por su naturaleza atentan también contra otros bienes jurídicos tutelados, catalogados como tradicionales, ya sea subsidiariamente o de forma paralela.

La información y los datos ostentan la categoría de bienes jurídicos de interés de la sociedad con implicancias en lo personal, económico, comercial, estatal, relaciones internacionales y en otros órdenes, en ello radican los factores preponderantes para su protección penal, ya que en la medida en que opere su efectiva salvaguarda también se resguardarán otros derechos y libertades como la dignidad, la intimidad, la privacidad, el honor, la autodeterminación informativa o el patrimonio.

- **Acción (conducta)**

La acción, como elemento descrito que ha de desplegar el sujeto activo, es considerado como el núcleo del tipo. Muñoz y García (2010), definen a la conducta como el comportamiento humano ya sea acción u omisión, representado como verbo rector, que indica una acción positiva u omisión. A su vez, de acuerdo a las exigencias del tipo puede dar lugar a delitos de mera actividad (el tipo sólo exige la realización de la acción sin más) o mera inactividad (omisión pura); no obstante, en otros casos se exige la producción de un resultado material de lesión o puesta en peligro del bien jurídico (delitos de resultado) (p. 260).

Como elemento descrito en el tipo desplegado por el sujeto activo, Jakobs, (citado por Nava, 2018), esboza respecto a la acción:

> (…) un concepto jurídico-penal de acción debe combinar sociedad y Derecho penal. So pena de degenerar hasta quedar convertido en un concepto de mera utilidad didáctica que describa un escalón inicial del delito, debe contener una teoría lo más completa posible del comportamiento jurídico-penalmente relevante. El concepto de acción, en cuanto concepto jurídico-penal, debe garantizar que la definición de los comportamientos jurídico-penalmente imputables no sea una mezcolanza de elementos heterogéneos agrupados de cualquier manera, sino una unidad conceptual. (p.116)

En el área informática las conductas reprochables o punibles son variadas, desde el robo de información hasta daños patrimoniales y pueden presentarse no solo mediante figuras comisivas sino también omisivas. Para Posada (2017, pp. 85-86) la acción en los ciberdelitos se caracteriza por ser ejecutada en la realidad virtual, representando la realización de instrucciones procesables por los sistemas informáticos y como una conducta deslocalizada

o desubicada físicamente, pues el ciberespacio como realidad virtual es precisamente un ámbito de interacción lógica. Así las cosas, con el advenimiento de la ciberdelincuencia la acción también se traslada al mundo virtual, irrumpiendo con la tradicional concepción de espacio y tiempo, ya que se está frente a una conducta que puede ser automatizada y programable, porque a partir de la generación de un proceso automatizado se pueden proyectar ciberataques en gran escala y dirigirlos a diversos lugares del mundo, siendo únicamente inicial la intervención del ser humano.

Respecto a los datos personales y las conductas consideradas como delictivas, Mata (2003) señala:

> (…) el apoderamiento debe entenderse (…) como aprehensión de algún tipo de materialización de los datos contenidos en el fichero. Ahora se trata de datos consignados en un fichero automatizado (…). La utilización de los datos se entiende como cualquier comportamiento de aprovechamiento posterior de los mismos. La modificación supone el cambio o transformación de los datos almacenados en el fichero. Modificación y alteración son conductas equivalentes (…). Con el acceso se produce la captación intelectual de la información almacenada en el sistema informático". (pp.159-160)

Para Morales (1996), de acuerdo a la distinción de las fases del ciclo informático (recolección, registro o "programación" y transmisión de la información), la protección jurídico penal se extiende a partir de la etapa de tratamiento o programación, por lo que las fases previas como la de recolección y almacenamiento se protegen o tutelan en la vía civil y/o administrativa. En una posición divergente, Arroyo (1995, p. 306), manifiesta que la tutela penal, para ser eficaz debe extenderse a todas las fases del ciclo informático, desde la creación de los ficheros informáticos hasta la alteración y transmisión ilícita de los datos registrados.

A su vez, las legislaciones que incorporaron tipos penales para la tutela de datos personales han incluido conductas tales como utilizar, insertar, modificar, proporcionar o revelar datos (Ley especial contra los delitos informáticos y conexos - El Salvador, 2016, Art. 24); la creación, ingreso o utilización de una base de datos (Ley de delitos informáticos N°30096 - Perú, 2013, Artículo 6); apoderarse, modificar, interferir, acceder, copiar, transmitir, publicar, difundir, recopilar, inutilizar, interceptar, retener, vender, comprar o desviar para un fin distinto datos personales (Código Penal – Costa Rica, 2012, Art. 196 bis.). En síntesis, estos ilícitos involucran conductas que van desde la creación de bases de datos, accesos, apoderamientos, utilización, alteración y difusión no autorizados hasta la inutilización de datos, es decir comprenden una gama de procesamientos o tratamientos de los cuales pueden ser objeto los

datos personales, usualmente consignados en bases o bancos de datos o contenidos en diversos soportes de las Tecnologías de Información y Comunicación.

- **El resultado**

El resultado es en la teoría del delito: "(…) la manifestación fenomenológica del mismo, cuya existencia presume una conducta probablemente reprochable" (Nava, 2018, p.117), es una derivación de la afectación de un bien jurídico o la modificación verificable del mundo exterior trascendente en el ámbito penal. Nava (2018, p. 117), asiente que el resultado en los delitos informáticos se manifiesta a través de la lesión de distintos bienes jurídicos protegidos como el patrimonio, la privacidad, la honra y hasta la vida. En consecuencia, la puesta en peligro o lesión de bienes jurídicos como la información y los datos, constituyen también el resultado de los ilícitos de esta naturaleza.

En el caso de los cibercrímenes, no obstante de exigir excepcionalmente resultados materiales para consumar ciertos delitos, en general prevén categorías de resultado lógico (como modalidad del resultado inmaterial), por ejemplo el daño informático que castiga la destrucción, daño, borrado, deterioro, alteración, supresión de datos informáticos o de sistemas de tratamiento de información; el impedir el acceso normal a un sistema informático o a los datos; la interceptación de datos informáticos; la obtención, sustracción, interceptación o modificación de códigos personales o datos personales contenidos en ficheros o archivos; la modificación del sistema de resolución de nombres de dominio; y el conseguir la transferencia no consentida de activos, exigen para su consumación resultados inmateriales que suponen una modificación lógica de los objetos sobre los cuales recae la acción criminal, dentro de los sistemas informáticos, en la web o en medios de almacenamiento como la nube (cloud computing) (Posada, 2017, pp. 97-98).

Los comportamientos digitales, aunque tienen origen físico en una acción, producen resultados en el mundo digital, pues se dan mediante el tratamiento, la manipulación y el almacenamiento de datos informáticos, es decir los resultados lógicos no trascienden al mundo físico, aunque pueden impedir a los usuarios la disponibilidad posterior (acceso y funcionamiento normal) de los datos o los sistemas informáticos.

Las peculiaridades señaladas son también aplicables a los delitos contra los datos personales, en los que los resultados pueden trascender de manera material y también inmaterial, como consecuencia de la utilización de las TIC.

- **Objeto material**

Conforme señala Nava (2018), el objeto material es:

> (…) la persona o cosa (todo lo que tiene entidad, ya sea corporal o espiritual, natural o artificial, real o abstracta) sobre la que recae directamente el delito o el daño causado por el delito cometido. Lo pueden ser cualquiera de los sujetos pasivos, las cosas animadas o inanimadas y ahora, las virtuales. (p.117)

De acuerdo al citado concepto, respecto a algunos delitos informáticos en los que opera el robo de información o su pérdida, el objeto es la información misma, que puede no necesariamente ser material. Lo anterior es aplicable a los datos personales los cuales pueden estar contenidos en soportes de papel, digitales o virtuales. Al respecto, Suárez (2019), sustenta que el objeto material es "fenomenológico" compuesto por el código personal y el dato personal, contenidos en ficheros, archivos, base de datos o medios semejantes (p. 50). Es decir, ya no se está frente a una cosa corpórea, sino a un bien inmaterial que debe distinguirse del soporte material que lo contiene. Para Posada (2017) el cibercrimen es un comportamiento tecnológico particular, que no puede ser subsumido o consumido por otras conductas punibles diseñadas para proteger objetos físicos o materiales, agrupando como objetos propios de los ciberdelitos a: los datos informáticos, la información, el software y los sistemas informáticos (pp. 93-96).

Sintetizando lo señalado, el objeto material, lo constituyen la información y el dato en sí mismo, en las distintas formas que este puede adoptar, en el caso particular los datos personales pueden ser de diversa naturaleza, ya sea nominativos, numéricos, imágenes, datos biométricos o médicos, etc. y en los diversos soportes en los que éstos pueden estar contenidos.

- **Medios comisivos**

El libro Programa de Derecho Penal, de Celestino Porte Petit (citado en Nava, 2018), referido a la obra de Mezger, expresa: "En numerosos casos los tipos exigen determinados medios, originándose los llamados tipos con medios legalmente determinados o limitados. Ello quiere decir que para que pueda darse la tipicidad deben concurrir los medios que exija el tipo correspondiente (…) el medio exigido por el tipo puede dar lugar a resultados diversos" (p.118); consiguientemente, estos medios son empleados para alcanzar un resultado establecido, aunque el legislador en algunos casos prescinde de los mismos o en otros no los define claramente, mientras que en ciertos tipos penales son introducidos para agravar la

sanción. La información y los datos personales, pueden ser vulnerados a través de medios comisivos tradicionales; y así también, por medios digitales, informáticos, telemáticos o virtuales, estos últimos como consecuencia de los avances tecnológicos y la incorporación de las TIC a una pluralidad de actividades de la sociedad actual, ya sea en instancias privadas o estatales. Respecto a éstos últimos Riascos (2009) señala:

> (…) medios informáticos, electrónicos o telemáticos, tanto de hardware (equipos computacionales o unidades periféricas: MODEM, impresoras, videocámaras, scanners, tableros ópticos, multimedia, cámaras digitales, etc.) como de software (programas de computador utilitarios, educativos, publicitarios, chats room, páginas de WEB, WWW –World Wide Web--, hipertexto, correo electrónico, tableros electrónicos, lúdicos, etc.) y sean idóneos para el tratamiento o procesamiento de datos (…). (p. 11)

En dicho sentido, las TIC adquieren primordial relevancia, ya que se emplean como medio comisivo de ilícitos contra la información y los datos personales, situación ante la cual el derecho penal debe responder apropiadamente.

- **Elementos normativos y descriptivos**

En la descripción del tipo, se emplean elementos de lenguaje, estos pueden ser descriptivos o normativos. Se entiende por elemento descriptivo aquel término legal cuyo contenido viene determinado por el sentido que el uso del lenguaje da a la expresión, cuyo contenido y significado se obtiene por medio de conceptos que proporciona la experiencia y el propio significado gramatical de los términos. Los elementos normativos, en cambio, son las valoraciones de tipo jurídico inmersas en el tipo penal, cuando este contiene vocablos como por ejemplo: “indebidamente”, “ilícitamente” o “clandestinamente”, de cuya valoración depende que una acción pueda ser considerada como ilícito penal (Nava, 2018, p. 125).

Ambos aspectos deben ser observados en los tipos penales referidos a delitos informáticos y en particular a aquellos orientados a la tutela de la información y los datos personales.

e) Tipicidad subjetiva

Respecto a los delitos informáticos y en particular aquellos que atentan contra datos personales, el derecho penal debe también prevenir la comisión de este tipo de hechos “(…) que de ninguna manera pueden ser entendidos como errores involuntarios, pues son realizados por personas que generalmente están familiarizadas y especializadas en el trabajo con computadoras, por lo que fácilmente pueden conocer cómo entrar en los archivos de

datos de cualquier individuo” (Vizcardo, 2014, p. 71). Bajo dicho razonamiento, los delitos informáticos son acciones a las que el legislador le ha asignado una connotación primordialmente dolosa porque provocan perjuicio de diversa naturaleza, sin que necesariamente conlleven beneficios materiales para el autor.

En consecuencia, se caracterizan por ser esencialmente dolosos, puesto que demandan que el sujeto activo conozca lo ilícito de su accionar, y que éste sea efectivizado con voluntad, de no existir uno de estos elementos no se configuraría como delito. Sin perjuicio de lo anterior, también es posible la comisión de un delito contra los datos personales bajo la modalidad culposa, es decir a través de la falta del deber de cuidado; no obstante, de acuerdo al derecho comparado, las legislaciones han optado por excluirlo de la esfera sancionatoria del derecho penal.

f) Sanción

La pena constituye la consecuencia jurídica del delito, establecida por la ley penal e impuesta como sanción por el órgano jurisdiccional competente al sujeto que comete un delito o realiza una conducta punible. Expresa un juicio de reproche hacia la conducta antijurídica del delincuente que viola y transgrede la norma alterando la estabilidad del sistema penal por su actitud de rechazo y negación del carácter obligatorio de la misma. Por ello, implica la imposición de un mal que supone la restricción o privación de derechos (libertad, patrimonio, derechos políticos, profesión, etc.), justificado en la protección de los bienes jurídicos vulnerados con su acción típica, antijurídica y culpable.

De este modo, a la luz de los principios de legalidad, seguridad jurídica y proporcionalidad, el legislador penal debe expresar de manera precisa y concisa el tipo de pena aplicable que corresponde a cada tipo penal y el tiempo de su duración fijando el margen de mínimos y máximos, dentro del cual el juez podrá moverse para determinar la pena en el caso concreto, excluyendo aquellas que vulneren la dignidad e integridad de la persona. Bajo estos parámetros, los delitos informáticos y los delitos que atentan contra los datos personales, de acuerdo a la legislación comparada imponen penas privativas de libertad, penas inhabilitantes y penas pecuniarias.

2.2.8 Principios concernientes a la función protectora del derecho penal

Estos principios establecen límites al legislador sobre el contenido de la norma penal, con la finalidad de restringir el poder punitivo del Estado.

a) Principio de mínima intervención

Según Muñoz y García (2010), "(…) el Derecho penal sólo debe intervenir en los casos de ataques muy graves a los bienes jurídicos más importantes (…) Las perturbaciones más leves del orden jurídico son objeto de otras ramas del Derecho" (p. 72); por consiguiente, no podrán sancionarse desde la esfera del derecho penal, todos los hechos que transgreden la información y la protección de datos personales, sino solo aquellos que revisten mayor gravedad, con relación al daño generado a los titulares de los mismos; consiguientemente, el tratamiento de las cuestiones que ameritan menor ofensividad, corresponderán a otras áreas del derecho como la administrativa o civil.

b) Principio de subsidiariedad

El derecho penal interviene únicamente cuando fracasan las demás ramas del derecho, es decir, cuando la protección no satisface en su totalidad a las necesidades de prevención y motivación de la política criminal. Sobre el particular, Mir Puig (2008) expresa: "Para proteger los intereses sociales el Estado debe agotar los medios menos lesivos que el Derecho penal antes de acudir a éste, que en este sentido debe constituir un arma subsidiaria, una última ratio (…)" (p. 118).

c) Principio de carácter fragmentario

Para Mir Puig (2008): "(…) el Derecho penal no ha de sancionar todas las conductas lesivas de los bienes que protege, sino sólo las modalidades de ataque más peligrosas para ellos" (p. 118). El carácter fragmentario consiste en limitar la actuación del derecho penal a los ataques más violentos contra los bienes jurídicos de mayor relevancia.

Con relación a los datos personales, usualmente su tutela corresponde a sede administrativa y constitucional, pero las mismas han demostrado ser insuficientes en los casos más graves, dejando en indefensión a los titulares de los datos que sufrieron la vulneración de su derecho a la autodeterminación informativa y otros vinculados; a su vez, el citado factor genera impunidad porque los individuos que perpetran este tipo de atentados, únicamente cumplen sanciones administrativas leves, frente al daño que producen al titular de los datos personales, muchas veces de valor incuantificable.

d) El principio de exclusiva protección de bienes jurídicos

Conforme señala Mir Puig (2008), “Los intereses sociales que por su importancia pueden merecer la protección del Derecho se denominan «bienes jurídicos»” (p. 119), en dicho sentido, este principio constituye una limitante del poder punitivo del Estado en la medida en que su intervención se circunscribirá a la protección de determinados bienes jurídicos. Es así que la puesta en peligro o lesión de un bien jurídico constituye la parte sustancial de cualquier delito. Sólo se van a castigar penalmente conductas que lesionen o pongan en riesgo un bien jurídico, por lo cual este principio armoniza con el principio de ofensividad. La información y los datos, cuya categoría comprende a los datos personales; por su connotación actual, su vinculación con las TIC y su relación con la protección de otros bienes jurídicos, ameritan una tutela penal específica.

e) Principio de proporcionalidad de las penas

Sobre el particular, “No sólo es preciso que pueda «culparse» al autor de aquello que motiva la pena, sino también que la gravedad de ésta resulte proporcionada a la del hecho cometido - criterio éste que sirve de base a la graduación de las penalidades” (Mir Puig, 2008, p. 127).

En dicho contexto, la pena que establezca el legislador, deberá ser proporcional a la importancia social del hecho, no se admitirán penas o medidas de seguridad, exageradas o irracionales en relación con la prevención del delito.

A partir de lo anterior, se debe distinguir dos exigencias:

1) La pena debe ser proporcional al delito, y no excesiva.
2) La proporcionalidad se medirá en base a la importancia social del hecho.

La proporcionalidad deviene de la exigencia de una prevención general capaz de producir sus efectos en la colectividad. Así las cosas, el derecho penal debe ajustar la gravedad de las penas a la trascendencia que para la sociedad tienen los hechos reprochables y según el grado de afectación al bien jurídico.

2.2.9 Principios relativos a la forma y aplicación de la norma penal

Son aquellos que imponen límites al Estado respecto a la configuración de la norma penal; a los efectos de la presente investigación, se hará referencia al principio de legalidad.

- **Principio de Legalidad**

Este principio involucra que tanto el delito como la pena deben estar previstos en una ley, configura así la seguridad jurídica en un Estado. En virtud de su aplicación, se señalan los alcances de la norma jurídica, por lo cual sólo pueden ser sancionados como delitos, aquellas acciones que sean descritas como punibles en una determinada ley anterior a la acción. Este principio tiene su expresión en el aforismo “nullum crimen, nulla poena sine lege”, formulado por Feuerbach, cuyo origen se remonta a la revolución francesa.

Dicho principio es de aplicación del legislador y los operadores de justicia, encerrando en sí mismo las siguientes garantías:

- ✓ Garantía criminal, exige que el delito se halle determinado por la ley (nullum crimen sine lege).
- ✓ Garantía penal, requiere que la ley señale la pena que corresponda al hecho (nulla poena sine lege).
- ✓ Garantía jurisdiccional, exige que la existencia del delito y la imposición de la pena se determinen por medio de una sentencia judicial y según un procedimiento establecido legalmente.
- ✓ Garantía de ejecución, requiere que la ejecución de la pena se sujete a una ley que la regule.

Roxin (1997, pp.140 -141), señala cuatro consecuencias derivadas del principio de legalidad, representadas en forma de prohibiciones, de las cuales las dos primeras se dirigen al juez y las dos últimas al legislador, estas son:

- ✓ Prohibición de analogía (nullum crimen, nulla poena sine lege stricta): el trasladar una regla jurídica a otro caso no regulado en la ley por la vía del argumento de la semejanza, queda proscrito en el derecho penal. Se formula la distinción entre analogía legal y analogía jurídica, en el primer caso, la regla jurídica que va a trasladarse procede de un precepto concreto; en el segundo, procede de una idea jurídica que se desprende de varios preceptos.
- ✓ Prohibición del derecho consuetudinario para fundamentar o agravar la pena (nullum crimen, nulla poena sine lege scripta): resulta de la consecuencia de que la norma prescribe que la punibilidad sólo puede determinarse legalmente.

- ✓ Prohibición de la retroactividad (nullum crimen, nulla poena sine lege praevia): es inadmisible la retroactividad, sin que la punibilidad (en su clase o cantidad) no esté declarada y determinada legalmente antes del hecho.
- ✓ Prohibición de leyes penales y penas indeterminadas (nullum crimen, nulla poena sine lege certa): son inadmisibles la punibilidad y las penas indeterminadas, puesto que no permiten reconocer las características de la conducta punible, al no estar legalmente determinada; de similar manera, sería anticonstitucional y nulo no precisar qué pena y cuantía se impondrá como sanción.

A su vez, se imponen ciertos requisitos a la norma jurídica, conocidos como la triple exigencia de lex praevia, lex scripta y lex stricta, consistentes en:

- ✓ Lex praevia, tiene su expresión en la prohibición de retroactividad de las leyes que castigan nuevos delitos o agravan su punición, el individuo en su actuar debe tener certeza respecto a si incurrirá en algún delito, aspecto relacionado con el principio de seguridad jurídica. Cabe señalar, que tiene su excepción cuando se trata de retroactividad de leyes penales más favorables, que suprimen delitos o atenúan las penas.
- ✓ Lex scripta, involucra que la norma penal debe ostentar el rango de ley, emanada del órgano legislativo en su condición de representante del pueblo, como garantía política del principio de legalidad.
- ✓ Lex stricta, impone un cierto grado de precisión de la ley penal y excluye la analogía en cuanto perjudique al reo (analogía in malam partem). Da lugar al denominado mandato de determinación, que exige que la ley determine de forma suficientemente diferenciada las distintas conductas punibles y las penas que pueden acarrear. Constituye éste un aspecto material del principio de legalidad.

- **Principio de taxatividad**

De lo anterior se desprende el conocido principio de taxatividad, el cual postula que la ley penal debe describir con la mayor exactitud posible las conductas que están prohibidas y constituyen delitos, así como las sanciones aplicables. Sobre el particular, Carbonell (2006) señala: “La taxatividad es una especie del genérico principio de legalidad en materia penal y tiene por objeto preservar la certeza jurídica (que a su vez es una especie de la seguridad jurídica) y la imparcialidad en la aplicación de la ley penal” (p.38). Por su parte Ferrajoli, (1995), expresa:

> (…) puede ser caracterizado ahora como una regla semántica metalegal de formación de la lengua legal que prescribe al legislador penal: a) que los términos usados por la ley para designar las figuras de delito sean dotados de extensión determinada, por donde sea posible su uso como predicados “verdaderos de los" hechos empíricos por ellos denotados; b) que con tal fin sea connotada su intención con palabras no vagas ni valorativas, sino lo más claras y precisas posible; c) que, en fin, sean excluidas de la lengua legal las antinomias semánticas o cuando menos que sean predispuestas normas para su solución. De ahí se sigue, conforme a esta regla, que las figuras abstractas de delito deben ser connotadas por la ley mediante propiedades o características esenciales idóneas para determinar su campo de denotación (o de aplicación) de manera exhaustiva, de forma que los hechos concretos que entran allí sean denotados por ellas en proposiciones verdaderas, y de manera exclusiva, de modo que tales hechos no sean denotados también en proposiciones contradictorias por otras figuras de delito connotadas por normas concurrentes. (p. 121)

En los ordenamientos jurídicos penales, existen delitos que están más correctamente descritos que otros y esto depende de la precisión de la descripción, siendo en muchas ocasiones un ejemplo de ausencia de taxatividad. Por tanto, el principio de taxatividad exige precisión a la hora de formular los supuestos de hecho contenidos en las normas penales. Y esta precisión viene dada por dos vías diferenciadas:

- ✓ Reducir la imprecisión de los conceptos que se utilizan para fijar comportamientos que se van a considerar como prohibidos, por considerarse que los mismos dan lugar a una conducta delictiva.
- ✓ Lograr la preponderancia de los conceptos descriptivos frente a los conceptos valorativos para la determinación de un delito concreto.

Por los fundamentos vertidos, el principio de legalidad no conforma solo una exigencia de seguridad jurídica, sino la garantía política de que el ciudadano no podrá verse sometido a penas que no admita la sociedad a través de sus representantes del Órgano Legislativo. Así también, en aplicación del principio de taxatividad se evitará la construcción de normas penales genéricas, ambiguas o indeterminadas, debiendo observarse una formulación lo más clara y precisa posible.

2.3 Instrumentos internacionales referidos a la protección de datos personales

El derecho a la protección de datos no se encuentra reconocido expresamente en instrumentos internacionales de los Sistemas Universal e Interamericano de Derechos Humanos, ya que la mayor parte de ellos fueron aprobados con anterioridad a que se susciten

problemas jurídicos en este ámbito. Su debate internacional inició en 1968, durante la celebración de la Conferencia Internacional de Derechos Humanos de Teherán, organizada por Naciones Unidas, en la que se consideraron los límites que una sociedad democrática debía imponer para proteger los derechos humanos frente al creciente uso de la tecnología (Cerda, 2003, pp. 55-56). En el Sistema Europeo, el reconocimiento de este derecho se manifestó por primera vez en el ámbito del Consejo de Europa y se plasmó en el Convenio N° 108 de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. No obstante, la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y la Convención sobre los Derechos del Niño, contienen disposiciones aplicables a la protección de datos personales desde la perspectiva del resguardo de los derechos a la privacidad, dignidad, honra y reputación.

a) Declaración Universal de Derechos Humanos

La Declaración Universal de Derechos Humanos, aprobada y proclamada por la Asamblea General de las Naciones Unidas del 10 de diciembre de 1948, mediante Resolución N°217 A (III), confiere a la privacidad el reconocimiento de derecho humano fundamental, expresando en su Artículo 12, que: “Nadie será objeto de injerencias arbitrarias en su vida privada su familia su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

b) Pacto Internacional de Derechos Civiles y Políticos

El Pacto Internacional de Derechos Civiles y Políticos, entró en vigor el 23 de marzo de 1976, fue ratificado en Bolivia por Ley Nº2119 promulgada el 11 de septiembre de 2000, y de igual manera establece una protección para el derecho a la privacidad en su Artículo 17 numerales 1 y 2:

> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

c) Convención Americana sobre Derechos Humanos

El también denominado Pacto de San José de Costa Rica, fue suscrito como resultado de la Conferencia Especializada Interamericana de Derechos Humanos, el 22 de noviembre de

1969 en la ciudad de San José, Costa Rica y entró en vigor el 18 de julio de 1978, fue ratificado en Bolivia por Ley Nº1430 promulgada el 11 de febrero de 1993.

En su Artículo 11, manifiesta:

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

d) Convención sobre los derechos del niño

Es un tratado internacional que reconoce los derechos humanos de los menores de 18 años, fue aprobada el 20 de noviembre de 1989 por la Asamblea General de la Organización de Naciones Unidas y establece que los Estados Partes deben asegurar que los niños y adolescentes sean beneficiarios de una serie de medidas particulares de asistencia y protección. Esta Convención, ratificada por Bolivia mediante Ley N°1152 de 14 de mayo de 1990; en su Artículo 16 determina:

> 1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.
> 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

Estos instrumentos internacionales forman parte del bloque de constitucionalidad y obligan al Estado boliviano a su aplicación, han sido recogidos como sustrato esencial de un sinnúmero de jurisprudencia constitucional, en particular respecto a los derechos de autodeterminación informativa, privacidad e intimidad, en el marco de un orden constitucional progresista y garante de los derechos humanos, que otorga una aplicación preferente a tratados y convenios internacionales cuando prevean normas más favorables, en observancia de los Artículos 13 parágrafos II y IV; 256 parágrafos I y II y 410 parágrafo II de la Constitución Política del Estado.

e) Otros instrumentos

Las Tecnologías de Información y Comunicación, su llegada vertiginosa a un mayor número de usuarios y su expansión imparable, han motivado que la protección de datos personales adquiera trascendencia a nivel internacional, originando diversos pronunciamientos vinculantes y no vinculantes de organismos internacionales que reconociendo su capital

preeminencia, emitieron directrices a considerarse por los distintos estados alrededor del orbe. Estos documentos, incluyen aspectos referentes al adecuado ejercicio y resguardo del derecho a la privacidad, la información y la protección de datos personales, entre los que destacan la formulación de leyes que establezcan sanciones para el caso de violación de los mismos, los mecanismos para su restitución, así como un régimen y medidas de reparación de daños y perjuicios.

Tabla N°2

Instrumentos internacionales referidos a la protección de datos personales

AÑO	INSTRUMENTO – ESTANDAR	ORGANISMO QUE FORMULA Y/O APRUEBA	FINALIDAD
1980	Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales. Posteriormente fue actualizada el 2013.	Organización para la Cooperación y el Desarrollo Económicos (OCDE).	Promueve la protección de la privacidad y las libertades individuales en relación con los datos personales, a través de la aprobación de legislación nacional adecuada; procurando las oportunas sanciones y soluciones en caso de incumplimiento. (Cuarta Parte)
1981	Convenio N° 108 del Consejo de Europa para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. El Convenio fue actualizado el 2018.	Consejo de Europa.	Garantiza el respeto de derechos y libertades fundamentales, incluido el derecho a la vida privada en relación al tratamiento automatizado de datos de carácter personal. Determina la protección de datos sensibles y el establecimiento de sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno y que cada Parte, puede conceder una protección más amplia que la prevista en el Convenio. (Artículos 6, 10 y 11).
1990	Resolución N° 45/95 Principios rectores para la reglamentación de los ficheros computarizados de datos personales.	Asamblea General de la Organización de Naciones Unidas (ONU).	Establece principios relativos a las garantías mínimas que deben contener las legislaciones nacionales en materia de datos personales. Destaca los principios de legalidad, seguridad y de no discriminación que incoan a no registrar datos sensibles. En caso de violación de las disposiciones de la legislación interna, determina que se prevean sanciones penales y de otro tipo. Los principios son aplicables también a ficheros manuales. (numerales 1, 5, 7 y 8)
2004	Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC).	Foro de Cooperación Económica Asia Pacífico (APEC).	Uno de sus objetivos fundamentales es la prevención del mal uso de la información personal a través de esfuerzos

			autorreguladores, campañas de educación, leyes, regulaciones y mecanismos de seguridad para prevenir daño a los individuos por la recolección ilegal y el mal uso de su información personal. Los remedios para violaciones a la privacidad deben ser proporcionales a la probabilidad y a la severidad de cualquier daño y sensibilidad de la información por la recolección o uso de la información personal. (numerales 22, 31 y 38)
2005	Agenda de Túnez para la Sociedad de la Información.	Organización de Naciones Unidas - Unión Internacional de Telecomunicaciones.	Insta a enjuiciar la ciberdelincuencia, destacando la necesidad de concebir para ello instrumentos eficaces y eficientes, exhortando a garantizar la protección de la información, privacidad y datos personales, mediante la adopción de medidas legislativas pertinentes. (apartados 40 y 46)
2009	Estándares Internacionales sobre protección de datos personales y privacidad. Resolución de Madrid.	Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.	Impulsa la promoción de medidas adecuadas para facilitar el acceso de los interesados a los procesos judiciales o administrativos, para la obtención de la reparación de daños y/o perjuicios. Incluye la protección de datos sensibles y el establecimiento de responsabilidad por daños y perjuicios morales y materiales, como consecuencia de vulneración de la normativa de protección de datos, la cual existirá sin perjuicio de las sanciones penales, civiles o administrativas previstas. (apartados 13 y 25)
2013	Resolución N° A/RES/68/167 “El derecho a la privacidad en la era digital” de la Asamblea General de Naciones Unidas. Posteriormente actualizada el 2016, mediante Resolución A/C.3/71/L.39	Organización de Naciones Unidas (ONU).	Pone en relieve la recopilación ilícita o arbitraria de datos personales como un acto de intrusión grave, que viola el derecho a la privacidad. Exhorta a los estados miembros, a examinar sus procedimientos, prácticas y legislación con miras a afianzar el derecho a la privacidad, su respeto y protección a través de medidas para poner fin a las violaciones, cerciorándose que la legislación nacional se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos. (numeral 4)

			La actualización del 2016, exhorta además a aplicar una legislación adecuada, con sanciones y recursos eficaces que protejan a las personas contra las prácticas que atentan contra el derecho a la privacidad, la recopilación y el tratamiento ilegal y arbitrario, retención o el uso de datos personales por particulares, empresas y organizaciones privadas. (numeral 5 inciso f)
2015	Principios de la OEA sobre la privacidad y la protección de datos personales.	Organización de Estados Americanos (OEA).	Enuncia principios a ser incluidos en las legislaciones de los estados, entre estos los principios de: protección y seguridad, el de responsabilidad y el de protección de datos sensibles; para evitar daños a las personas por accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación de sus datos personales. Asimismo, refiere la incidencia creciente de intrusiones externas ("violaciones de los datos personales"), la cual suscita preocupaciones relacionadas con el ámbito penal, por lo que incoa a imponer sanciones a los controladores de datos, que sean proporcionales al grado del perjuicio o riesgo y su indemnización. (Principios Seis: protección y seguridad, Nueve: datos personales sensibles y Diez: responsabilidad)
2017	Estándares de Protección de Datos Personales para los Estados Iberoamericanos.	Red Iberoamericana de Protección de Datos.	Formula directrices, principios y derechos para la protección de datos personales a desarrollarse en la normativa de los países iberoamericanos, que incluyan procedimientos de reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos los derechos de los individuos. Incoa el establecimiento de un régimen de medidas correctivas, sanciones y reparación de daños y perjuicios. (numeral 43)

Fuente: elaboración propia (2019)

En función a lo descrito, es posible afirmar que la incursión de las Tecnologías de Información y Comunicación en la actividad delictiva a escala global, ha atraído la atención de los citados organismos internacionales, en el afán de encontrar soluciones tendientes a combatir las

nuevas formas de criminalidad que atentan contra la información y datos personales, rebasando el ámbito local y adoptando un alcance transnacional.

2.4 Iniciativas de la OCDE, ONU, OEA y Consejo de Europa

- **Organización para la Cooperación y el Desarrollo Económicos (OCDE)**

Hacia el año 1983, la Organización para la Cooperación y el Desarrollo Económicos (OCDE), emprendió un estudio que consideró la armonización de leyes penales en el plano internacional, para la lucha contra el uso indebido de programas computacionales. En 1986, emitió el Informe denominado Delitos de informática: análisis de la normativa jurídica; el cual identifica la normativa vigente y las propuestas de reforma de varios estados miembros recomendando una lista mínima de ejemplos para incluir en la legislación penal (Jimeno, 2019, p. 70).

Más adelante en 1992, este organismo, elaboró un conjunto de normas denominado Guías de Seguridad de los Sistemas de Información, con la intención de instituir directrices y un marco de seguridad de los sistemas informáticos para los Estados y sector privado, estos lineamientos fueron actualizados el 2002 y confluyen en principios complementarios (concientización, responsabilidad, respuesta, ética, democracia, evaluación del riesgo, diseño e implementación de seguridad, administración de la seguridad y reevaluación) a ser aplicados en la esfera política y operacional.

A su vez, en dicho documento, la OCDE reconoce que los datos e información almacenados y transmitidos a través de los sistemas de información y redes están expuestos a: accesos, usos, apropiación y alteración no autorizados, requiriendo de mecanismos apropiados para su salvaguarda; en consecuencia, incoa el establecimiento o modificación de políticas, prácticas, medidas y procedimientos para la adopción y promoción de una cultura de seguridad (Organización para la Cooperación y Desarrollo Económicos - OCDE, 2002).

- **Organización de Naciones Unidas (ONU)**

Por su parte, la Organización de Naciones Unidas (ONU), a partir de 1955, viene realizando Congresos para la prevención del delito y justicia penal, los cuales son celebrados cada 5 años. En ese marco, durante el Octavo Congreso realizado en La Habana - Cuba en 1990, se destacó que la delincuencia informática es consecuencia del empleo de datos en las economías y burocracias de los distintos países del orbe.

La ONU reconoce determinados delitos informáticos, entre los cuales, en función al objeto de la presente investigación, es pertinente resaltar los siguientes:

> **a) Manipulación de los datos de entrada.** Configura un tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común.
> **b) Falsificaciones informáticas, como objeto.** Consiste en alterar datos de los documentos almacenados en forma computarizada.
> **c) Acceso no autorizado a servicios y sistemas informáticos.** Puede darse por móviles diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Estos delitos, resultan aplicables a la esfera de los datos personales, puesto que se está frente a conductas que giran en torno a información susceptible de manipulación, acceso y/o alteración, perpetrados con finalidades ilícitas. Desde esa perspectiva, los delitos citados, constituyen lineamientos para el desarrollo de normativa referida a la categoría de datos personales.

- **Organización de Estados Americanos (OEA)**

La Organización de los Estados Americanos (OEA), también se ha manifestado creando una Estrategia Interamericana Integral de Seguridad Cibernética, que involucra:

> 1. La Declaración de Montevideo (CICTE/DEC. 1/04 rev. 3) de 2004, documento que expresa el compromiso de identificar y combatir las amenazas terroristas emergentes, independientemente de su origen o motivación, incluyendo las amenazas a la seguridad cibernética.
> 2. La Resolución N° AG/RES.2004 (XXXIV-O/04) de 8 de junio de 2004, que resuelve adoptar la: Estrategia Interamericana Integral de Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética.

La Estrategia, que se desarrolla en el Anexo “A” de la citada Resolución, se basa en acciones a implementar por parte de:

> a) El Comité Interamericano contra el Terrorismo (CICTE), a través de la Formación de una Red Interamericana de Vigilancia y Alerta para la rápida divulgación de

información sobre seguridad cibernética y la respuesta a crisis, incidentes y amenazas a la seguridad informática.

b) La Comisión Interamericana de Telecomunicaciones (CITEL), mediante la identificación y adopción de normas técnicas para una arquitectura segura de Internet.

c) La Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA), cuya misión radica en asegurar que los Estados Miembros de la OEA cuenten con los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información.

Esta última instancia, por medio de las iniciativas del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, tiene como objetivo asegurar que los Estados Miembros de la OEA adopten una legislación en la materia para brindar protección adecuada a sus ciudadanos a través de Leyes sustantivas, estableciendo prohibiciones de carácter penal a los ataques contra la confidencialidad, integridad y seguridad de los sistemas informáticos, incorporando como ilícitos conductas inherentes acceso a computadoras sin autorización, la intercepción ilícita de datos, la interferencia con la disponibilidad de sistemas informáticos, el robo y el sabotaje de datos. A partir de lo anterior, estas instancias vienen desarrollado sus actividades y trabajando para prevenir y combatir la criminalidad cibernética.

- **Consejo de Europa – Convenio sobre la ciberdelincuencia**

El Consejo de Europa el 23 de noviembre de 2001 en Budapest, aprobó el Convenio sobre la Ciberdelincuencia que constituye el primer tratado internacional para homogenizar la normativa sustantiva y adjetiva penal emergente de delitos cibernéticos y optimizar la cooperación entre los estados miembros. El acuerdo que entró en vigor el 1 de julio de 2004, en su preámbulo alude a la importancia del derecho a la protección de datos personales, en base al Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales, exteriorizando la creciente preocupación en torno a los cambios provocados por la digitalización, la convergencia y la globalización de la redes informáticas, así como el riesgo de que dichas herramientas y la información electrónica sean utilizadas para la comisión de delitos.

Este instrumento de carácter vinculante, describe ilícitos informáticos a incorporarse en la normativa penal de los países miembros, e incoa a tipificar los siguientes delitos que tienden transgredir la información y los datos:

(…) Artículo 2. Acceso ilícito.

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.
> (…) Artículo 4. Ataques a la integridad de los datos.
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo de actos que dañe, borre, deteriore, altere o suprima datos informáticos.
> 2. Las partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.
> Artículo 5. Ataques a la integridad de sistema
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Cabe señalar que el Convenio, no solo pretende la implementación de nuevos tipos penales, sino también el establecimiento de facultades de investigación más robustas para la persecución de los ciberdelincuentes; además se encuentra abierto para la libre adhesión de otros estados del orbe. Al presente, son más de 56 países que han suscrito el Convenio, en Latinoamérica son parte del mismo: Chile, Colombia, Paraguay, Costa Rica, República Dominicana, Panamá, Argentina y Perú.

2.5 La protección de datos personales en la legislación boliviana

2.5.1 Constitución Política del Estado

Es innegable la relación que prima entre la Constitución y el derecho penal, la primera, como expresión de los principios esenciales que inspiran el ordenamiento jurídico e irradian todas las normas que lo componen; mientras que el segundo, define a través de la ley penal los delitos y faltas como presupuesto de la aplicación de la norma suprema a través de la tutela de los valores y principios básicos de la convivencia social.

Sobre esta vinculación e influencia, Landa (2013), expresa lo siguiente:

> (…) el derecho constitucional incide en el derecho penal, por un lado, respecto de la privación de la libertad sobre la base del principio de legalidad. Esto como consecuencia de que el poder punitivo del Estado recae directamente sobre la persona, cuyo respeto a su dignidad es el fin

> supremo de la sociedad y el Estado (…) dicho poder no puede ser ejercido arbitrariamente, sino dentro de los valores superiores, principios constitucionales y derechos fundamentales que la Constitución reconoce. (p.23)

La Constitución Política del Estado Plurinacional de Bolivia, conforme a su Artículo 8 parágrafo II, asume como valores en que se sustenta el Estado: la igualdad, la dignidad, la libertad, el respeto, la armonía, la transparencia, el bienestar común, la responsabilidad y justicia social.

Asimismo, en su Artículo 9, refiere que son fines y funciones esenciales del Estado:

> 1. Constituir una sociedad justa y armoniosa, cimentada en la descolonización, sin discriminación ni explotación, con plena justicia social, para consolidar las identidades plurinacionales.
> 2. Garantizar el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades, y fomentar el respeto mutuo y el diálogo intracultural, intercultural y plurilingüe.
> (…) 4. Garantizar el cumplimiento de los principios, valores, derechos y deberes reconocidos y consagrados en esta Constitución.

Por su parte, el Artículo 14, del texto constitucional en sus parágrafos I, II y III, señala:

> I. Todo ser humano tiene personalidad y capacidad jurídica con arreglo a las leyes y goza de los derechos reconocidos por esta Constitución, sin distinción alguna.
> II. El Estado prohíbe y sanciona toda forma de discriminación fundada en razón de sexo, color, edad, orientación sexual, identidad de género, origen, cultura, nacionalidad, ciudadanía, idioma, credo religioso, ideología, filiación política o filosófica, estado civil, condición económica o social, tipo de ocupación, grado de instrucción, discapacidad, embarazo, u otras que tengan por objetivo o resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos de toda persona.
> III. El Estado garantiza a todas las personas y colectividades, sin discriminación alguna, el libre y eficaz ejercicio de los derechos establecidos en esta Constitución, las leyes y los tratados internacionales de derechos humanos.

La Norma Fundamental, también tutela el derecho a la integridad psicológica prohibiendo los tratos crueles, inhumanos, degradantes o humillantes y prevé la obligación del Estado de adoptar las medidas necesarias para prevenir, eliminar y sancionar toda acción u omisión que tenga por objeto degradar la condición humana, causar dolor y sufrimiento físico, sexual o psicológico, tanto en el ámbito público como privado (Artículo 15, parágrafos I y III).

De igual manera, en sus Artículos 21, numerales 2, 3 y 6 recoge los derechos a la privacidad, intimidad, honra, honor, propia imagen, dignidad, libertad de pensamiento, espiritualidad, religión y culto, y el derecho a acceder a la información, este último también reconocido en el Artículo 106 parágrafo I. En estrecha relación, el Artículo 22 de la citada Norma Fundamental determina: “La dignidad y la libertad de la persona son inviolables. Respetarlas y protegerlas es deber primordial del Estado”. En su Artículo 25, salvaguarda el secreto de las comunicaciones privadas en todas sus formas, la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, que sólo podrán ser incautados en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente. Respecto a los derechos de los menores de edad, la Constitución boliviana establece:

> Artículo 58.
> (…) Las niñas, niños y adolescentes son titulares de los derechos reconocidos en la Constitución, con los límites establecidos en ésta, y de los derechos específicos inherentes a su proceso de desarrollo; a su identidad étnica, sociocultural, de género y generacional; y a la satisfacción de sus necesidades, intereses y aspiraciones.
> Artículo 59.
> (…) V. El Estado y la sociedad garantizarán la protección, promoción y activa participación de las jóvenes y los jóvenes en el desarrollo productivo, político, social, económico y cultural, sin discriminación alguna, de acuerdo con la ley.
> Artículo 60.
> Es deber del Estado, la sociedad y la familia garantizar la prioridad del interés superior de la niña, niño y adolescente, que comprende la preeminencia de sus derechos, la primacía en recibir protección y socorro en cualquier circunstancia, la prioridad en la atención de los servicios públicos y privados, y el acceso a una administración de justicia pronta, oportuna y con asistencia de personal especializado.
> Artículo 61.
> I. Se prohíbe y sanciona toda forma de violencia contra las niñas, niños y adolescentes, tanto en la familia como en la sociedad.
> II. Se prohíbe el trabajo forzado y la explotación infantil. Las actividades que realicen las niñas, niños y adolescentes en el marco familiar y social estarán orientadas a su formación integral como ciudadanas y ciudadanos, y tendrán una función formativa. Sus derechos, garantías y mecanismos institucionales de protección serán objeto de regulación especial.

Bajo este paraguas normativo, los niños y adolescentes ameritan una salvaguarda especial, aspecto extensible a la protección de sus datos personales, máxime si se tiene presente que en la actualidad constituyen un sector altamente enlazado a las Tecnologías de Información y Comunicación.

Los anteriores artículos se encuentran vinculados a la protección de datos personales, respecto a aquellos datos de carácter general, así como los que conciernen a menores de edad, y también los datos sensibles que pueden acarrear situaciones discriminatorias, todo con asidero medular en la dignidad del individuo, convirtiéndose este último en el derecho que legitima y cimenta los otros derechos fundamentales.

En lo concerniente al derecho de autodeterminación informativa, la Constitución Política del Estado lo incluye en el texto del Artículo 130 referente a la Acción de Protección de Privacidad, como garantía para la defensa de la intimidad y privacidad personal o familiar, propia imagen, honra y reputación, cuando la persona individual o colectiva crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados. Cabe añadir que el Tribunal Constitucional, en ejercicio de sus atribuciones, en el ámbito de la resolución de Recursos de Habeas Data y Acciones de Protección de Privacidad ha emitido a través de sus Sentencias Constitucionales, líneas jurisprudenciales para la protección de los datos personales, reconociendo el carácter de derecho humano de la autodeterminación informativa o informática como también la denomina, expresando lo siguiente:

> (…) 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 (referido a los derechos fundamentales a la intimidad y la privacidad de la persona). (SC N° 0127/2010-R de 10 de mayo de 2010, SSCCPP Nrs. 0080/2014-S2 de 4 de noviembre de 2014 y 2175/2012 de 8 de noviembre de 2012)

Así también, en su Sentencia Constitucional N°0127/2010-R, el nombrado Tribunal ha desarrollado el entendimiento de que la Acción de Protección de Privacidad tiene por objeto la defensa de la autodeterminación informativa, constituyéndose en una vía instrumental que precautela los derechos de la persona para que pueda acceder al conocimiento de los datos e informaciones referidos a su vida privada o íntima, obtenidos y almacenados en los bancos de datos públicos o privados, y saber el uso que se le dará a esa información; reconociendo la categoría de derecho a la autodeterminación informativa, como: “(…) facultad de una persona para conocer, actualizar, rectificar o cancelar la información existente en una base de datos pública o privada (…)” (SSCCPP Nrs. 0089/2014-S2 de 4 de noviembre de 2014 y 0332/2015-S1 de 6 de abril de 2015).

En consonancia, Rivera (2010), expresa que la Acción de Protección de Privacidad: "(…) tutela el derecho a la autodeterminación informativa, ampliando sus alcances a la protección de los derechos a la imagen, a la honra y a la reputación" (p. 676). A su vez, la Constitución consagra el principio de progresividad de los derechos e incluye una cláusula abierta respecto a los mismos, otorgándoles igual jerarquía y regulando su interpretación conforme a los tratados internacionales de derechos humanos ratificados por Bolivia, tal como se establece en su Artículo 13, que enuncia:

> I. Los derechos reconocidos por esta Constitución son inviolables, universales, interdependientes, indivisibles y progresivos. El Estado tiene el deber de promoverlos, protegerlos y respetarlos.
> II. Los derechos que proclama esta Constitución no serán entendidos como negación de otros derechos no enunciados.
> III. La clasificación de los derechos establecida en esta Constitución no determina jerarquía alguna ni superioridad de unos derechos sobre otros.
> IV. 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.

En este sentido, existe una inserción explícita cuando los ordenamientos constitucionales contemplan expresamente los derechos humanos y les asignan una supremacía constitucional, por otra parte, concurre una inserción implícita, cuando a través de las cláusulas abiertas o numerus apertus son reconocidos derechos no contenidos en el texto constitucional (León y Wong, 2015, p. 103). Por su parte, el Artículo 109 de la Norma Fundamental, determina en sus parágrafos I y II, que todos los derechos reconocidos en la misma, son directamente aplicables y gozan de iguales garantías para su protección, los cuales sólo podrán ser regulados por la ley.

En concordancia, en su Artículo 256 parágrafos I y II le atribuye un carácter de supraconstitucionalidad a los tratados e instrumentos internacionales en materia de derechos humanos firmados, ratificados o a los que se hubiera adherido el Estado, siempre que declaren derechos más favorables, regulando además que los derechos reconocidos en la Constitución serán interpretados de acuerdo a estos tratados e instrumentos, cuando prevean normas más favorables.

De lo anterior, es posible afirmar que la tutela constitucional en Bolivia alcanza al derecho de autodeterminación informativa, a partir de lo cual es viable su protección a través del desarrollo de leyes específicas en distintos ámbitos y desde luego en la esfera penal. El uso de las TIC, no se caracteriza únicamente por el potencial de almacenamiento y transmisión de datos, sino también por la capacidad de transformación de la información, de esta forma, su trascendencia radica en que se pueden reconstruir las actividades de una persona, tener conocimiento de sus creencias, sus opiniones políticas, sus movimientos financieros, sus actividades comerciales o sus preferencias sexuales, entre tantos otros, a partir de registros simples por conexión a otros datos, obteniéndose nueva información, denominada, de segundo grado.

Desde esta representación, en el marco de las TIC, el derecho a la intimidad adquiere una nueva dimensión, resultando insuficiente concebir a la intimidad desde su status negativo, como defensa de intromisiones en la vida privada, siendo necesario una concepción desde un status positivo, como el derecho a controlar el flujo de información del individuo, entrañando la facultad de disposición sobre la revelación y el uso de los datos personales en todas las fases del procesamiento de los mismos, que van desde su recolección, acumulación, transmisión, rectificación, hasta su cancelación.

2.5.2 Código Civil

El Código Civil de 6 de agosto de 1975, en sus Artículos 16, 17 y 18, contiene preceptos sobre los derechos a la imagen, honor e intimidad:

> Artículo 16. (DERECHO A LA IMAGEN).
> I. Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por la ley, que el juez haga cesar el hecho lesivo.
> II. Se comprende en la regla anterior la reproducción de la voz de una persona.
> Artículo 17. (DERECHO AL HONOR). Toda persona tiene derecho a que sea respetado su buen nombre. La protección al honor se efectúa por este Código y demás leyes pertinentes.
> Artículo 18. (DERECHO A LA INTIMIDAD). Nadie puede perturbar ni divulgar la vida íntima de una persona. Se tendrá en cuenta la condición de ella. Se salva los casos previstos por la ley.

Este cuerpo legal proporciona los parámetros para considerar qué se entiende por imagen, honor e intimidad, en su calidad de derechos vinculados a la autodeterminación informativa.

Desde esta concepción, la imagen también constituye un dato personal, lo mismo que las grabaciones que contengan registros de voz, que actualmente pueden hallarse contenidas en un sinnúmero de medios y dispositivos tecnológicos.

Los derechos al honor, intimidad e imagen se encuentran ligados a la dignidad humana, reconocida también como derecho fundamental y como eje central, fuente y sustrato para la afirmación de otros derechos, que no pueden ser trastocados por particulares ni por entes públicos o privados. En consecuencia, el legislador boliviano, ya en la vía civil otorga protección a estos derechos y por medio de ellos la tutela es extensiva a los datos personales.

2.5.3 Código Penal

El Código Penal Boliviano, no contempla figuras específicas para la protección de datos personales; no obstante, prevé conductas delictivas relacionadas a delitos informáticos en el Capítulo XI, cuya inclusión operó mediante la reforma introducida por la Ley Nº1768 de Modificaciones del Código Penal del 10 de marzo de 1997, que incorporó los siguientes Artículos:

> Artículo 363 bis. (MANIPULACIÓN INFORMÁTICA). El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.
>
> Artículo 363 ter. (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

Ambos artículos consideran a los sistemas informáticos dentro de la configuración del tipo penal, coligiéndose de su redacción que le otorgan a las operaciones de procesamiento y transferencia una connotación significativa, cuyo valor radica en el contenido de la información ya sea personal, patrimonial o de cualquier otra índole; bajo este razonamiento, intrínsecamente estas figuras penales también involucran a datos de carácter personal. En los dos tipos penales citados, se requiere para su comisión un sistema informático, toda vez que se perpetran por medio del uso de las computadoras o soportes informáticos, y en contra del sistema, es decir la conducta delictiva atenta y lesiona a la información.

Respecto al Artículo 363 bis, este tipo penal contempla la manipulación, que constituye un manejo de datos informáticos y opera durante su procesamiento o transferencia, conocida también como cesión o transmisión, cuando se da lugar a un resultado incorrecto o se evita un proceso cuyo resultado hubiere sido correcto, en ambos casos vinculado a una transferencia patrimonial en perjuicio de un tercero. El sujeto activo es indeterminado, por lo que comprende a cualquier persona, mientras que el sujeto pasivo no queda claramente establecido, toda vez que señala a un "tercero", que bien podría ser el titular de la información e incluso otra persona, en el entendido que la afectación trasciende a la esfera de individuo, pudiendo generar daños a instituciones privadas y al Estado. Es un tipo de resultado, ya que para que se perfeccione debe producirse una transferencia patrimonial que cause perjuicio.

Cabe señalar que no considera el procesamiento de datos mediante un acceso no autorizado, tampoco la posibilidad de vulneración o violación de los sistemas de seguridad. Protege el patrimonio, más que la información propiamente dicha, en este sentido, Villamor (2007) señala: "El bien jurídico tutelado es el patrimonio y, colateralmente, la fe pública, es decir la confianza que se debe tener en los datos informáticos" (p. 339).

Por su parte, el Artículo 363 ter, prevé y sanciona las conductas de acceso, apoderamiento, utilización, modificación, supresión o inutilización de datos sin autorización y contenidos en soportes informáticos, estableciendo como exigencia para su consumación la producción de un perjuicio al titular de la información, aunque no especifica la naturaleza de dicho menoscabo, que pudiera ser material o inmaterial; es también un delito de resultado que requiere la verificación de la conducta. En la categoría de sujeto activo comprende a cualquier persona y en cuanto al sujeto pasivo al titular de la información; en líneas generales, tampoco hace referencia expresa a datos personales; empero, de acuerdo a la Exposición de Motivos de 1997, se justifica su inclusión para proteger datos informáticos de carácter reservado, contra el uso indebido de terceros, en virtud del progreso tecnológico que genera nuevas formas de criminalidad, en las que el objeto del delito no consiste en cosas materiales sino en datos de naturaleza inmaterial.

En ambos casos se advierte que no incluyen el manejo de datos en otros soportes que no sean informáticos; asimismo, están orientados de manera general a ilícitos informáticos más no así específicamente a la protección de datos personales; en consecuencia, son amplios y generales, exentos de manera tangencial a la problemática vigente acerca de los datos personales y a la relevancia que éstos han adquirido en el contexto actual, que incluso amerita

una protección particular para el caso de los datos personales sensibles y de menores de edad, por su afectación a las esferas de la privacidad e intimidad.

Otro aspecto debatible, es la pena que señalan los citados tipos penales, siendo así que el Artículo 363 bis., establece la reclusión de uno a cinco años y multa de sesenta a doscientos días; mientras que el Artículo 363 ter. únicamente sanciona con la prestación de trabajo hasta un año o multa de hasta doscientos días, es decir, salvo la pena de reclusión, imponen un castigo en beneficio de la comunidad o de carácter pecuniario de acuerdo a los Artículos 28 y 29 del Código Penal referidos a las penas de prestación de trabajo y días multa, consideradas como penas exiguas que no posibilitan que la prevención general de la norma sea efectiva, máxime si se trae a colación los perjuicios y el daño moral y económico que emanan de estos ilícitos.

Del análisis anterior se desprende que, si bien en su momento la inclusión de los citados artículos fue novedosa para su época, actualmente se encuentran desactualizados y al margen del contexto de la sociedad globalizada de la que es parte Bolivia, y de la Era Digital caracterizada por el influjo de las Tecnologías de Información y Comunicación que han propiciado no solo el surgimiento de nuevos derechos, sino también de nuevas formas de delinquir.

Sobre los datos personales sensibles, la actual norma sustantiva penal, tampoco contempla un tipo penal especifico; sin embargo, mediante Ley Integral contra la trata y tráfico de personas N°263 de 31 de julio de 2012, se modificó el Artículo 323 bis (PORNOGRAFÍA) de Código Penal, con el siguiente texto:

> I. Quien procure, obligue, facilite o induzca por cualquier medio, por si o tercera persona a otra que no dé su consentimiento a realizar actos sexuales o de exhibicionismo corporal con fines lascivos con el objeto de video grabarlos, fotografiarlos, filmarlos, exhibirlos o describirlos a través de anuncios impresos, transmisión de archivos de datos en red pública o de comunicaciones, sistemas informáticos, electrónicos o similares, será sancionada con pena privativa de libertad de diez (10) a quince (15) años.
>
> Igual sanción será impuesta cuando el autor o participe reproduzca o almacene, distribuya o venda material pornográfico.
>
> II. La pena privativa de libertad será agravada en un tercio cuando:
>
> 1. La víctima sea niño, niña o adolescente o persona con discapacidad.
> 2. La autora o el autor sea cónyuge, conviviente, padre, madre o la persona que ejerza algún tipo de autoridad o responsabilidad legal sobre la víctima.

3. La autora o el autor mantenga una relación laboral, de parentesco consanguíneo o de afinidad con la víctima.
4. La víctima sea una mujer embarazada.
5. La autora o el autor sea servidora o servidor público.
6. La autora o el autor sea la persona encargada de proteger los derechos e integridad de las personas en situación vulnerable.
7. La autora o el autor hubiera sido parte o integrante de una delegación o misión diplomática, en el momento de haberse cometido el delito.
8. El delito se cometa contra más de una persona.
9. La actividad sea habitual y con fines de lucro.
10. La autora o el autor sea parte de una organización criminal.

III. Quien compre, arriende o venda material pornográfico, donde se exhiba imágenes de niños, niñas y adolescentes, será sancionado con pena privativa de libertad de cinco (5) a ocho (8) años.

El citado Artículo 323 bis, si bien hace referencia a datos personales como: impresiones, videos, fotografías y filmaciones que contengan actos de exhibicionismo corporal, lascivos o sexuales de adultos y de menores de edad o de personas incapaces, se encuentra orientado específicamente a sancionar conductas inherentes al ilícito de pornografía. Así también, el tipo penal exige que no exista el consentimiento de la víctima para que se configure el delito, ya que de existir este, es posible aplicar la exención de la responsabilidad penal, al no operar la tipicidad; no obstante, en los hechos se presentan casos en los que es la víctima quien presta su acuerdo o proporciona imágenes o grabaciones íntimas (sexting) a sus parejas sentimentales (cónyuge, conviviente, novio, etc.), en un contexto de privacidad más no así con la finalidad de su difusión, por lo que ante una eventual publicación o distribución de las mismas por cualquier medio, no sería posible su persecución por la vía penal.

Por otra parte, debe considerarse que en la Sociedad de la Información, es cotidiano que los niños y adolescentes accedan a las TIC, no siendo conscientes de las consecuencias que pueden acarrear las operaciones realizadas por medio de las mismas, ignorando en su mayoría, que están consintiendo el tratamiento de sus datos personales, desde aquellos de índole pública hasta los más íntimos y reservados. Es así que datos como su nombre y apellidos, dirección, edad, ubicación, número de teléfono, fotografías, lugares visitados, viajes realizados, colegio al que asisten, relaciones familiares e interpersonales, entre tantos otros, se encuentran en la red Internet a través de plataformas como Instagram, Facebook o WhatsApp y en multiplicidad de páginas web, almacenados en bases de datos y al alcance de un sinnúmero de personas que pueden utilizarlos para distintos fines lícitos e ilícitos, generando en este último caso, afectación para sus titulares y su entorno familiar.

En virtud a lo descrito, se justifica la inclusión de un tipo penal que tutele una amplia gama de datos personales sensibles y de menores de edad, para brindar así un amparo integral a los titulares de estas categorías de información especialmente vulnerable.

Ya se ha precisado con anterioridad, la importancia de la información y concretamente de los datos personales, en mérito a lo cual la autodeterminación informativa como derecho fundamental desempeña un rol primordial, dado su carácter instrumental que coadyuva a la tutela de otros derechos, factores que ameritan ser considerados por la normativa penal vigente en Bolivia. Los datos personales de los individuos, hoy más que nunca están expuestos a riesgos, que van desde afectaciones a la intimidad, la identidad, el honor o la privacidad e incluso confluyen en atentados contra la integridad personal, porque pueden originar y servir como base para secuestros, agresiones físicas o sexuales, trata y tráfico de personas y en el peor de los casos delitos contra la vida, de lo cual emerge la necesidad de incluir reformas en la ley penal.

Por los fundamentos señalados, es posible afirmar que el Código Penal del Estado Plurinacional de Bolivia, adolece de un vacío legal respecto a la protección de datos personales, máxime si se considera que actualmente la sociedad boliviana se encuentra inmersa en la Era Digital y sumida en la Sociedad de la Información bajo el influjo de las TIC, por lo que habiéndose modificado el orden social, el derecho penal debe ajustarse a estos cambios, no siendo admisible una interpretación analógica para sancionar conductas referidas a la vulneración de datos personales, porque ello conllevaría una persecución penal e imposición arbitraria de sanciones, como resultado de subsumir estas conductas en las figuras existentes que no se encuentran diseñadas para abarcar dichos comportamientos, vulnerando así el principio de legalidad.

Así también, la incorporación de tipos penales referidos a datos de carácter personal, posibilitará la persecución penal y la consiguiente imposición de sanciones respecto a los delincuentes, más la reparación del daño en favor de las víctimas de estos ilícitos, evitando acrecentar la brecha de impunidad.

2.5.4 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación y sus reglamentos

La Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación N°164 de 8 de agosto de 2011, fue sancionada con el objeto de establecer el régimen general de telecomunicaciones y tecnologías de información y comunicación, el servicio postal y el

sistema de regulación, en procura del vivir bien, garantizando el derecho humano individual y colectivo a la comunicación. Esta norma incluye aspectos relacionados con la protección de datos personales en varios de sus artículos citados a continuación:

> Artículo 54. (DERECHOS DE LAS USUARIAS Y USUARIOS)
> (…) 9. Solicitar la exclusión, sin costo alguno, de las guías de usuarias o usuarios disponibles al público, ya sean impresas o electrónicas. Las usuarias o usuarios podrán decidir cuáles datos personales se incluyen, así como comprobarlos, corregirlos o suprimirlos.
> (…) 17. Recibir protección del proveedor del servicio sobre los datos personales contra la publicidad no autorizada por la usuaria o usuario, en el marco de la Constitución Política del Estado y la presente Ley.
> (…) Artículo 56. (INVIOLABILIDAD Y SECRETO DE LAS COMUNICACIONES). En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma.
> (…) Artículo 59. (OBLIGACIONES DE LOS OPERADORES Y PROVEEDORES)
> (…)13. Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley.
> (…) Artículo 84. (REGLAMENTACIÓN). El reglamento referido a firmas y certificados digitales comprenderá:
> (…) 3. Las definiciones, principios y procedimientos relativos al tratamiento de los datos personales.

La Ley N°164 establece un régimen sancionatorio en caso de incumplimiento, el cual se efectiviza sin perjuicio de la acción penal que corresponda, aplicando a los infractores las sanciones de apercibimiento, secuestro o embargo de equipos y material, así como multas e inhabilitación temporal para ejercer las actividades en telecomunicaciones y TIC (Artículo 94).

Por su parte, el Reglamento aprobado por Decreto Supremo N° 1391 de 24 de octubre de 2012, cuyo objeto de acuerdo a su Artículo 1 es regular las actividades del sector de telecomunicaciones, obliga al personal y proveedores de servicios a proteger los datos personales y la intimidad de los usuarios, debiendo adoptar medidas idóneas para tal efecto, coadyuvando en su caso a la identificación de los presuntos responsables de las vulneraciones, estableciendo adicionalmente la prohibición de permitir el acceso a registros o bases de datos de usuarios, ya sea de manera individual o a través de listas con fines comerciales o de publicidad, salvo autorización previa, expresa y escrita del usuario (Artículo 176).

De similar manera, el Reglamento a la Ley N° 164, aprobado por Decreto Supremo N°1793 de 13 de noviembre de 2013, cuya esfera de aplicación la constituyen las actividades o servicios inherentes a certificación digital, gobierno electrónico, software libre, correo electrónico y el uso de documentos y firmas digitales en el Estado Plurinacional de Bolivia, establece disposiciones inherentes al tema de estudio. Es así que en su Artículo 3 parágrafo IV inciso a), señala que los datos personales son: "(…) toda información concerniente a una persona natural o jurídica que la identifica o la hace identificable"; asimismo, en su inciso b) incluye el consentimiento previo, expreso e informado del titular como requisito para llevar a cabo el tratamiento de datos personales; y en su inciso c) define a este último como: "(…) cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión".

La citada disposición, en su Artículo 4, parágrafo II, instituye los principios por los que se rige el tratamiento de datos personales en el servicio de certificación digital, enunciado como tales: la finalidad, la veracidad, la seguridad y la confidencialidad. Así también en su Artículo 40 inciso h) especifica entre las funciones de la agencia de registro, cumplir con las normas y recaudos para la protección de datos personales; mientras que, para garantizar la seguridad de los datos personales del titular del certificado digital, en su Artículo 56, señala:

> a. La utilización de los datos personales respetará los derechos fundamentales y garantías establecidas en la Constitución Política del Estado;
> b. El tratamiento técnico de datos personales en el sector público y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, conservación, procesamiento, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del conocimiento previo y el consentimiento expreso del titular, el que será brindado por escrito u otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo;
> c. Las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y registro de éstos; de los potenciales destinatarios de la información; de la identidad y domicilio del responsable del tratamiento o de su representante; y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes. Los datos personales objeto de tratamiento no podrán ser utilizados para finalidades distintas de las expresadas al momento de su recolección y registro;

> d. Los datos personales objeto de tratamiento sólo podrán ser utilizados, comunicados o transferidos a un tercero, previo consentimiento del titular u orden escrita de autoridad judicial competente;
> e. El responsable del tratamiento de los datos personales, tanto 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.

La citada reglamentación, desarrolla varios aspectos referentes a la protección de datos personales en el rubro de las telecomunicaciones, así como la firma y certificado digital, que comprende a los operadores, proveedores y usuarios de estos servicios, consecuentemente conforman un marco normativo de carácter administrativo para dicho ámbito.

2.5.5 Ley del Órgano Electoral Plurinacional

La Ley del Órgano Electoral Plurinacional, N°018 de 16 de junio de 2010, en su Artículo 72, entre las obligaciones del Servicio de Registro Cívico (SERECI) menciona:

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

Mientras que en su Artículo 76, regula la conformación del Padrón Electoral como Sistema de Registro Biométrico de los bolivianos en edad de votar y de extranjeros habilitados, integrado por datos biométricos, nombres y apellidos, fecha de nacimiento, sexo, grado de instrucción, domicilio, tipo y número de documento, nacionalidad, país, departamento, provincia, municipio, territorio indígena originario campesino, localidad de nacimiento, asiento y zona electoral, además del recinto de votación.

De acuerdo al Artículo 79, parágrafo III de la aludida Ley, los datos de las personas que cursen en el Padrón pueden ser proporcionados a requerimiento escrito y fundado del Ministerio Público o del Juez o Tribunal competente y la información será únicamente utilizada para los fines solicitados. Así también, el nombrado artículo en su parágrafo IV señala que las instituciones públicas podrán verificar la identidad de las personas naturales, previo

cumplimiento de las condiciones y requisitos establecidos mediante Reglamento por el Tribunal Supremo Electoral.

En ese contexto, la Ley N°1057 de 10 de mayo de 2018, incorporó el Artículo 79 bis a la Ley del Órgano Electoral Plurinacional, facultando al Servicio de Registro Cívico (SERECI) y al Servicio General de Identificación Personal (SEGIP), consultar recíprocamente los datos personales de los ciudadanos contenidos en sus bases de datos a través del acceso a los mismos, a los fines de actualización, verificación de autenticidad, veracidad de la información y documentación, empleando para tal cometido mecanismos de interoperabilidad. La modificación incluyó además los siguientes parágrafos:

> (…) IV. El Servicio de Registro Cívico – SERECI, mediante el Tribunal Supremo Electoral, podrá suscribir convenios y contratos con otras entidades públicas y privadas que requieran servicios de consulta para verificar y autenticar la información de nacimientos, estado civil y existencias de registro de defunciones, mediante mecanismos de consulta biográficos y/o biométricos. La información verificada y contrastada no podrá ser certificada, divulgada ni transferida a otras entidades.
>
> V. La Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación – AGETIC, en el marco de la implementación del Gobierno electrónico, a través de la Plataforma de Interoperabilidad que administra, brindará a las entidades públicas en el marco de sus atribuciones, acceso a servicios de consulta en línea de los datos de nacimiento, estado civil, filiación, registro biométrico y de defunción de las personas naturales registradas en la base de datos del SERECI, en coordinación con el Tribunal Supremo Electoral y en el marco de la normativa vigente.

Por su parte, la Disposición Transitoria Única de la enunciada Ley, determina que a objeto del cumplimiento del Parágrafo IV, el Tribunal Supremo Electoral, en el plazo de noventa días emitirá reglamentación que garantice el consentimiento voluntario de las personas al acceso de su información por terceros. Es innegable que varias entidades públicas, antes de la puesta en vigencia de la norma descrita, en cumplimiento de sus especificas funciones y por la naturaleza de sus atribuciones, ya gozaban del acceso a los datos personales de los ciudadanos en mayor o menor grado, ya sea de manera directa o a través de la suscripción de convenios; sin embargo, con las modificaciones descritas con anterioridad, esta facultad se amplifica aún más, posibilitando que entes tanto públicos como privados tengan mayor acceso a los datos personales incluso biográficos y biométricos, justificando requerir servicios de consulta.

Así también, es debatible que se confiera a la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, el acceso a los datos del SERECI, para que ésta a su vez los

ponga a disposición para consulta de otros entes públicos a través de la Plataforma de Interoperabilidad en el marco del gobierno electrónico. Lo descrito, genero controversias al interior de la Asamblea Legislativa Plurinacional, por lo cual se incluyó la nombrada Disposición Transitoria.

2.5.6 Ley de Servicios Financieros

La Ley de Servicios Financieros N°393 de 21 de agosto de 2013, regula las actividades de intermediación financiera y la prestación de los servicios financieros, así como la organización y funcionamiento de las entidades que brindan estos servicios. Esta norma, en relación con la información de los consumidores y usuarios determina:

> Artículo 74. (DERECHOS DEL CONSUMIDOR FINANCIERO).
> I. Los consumidores financieros gozan de los siguientes derechos:
> (…) f) A la confidencialidad, con las excepciones establecidas por Ley.
> (…) Artículo 472. (DERECHO A LA RESERVA Y CONFIDENCIALIDAD). Las operaciones financieras realizadas por personas naturales o jurídicas, bolivianas o extranjeras, con entidades financieras gozarán del derecho de reserva y confidencialidad. Cualquier información referida a estas operaciones será proporcionada al titular, a quien éste autorice o a quien lo represente legalmente, además de los casos señalados en el Artículo 473 de la presente Ley.
> (…) Artículo 476. (CONFIDENCIALIDAD DE LOS FUNCIONARIOS DE LA AUTORIDAD DE SUPERVISIÓN DEL SISTEMA FINANCIERO - ASFI). La Directora Ejecutiva o Director Ejecutivo y los empleados de la Autoridad de Supervisión del Sistema Financiero - ASFI, aún después de cesar en sus funciones, están prohibidos de dar a conocer información relacionada con los documentos, informes u operaciones de las entidades financieras o de personas relacionadas con el sistema financiero. El ejecutivo o empleado que infrinja esta prohibición, será destituido de su cargo, sin perjuicio de las responsabilidades civil o penal que correspondan.
> Artículo 477. (ACCIÓN DE PROTECCIÓN DE LA PRIVACIDAD). Toda persona individual o colectiva que considere estar indebidamente o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por las entidades financieras, 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 o privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de la Privacidad prevista en el Artículo 131 de la Constitución Política del Estado.
> (…) Artículo 494. (ATENCIÓN A REQUERIMIENTOS DE INFORMACIÓN).
> I. La Autoridad de Supervisión del Sistema Financiero - ASFI por sí sola o a través de la Unidad de Investigaciones Financieras, sin incurrir en violación del derecho a la reserva y confidencialidad de la información al que se refiere el Artículo 472 de la presente Ley, previa solicitud y sin necesidad de reciprocidad, podrá intercambiar información relativa a la persecución de la actividad financiera ilegal, legitimación de ganancias ilícitas y delitos financieros, con

> instituciones u órganos internacionales análogos, así como con instituciones del orden y autoridades judiciales nacionales, extranjeras o internacionales, observando las formalidades de los tratados y convenios internacionales de los cuales el Estado Plurinacional de Bolivia es suscriptor.
> II. La información solicitada por la Autoridad de Supervisión del Sistema Financiero - ASFI a órganos o instituciones nacionales o extranjeros, a efectos de investigación de las actividades financieras ilegales, legitimación de ganancias ilícitas, delitos financieros o de infracciones a las normas de supervisión, regulación y control, dentro del territorio nacional, no requerirán de ninguna formalidad judicial o administrativa para su presentación a las autoridades judiciales.

De la normativa aludida, se colige que las instituciones financieras deben otorgar protección a la información concerniente a los depósitos y movimientos bancarios de sus clientes, estableciendo la confidencialidad como una manifestación del derecho a la intimidad, por lo que solamente aquellos facultados por la Ley pueden acceder a información de esta naturaleza; de lo contrario, los datos quedarían a merced de ser utilizados ilícitamente por quien los recopila e inclusive por terceros. Dicha información únicamente puede ser proporcionada al titular o a quien este autorice o lo represente legalmente, a su vez las autoridades judiciales y administrativas (autoridades tributarias, Autoridad de Supervisión del Sistema Financiero o la Unidad de Investigaciones Financieras) en la investigación de ilícitos, quedan facultadas para tener acceso a la misma.

2.5.7 Código Niña, Niño y Adolescente

El Código Niña, Niño y Adolescente, Ley N°548 de 14 de julio de 2014, cuyo objeto de conformidad a su Artículo 1 es: reconocer, desarrollar y regular el ejercicio de los derechos de los menores de edad implementando el Sistema Plurinacional Integral de la Niña, Niño y Adolescente, para garantizar sus derechos mediante la corresponsabilidad del Estado en todos sus niveles, la familia y la sociedad, contiene varios artículos relacionados con los datos personales:

> Artículo 138. (REGISTRO DE ACTIVIDAD LABORAL O TRABAJO POR CUENTA PROPIA O AJENA).
> I. Las Defensorías de la Niñez y Adolescencia, tendrán a su cargo el registro de la autorización de las niñas, niños y adolescentes de diez (10) a catorce (14) años que realicen actividad laboral o trabajo por cuenta propia o cuenta ajena.
> II. La copia del registro de las y los adolescentes trabajadores por cuenta ajena de doce (12) a catorce (14) años, deberá ser remitida al Ministerio de Trabajo, Empleo y Previsión Social, por las Defensorías de la Niñez y Adolescencia, a los efectos de la inspección y supervisión correspondiente.

III. El Ministerio de Trabajo, Empleo y Previsión Social, tendrá a su cargo el registro de la autorización de las y los adolescentes mayores de catorce (14) años que realicen trabajo por cuenta ajena.

IV. El Ministerio de Trabajo, Empleo y Previsión Social, los Gobiernos Autónomos Municipales, y las Defensorías de la Niñez y Adolescencia, garantizarán la gratuidad de todo el proceso de registro.

V. Los datos del registro serán remitidos mensualmente por las Defensorías de la Niñez y Adolescencia, y el Ministerio de Trabajo, Empleo y Previsión Social, al Ministerio de Justicia e incorporados al Sistema de Información de Niñas, Niños y Adolescentes-SINNA.

(…) Artículo 142. (DERECHO AL RESPETO Y A LA DIGNIDAD).

I. La niña, niño y adolescente, tiene derecho a ser respetado en su dignidad física, psicológica, cultural, afectiva y sexual.

II. Si la o el adolescente estuviere sujeto a medidas socio-educativas privativas de libertad, tiene derecho a ser tratada y tratado con el respeto que merece su dignidad. Gozan de todos los derechos y garantías establecidos en la Constitución Política del Estado, sin perjuicio de los establecidos a su favor en este Código; salvo los restringidos por las sanciones legalmente impuestas.

Artículo 143. (DERECHO A LA PRIVACIDAD E INTIMIDAD FAMILIAR).

I. La niña, niño y adolescente tiene derecho a la privacidad e intimidad de la vida familiar.

(…) Artículo 179. (MINISTERIO DE JUSTICIA). Son atribuciones del Ministerio de Justicia como ente rector del Sistema Plurinacional de Protección Integral de la Niña, Niño y Adolescente-SIPPROINA:

(…) n. Crear, administrar y actualizar permanentemente, en coordinación con el Instituto Nacional de Estadísticas-INE, el Sistema de Información de Niñas, Niños y Adolescentes-SINNA, que registrará y contendrá información especializada sobre los derechos de la niña, niño y adolescente, así como datos referentes a la actividad laboral o trabajo realizado por cuenta propia o ajena, conforme a reglamentación específica, idónea para la adopción y monitoreo de políticas públicas;

(…) Artículo 212. (CITACIÓN POR EDICTO).

I. En caso de desconocerse el domicilio de la o el demandado o tratándose de personas desconocidas o indeterminadas, la parte solicitará la citación mediante edictos, previo juramento de desconocimiento. Diferida la solicitud, el edicto se publicará por dos veces con intervalo no menor a cinco (5) días, en un periódico de circulación nacional, o a falta de éste, se difundirá en una radiodifusora o medio televisivo, nacional o local, en la misma forma y plazo previstos, manteniendo la reserva y resguardando la identidad de la niña, niño y adolescente involucrado, preservando que los datos contenidos no afecten a su imagen y la dignidad. En caso de que la Defensoría de la Niñez y Adolescencia sea la demandante, ésta asumirá el costo del edicto.

(….) Artículo 262. (DERECHOS Y GARANTÍAS).

I. La o el adolescente en el Sistema Penal, desde el inicio del proceso, así como durante la ejecución de la medida socio-educativa, tienen los siguientes derechos y garantías:

> (…) l. A la Privacidad. A que se respete su privacidad y la de su grupo familiar;
> m. Confidencialidad. Se prohíbe la publicación de datos de la investigación o del juicio, que directa o indirectamente posibiliten identificar a la o el adolescente, exceptuando las informaciones estadísticas;
> Artículo 263. (RESERVA DE ACTUACIONES).
> I. Está prohibida la obtención o difusión de imágenes, así como la divulgación de su identidad o de las personas relacionadas con las actuaciones procesales, policiales o administrativas.
> II. El registro de antecedentes penales y policiales, será reservado y sólo podrá certificarse mediante auto motivado, emitido por la Jueza o el Juez Público en materia de Niñez y Adolescencia.
> III. En el caso de la persona adolescente declarada rebelde, se publicarán únicamente los datos indispensables para su aprehensión.

El nombrado Código en varios artículos autoriza y dispone la recolección y registro de diferentes datos personales de los menores de edad y su entorno familiar, principalmente relacionados con la actividad laboral. También se incorporan disposiciones sobre la reserva y resguardo de la identidad de los menores.

En el caso de los adolescentes, la Ley N° 548, establece que dentro del sistema penal, tienen derecho a la confidencialidad y protección de su información; en consecuencia, respecto a aquellos sobre quienes pesa una declaratoria de rebeldía deben publicarse únicamente los datos indispensables para su aprehensión. Por consiguiente, este cuerpo legal otorga protección a la dignidad, privacidad e intimidad de los niños y adolescentes.

Conforme al Estudio publicado el 2019 por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, denominado: Juventudes TIC, Estudio sobre las TIC en adolescentes y jóvenes en Bolivia; a nivel nacional se ha experimentado un crecimiento exponencial del uso de las Tecnologías de Información y Comunicación, principalmente en lo que refiere a la cobertura de Internet y al uso de teléfonos móviles inteligentes, siendo así que:

> El 67,5% de las y los bolivianos mayores de 14 años de edad es internauta, de los cuales 39% es joven y se encuentra entre los 15 y 24 años. Las TIC son cada vez más importantes en la vida cotidiana de la juventud boliviana. El 98% de estos internautas tiene celulares inteligentes, 100% utiliza al menos una red social y, en promedio, se conecta a internet, a través de sus teléfonos móviles, los siete días de la semana. (AGETIC, 2019, p. 21)

Dado que el sector conformado por la niñez y adolescencia es altamente vulnerable, deben primar sus intereses, siendo fundamental instaurar medidas oportunas y pertinentes

para la tutela de sus datos personales, que contribuyan al ejercicio del derecho de autodeterminación informativa, sobre todo frente al riesgo que plantea el uso de las Tecnologías de Información y Comunicación y primordialmente la red Internet (ODIB, 2019), como ámbito en el que se desenvuelven los ciberdelincuentes para perpetrar ilícitos, considerando además que en la realidad boliviana se han presentado casos que involucran el uso de datos personales de menores de edad en conductas tales como: trata y tráfico, ciberacoso, violencia sexual, pornografía, grooming, sexting, secuestro y asesinato (Opinión, 2015; La Patria, 2018; La Época, 2019; El Deber, 2019).

2.5.8 Ley de Ciudadanía Digital

La Ley N°1080 de Ciudadanía Digital de 11 de julio de 2018, cuyo objeto es establecer las condiciones, responsabilidades, acceso y ejercicio de la ciudadanía digital, orientada a los ciudadanos y entes del sector público y privado que presten servicios públicos delegados por el Estado, en su Artículo 5 determina que tanto los bolivianos como extranjeros residentes en el territorio nacional que sean mayores de 18 años de edad y también los menores conforme a la capacidad que les reconozca el ordenamiento jurídico, deben registrarse ante las entidades responsables y obtener credenciales de ciudadanía digital.

Dicho Artículo en su parágrafo II dispone que la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, desarrollará lineamientos técnicos del registro para acceder a la ciudadanía digital, y en su parágrafo III, determina que los entes públicos y privados que presten servicios públicos deben compartir los datos de información que generen a través de mecanismos de interoperabilidad, entendida como: “(…) la capacidad de dos o más sistemas (agencias, administraciones públicas, niveles de gobierno, etc.) para interaccionar e intercambiar datos de acuerdo con un método común, con el fin de obtener los resultados esperados (…)” (Criado y Gil - García, 2013, p.19).

Es sustancial, recapitular que esta norma confiere plena validez jurídica a todos los actos realizados en ejercicio de la ciudadanía digital. Por último, conforme al Artículo 12 de la Ley de Ciudadanía Digital, los datos personales e información generada deberán ser utilizados únicamente para los fines previstos en la normativa vigente; lo contrario, generará responsabilidad por la función pública respecto a los servidores públicos, mientras que en el caso de las entidades privadas que prestan servicios públicos su responsabilidad se sujetará a la regulación emanada de los entes que los supervisen.

2.5.9 Decreto Supremo N°28168

El Decreto Supremo N°28168 de 17 de mayo de 2005, cuyo objeto es garantizar el acceso a la información, como derecho fundamental y la transparencia en la gestión del Poder Ejecutivo, regula en su Artículo 19 la petición de Habeas Data en la vía administrativa, como un medio a través del cual puede solicitarse a las autoridades encargadas de los archivos o registros, la actualización, complementación, eliminación o rectificación de datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a derechos fundamentales a la identidad, intimidad, imagen y privacidad.

Esta normativa, otorga la facultad para poder 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. Cabe señalar, que conforme al parágrafo III del nombrado Artículo 19, la petición de Habeas Data no reemplaza ni sustituye el Recurso Constitucional, no estando condicionado el acceso a la vía judicial a la previa utilización ni agotamiento de la vía administrativa. En consecuencia, el Decreto Supremo N° 28168 configura un mecanismo en la vía administrativa para incoar el procedimiento de Habeas Data en el ámbito de entidades del órgano ejecutivo.

2.5.10 Decreto Supremo N°2514

El Decreto Supremo N°2514 de 9 de septiembre de 2015 crea por una parte la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación - AGETIC, como ente descentralizado bajo tuición del Ministerio de la Presidencia, y por otra, los Comités Interinstitucionales de Simplificación de Trámites.

Conforme al Artículo 7 inciso a) del nombrado Decreto, la AGETIC como nuevo ente tiene entre sus funciones: “Elaborar, proponer e implementar políticas, planes y estrategias de Gobierno Electrónico y Tecnologías de Información y Comunicación para las entidades del sector público”; asimismo, en sus Artículos 12 y 13 establece que las entidades públicas desarrollaran programas y proyectos de gobierno electrónico, reingeniería de procesos y procedimientos para la simplificación de trámites a través de las Tecnologías de Información y Comunicación, a efectos de reducir costo y tiempo en las gestiones de la ciudadanía ante el sector público, debiendo coordinar con la AGETIC estas actividades.

La enunciada norma, además determina en su Artículo 19:

> 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.

De acuerdo al Artículo 20 del ya citado Decreto Supremo, las entidades públicas y privadas que prestan servicios públicos delegados por el Estado, deben coordinar con la AGETIC la implementación de planes, programas, proyectos y servicios de Gobierno Electrónico y Tecnologías de Información y Comunicación. Esta norma, bajo la premisa de impulsar la implementación del gobierno electrónico para la simplificación de trámites de la ciudadanía ante instancias públicas y/o privadas que administren servicios delegados por el Estado, autoriza la recolección, tratamiento e interoperabilidad de datos a través de la utilización de las Tecnologías de Información y Comunicación.

2.5.11 Decreto Supremo N°3251

El Decreto Supremo N°3251 de 12 de julio de 2017, aprueba el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre, Estándares Abiertos y su puesta en marcha en el Estado Plurinacional de Bolivia. En su Artículo 4 autoriza a las entidades públicas a compartir información por medio de mecanismos de interoperabilidad y de acuerdo a determinaciones emanadas del Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC), en coordinación con la AGETIC, en el marco de las normas vigentes y disposiciones específicas de sectores estratégicos. También dispone que las entidades públicas a través de la AGETIC, habiliten los accesos a la información pertinente. Asimismo, faculta la suscripción de convenios de interoperabilidad entre entes públicos, con el fin de garantizar el intercambio de información.

2.5.12 Decreto Supremo N°3525

El Decreto Supremo N°3525 de 4 de abril de 2018, establece la Política de Atención a la Ciudadanía: Bolivia a tu servicio y el Portal de trámites del Estado; regula el archivo digital, la interoperabilidad y la tramitación digital, su ámbito de aplicación comprende a las entidades

públicas y aquellas privadas que presten servicios públicos delegados por el Estado, con el propósito de:

> (…) brindar mayor transparencia y fluidez en la interacción entre los administrados y el sector público, la transferencia de información entre entidades del estado y entre estas con la población, de acuerdo al ordenamiento jurídico de manera accesible e inmediata; y promover la celeridad de los trámites administrativos. (Artículo 3)

Con esta norma, se aspira gestionar la participación digital de los ciudadanos en trámites con el Estado a través de sus páginas web institucionales. A su vez, en su Artículo 9, el Decreto Supremo N°3525, establece la implementación del Portal de trámites del Estado, para optimizar la interacción entre los administrados y el sector público, siendo un mandato para las entidades públicas y privadas que presten servicios delegados por el Estado publicar los tramites que brindan, con un mínimo de información a ser actualizada periódicamente.

Otro aspecto relevante, se encuentra comprendido en el Artículo 12 de la citada norma, que dispone que los entes públicos prioricen el uso de las TIC en los trámites a su cargo. Así también, se incorpora la figura de la interoperabilidad de datos entre entes públicos, destinada a la simplificación de trámites, cuyos mecanismos, condiciones de publicación y accesos, están a cargo del Ministerio de la Presidencia en su condición de ente rector del Gobierno Electrónico y Tecnologías de Información y Comunicación. Por su parte, el Artículo 13 del Decreto Supremo N°3525, señala:

> I. Las entidades que conforme a sus atribuciones recolectan, generan, transforman y validan datos o información, son responsables en observancia de su normativa legal específica, de publicar la información y datos como fuente primaria a través de la plataforma de interoperabilidad establecida en el Plan de Implementación de Gobierno Electrónico aprobado mediante el Decreto Supremo N°3251, de 12 de julio de 2017.
> II. En el marco de procesos de actualización, certificación o emisión de copias legalizadas de documentos que aún se encuentran en formato físico, los datos e información pertinente consignados en los mismos deberán ser registrados en medios digitales que permitan ser publicados mediante servicios de interoperabilidad.

A su turno, los Artículos 14,15 y 16 establecen la validez de los documentos firmados digitalmente en las actuaciones administrativas, incorporando la gestión documental digital, la conversión de documentos de soporte de papel a digital y viceversa, así como el registro de orden cronológico y de integridad de los documentos digitales. Finalmente, el ya citado Decreto Supremo, en su Disposición Adicional Única, parágrafo II, modifica el Artículo 45 del

Decreto Supremo N°27113 de 23 de julio de 2003 referido a las notificaciones electrónicas a través de correo electrónico u otros medios digitales, ratificando la validez de este tipo de comunicación, siempre que los administrados se hubieran registrado voluntariamente y manifestado su conformidad ya sea por vía escrita o por medios digitales.

2.5.13 Código del Sistema Penal

El 15 de diciembre de 2017, fue promulgada la Ley N°1005 denominada: Código del Sistema Penal, generando una serie de protestas en diferentes sectores sociales, que identificaron una afectación a sus derechos por parte de varios artículos del texto normativo, obligando al Órgano Legislativo a su abrogación mediante Ley N°1027 de 25 de enero de 2018. Este cuerpo legal, contempló disposiciones inherentes a los datos personales, en sus siguientes artículos:

> Artículo 246. (USO INDEBIDO DE DATOS AJENOS EN MEDIOS INFORMÁTICOS). I. La persona que, sin autorización, con intención de obtener beneficio indebido o con el fin de afectar la imagen y dignidad de la víctima, utilice los datos o información confidencial ajena, sea personal, institucional o financiera, consignada en medios informáticos o electrónicos o suplante la identidad de otra a través de un medio electrónico o digital generándole perjuicio al titular de la información o a un tercero, será sancionada con prisión de dos (2) a cuatro (4) años y reparación económica.
>
> II. La sanción será agravada a prisión de tres (3) a seis (6) años y reparación económica, cuando la víctima sea niña, niño o adolescente.
>
> (…) Artículo 250. (AGRAVANTES EN DELITOS INFORMÁTICOS). La sanción prevista en cada uno de los Artículos precedentes, será agravada a prisión de tres (3) a seis (6) años y reparación económica, cuando:
>
> 1. El sistema o los datos informáticos pertenezcan a una entidad estatal, un proveedor de servicios de salud o un proveedor de servicios financieros;
> 2. Los datos ilegítimamente obtenidos sean transferidos, a cualquier título, a terceros;
> 3. La persona autora tenga el deber de resguardar el sistema o los datos informáticos;
> 4. La persona autora sea servidora o servidor público; o,
> 5. La persona autora abuse de un vínculo sentimental, afectivo, emocional o de confianza para cometer el hecho.

De lo señalado, se advierte que dicha norma en su Artículo 246 incorporó la tutela penal específica de los datos personales, sancionando con una pena de 2 a 4 años su utilización no autorizada y en caso de tratarse de menores de edad agravando la sanción de 3 a 6 años.

Mientras que, en su Artículo 250 insertó agravantes para incrementar la pena en la proporción precedentemente señalada al tratarse de: datos pertenecientes a un ente público; proveedores de servicios de salud y financieros; o cuando opere la transferencia de los datos a terceros; así también, si el sujeto activo tiene el deber de resguardar los datos o el sistema, aspecto que comprende a los responsables y encargados de los datos personales. De similar manera, se estableció la agravante para la intervención como autor de un servidor público o una persona vinculada sentimentalmente o través de una relación de confianza con la víctima.

Es de observar que el Artículo 246, no contempló una protección al margen de los entornos informáticos o electrónicos, es decir en otros soportes o en formatos físicos tradicionales como el papel, medios por los cuales también es posible vulnerar datos personales; asimismo, incluyó únicamente la utilización no autorizada de datos ya consignados en medios informáticos o electrónicos, dejando de lado el posible escenario de una recopilación ilícita de datos y transgresiones que pueden suscitarse en otras fases del procesamiento o tratamiento de datos. Cabe añadir que, fuera de la agravante del Artículo 250 numeral 1) para los casos en que se involucren datos de proveedores de salud, este artículo no consideró la salvaguarda de datos personales sensibles.

A su vez, es de destacar que el Código abrogado inspiró la redacción de los nombrados tipos penales en el Convenio sobre la Ciberdelincuencia de Budapest. Con todo, la inclusión de tipos penales de naturaleza informática, orientados a tutelar la información y datos personales, hubiera significado un gran avance para el país, no solo por permitir una persecución y sanción penal de este tipo de conductas, sino además por su armonización con los preceptos emanados del antedicho Convenio.

Una vez analizadas las normas precedentes, se avizora con meridiana claridad, una nueva etapa de relaciones entre el ciudadano y el Estado, impulsada por la creciente incorporación de las Tecnologías de Información y Comunicación, que tienen impacto en distintos y variados aspectos de la vida cotidiana de las personas, fenómeno que se verifica a escala global.

Debemos reconocer como positivo que, bajo ese contexto, el Estado persigue como objetivo brindar mejores servicios a los ciudadanos, con transparencia y fluidez, incentivando la participación digital, con miras a desburocratizar la administración pública. En contraposición, la información personal se encuentra cada vez más expuesta, y los entes estatales y privados tienen facultades para el tratamiento de la misma, recolectando, actualizando, intercambiando, transfiriendo, publicando y poniendo datos a disposición de quien los requiera, usualmente sin el conocimiento ni consentimiento de sus titulares.

Frente a este escenario, en el marco de la protección de datos personales, se identifica normativa en varios cuerpos legales que brindan amparo en sede civil, administrativa y constitucional. Paralelamente, es ostensible la vigencia de un conjunto de disposiciones jurídicas que viabilizan un mayor intercambio y tráfico de datos e información personal en torno a las Tecnologías de Información y Comunicación, lo cual demanda el afianzamiento de medidas legales conducentes a su adecuada tutela.

Bajo dichos parámetros, no existe una norma penal que sancione los más graves ataques perpetrados contra la información y los datos cuya lesión repercute en un menoscabo del derecho a la autodeterminación informativa, y amerita la intervención del derecho penal, a través del establecimiento de leyes sustantivas precisas, sometidas al principio de taxatividad, siendo que en los hechos, este tipo de atentado es cada vez más recurrente, con nefastas consecuencias para los titulares de los datos personales, dando lugar a que los afectados tengan que optar por iniciar procesos judiciales aplicando otros tipos penales, a los cuales se trata de subsumir las conductas de los infractores. En ese contexto, los datos personales requieren una salvaguarda penal, máxime si se trata de datos sensibles que ameritan una protección adicional, pues el grado de afectación que de ellos emana es mayor por el nivel de intimidad involucrado y por el potencial discriminatorio que de ellos emana; similar escenario acontece con los datos de los menores de edad, respecto a los cuales además se incrementa su vulnerabilidad a raíz de las singulares condiciones y características fisiológicas y psicológicas de sus titulares.

Si el ordenamiento jurídico penal es incompleto e insuficiente en su función reguladora de las conductas humanas, se debe optar por promulgar nuevas reglas penales, partiendo de analizar si los tipos penales vigentes en un orden jurídico, resultan o no eficaces para dar respuesta a los fenómenos que aparejan las Tecnologías de Información y Comunicación en una realidad concreta. En suma, a decir de Gómez (2008) la inclusión de un resguardo penal específico en el ámbito precedentemente señalado: “redundaría en una protección más correcta y eficaz de los datos personales y, en consecuencia, en una tutela más adecuada del irrenunciable y esencial derecho fundamental a la autodeterminación informativa, libertad informática o habeas data” (p. 325).

2.6 Jurisprudencia constitucional

Ya se ha mencionado con anterioridad que el Tribunal Constitucional de Bolivia, ha emitido a través de sus Sentencias Constitucionales, líneas jurisprudenciales emanadas de Recursos

de Habeas Data y Acciones de Protección de Privacidad, en las que se reconoce el carácter de derecho humano de la autodeterminación informativa.

Asimismo, el órgano guardián de la Constitución, producto de su labor interpretativa, ha manifestado que la autodeterminación informativa constituye la dimensión positiva del ejercicio del derecho fundamental a la intimidad y la privacidad, como el derecho que tiene la persona de acceder a los bancos de datos públicos y privados con el fin de tener conocimiento de cuanta información se ha almacenado, hacia donde fluyó, o datos de la misma y para que fines; por lo que, sin una autorización expresa, tan solo el titular de ese derecho tiene la potestad de disponer la información concerniente a sus datos de carácter personal, de preservar la propia identidad informática, o lo que es igual, de consentir, controlar, o incluso rectificar los datos informáticos de carácter personal (SCP N°0819/2015-S3 de 10 de agosto de 2015).

En consonancia, la Sentencia Constitucional N°0189/2010 – R de 24 de mayo de 2010, le asigna el carácter de derecho fundamental, al señalar:

> (…) la teoría general de los Derechos Humanos, en su clasificación, reconoce dos categorías concretas de derechos a saber: En primer orden se encuentran los derechos fundantes, como ser el Derecho a la vida o la libertad de tránsito entre otros y en segundo lugar, se tienen los derechos fundamentales derivados, entre los cuales inequívocamente se encuentra el llamado derecho de “autotutela informativa”.

Por su parte, la Sentencia Constitucional N°0030/2006-R de 11 de enero de 2006, establece el ámbito de protección del habeas data como: “(…) una vía procesal instrumental de protección al *derecho a la autodeterminación informativa*, referido a los derechos fundamentales a la intimidad y la privacidad de la persona (…)”.

Así también, la Sentencia Constitucional N°0965/2004-R de 23 de junio de 2004, expresa que el objetivo del hábeas data es: “(…) contrarrestar los peligros que conlleva el desarrollo de la informática en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona (…)”, y tiene por finalidad principal: “(…) proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios (…)”. En concordancia, la Sentencia Constitucional Plurinacional N°0080/2014-S2 de 4 de noviembre de 2014, precisa que la Acción de Protección de Privacidad es una garantía constitucional, que brinda a la persona una protección efectiva e idónea frente al manejo o uso ilegal e indebido de

información o datos personales generados, registrados o almacenados en bancos de datos públicos o privados, que son distribuidos a través de medios o soportes informáticos.

Y, la Jurisprudencia desarrollada en la Sentencia Constitucional N°965/2004-R de 23 de junio de 2004, refiere que la protección que brinda el Hábeas Data abarca los siguientes ámbitos:

> a) Derecho de acceso a la información o registro de datos personales obtenidos y almacenados en un banco de datos de la entidad pública o privada, para conocer qué es lo que se dice respecto a la persona que plantea el hábeas data, de manera que pueda verificar si la información y los datos obtenidos y almacenados son los correctos y verídicos; si no afectan las áreas calificadas como sensibles para su honor, la honra y la buena imagen personal;
> b) Derecho a la actualización de la información o los datos personales registrados en el banco de datos, añadiendo los datos omitidos o actualizando los datos atrasados; con la finalidad de evitar el uso o distribución de una información inadecuada, incorrecta o imprecisa que podría ocasionar graves daños y perjuicios a la persona;
> c) Derecho de corrección o modificación de la información o los datos personales inexactos registrados en el banco de datos público o privado, tiene la finalidad de eliminar los datos falsos que contiene la información, los datos que no se ajustan de manera alguna a la verdad, cuyo uso podría ocasionar graves daños y perjuicios a la persona;
> d) Derecho a la confidencialidad de cierta información legalmente obtenida, pero que no debería trascender a terceros porque su difusión podría causar daños y perjuicios a la persona;
> e) Derecho de exclusión de la llamada “información sensible” relacionada al ámbito de la intimidad de la persona, es decir, aquellos datos mediante los cuales se pueden determinar aspectos considerados básicos dentro del desarrollo de la personalidad, tales como las ideas religiosas, políticas o gremiales, comportamiento sexual; información que potencialmente podría generar discriminación o que podría romper la privacidad del registrado.

La Sentencia anterior, reconoce que en sí mismo el Habeas Data tutela el ejercicio de otros derechos, los cuales facultan al individuo a acceder a bancos de datos privados y públicos para conocer información o datos personales que cursan en los mismos, corregirlos, actualizarlos, modificarlos, mantener bajo confidencialidad cierta información y la exclusión de la información sensible, en suma, decidir qué datos pueden ser o no conocidos, y en qué medida. De acuerdo al razonamiento precedente, es posible equipar estos derechos con los derechos ARCO.

Asimismo, la mencionada Sentencia, reseña las particulares características de los datos personales sensibles, que constituyen el sustento para justificar su tutela especializada, toda vez que generan afectación a la esfera más íntima del individuo, por lo que ameritan el consentimiento expreso e inequívoco de su titular para su recolección y tratamiento, dado su

potencial discriminatorio y la afectación a otros derechos fundamentales que conllevan, tales como la libertad de religión y creencias, derechos sexuales, laborales y de salud, entre otros.

Es sustancial señalar, que los Artículos 130 de la Constitución y 58 del Código Procesal Constitucional, respectivamente, engloban los derechos de acceso, rectificación y de eliminación de la información cursante en bancos de datos públicos o privados (SC N° 1978/2011-R de 7 de diciembre de 2011 y SCP N° 0426/2015-S3 de 20 de abril de 2015), conocidos por la doctrina como habeas data informativo, correctivo o de rectificación y cancelatorio. Como puede colegirse de la jurisprudencia glosada, el Tribunal Constitucional boliviano, vincula el derecho a la autodeterminación informativa a los derechos de la privacidad e intimidad personal o familiar, imagen, honra y reputación, pero además reconoce su carácter de derecho humano y fundamental, como facultad para ejercer un control sobre los datos de carácter personal, puntualizando que debe operar un consentimiento expreso del titular de los datos respecto al tratamiento de los mismos.

CAPÍTULO III
MARCO PRÁCTICO

3.1 Presentación y análisis de los resultados de la encuesta

Se aplicó el cuestionario a abogados de la ciudad de La Paz que ejercen la profesión en el área del derecho penal, recolectando los datos a través de la técnica de la encuesta.

En lo que respecta a los procedimientos matemáticos, se utilizó una tabla de distribución de frecuencias en el programa Excel, toda vez que con ello se representa un conjunto de puntuaciones ordenadas en sus respectivas categorías, posteriormente, se tabularon los resultados y se efectuó el cálculo porcentual de cada ítem. Luego se realizó la interpretación y análisis de cada una de las respuestas.

A continuación, se presentan los resultados cuantitativos derivados de los datos obtenidos de la aplicación del cuestionario, correspondientes a la variable dependiente: “tutela del derecho de autodeterminación informativa” y la variable independiente: “falta de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia”.

Resultados de la pregunta N°1. Los datos personales son cualquier tipo de datos que identifican de forma directa o indirecta a un individuo, como el nombre y apellidos, cédula de identidad, dirección, orientación sexual, historial médico y datos biométricos, entre otros.

Tabla N°3

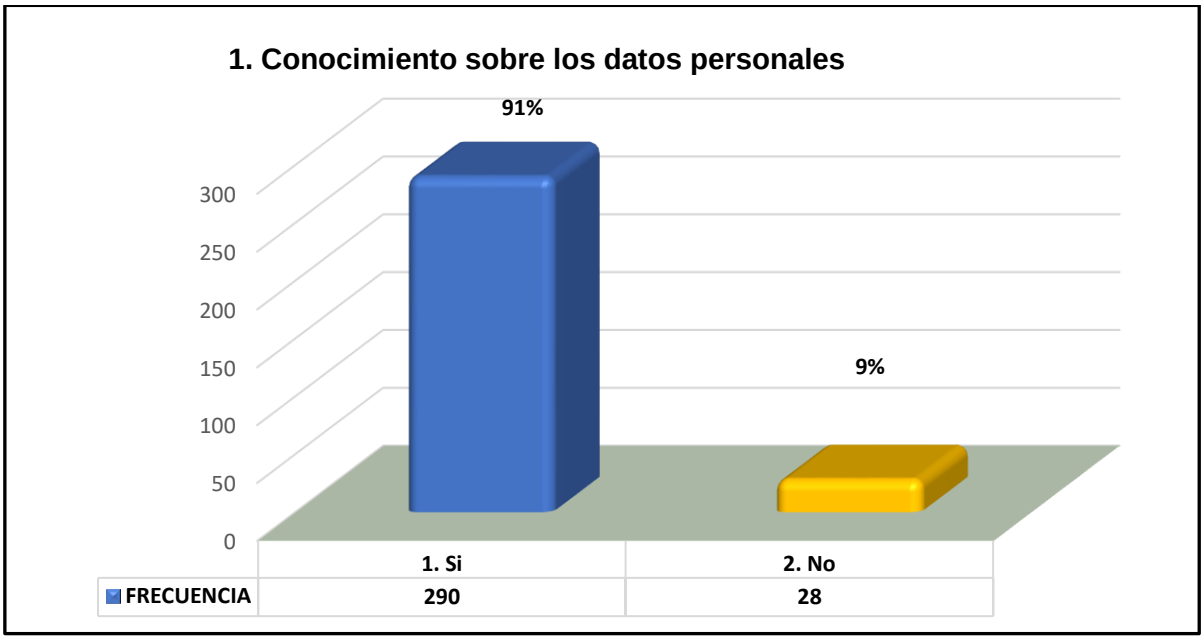
Resultados de la pregunta N°1

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Si	290	91%
2. No	28	9%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°1

Resultados de la pregunta N°1



Fuente: elaboración propia (2019)

El 91% de los encuestados seleccionó la opción que refiere que un dato personal, es aquel que identifica de forma directa o indirecta a un individuo, comprendiendo entre otros, el nombre y apellidos, cédula de identidad, dirección, orientación sexual, historial médico y datos biométricos; mientras que el 9%, difiere de la noción formulada.

El estudio considera que el resultado arribado obedece a la muestra seleccionada, conformada por abogados que por su formación académica y actividad laboral están versados en la teoría y praxis e ilustrados en mayor o menor medida respecto a la temática de los datos personales, lo cual denota un puntual conocimiento sobre lo que involucra la definición. Este factor se pondera como positivo para la investigación, porque permitió la obtención de un criterio especializado respecto a la problemática en particular y sus implicancias, toda vez que los encuestados por su expertise brindaron una visión más precisa respecto la temática de los datos personales desde la perspectiva del derecho penal.

Resultados de la pregunta N°2. ¿Con que regularidad comparte sus datos personales por medio de las Tecnologías de Información y Comunicación? (dispositivos digitales, internet, redes sociales, entre otros)

Tabla N°4

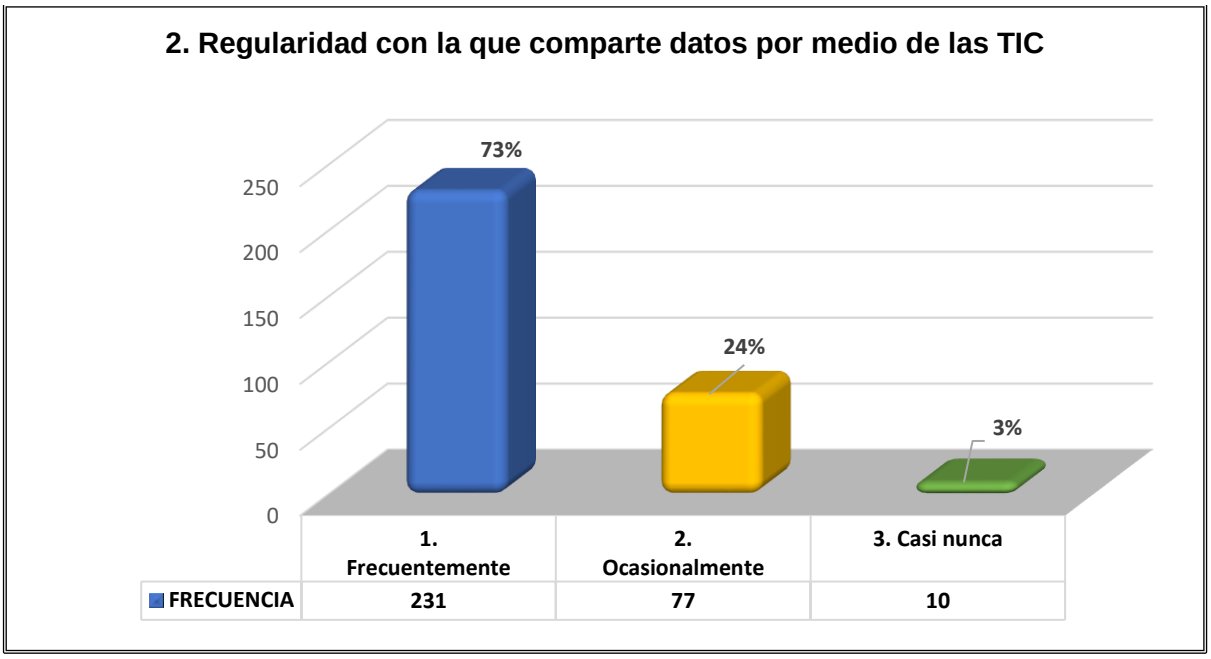
Resultados de la pregunta N°2

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Frecuentemente	231	73%
2. Ocasionalmente	77	24%
3. Casi nunca	10	3%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°2

Resultados de la pregunta N°2



Fuente: elaboración propia (2019)

De acuerdo a la Tabla y Gráfico precedentes, un 73% de los abogados, refiere compartir sus datos personales por medio de las Tecnologías de Información y Comunicación frecuentemente, frente a un 24% que alude que lo hace ocasionalmente, en tanto que un 3%, expresa que casi nunca comparte estos datos por dicha vía.

Este resultado, denota el alto influjo de las Tecnologías de Información y Comunicación a momento de compartir datos personales para facilitar tareas cotidianas, aspecto sin duda benéfico, pero que también acarrea riesgos potenciales y reales. Para ejemplificar lo anterior, por el solo hecho de adscribirse a plataformas como WhatsApp, Facebook, o Instagram, se proporcionan datos personales como el nombre y apellidos, nacionalidad, país y lugar de residencia y se otorga el acceso a imágenes, direcciones, ubicación, videos, etc.; que también constituyen datos personales, entonces, se entrega información a cambio de un servicio

aparentemente gratuito, desconociendo los usuarios, el cómo y para qué serán utilizados sus datos. Similar escenario, acontece en la red Internet, donde permanentemente, se dejan huellas digitales de la actividad por las páginas públicas y privadas a las que se accede.

En el caso específico boliviano, las aplicaciones que se descargan en los dispositivos digitales, como “Pedidos Ya” o “Doble Aguinaldo”, solicitan datos personales, sin una clara restricción por parte de quien recopila esta información, lo cual genera una gran vulnerabilidad para los usuarios.

Sobre el particular, Soto (2017) señala:

> Cada clic, cada uso del teléfono, cada utilización de la tarjeta de crédito y cada navegación en Internet suministra excelentes informaciones sobre cada uno de nosotros, que se apresura a analizar un imperio en la sombra al servicio de corporaciones comerciales, de empresas publicitarias, de entidades financieras, de partidos políticos o de autoridades gubernamentales (…). (p. 105)

Por otra parte, como resultado del conjunto de planes, políticas y medidas normativas adoptadas por el Estado; las entidades públicas y privadas interactúan con los ciudadanos en torno a las TIC, y a su vez, han adoptado medidas de interoperabilidad a través de mecanismos técnicos y legales que permiten compartir datos e información, esto con el fin de brindar mejores servicios y optimizar sus labores en términos de eficacia y eficiencia, situación que en contraposición con el beneficio brindado, genera vulnerabilidad de los datos personales de los bolivianos.

En síntesis, a través de una amplia gama de dispositivos (computadora personal, portátil, tabletas, teléfonos inteligentes, etc.) con conexión a internet y como resultado de las políticas y medidas normativas adoptadas por el Estado Plurinacional de Bolivia, los individuos comparten fluidamente sus datos personales y es diametralmente bajo el porcentaje de aquellos que ocasionalmente o casi nunca utilizan las Tecnologías de Información y Comunicación para dicho efecto, siendo la tendencia a un incremento por los factores precedentemente analizados, aspecto que amerita el establecimiento de medidas normativas adecuadas y oportunas de tutela, que se adapten al dinamismo de la sociedad.

Resultados de la pregunta N°3. Desde su percepción, los datos personales proporcionados a las entidades públicas del Estado Plurinacional de Bolivia se encuentran:

Tabla N°5

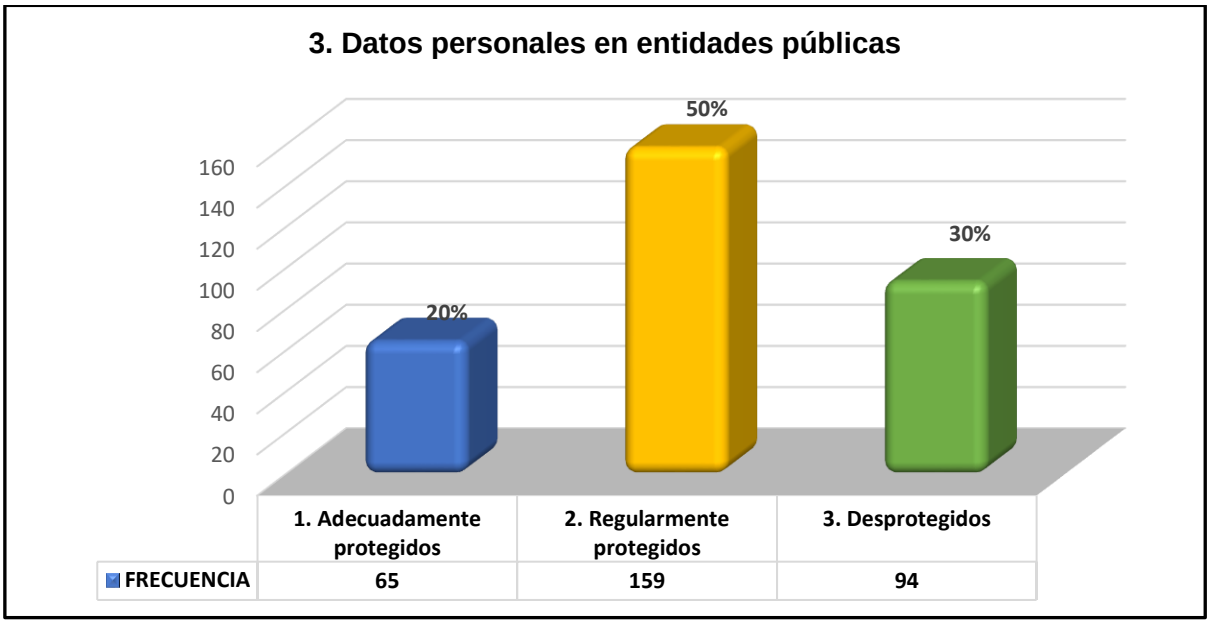
Resultados de la pregunta N°3

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Adecuadamente protegidos	65	20%
2. Regularmente protegidos	159	50%
3. Desprotegidos	94	30%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°3

Resultados de la pregunta N°3



Fuente: elaboración propia (2019)

A criterio del 50% de los encuestados, los datos personales en entidades públicas se encuentran regularmente protegidos, un 30% cree que existe desprotección y un 20% expresa que están adecuadamente protegidos.

En líneas generales, lo anterior refleja una percepción de inseguridad respecto a cómo resguarda el Estado boliviano los datos personales de sus habitantes. En lo fáctico, todas las entidades públicas recaban y acceden en mayor o menor medida a datos personales en función de sus competencias, constituyéndose en grandes detentadores de dicho insumo; no obstante, esta recopilación desde el inicio debe ser proporcional y adecuada a los fines pertinentes. Para ilustrar lo anterior, una Universidad del sistema público, no necesitará recabar información de números de cuentas bancarias de los estudiantes, o información registral de bienes inmuebles o automotores, debiendo limitarse a la obtención de datos académicos.

A su vez, las entidades estatales deben acceder y utilizar los datos personales, únicamente para los fines que fueron recabados; no obstante, en la realidad boliviana, se presentan cotidianamente casos en los que servidores públicos, los responsables de las bases de datos o los encargados del tratamiento, brindan esta información a terceros que requieren conocerlos o consultarlos, accediendo de manera extraoficial a los mismos, sin el consentimiento ni conocimiento de sus titulares, vulnerando las disposiciones normativas vigentes contenidas en la Constitución Política del Estado, leyes y ordenamiento jurídico administrativo, utilizándolos en muchos casos para la concreción de actividades delictivas, generando perjuicios de naturaleza moral y patrimonial, con nefastas consecuencias para las víctimas y su entorno.

Aunado a lo anterior, como ya fue señalado en puntos precedentes, rige en Bolivia el gobierno electrónico y la ciudadanía digital para mejorar los canales de comunicación entre el Estado y los ciudadanos, situación que demanda acciones concretas del Estado que propendan a la protección de los datos personales.

Resultados de la pregunta N°4. Desde su percepción, los datos personales proporcionados a las entidades privadas del Estado Plurinacional de Bolivia se encuentran:

Tabla N°6

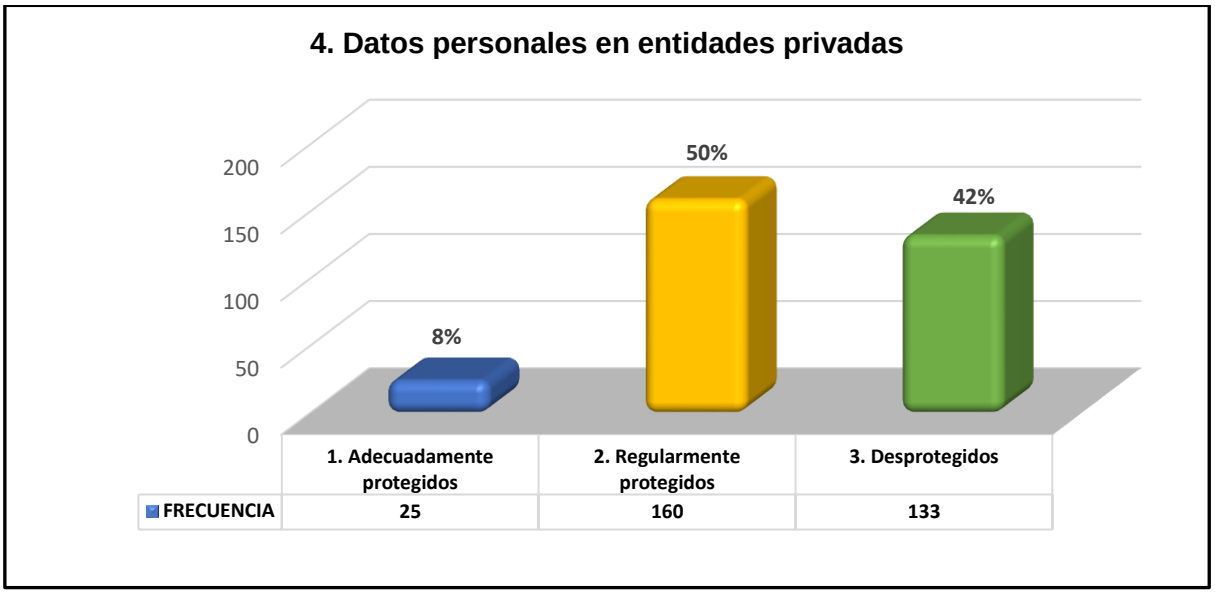
Resultados de la pregunta N°4

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Adecuadamente protegidos	25	8%
2. Regularmente protegidos	160	50%
3. Desprotegidos	133	42%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°4

Resultados de la pregunta N°4



Fuente: elaboración propia (2019)

Los resultados arrojan que un 50% de los encuestados considera que los datos personales se encuentran regularmente protegidos en las entidades privadas, un 42% expresa que estos están desprotegidos, en tanto que el 8% manifiesta su adecuada protección por parte de dichos entes. De acuerdo a la normativa analizada en el Capítulo II Marco Teórico, las regulaciones jurídicas referentes a la protección de datos personales en Bolivia se encuentran orientadas prioritariamente al sector público. Asimismo, cabe señalar que este ámbito cuenta con un régimen legal de responsabilidad por la función pública, en contraste con el sector privado que en su mayoría, salvo el rubro financiero, carece de similares normas, lo cual incide en una desprotección a los individuos que proporcionan y comparten sus datos ante dichos entes.

Resultados de la pregunta N°5. ¿Cuáles considera que son las formas más recurrentes en que se vulnera el derecho a la protección de datos personales en el Estado Plurinacional de Bolivia?

Tabla N°7

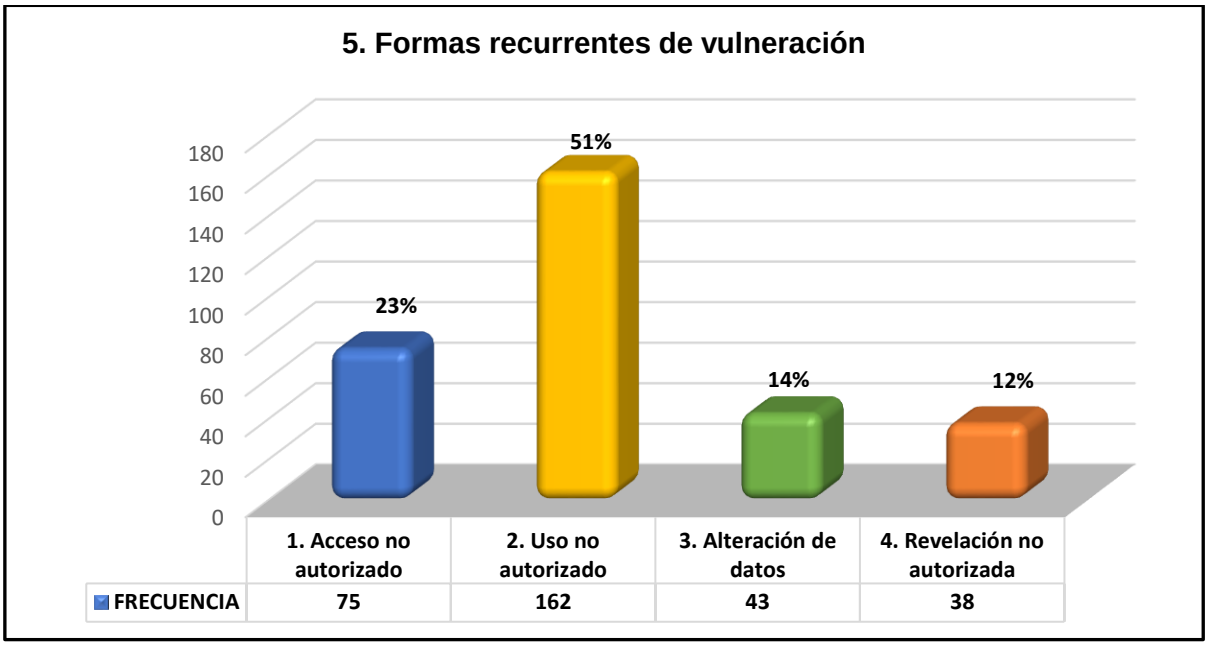
Resultados de la pregunta N°5

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Acceso no autorizado	75	23%
2. Uso no autorizado	162	51%
3. Alteración de datos	43	14%
4. Revelación no autorizada	38	12%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°5

Resultados de la pregunta N°5



Fuente: elaboración propia (2019)

El 51% señala que la forma más recurrente de vulnerar el derecho a la protección de datos personales, es el uso no autorizado, el 23% se inclina por el acceso no autorizado, el 14% manifiesta que es la alteración de datos y el 12% optó por la opción de revelación no autorizada.

Se debe considerar que todas las opciones constituyen situaciones que soslayan el derecho a la autodeterminación informativa como facultad del individuo de ejercer un control sobre sus datos personales; en ese contexto, de acuerdo al resultado precedentemente glosado, en nuestro medio el uso no consentido es la forma más habitual de vulneración, ya que sin la anuencia del titular se utiliza su información personal para diversos fines.

En la actualidad es relativamente fácil que un tercero obtenga información sobre una persona, sin que la misma lo haya autorizado o se entere de lo que acontece con sus datos de carácter personal, es decir quién los tiene o para qué los utiliza, tal es el caso de datos que se usan para obtener créditos en favor de personas distintas a sus titulares, la suplantación de identidad, secuestros, pornografía o la inscripción de ciudadanos a partidos políticos y agrupaciones ciudadanas en calidad de militantes sin que pertenezcan a los mismos, solo para citar algunos acontecimientos que se verificaron en nuestro medio.

El resultado de la encuesta devela también que la alteración de datos es otra forma en que se transgrede la autodeterminación informativa en Bolivia; así también, la revelación no autorizada, esta última atenta sobre todo a información de carácter sensible por el potencial discriminatorio y de afectación de las esferas más íntimas que estos involucran; en suma, los datos personales pueden convertirse en una llave para la comisión de variados delitos.

Resultados de la pregunta N°6. ¿Existe un artículo en el Código Penal que tipifique atentados contra los datos personales?

Tabla N° 8

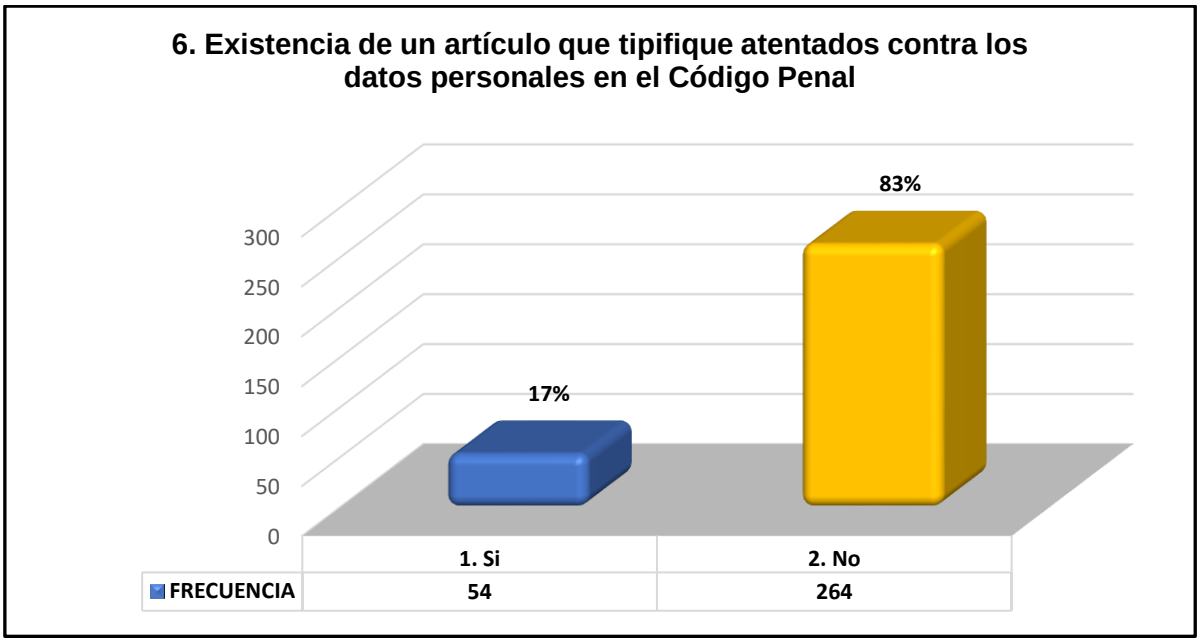
Resultados de la pregunta N°6

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Si	54	17%
2. No	264	83%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°6

Resultados de la pregunta N°6



Fuente: elaboración propia (2019)

Con relación a la existencia de un artículo en el Código Penal que tipifique los atentados contra los datos personales, el 83% de los encuestados seleccionaron la opción no, mientras que el 17% expresó que si existe.

Sobre el particular, la norma sustantiva penal en vigencia, no regula conductas que con especificidad lesionen datos personales, únicamente el Art. 363 ter hace referencia a datos informáticos, contenidos en una computadora o cualquier soporte informático. En este entender, toda conducta traducida ya sea en acción u omisión debe ajustarse a los presupuestos detalladamente establecidos como delito dentro de un cuerpo legal, lo que conlleva que, para que una conducta sea típica, debe constar específica y prolijamente como delito dentro de la ley penal, situación que en el caso boliviano debiera considerarse respecto a los atentados que involucran el tratamiento de información y los datos personales. En consecuencia, este tipo de conductas presentan inconvenientes en su persecución y sanción desde al ámbito penal, factor que incide en su impunidad, operando a la vez un detrimento de los derechos vinculados. Por su parte, el 17% que contestó afirmativamente la interrogante planteada en la Pregunta N°6, identificó los siguientes artículos del Código Penal, que a criterio de los encuestados tipifican ataques contra los datos personales:

Tabla N°9

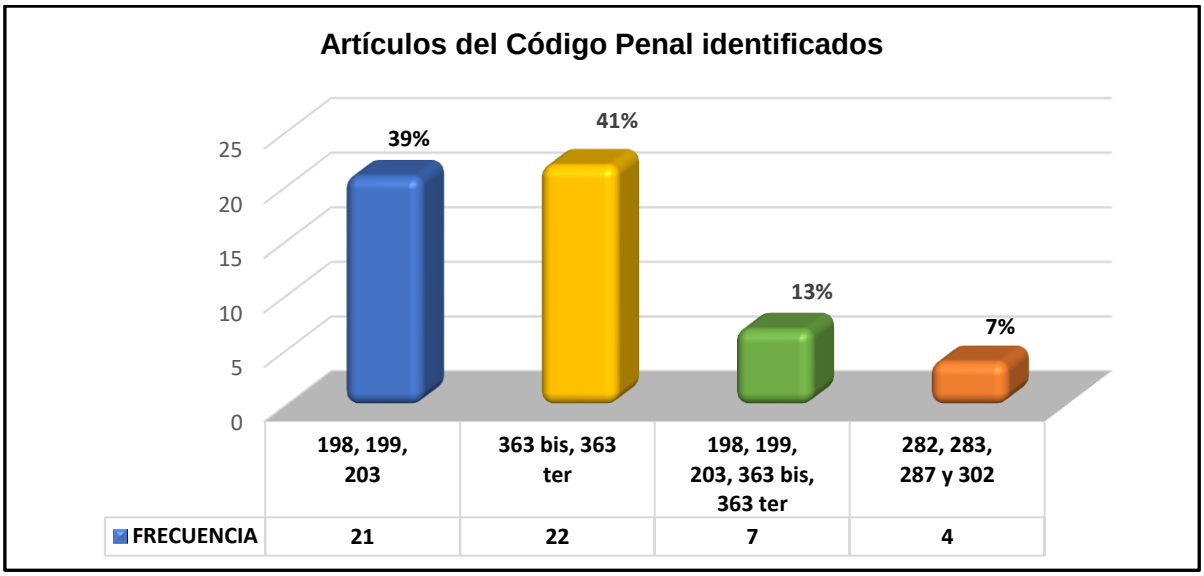
Resultados de la pregunta N°6 – Subcategoría: “Si existe”

ARTÍCULOS DEL CÓDIGO PENAL	FRECUENCIA	PORCENTAJE
198, 199, 203	21	39%
363 bis, 363 ter	22	41%
198, 199, 203, 363 bis, 363 ter	7	13%
282, 283, 287, 302	4	7%
TOTAL	**54**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°7

Resultados de la pregunta N°6 – Subcategoría: “Si existe”



Fuente: elaboración propia (2019)

El 41% expresa que el Código Penal tipifica atentados contra los datos personales, en los Artículos 363 bis (Manipulación informática) y 363 ter (Alteración, acceso y uso indebido de datos informáticos); sobre el particular, como fue analizado en el apartado: La protección de datos personales en la legislación boliviana, estos artículos están orientados de manera general a delitos informáticos, siendo de carácter amplio y exiguo para abarcar en la Era digital los distintos tipos de criminalidad informática y ciberdelitos; así también, no incluyen el uso y manejo de información y datos personales en soportes que no sean informáticos.

Por su parte, el 39% identificó a los Artículos 198 (Falsedad material), 199 (Falsedad ideológica) y 203 (Uso de instrumento falsificado) del Código Penal, lo cual denota que, desde la perspectiva de este porcentaje de encuestados, la falsificación de documentos y su uso, contienen disposiciones aplicables a los datos personales. Al respecto, estos artículos señalan:

> Artículo 198.- (FALSEDAD MATERIAL). El que forjare en todo o en parte un documento público falso o alterare uno verdadero, de modo que pueda resultar perjuicio, incurrirá en privación de libertad de uno a seis años.
> Artículo 199.- (FALSEDAD IDEOLÓGICA). El que insertare o hiciere insertar en un instrumento público verdadero declaraciones falsas concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con privación de libertad de uno a seis años.
> En ambas falsedades, si el autor fuere un funcionario público y las cometiere en el ejercicio de sus funciones la sanción será de privación de libertad de dos a ocho años.
> (…) Artículo 203.- (USO DE INSTRUMENTO FALSIFICADO). El que a sabiendas hiciere uso de un documento falso o adulterado será sancionado como si fuere autor de la falsedad.

Como se colige de lo anterior, estos delitos, no incluyen disposiciones específicas respecto a datos personales y si bien los documentos en su generalidad pueden contener datos pasibles de falsificación, estos tipos penales, no contemplan otros soportes al margen de los documentales (documento público o instrumento público).

Aun cuando este factor puede ser salvado considerando la regulación vigente inherente a documentos digitales; el tipo penal no describe otras modalidades en las que se atenta contra un dato personal fidedigno, como ser su acceso y uso no autorizado, su revelación no autorizada u otras variedades de tratamiento, limitándose a la falsedad, es decir a la alteración y utilización de un documento falso o adulterado. Por su parte, el 13% citó a los Artículos 198 (Falsedad material), 199 (Falsedad ideológica), 200 (Uso de instrumento falsificado), 363 bis (Manipulación informática) y 363 ter (Alteración, acceso y uso indebido de datos informáticos)

de manera conjunta y por último el 7% manifestó otras opciones en las que se incluyen los Artículos 282 (Difamación), 283 (Calumnia), 287 (Injuria) y 302 (Revelación de secreto profesional), los cuales expresan:

> Artículo 282.- (DIFAMACIÓN). El que de manera pública, tendenciosa y repetida, revelare o divulgare un hecho, una calidad, o una conducta capaces de afectar la reputación de una persona individual o colectiva, incurrirá en prestación de trabajo de un mes a un año o multa de veinte a doscientos cuarenta días.
> Artículo 283.- (CALUMNIA). El que por cualquier medio imputare a otro falsamente la comisión de un delito, será sancionado con privación de libertad de seis meses a dos años, y multa de cien a trescientos días.
> (…) Artículo 287.- (INJURIA). El que por cualquier medio y de un modo directo ofendiere a otro en su dignidad o decoro, incurrirá en prestación de trabajo de un mes a un año y multa de treinta a cien días.
> Si el hecho previsto en el Art. 283 y la injuria a que se refiere este artículo fueren cometidos mediante impreso, mecanografiado o manuscrito, su autor será considerado reo de libelo infamatorio y sancionado con multa de sesenta a ciento cincuenta días, sin perjuicio de las penas correspondientes.
> (…) Artículo 302.- (REVELACIÓN DE SECRETO PROFESIONAL). El que teniendo conocimiento de secretos en virtud de su estado, ministerio, profesión, empleo, oficio, arte o comisión, los revelare sin justa causa, o los usare en beneficio propio o ajeno, si de ello se siguiere algún perjuicio, será sancionado con privación de libertad de tres meses a un año y multa de treinta a cien días.

Sobre el particular, señalar que la difamación supone vulnerar la buena fama de una persona mediante la publicación de hechos o información que ocasione daños a su reputación; la calumnia, es entendida como la atribución falsa de un delito a otra persona. A su turno, la injuria involucra la ofensa en el honor a través de un insulto o acto que denigre la dignidad de la persona; por consiguiente, lo que se protege en estos artículos es la dignidad, el honor y la honra de las personas de acciones que atenten contra los mismos. Si bien estos tipos penales circunstancialmente tienen relación con datos personales; empero, estos ataques no se circunscriben únicamente a hechos de esta naturaleza, así como tampoco las citadas figuras penales contemplan otras conductas que específicamente lesionan la información y los datos personales, como su acceso, cesión, alteración ilícita u otras modalidades de procesamiento.

En cuanto al Artículo 302, se encuentra orientado a las personas que en virtud de su estado, ministerio, profesión, empleo, oficio, arte o comisión tienen conocimiento de determinada información secreta y la revelan o usan causando perjuicio, fuera de ello el tipo penal no

comprende datos de otra naturaleza, como tampoco incluye conductas inherentes a la difusión o cesión de datos no autorizados, que en los hechos se presentan habitualmente.

El resultado global indica desde la visión de los encuestados, que los citados ilícitos resultan aplicables a hechos que atentan contra la información y los datos personales; aun cuando no consideran su tutela de manera específica; en consecuencia, el estudio devela que, en la praxis, de presentarse casos en los que se soslayan datos personales, se subsumen los hechos a disposiciones penales consideradas como delitos tradicionales.

Debe tenerse presente que los datos personales, conciernen a un individuo identificado o identificable, sea que se trate de información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, es decir aquellos datos que nominada e individualmente permiten determinar con precisión los antecedentes personales de los ciudadanos, como el nombre, dirección, teléfono, número de identificación tributaria, o datos sensibles como los vinculados a la salud, biométricos, u orientación sexual, entre otros. En lo anterior radica un fundamento más para incluir en la normativa jurídico penal regulaciones precisas, que se ajusten a los requerimientos actuales y sean empleadas por las autoridades del Órgano Judicial, Ministerio Público y abogados litigantes, y que coadyuven a investigar, tipificar y sancionar conductas ilícitas derivadas del uso inapropiado de datos personales, de lo que se colige, que se está frente a un bien jurídico cuya salvaguarda incide en la tutela del derecho de autodeterminación informativa, como facultad del individuo para ejercer un control efectivo sobre sus datos.

Resultados de la pregunta N°7. ¿Se debería incorporar un tipo penal para la protección de datos personales en el Código Penal?

Tabla N°10

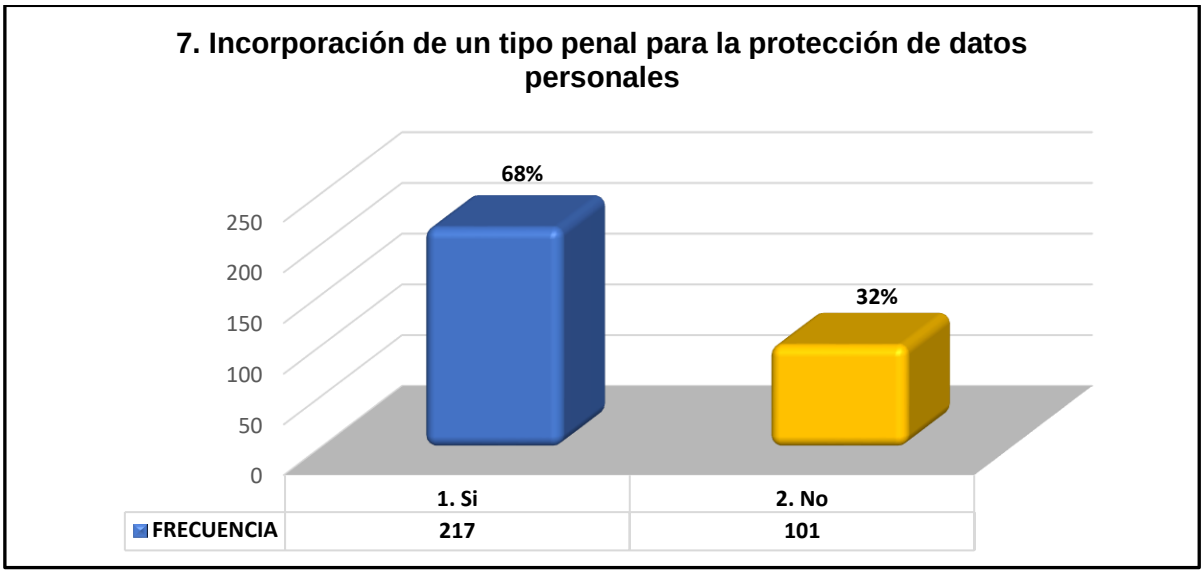
Resultados de la pregunta N°7

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Si	217	68%
2. No	101	32%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°8

Resultados de la pregunta N°7



Fuente: elaboración propia (2019)

El 68% respondió afirmativamente a la cuestionante, mientras que el 32% indica no estar de acuerdo con incorporar un tipo penal para la protección de datos personales en la norma sustantiva penal boliviana.

El criterio mayoritario de los encuestados, refleja desde su perspectiva que consideran pertinente la inclusión de nuevas disposiciones en el Código Penal respecto a datos personales. Cabe agregar que conforme a lo analizado en el acápite subtitulado: La protección de datos personales en la legislación boliviana del Marco Teórico de la presente investigación, las actuales disposiciones normativas penales no están diseñadas con especificidad para la persecución y sanción de conductas de esta naturaleza, resultado que, de similar manera, concuerda con los datos arrojados en respuesta a la Pregunta N°6 del presente cuestionario.

El acceso a la información relacionada con los datos personales permite a los delincuentes intervenir en muchos ámbitos de la vida económica y social. Por otra parte, esta información, además de procesarse, generalmente se almacena en bases de datos, que son por ese motivo un blanco potencial para los delincuentes. En la actualidad, la información sobre las cuentas, las contraseñas, las direcciones de correo electrónico y las direcciones IP, entre otros, se han convertido en elementos tan importantes como la cédula de identidad o el pasaporte, para verificar, identificar o autenticar operaciones realizadas en las redes.

Las Tecnologías de Información y Comunicación permiten que los delincuentes obtengan una infinidad de datos personales con el mínimo esfuerzo, pues muchos datos están a disposición

de quien tenga interés en los mismos, es así que otro factor de relevancia para tipificar estas vulneraciones, radica en que el uso ilícito de información personal puede dar lugar en lo posterior a una variedad de delitos que tienen como insumo estos datos, razón por la que con la inclusión de este tipo penal, se habilitaría al sistema de justicia para que intervenga desde fases iniciales evitando que otras transgresiones mayores se consumen. No debe pasarse por alto que la misión fundamental del derecho penal es la protección de aquellos intereses que son estimados esenciales para la sociedad y que permiten mantener la paz social, es por ello que esta rama jurídica no puede ser ajena a la evolución tecnológica, dado que los delitos de la nomenclatura tradicional, resultan insuficientes y llegan a convertirse en obsoletos, consecuentemente, incapaces de hacer frente a las actuales demandas de la sociedad, dentro de los límites que el propio derecho penal establece.

Resultados de la pregunta N°8. ¿Se debería incorporar un tipo penal para la protección de datos personales sensibles y datos de menores de edad en el Código Penal?

Tabla N°11

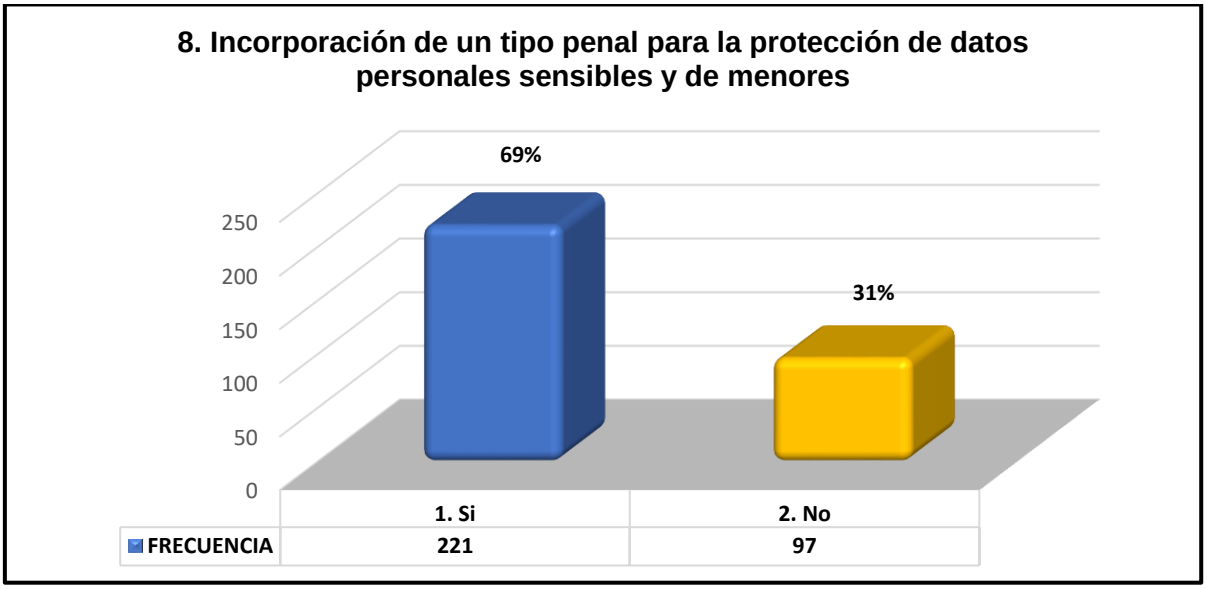
Resultados de la pregunta N°8

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Si	221	69%
2. No	97	31%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°9

Resultados de la pregunta N°8



Fuente: elaboración propia (2019)

De acuerdo a la Tabla y Gráfico precedentes, el 69% de los profesionales encuestados manifiesta su aquiescencia con la incorporación de un tipo penal para la protección de datos personales sensibles y datos de menores de edad en el Código Penal; en contraste, el 31% no apoya esta noción. Los datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información referente a la salud, vida y orientación sexual, datos genéticos y biométricos, entre otros, ameritan especial protección, dado su elevado potencial de afectación de los derechos de los individuos.

De similar manera acontece con los datos de menores de edad, quienes en la actualidad conforman un sector caracterizado por el alto empleo de aparatos tecnológicos como ordenadores, smartphones o tablets y su interacción mediante las redes sociales, aplicaciones u otros medios por los que proporcionan y comparten datos, dando lugar a situaciones de riesgo y vulnerabilidad ya que esta información personal es pasible de ser utilizada para la comisión de delitos de diversa índole.

Los datos sensibles denominados también especialmente protegidos en virtud de la particular atención que les brinda el legislador, requieren de garantías exclusivas y reforzadas y es que no todos los datos ostentan esta calidad ya que su revelación indebida puede perturbar la esfera más íntima del ser humano, con efectos discriminatorios y grave perjuicio, aspectos que justifican la inclusión de su tutela en el actual catálogo de delitos.

De acuerdo a la normativa boliviana analizada, los atentados contra este tipo de datos, no goza de una protección específica en la legislación penal vigente, siendo que es cada vez más recurrente su uso no autorizado y gracias a las Tecnologías de Información y Comunicación, su potencial de difusión se ha incrementado exponencialmente, con nefastos efectos para sus titulares, no encontrando parangón su revelación y divulgación por los clásicos medios impresos u orales, con la publicación y difusión por la red Internet, en la que se rompen barreras de espacio y tiempo, pudiendo ser la información conocida en varios lugares del orbe y accedida en todo momento de manera atemporal.

En consecuencia, los resultados de la encuesta permiten sustentar el planteamiento de incorporación en el Código Penal de un tipo penal para la protección de datos sensibles y de menores de edad, adicionando además que es ostensible la necesidad de su inclusión por la habitual frecuencia con la que se presentan estos hechos y por su incidencia en el contexto actual, de modo que se cuente con un marco jurídico efectivo y coherente con la realidad boliviana.

Resultados de la pregunta N°9. ¿Cuáles deberían ser las principales conductas a incluir en los tipos penales para la protección de datos personales?

Tabla N°12

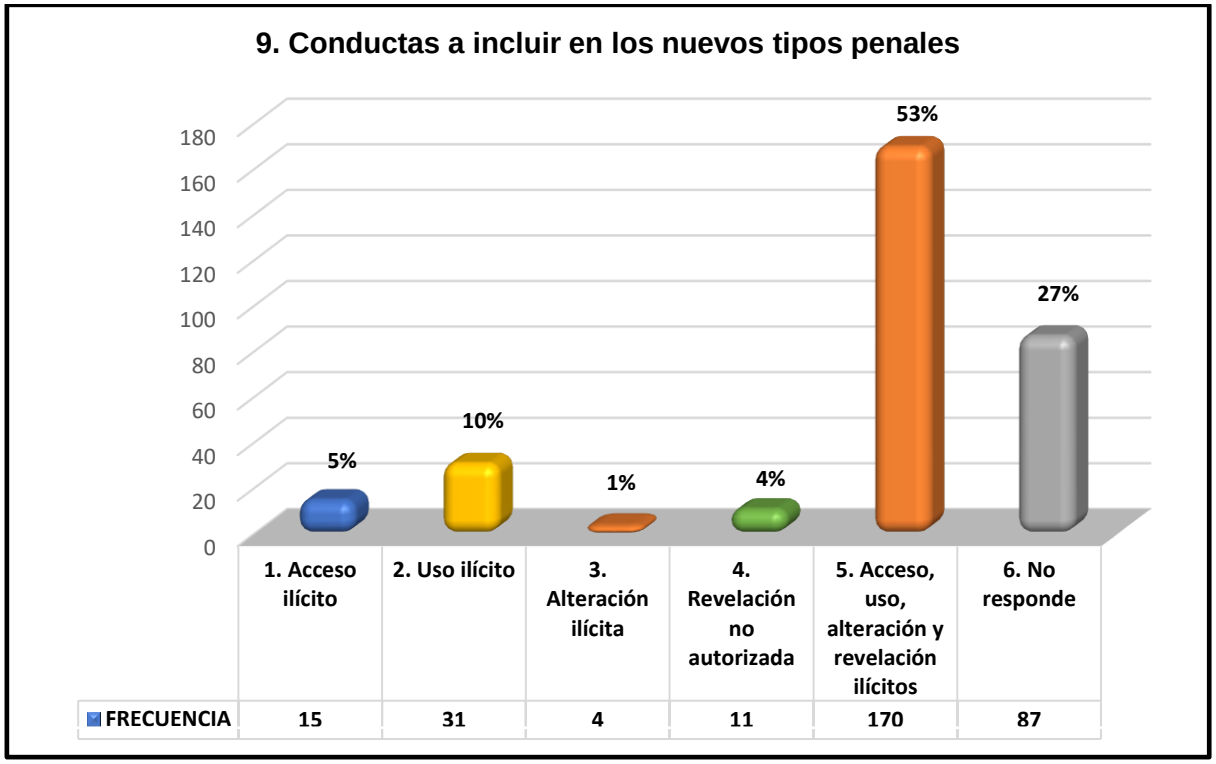
Resultados de la pregunta N°9

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Acceso ilícito	15	5%
2. Uso ilícito	31	10%
3. Alteración ilícita	4	1%
4. Revelación no autorizada	11	4%
5. Acceso, uso, alteración y revelación ilícitos	170	53%
6. No responde	87	27%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°10

Resultados de la pregunta N°9



Fuente: elaboración propia (2019)

Se aprecia que el 53% de los encuestados señaló que el acceso, uso, alteración y revelación ilícitos de datos personales, deberían incluirse como conductas en el tipo penal cuya creación

se propone; el 27% corresponde a aquellos individuos que no contestaron la interrogante. Por su parte, el 10% eligió la opción uso ilícito, el 5% acceso ilícito, el 4% revelación no autorizada y el 1% alteración ilícita.

El uso impropio de las Tecnologías de Información y Comunicación, puede dar como resultado un acceso, utilización y revelación de información personal, sin que sus titulares tengan conocimiento ni presten su consentimiento. En muchos casos los datos personales como el nombre, domicilio, fotografía, cédula de identidad y correo electrónico, son publicados en sitios web a los que no se accedió ni se otorgó tal información. Estos datos también pueden ser alterados, máxime si se considera los avances tecnológicos actuales. Sobre el particular, uno de los hechos más reiterados en la realidad boliviana es la difusión de imágenes íntimas con el fin de causar daño u obtener un beneficio usualmente de carácter económico. En consecuencia, a raíz de ello se menoscaban los derechos de los individuos afectados y de su entorno familiar.

En las conductas que atentan contra los datos personales, el delincuente actúa sin el consentimiento del titular del dato, de manera ilegal, utilizando datos de carácter público como privado. Se excluyen de esta noción los actos autorizados y establecidos por la normativa vigente, a fin de no afectar actividades de la administración pública o empresariales, investigaciones judiciales u otros procedimientos de similar naturaleza; en consecuencia, dicha información queda al margen de la penalización.

Por último, cabe señalar que el porcentaje que no respondió a este punto de la encuesta, deviene de aquellos que manifestaron no estar de acuerdo con la incorporación de estos tipos penales en la norma sustantiva penal vigente.

Resultados de la pregunta N°10. Considera pertinente incluir como sujeto activo a:

Tabla N°13

Resultados de la pregunta N°10

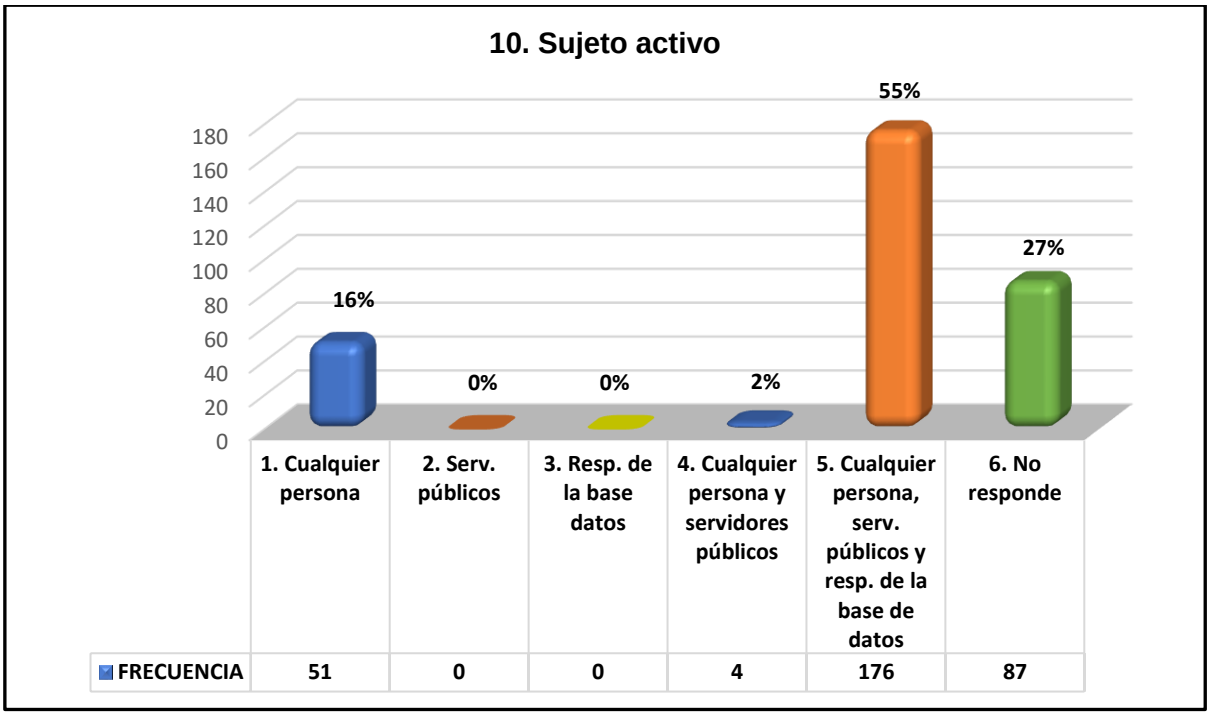
CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Cualquier persona	51	16%
2. Servidores públicos	0	0%
3. Responsable de la base datos	0	0%
4. Cualquier persona y servidores públicos	4	2%

5. Cualquier persona, servidores públicos y responsable de la base de datos	176	55%
6. No responde	87	27%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°11

Resultados de la pregunta N°10



Fuente: elaboración propia (2019)

El 55% de los abogados optó por incluir como sujeto activo en los tipos penales cuya creación se propone a: cualquier persona, servidores públicos y responsables de las bases de datos.

Un 27% corresponde a aquellos profesionales que no respondieron el cuestionario; en tanto que el 16% seleccionó la opción: cualquier persona, y el 2% eligió: cualquier persona y servidores públicos. Las opciones servidores públicos y responsable de la base de datos reflejan cada una el 0%, respectivamente.

El resultado arribado denota que no únicamente cualquier persona, sino los funcionarios públicos y los responsables de las bases de datos, pueden incidir en conductas que atenten contra los datos personales, con repercusiones nefastas para el derecho de autodeterminación informativa, puesto que particularmente éstas dos últimas categorías de sujeto activo, por la labor que efectúan poseen una especial capacidad para acceder a los

datos personales y decidir sobre su tratamiento y adicionalmente tienen el deber de observar las medidas necesarias conducentes a preservar su integridad y seguridad; no obstante, en muchas ocasiones esta condición es aprovechada para vulnerar los datos e información personal, disponer de ellos y cometer delitos.

Resultados de la pregunta N°11. Los tipos penales contra los datos personales deberían incluir la forma:

Tabla N°14

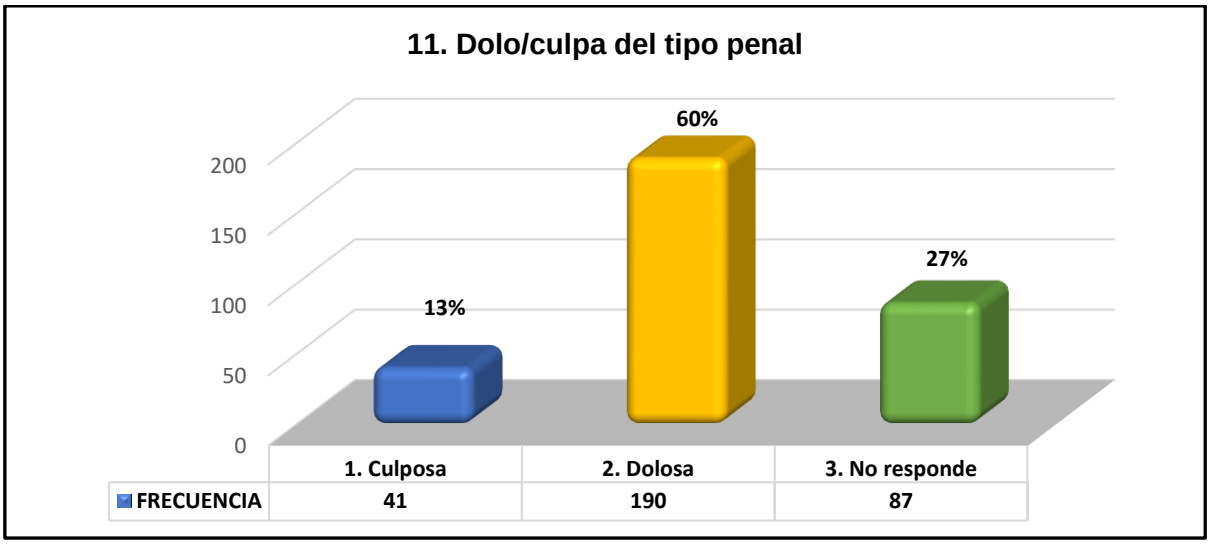
Resultados de la pregunta N°11

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Culposa	41	13%
2. Dolosa	190	60%
3. No responde	87	27%
TOTAL	318	100%

Fuente: elaboración propia (2019)

Gráfico N°12

Resultados de la pregunta N°11



Fuente: elaboración propia (2019)

Según la Tabla y el Gráfico precedentes un 60% de los encuestados señala que los tipos penales cuya creación se propone deben incluir la forma dolosa, el 27% de los encuestados no responde, mientras el 13% se inclina por incluir la forma culposa. De acuerdo al anterior resultado, los tipos penales de protección de datos personales, deben revestir la forma dolosa, cometidos bajo conciencia y voluntad de un individuo para realizar una o varias acciones ya sea con el fin de obtener un beneficio propio o para un tercero y generando un perjuicio a otra

persona, es decir querer desencadenar el resultado típico. En lo concerniente a la tutela penal de los datos personales, de acuerdo al Capítulo IV Legislación Comparada de la presente investigación, se incluyen en el catálogo penal aquellas conductas en las que existe una intención clara de producir el resultado final de manera deliberada, no dejando lugar para la culpa como manifestación de la imprudencia, impericia o negligencia.

Sobre el particular el Código Penal boliviano, en su Artículo 13 quater, dispone: “Cuando la ley no conmina expresamente con pena el delito culposo, sólo es punible el delito doloso”; es decir que para que un delito se considere culposo debe estar previsto explícitamente de ese modo. El dolo consta de un elemento intelectivo y de otro volitivo, de conciencia y de voluntad, de conocimiento de la presencia de los elementos de un delito y del querer realizar tales hechos. Bajo dichos parámetros, los delitos contra los datos personales se presentan como tipos eminentemente dolosos ya que se imputa el hecho delictivo al sujeto que goza de pleno y suficiente conocimiento de que con su actuar cuestiona la vigencia de una expectativa social básica contenida en la norma penal; y no obstante de ello, recaba, accede, utiliza, altera, cede, revela o efectúa un tratamiento ilícito de datos personales, generando perjuicio a los titulares de estos datos, usualmente con el fin de lograr un beneficio, es decir habiendo tenido la posibilidad de actuar conforme a derecho no lo hace. En cuanto a las acciones u omisiones culposas, a criterio del estudio debieran tratarse desde la óptica del derecho administrativo que impone sanciones menos gravosas, frente al derecho penal que afecta la libertad individual.

Al respecto, manifestar que el concepto de culpa desde el ámbito administrativo se asocia con la debida diligencia más que con el elemento doloso o culposo del derecho penal, ya que las sanciones administrativas no exigen la presencia del dolo, sino que basta con el descuido para que se configure la infracción, es así que la exigencia de un comportamiento culpable debe entenderse, salvo en los supuestos que se exija la concurrencia de una conducta deliberada, como el mero incumplimiento del deber de actuar diligentemente (Balbín, 2011, p. 467). En similar sentido, Mendoza (2016, p.45), asiente: “(…) para la configuración de las infracciones basta la culpa, a menos que una norma exija el dolo (…) En los delitos, en cambio, se exige el dolo, salvo que una disposición particular requiera la culpa para un delito determinado”.

Resultados de la pregunta N°12. Los delitos contra los datos personales deberían sancionarse con una pena de:

Tabla N°15

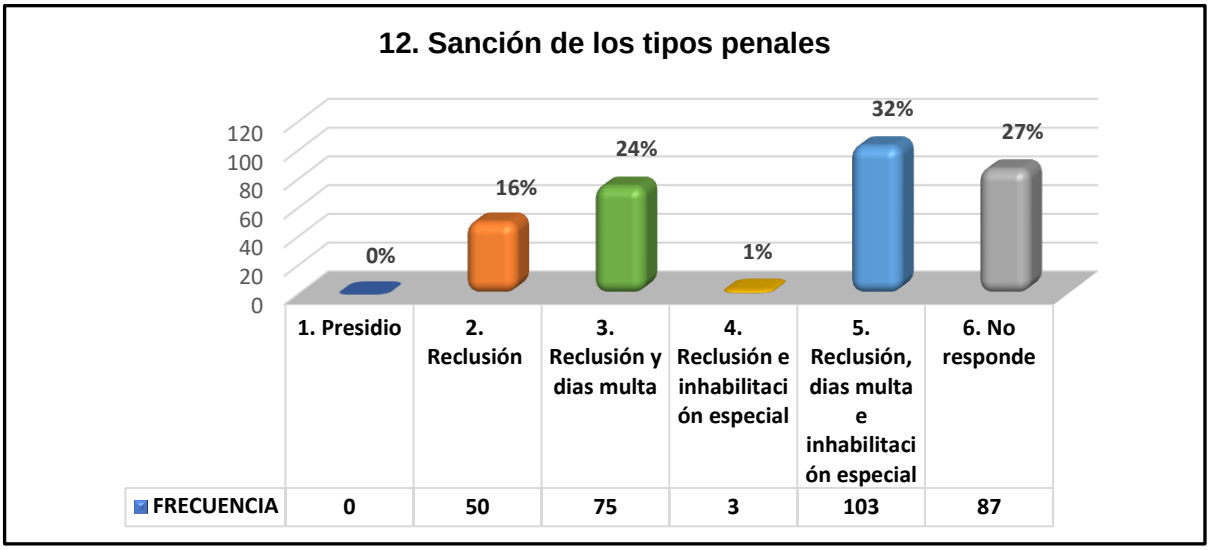
Resultados de la pregunta N°12

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Presidio	0	0%
2. Reclusión	50	16%
3. Reclusión y días multa	75	24%
4. Reclusión e inhabilitación especial	3	1%
5. Reclusión, días multa e inhabilitación especial	103	32%
6. No responde	87	27%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°13

Resultados de la pregunta N°12



Fuente: elaboración propia (2019)

Los resultados develan que un 32% está de acuerdo con que la sanción a establecerse en los tipos penales de protección de datos personales sea de reclusión, días multa e inhabilitación especial, es decir que contemplen una pena privativa de libertad, otra de carácter pecuniario y otra privativa de derechos. El 27%, corresponde a aquellos encuestados que no contestaron este punto del cuestionario. El 24%, optó por elegir la opción de incorporar en los tipos penales propuestos, la pena de reclusión y días multa, el 16% se inclinó por la pena de reclusión, en tanto que el 1% consideró la opción reclusión e inhabilitación especial, y por último el 0% concierne a la pena de presidio. El criterio mayoritario, concuerda con los resultados de la Pregunta N°10, toda vez que al considerarse como sujeto activo a los servidores públicos y responsables de las bases de datos, además de la pena privativa de libertad ameritaría una sanción de inhabilitación especial para el ejercicio del cargo o actividad laboral de los cuales se valieron para cometer los hechos delictivos. También devela que los profesionales

encuestados consideran que debe sancionarse este ilícito con rigurosidad, al incluir penas pecuniarias y privativas de derechos para los sujetos que transgredan la norma penal.

Resultados de la pregunta N°13. Con la incorporación de tipos penales orientados a la protección de datos personales en el Código Penal boliviano, se contribuirá a que la tutela del derecho de autodeterminación informativa:

Tabla N°16

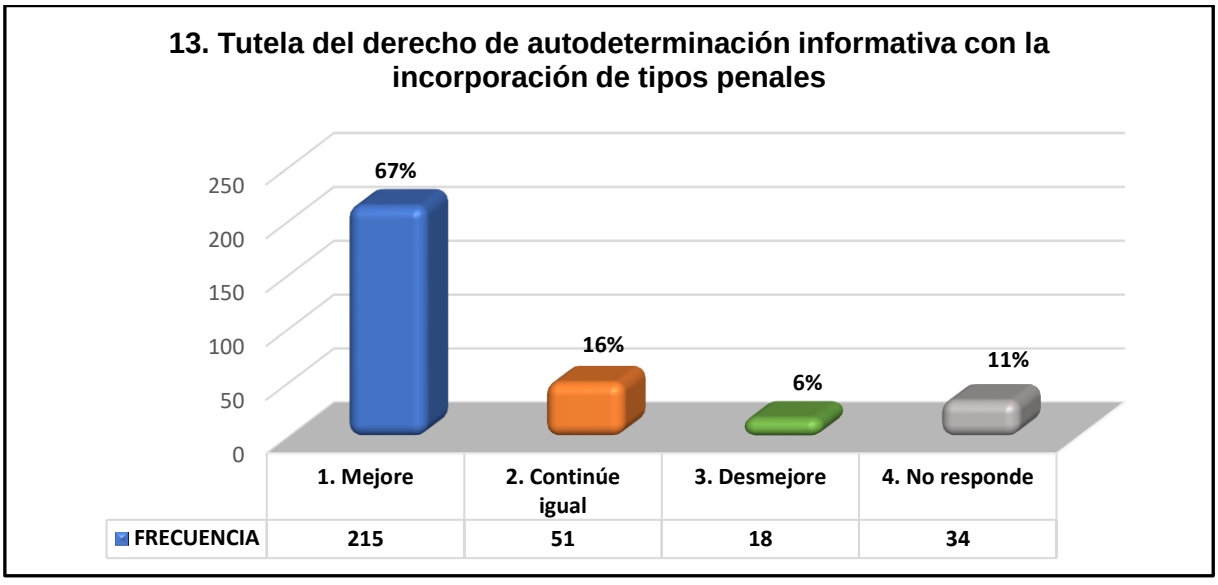
Resultados de la pregunta N°13

CATEGORÍA	FRECUENCIA	PORCENTAJE
1. Mejore	215	67%
2. Continúe igual	51	16%
3. Desmejore	18	6%
4. No responde	34	11%
TOTAL	**318**	**100%**

Fuente: elaboración propia (2019)

Gráfico N°14

Resultados de la pregunta N°13



Fuente: elaboración propia (2019)

Un 67%, señala que, con la incorporación de tipos penales de protección de datos personales en el Código Penal, se contribuirá a mejorar la tutela del derecho de autodeterminación informativa en el Estado Plurinacional de Bolivia; el 16% indica que continuaría igual, el 11% comprende aquellos encuestados que no responden, en tanto que el 6% asevera que desmejoraría.

Como se infiere de la Tabla y el Gráfico respectivos, es categórica la percepción de los encuestados en torno a la optimización del derecho a la protección de datos personales, si opera la incorporación de los enunciados tipos penales, sustentando esta necesidad ante un vacío jurídico ostensible en dicho ámbito. Así también se coadyuvará a evitar mayores daños a los derechos de privacidad, intimidad y otros vinculados y podrán imponerse las respectivas sanciones a los responsables, por lo que hechos de esta naturaleza no quedarán impunes.

En ese contexto, recalcar que la recopilación y el análisis de los datos personales, así como sus posibles usos inciden directamente no sólo en el efectivo disfrute de los derechos fundamentales, sino también en la dignidad y autonomía de las personas (Garriga, 2016, p.57).

Finalmente, corresponde señalar que compete al Estado la protección de los derechos fundamentales, instaurando mecanismos de garantía efectivos para este fin, máxime si se tiene presente que es precisamente el Estado el mayor recolector de datos personales; lo contrario, implica un incumplimiento de imperativos contenidos en los Artículos 9 numerales 2 y 4; 14 parágrafos I y III y 22 de la Constitución Política del Estado, que refieren el deber de garantizar el bienestar, el desarrollo, la protección y la seguridad de las personas, en el marco del cumplimiento de los principios, valores, derechos y deberes reconocidos y consagrados en la Constitución, y su libre y eficaz ejercicio, así como la protección primordial de la dignidad y la libertad de los individuos.

3.2 Presentación y análisis de los resultados de la entrevista

Los resultados de la aplicación de la entrevista, se reseñan a continuación:

Pregunta Nº 1: ¿Cuál es la importancia de los datos personales?

- (…) esto yace en lo que denominamos como libertad informática, ha venido a surgir como un neologismo a partir del catálogo fundamental que desde la Declaración Universal de Derechos Humanos se ha gestado (…) ya la comunidad internacional ha dejado por sentado que es un derecho humano, entonces la importancia de un dato personal hace a la propia determinación del ser humano, nos configuramos como humanos a partir del ejercicio pleno de los datos personales que nosotros queremos determinar, restringir, establecer. A partir de la libertad informática, te da lugar a otro neologismo del derecho que hace a la autodeterminación informativa, entonces surge

una protección más particular y más especial en un espacio que no es espacio, que es el ciberespacio, la sociedad de la información (…). (Entrevistado N°1)

- (…) se refiere a la información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo. Por tanto, se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente. (Entrevistado N°2)
- (…) los datos personales como tal se refuerzan a través de nuevos derechos como el derecho de autodeterminación informativa, tienen una protección extra, va más allá, cuando hablamos del derecho a la protección de datos personales, hablamos de la libertad que tiene cada persona de decidir que va a pasar con su información, esa es la importancia de los datos personales. (Entrevistado N°3)

Pregunta N° 2: ¿Cuál es la incidencia de las Tecnologías de Información y Comunicación en la recolección y difusión de datos personales?

- (…) los problemas a los que se han tenido que enfrentar estos datos personales, la privacidad y la intimidad de los ciudadanos han sido particularmente a partir de tres circunstancias o escenarios vamos a decir, ante la posible hipervigilancia de los Estados, sistemas de recolección, vigilancia, intromisión de datos a los que no se debiese ingresar pero se tiene acceso; mercantilización de los datos en el sector privado y comisión masiva de delitos en tanto a derechos sensibles de información que está en la red y se utiliza para fines delictivos, es una trilogía bastante sintética que se hace para encontrar la relevancia de la incidencia de las Tecnologías de la Información y Comunicación (…) hay una teoría que establece que hay un hiperdaño si vale el término, cuando se comete el delito a través de las redes por la masividad que implica aquello, que es el elemento trascendental de la incidencia de las Tecnologías de Información y Comunicación. (Entrevistado N°1)
- (…) en todos los aspectos de la sociedad actual, ha sido determinante y decisiva en la recolección y difusión de los datos personales, ya que los mismos pueden ser captados de manera instantánea y luego transmitidos automáticamente a los más diversos lugares, la herramienta más eficaz para esto lo ha constituido la red Internet ya que numerosos portales recopilan datos personales de sus usuarios. (Entrevistado N°2)
- (…) las nuevas Tecnologías de Información y Comunicación, han facilitado y agilizado el tratamiento de datos personales; por lo tanto, hacen cada vez más dificultosa la tarea de prestar una correcta protección, para el tratamiento de datos. La vulneración de datos personales ha existido desde siempre, mucho antes de la tecnología, pero

las nuevas tecnologías, han impulsado el tratamiento de los mismos y por lo tanto, generan muchas vulneraciones y no permite que el derecho tradicional abarque la protección de estos datos. (Entrevistado N°3)

Pregunta Nº3: ¿Considera que las entidades públicas y privadas brindan una efectiva protección de los datos personales de los bolivianos?

- Es un rotundo no, vamos a decir que la regla es que no en la pública y en la privada, (…) la excepción en el ámbito privado es el sector bancario, pero no es precisamente por una diligencia de proteger datos, no hay esa cultura de protección sino porque al estar adscritos a ciertos convenios con organismos internacionales que hacen al SWIFT o sea a entidades internacionales que establecen ciertos estándares, ellos están obligados a cumplir aquello y eso hace que tengan que afinar y optimizar sus medidas que hagan a una efectiva protección de datos de sus usuarios (…). (Entrevistado N°1)
- Existe en Bolivia una protección parcial a los datos personales de los ciudadanos, desde la promulgación de la nueva Constitución boliviana el año 2009, que incorpora en la sección respectiva sobre los derechos civiles, en el Artículo 21, numeral 2, que los bolivianos tienen derecho a la privacidad, intimidad, honra, honor, propia imagen y dignidad. Y lo contemplado en la Constitución con referencia a la Acción de Protección de la Privacidad. Asimismo, con la vigencia de la Ley N°164, Ley general de Telecomunicaciones, Tecnologías de Información y Comunicación, pero aún falta una visión integral, una ley marco específica, que sería la razón principal para considerar que las entidades públicas y privadas no brindan actualmente una adecuada protección a los datos personales de los bolivianos, en especial en el tema de la seguridad y el uso responsable. (Entrevistado N°2)
- No, lamentablemente en Bolivia las entidades públicas y privadas no cuentan con protocolos necesarios (…). (Entrevistado N°3)

Pregunta Nº4: Desde su experiencia, ¿cuáles son las formas más recurrentes en que se vulnera el derecho a la protección de datos personales o autodeterminación informativa en el Estado Plurinacional de Bolivia?

- (…) lamentablemente es lo que nosotros conocemos como el eslabón más débil de la cadena, que es el ser humano, más del 50%, casi el 62% se ha encontrado que vulnerabilidades, incidentes y amenazas que han llevado a un posterior y consecuente compromiso, han visto comprometidos el conjunto de protección de datos personales

por error humano, que responde a diferentes aristas, un error humano que hace a una mala configuración de la unidad informática, un error de la falta de capacitación del personal que ha abierto un correo que no debía abrir, un error de la persona que ha sincronizado su celular personal con el correo institucional y ha abierto a su lista de datos, se abre el abanico pero en fin, es error humano. (Entrevistado N°1)

- Un ejemplo claro lo tuvimos en la inclusión de personas fallecidas que aparecieron votando en las últimas elecciones nacionales de octubre pasado. (Entrevistado N°2)
- (…) a través de aplicaciones que se estaban desarrollando como la billetera móvil que se utilizó para el pago del segundo aguinaldo, esta plataforma vulneraba la protección de datos personales porque no nos estaba informando correctamente el tratamiento de los datos que estaba haciendo, cuál era el tratamiento real, con quién compartían o a quien comunicaban o transferían la información. Otro que es un hito en el tema de seguridad de la información, fue lo que pasó en el Tribunal Supremo Electoral, muchos aparecimos empadronados como militantes de partidos políticos, entonces ahí hubo un tratamiento de datos porque nadie sabe de dónde vertieron los datos, de dónde se nutrieron de estos datos, y más allá de eso, no nos daban un derecho de rectificación sobre los datos, porque solamente te permitían eliminar el dato, ósea la cancelación dentro de los derechos ARCO, pero no te permitían rectificarlo (…). (Entrevistado N°3)

Pregunta Nº5: ¿El Código Penal contempla previsiones para la tutela de los datos personales?

- Estamos ceñidos y adscritos, casi acorralados a valernos de los dos tipos penales existentes en el Código Penal, 363 bis y ter y de manera más particular entendemos que en la exposición de motivos de la inserción que se hace cuando se añade el 363 bis y ter, la naturaleza de la configuración de estos tipos penales responde más que todo a un interés patrimonial porque si tú haces una breve y fugaz teoría del delito en la tipología de los dos delitos, hacen a que los presupuestos tienen que ser en perjuicio de un tercero y que tiene que afectar al patrimonio de un tercero, entonces tienen una protección al bien jurídico patrimonial (…). (Entrevistado N°1)
- (…) la única referencia es el artículo 363 ter. del Capítulo XI del Código Penal, referente a Delitos Informáticos, que se refiere a alteración, acceso y uso indebido de datos informáticos. (Entrevistado N°2)
- (…) las herramientas de la cuales nos podríamos valer sería en analogía otros tipos penales que intenten abarcar derechos más complejos como podría ser delitos contra la intimidad, contra la honra, el honor, ese tipo de delitos, pero no son los móviles adecuados, yo creo que sería una suerte de forzar mucho la figura; lo mismo con el

secreto profesional en temas médicos, pero no son los móviles adecuados, porque en ellos la tutela específica no es el dato personal, sino una esfera más amplia como es la intimidad y como bien sabemos que la intimidad como tal no es un derecho tan exquisito como el de protección datos personales, entonces no hay un delito que tenga específicamente como bien jurídico tutelado el dato personal. (Entrevistado N°3)

Pregunta Nº6: ¿Las disposiciones existentes en el Código Penal son suficientes para sancionar conductas que atenten contra los datos personales?

- Esto me habilita para hacer una crítica en el régimen sancionatorio, porque como bien te explicaba antes, si tu revisas la exposición de motivos de la inserción estos dos tipos penales de orden informático tienen la gran falencia de que la sanción es demasiado inferior, es demasiado baja, para el impacto del delito que se puede cometer (…) el daño que yo he provocado al banco en este caso digamos, es totalmente desproporcional de la sanción que se me va a dar porque cuando se ha redactado eso pareciera que no se tenía la dimensión o la concepción del posible hiperdaño que se iba a cometer por la masividad y colectividad de la información a la que se puede acceder a través de los datos, entonces las disposiciones existentes en el Código Penal son suficientes para sancionar conductas que atenten contra los datos personales, por supuesto que la respuesta es evidentemente negada, y con la particularidad de que las sanciones existentes son demasiado bajas. (Entrevistado N°1)
- (…) no son suficientes, pues está temática ha evolucionado mucho en su tratamiento penal. (Entrevistado N°2)
- Sí, no son suficientes porque son delitos que no están pensados para tutelar ese bien jurídico. (Entrevistado N°3)

Pregunta Nº7: ¿A su criterio, se debería incorporar tipos penales que sancionen los hechos más graves que atenten contra datos personales, datos personales sensibles y de menores de edad en el Código Penal?

- Ya se habría incorporado tipos penales que sancionen los hechos más graves que atenten contra datos personales y que a la vez subsanaban la crítica que hacía en la pregunta anterior, ya que se establecía una sanción más alta referida a las vulneraciones que hacen a este bien jurídico protegido de la privacidad y la intimidad, te hablo específicamente de la Ley del Sistema Penal abrogada por otro tipo de circunstancias, pero que para nosotros los entendidos en materia de la rama del

derecho informático era un gran avance el Capítulo que insertaba seis artículos que hacían a nuevos tipos penales que contemplaban esta posible vulneración de protección de datos personales. Esta estructura de un Capítulo que hacía a los delitos informáticos en la Ley del Sistema Penal se adscribía a la lógica del Convenio de Ciberdelincuencia de Budapest (…). (Entrevistado N°1)

- Si, sería conveniente, pues entre los datos personales en general se diferencian a los datos personales sensibles, los cuales se refieran a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, y está también el tema de los menores de edad, para lo cual se podrían incorporar tipos penales específicos. (Entrevistado N°2)
- Yo los podría incluir, pero más dirigidos a un ámbito público, dirigidos a los funcionarios públicos que en razón de su cargo traten datos personales con fines ilícitos, ilegales, sin respetar los principios y en ciertas circunstancias ajenas a lo normalmente permisible, en ese caso debería haber una penalización. Pero una penalización al sector privado lo veo un poco desmedido, quizás al sector privado lo podrías hacer cuando son datos personales sensibles que son datos más protegidos. (Entrevistado N°3)

Pregunta Nº8: ¿Cuáles deberían ser las conductas punibles en los tipos penales para la protección de datos personales?

- (…) el delito informático puede estar concebido como medio o como fin, en este caso estamos adscritos a que en el ámbito de la acción privada se ve el delito informático como un medio, es decir el daño está porque me has calumniado, pero en lugar de calumniarme en el periódico escrito me has calumniado en el Facebook, pero lo que no se termina de entender, es que cuando el medio es distinto el daño se intensifica, porque no es lo mismo que yo cuele en la pared en un papel un insulto contra una persona, o que lo publique en una red social porque en ese mismo segundo en el papel lo van a leer dos personas, en el otro dos mil (…).

  (…) hay casos particulares en los que amerita insertar esto, un tipo penal específico pero tenemos que tener muchísimo cuidado porque en palabras del Dr. Zaffaroni, estamos en el enfrentamiento de un libertinaje normativo de innovación de que a todo le quieres poner informático al final, y a una posición estacionaria en la cual dices ya está todo contemplado, no necesitas más, porque como decimos es sólo un medio, entonces todo bien jurídico ya está protegido, pero no es necesariamente así (…). (Entrevistado N°1)

- De forma general, podemos mencionar el apoderamiento, la utilización o la modificación, sin estar autorizado y en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro, que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de fichero o registro público o privado. El bien jurídico protegido sería el derecho a la intimidad, esta conducta por ejemplo se la denomina en Colombia como violación de datos personales. Sin embargo, debemos considerar también la comisión de delitos informáticos contra la información y los datos personales. (Entrevistado N°2)
- (…) englobar el tratamiento como acto me parece una técnica correcta, pero lo tienes que concatenar necesariamente con una finalidad, por que una persona no trata el dato de mala fe porque sí. (Entrevistado N°3)

Pregunta Nº9: ¿Quiénes deberían ser incluidos como sujetos activos en los ilícitos contra los datos personales?

- Cuando te estableces un mapa de la teoría del delito en el cual vas a establecer sujeto activo y sujeto pasivo, inevitablemente no puedes hacerlo personal tiene que ser impersonal tanto el sujeto activo como el sujeto pasivo, sin descuidar que posiblemente puedas establecer ciertos parámetros de particularidad en la función pública, en tanto a la normativa preexistente, en concreto la Ley del Estatuto del Funcionario Público y la ley SAFCO por ejemplo (…) quienes deberían ser incluidos, si tu intentas incluir a uno inevitablemente estas excluyendo a otros.
  (…) yo estoy de acuerdo con esta postura doctrinaria de quienes defienden que debiese darse una agravante en el ámbito de la comisión de delitos especiales, a quienes tienen algún conocimiento en el ámbito informático sean o no servidores públicos ¿por qué? porque alguien que tiene conocimientos específicos en el ámbito informático puede saber igual o más (…). (Entrevistado N°1)
- Todas aquellas personas que estén a cargo de administrar archivos correspondientes a datos personales ya sea en entidades públicas o privadas. (Entrevistado N°2)
- Orientada principalmente a los funcionarios públicos, no hay un delito penal para empresas, siempre se termina enjuiciando a la persona natural que está en representación. (Entrevistado N°3)

Pregunta Nº10: Los tipos penales contra los datos personales, ¿deberían contemplar la forma culposa o dolosa?

- Imposible que puedas decantarte sólo por el comportamiento doloso, porque en la configuración de la normativa clásica penal, encuentras que los tipos penales afectan en el ámbito procedimental no tanto en el ámbito sustantivo, encuentras que va a existir en el iter criminis una gama muchísimo más amplia de la que podemos conocer, cuando se está investigando o cuando se pretende cometer un delito informático, porque tiene aristas de espacios y problemáticas que antes no estaban en la casuística específica de que tienes que configurarte una nueva cadena de la custodia (…).
  Cuando no quieres contemplar formas culposas encuentras que en la mayoría de los casos hay personas que por ahí sin querer están siendo parte en un nivel de grado de participación de un delito (…) cuando desgranas cómo es que funciona el intercambio de criptomonedas encuentras que la tecnología tiene que ver con unos que se conocen como mineros o actividad de main mine que es una minería, es decir para tú validar los bitcoins o cualquier tipo de criptomoneda te vales de otros equipos, entonces si tú estás en tú computadora navegando buscando recetas de pasteles, fácilmente tú puedes en ese momento sólo por estar conectada en la red, ser parte de un intercambio de criptomonedas que está haciendo un secuestro de un equipo. (Entrevistado N°1)
- Considero que la forma dolosa. (Entrevistado N°2)
- Tendrían que revestir la forma dolosa, porque el ámbito de la culpa correspondería a una sanción de carácter más administrativo, es decir debe existir esa intencionalidad de generar un daño o lesión a los datos personales. (Entrevistado N°3)

Pregunta Nº11: ¿Qué tipo de sanción debería corresponder a los ilícitos que atentan contra los datos personales?

- (…) de acuerdo al lineamiento que establece el Convenio de Ciberdelincuencia, la piedra angular de que funcione es la Cooperación Internacional, pero la lógica tiene que ser más preventiva, porque de cierta forma encuentras que desnaturaliza la lógica del derecho penal la comisión de delitos informáticos porque casi nunca das con el responsable, es prácticamente imposible dar con el responsable lo mucho que puedes hacer es salvaguardar o información masiva que ha sido objeto de un delito o recuperar lo que se ha perdido, sea información sea patrimonio o ambos, pero casi nunca das con la persona. (Entrevistado N°1)

- El derecho comparado nos señala que corresponden sanciones de multa pecuniarias, y hasta penas de cárcel para delitos informáticos específicos. (Entrevistado N°2)
- Yo me voy por el tema de que se penalice al funcionario público y por tanto yo si me iría por el tema de privación de libertad e inhabilitación, en un orden de las cosas. Las sanciones pecuniarias son más para el tema de sanciones administrativas. (Entrevistado N°3)

Pregunta Nº12: ¿Con la incorporación de tipos penales orientados a la protección de datos personales en el Código Penal, se lograría mejorar la tutela del derecho de autodeterminación informativa?

- (…) debiésemos establecer una nueva categorización de la información como bien jurídico protegido, al entender este paradigma tu encuentras que la tutela judicial efectiva de la autodeterminación informativa que emerge de la libertad informática, va encontrarse más protegida, porque no solo vas a estar adscrito al recurso constitucional sino que te vas a poder valer como ya lo puedes hacer tanto desde el ámbito administrativo, como de la prosecución de orden público (…). (Entrevistado N°1)
- Considero que sí, si tomamos en cuenta que la autodeterminación informativa se constituye en un derecho fundamental derivado del derecho a la privacidad, que se refiere a la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente -pero no exclusivamente- los almacenados en medios informáticos. (Entrevistado N°2)
- (…) se lograría con una legislación base y un delito penal fuerte contra los funcionarios públicos. (Entrevistado N°3)

3.3 Presentación y análisis de los resultados del estudio de caso

Se efectuó el estudio de dos casos de relevada connotación, suscitados en Bolivia y vinculados a datos personales de carácter sensible, cuyo resultado se presenta a continuación:

Tabla N°17

Estudio de caso: obtención, uso, revelación y difusión de video que contiene datos personales sensibles

Relación y contexto de los hechos

La ciudadana P.B.G., encontrándose separada de su esposo M.S.M., a fines de la gestión 2011 inició una relación sentimental con O.M.R. (Barriga, 2013), en ese contexto, mientras mantenían relaciones sexuales en el domicilio de O.M.R., a través del uso de un dispositivo digital se efectuó una grabación sin su autorización, consentimiento ni conocimiento.

Posteriormente, en mayo de 2013, P.B.G. decidió terminar con la relación amorosa, empero, O.M.R. no aceptó, exteriorizando la existencia del citado video, exigiendo dinero a cambio del mismo (20 mil dólares americanos) y pidiéndole tener acceso carnal a P.B.G., expresando que de lo contrario haría pública la grabación a través de medios de comunicación e Internet (Belmonte, 2014a; Belmonte 2014b).

El 1 de noviembre de 2013, una fracción del video con imágenes del acto sexual, fue publicado en un sitio web de la red Internet denominado Bolivia-69.com, junto a un mensaje que refería que P.B.G había engañado a su esposo M.S.M., este material fue transmitido en otras páginas y compartido en innumerables cuentas de redes sociales, así también, comercializado en diferentes puestos de venta y ferias de las ciudades de La Paz y El Alto (Opinión, 2013).

El video fue vendido al sitio web en miles de dólares de acuerdo a los datos arrojados por la Fuerza Especial de Lucha contra el Crimen (Belmonte, 2014b).

CATEGORÍAS	DESCRIPCIÓN
Conductas que vulneraron el derecho de autodeterminación informativa	• Obtener sin conocimiento ni consentimiento un video que corresponde a un acto sexual • Utilizar el video • Revelar el video • Difundir el video
Calidad de los sujetos que realizaron las conductas	• Pareja sentimental • Responsables y/o encargados de los sitios web
Tipo de dato afectado	• Sensible: vida sexual
Medios utilizados	• Dispositivo digital de grabación, que capturó imagen y audio • Red Internet (sitios web, redes sociales)
Finalidad	• Generar perjuicio • Generar lucro
Principales derechos vulnerados	• Autodeterminación informativa • Privacidad • Intimidad • Honra • Honor • Propia imagen • Dignidad
Tipos penales que se aplicaron	• Violencia familiar y doméstica, Artículo 272 bis • Extorsión, Artículo 333
Observaciones	El caso se hizo mediático al ser la víctima una conocida periodista, presentadora de televisión y locutora de radio.

Fuente: elaboración propia (2019)

- **Acciones legales asumidas por la afectada**

P.B.G., presentó querella penal ante el Ministerio Público, por los delitos de Amenazas (Artículo 293) y Extorsión (Artículo 333), siendo finalmente O.M.R. imputado por los delitos de Violencia familiar y doméstica (Artículo 272 bis) y Extorsión (Artículo 333) del Código Penal, habiendo dispuesto el Juez Noveno de Instrucción en lo Penal de la Ciudad de La Paz, la detención domiciliaria para el imputado. Al respecto, los citados artículos determinan:

> Artículo 272 bis. (VIOLENCIA FAMILIAR O DOMÉSTICA). Quien agrediere físicamente, psicológica o sexualmente dentro los casos comprendidos en el numeral 1 al 4 del presente Artículo incurrirá en pena de reclusión de dos (2) a cuatro (4) años, siempre que no constituya otro delito.
> 1. El cónyuge o conviviente o por quien mantenga o hubiera mantenido con la víctima una relación análoga de afectividad o intimidad, aún sin convivencia.
> 2. La persona que haya procreado hijos o hijas con la víctima, aún sin convivencia.
> 3. Los ascendientes o descendientes, hermanos, hermanas, parientes consanguíneos o afines en línea directa y colateral hasta el cuarto grado.
> 4. La persona que estuviere encargada del cuidado o guarda de la víctima, o si ésta se encontrara en el hogar, bajo situación de dependencia o autoridad.
> En los demás casos la parte podrá hacer valer su pretensión por ante la vía correspondiente.
> (…) Artículo 333. (EXTORSIÓN). El que mediante intimidación o amenaza grave constriñere a una persona a hacer, tolerar que se haga o deje de hacer alguna cosa, con el fin de obtener para sí o un tercero indebida ventaja o beneficio económico, incurrirá en reclusión de uno a tres años.

El Artículo 272 bis está referido a agresiones físicas, psicológicas o sexuales, es decir un maltrato a nivel físico o emocional entre dos personas involucradas por vínculos de consanguinidad o afinidad que puede darse en el contexto doméstico u otro tipo de entornos, atentando contra la integridad de la víctima; mientras que el Artículo 333 exige que la persona haga, tolere u omita algo en razón de la amenaza potencial de daño que se cierne sobre ella, de modo tal que por el impacto psicológico actúe con voluntad viciada, en el caso concreto O.M.R. pretendió constreñir a P.B.G. al pago de una suma de dinero a cambio de no publicar el video con contenido sexual, empero no logró su cometido.

De lo señalado, se colige que ambos Artículos no engloban en su descripción la obtención, uso, revelación y difusión de videos o imágenes; asimismo, debe tenerse presente que el daño ocasionado al capturar y difundir este tipo de dato sensible, trasciende más allá de la propiedad como bien jurídico tutelado por la extorsión, afectando derechos como la honra, el honor, la privacidad, la intimidad, el derecho a la protección de datos personales o

autodeterminación informativa y la dignidad como bien supremo. Si bien el comportamiento del sujeto activo en el caso de análisis se puede encuadrar en los ilícitos de Extorsión y Violencia familiar y doméstica, también se hace patente la lesión a la información sensible de la víctima correspondiente a su vida sexual.

Sobre el particular, P.B.G. expresó:

> En determinado momento yo quería dejar de vivir, tú sabes, ha sido un linchamiento espantoso para mi familia más que para mí (…) no era fácil tener que afrontar todo lo que tuve que afrontar, llega un momento de angustia tal que, yo no comía yo no dormía yo lloraba todo el día" "lo he pagado con sangre" "lo voy a cargar el resto de mi vida". (Belmonte, 2014a)

Por otra parte, P.B.G. también formuló una Acción de Protección de Privacidad, en contra de O.M.R. de conformidad a los Artículos 130 y 131 de la Constitución Política del Estado, alegando la vulneración de los derechos de privacidad, intimidad, honra, honor, propia imagen, dignidad y autodeterminación informativa, citando al efecto los Artículos 21 numeral 2, 256 y 410 de la Constitución Política del Estado, V y VI (sic) de la Declaración Americana de los Derechos y Deberes del Hombre y 11 de la Convención Americana sobre Derechos Humanos (Sentencia Constitucional Plurinacional N° 0819/2015 – S3 de 10 de agosto de 2015). Como resultado, la Sala Penal Primera del Tribunal Departamental de Justicia de La Paz, denegó la tutela solicitada por no ostentar el accionado la legitimación pasiva; empero, dispuso que la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT) se encargue de retirar, anular y eliminar toda publicación que involucre a la ciudadana afectada; asimismo, que por las oficinas pertinentes de los Gobiernos Autónomos Municipales de La Paz y El Alto, así como la Gobernación, sea retirado todo material del mercado donde se involucre a P.B.G y O.M.R. A su turno, el Tribunal Constitucional Plurinacional, en revisión, confirmó en parte la Resolución del Juez de Garantías y concedió la tutela impetrada, más no así contra O.M.R., sino contra la Fiscalía General del Estado por no adoptar las medidas pertinentes de protección en favor de la víctima.

A la luz de las consideraciones que anteceden, en el caso particular, se advierte que no existe una figura penal que contemple la obtención, uso, revelación y difusión de datos personales sensibles como videos con contenido sexual y sin el consentimiento de su titular. Cabe manifestar, que el Tribunal Constitucional Plurinacional, en su Sentencia Constitucional Plurinacional N° 0819/2015 – S3, refiere que existe un vacío ante las conductas que a través del uso de las Tecnologías de Información y Comunicación vulneran derechos y que es deber del Estado adoptar las medidas necesarias de diversa índole para tutelar la autodeterminación informativa y la privacidad.

- **Medidas adoptadas por las autoridades en favor de la víctima**

Dentro del proceso penal, no se concretaron las medidas pertinentes para salvaguardar los derechos de la víctima, producto de la revelación y difusión del video con imágenes de contenido sexual, es así que de la Sentencia Constitucional Plurinacional N° 0819/2015 – S3, se infiere que el Ministerio Público en su Informe N° FGE/STRIA. GRAL./1/2015, justificó dicho aspecto bajo el argumento de: "(…) tratarse de un delito que no está relacionado con imágenes de contenido sexual". Consecuentemente, recién en lo posterior como resultado de la Acción de Protección de Privacidad, la Autoridad de Telecomunicaciones y Transportes (ATT), los Gobiernos Autónomos Municipales de La Paz y El Alto y el Gobierno Autónomo Departamental de La Paz, encararon gestiones para la eliminación y retiro del material en el territorio boliviano.

Cabe señalar que esta Acción es un mecanismo excepcional de garantía para la protección de datos personales, aplicable únicamente cuando se trate de información que curse en bancos de datos ya sea públicos o privados, circunscribiendo su tutela a esta condición.

- **Influencia de las Tecnologías de Información y Comunicación**

Las TIC conforman una vasta gama de dispositivos y tecnologías (que incluyen a los teléfonos móviles, desde los más simples hasta los más avanzados smartphones) propiciando acelerados e innovadores cambios en la sociedad, principalmente, porque facilitan la recopilación y transmisión de datos de toda naturaleza. Asimismo, por su carácter de interactividad, las personas a través de su uso, pueden interrelacionarse entre sí en el mundo virtual, aunque físicamente se encuentren en extremos opuestos del orbe, lo que ofrece posibilidades antes insospechadas, aspecto que también trajo consigo comportamientos ilícitos vinculados al derecho de la privacidad de la información y la autodeterminación informativa.

Actualmente, cualquier persona puede capturar con la cámara de video o fotográfica de su teléfono celular, imágenes de una amplia serie de hechos, desde aquellos que transcurren cotidianamente, hasta los más íntimos que acontecen en la privacidad de un domicilio; e inmediatamente, "colgarlo" en cuentas de YouTube, Facebook, Instagram, otras plataformas similares o la aplicación del sistema de mensajería WhatsApp, para citar algunos ejemplos, logrando que se difundan en cuestión de segundos en las más lejanas latitudes del planeta.

En el caso concreto, destaca la facilidad con que se capturó la grabación sin necesidad de complejos aparatos y especializados conocimientos, y es que gracias a las TIC no es primordial poseerlos para poder consumar este tipo de atentados. Es así que una vez cargado en la red Internet el video con contenido sexual, fue difundido y viralizado masivamente en otros sitios web y en cuentas de incontables redes sociales, dando lugar a que la víctima tenga que correr con los gastos de contratación de la empresa extranjera End Revenge Porn para eliminar estos contenidos, logrando suprimir material en 63 sitios de internet, además de requerir los servicios de profesionales informáticos y especialistas para coadyuvar en dicho cometido (La Razón, 2014).

Cabe agregar, que el esposo de la víctima mediante un correo electrónico solicitó al sitio web Bolivia 69 (en el cual se publicó inicialmente el video), que elimine el material de dicha página, sin embargo la respuesta del administrador del mismo (quien utilizó un pseudónimo), fue negativa manifestando que no retirará el video de la red, ya que a su criterio eso alimentaría más el morbo y sería contraproducente, optando por subir otros videos para desviar la atención (Belmonte, 2014a).

Otro punto a resaltar, es que el material no fue del todo eliminado ya que, hasta la fecha de la redacción de la presente Tesis, se constató que continúa circulando en la red Internet e incluso es usado habitualmente en la elaboración de una variedad de los denominados “memes” que se intercambian en redes sociales, originando una revictimización de la afectada. Por tratarse de un dato sensible, su revelación y difusión fue y continúa siendo muy lesiva para la víctima y su entorno familiar, al ser públicamente sometida a comentarios ofensivos, denigración y daños a su imagen, generando una situación discriminatoria, lo cual llevó a la víctima a pensar en atentar contra su propia vida (Belmonte, 2014a). El proceso penal conforme a los datos recabados del Tribunal Departamental de Justicia de La Paz, se encuentra para juicio oral.

El caso analizado abre el debate de incorporar un tipo penal específico para la tutela de los datos personales sensibles, que permita una persecución penal y consiguiente sanción de aquellos individuos que incurran en este tipo de conductas, considerando además la participación de otras personas como los encargados o administradores de los sitios web, quienes ante la falta de normativa que los sancione se encuentran amparados en la impunidad y si bien las conductas atribuibles al presunto autor principal pueden encuadrarse en tipos penales del Código Penal vigente, también develan una lesión a la información personal repercutiendo desfavorablemente en el óptimo ejercicio del derecho de autodeterminación informativa o derecho de protección de datos personales, vislumbrándose en este punto un vacío jurídico en la normativa penal boliviana.

Tabla N° 18

Estudio de caso: acceso, revelación y difusión de dato personal sensible

Relación y contexto de los hechos

En fecha 18 de diciembre de 2014, el entonces Ministro de Salud Juan Carlos Calvimontes, en conferencia de prensa reveló que el ex Magistrado del Tribunal Constitucional, G.C.M. en diciembre de 2012 fue diagnosticado con una enfermedad que causa la baja de sus defensas de forma avanzada (VIH) y que a raíz de ello padecía de una tuberculosis ganglionar (Los Tiempos, 2014).

Calvimontes explicó que G.C.M. recibía tratamiento para ambas enfermedades de forma gratuita mediante dos programas específicos y también manifestó que: "(…) desde hace cuatro meses ha dejado de ir a recibir la medicación para la tuberculosis" (Página Siete, 2014).

El dato fue revelado en medio de una coyuntura política en la que se encontraba inmerso G.C.M., sometido a un juicio de responsabilidades en la Cámara de Senadores de la Asamblea Legislativa Plurinacional, por actos en el ejercicio de sus funciones.

CATEGORÍAS	DESCRIPCIÓN
Conductas que vulneraron el derecho de autodeterminación informativa	• Acceder a historia clínica • Revelar datos relativos al estado de salud • Difundir datos relativos al estado de salud
Calidad de los sujetos que realizaron las conductas	• Servidor público (Máxima Autoridad Ejecutiva) • Servidor Público (Personal de salud) a cargo de la historia clínica
Tipo de dato afectado	• Sensible: salud
Medios utilizados	• Medios de comunicación televisiva, escritos y digitales (sitios web en internet) • Documentos
Finalidad	• Generar perjuicio, agravio, desprestigio
Principales derechos vulnerados	• Autodeterminación informativa • Privacidad • Intimidad • Honra • Honor • A no ser discriminado • Artículo 9 de la Ley 3729, promulgada en 2007: "Los pacientes no deberán ser objeto de publicaciones de prensa escrita, ni televisiva, sin su conocimiento expreso" • Dignidad
Tipos penales que se aplicaron	• Difamación, Artículo 282 • Calumnia, Artículo 283 • Discriminación agravada por funcionario público, Artículo 281 ter, par. I, inciso a)
Observaciones	El hecho fue ampliamente difundido, como resultado de la coyuntura política por la que atravesaba el país en ese momento, sumado a ello el cargo público que ostentaba la víctima como Magistrado del Tribunal Constitucional Plurinacional.

Fuente: elaboración propia (2019)

- **Acciones legales asumidas por el afectado**

El ex Magistrado G.C.M., inició procesos penales en contra del entonces Ministro de Salud, Juan Carlos Calvimontes, por los delitos de Discriminación (Artículo 281 ter), Difamación (Artículo 282) y Calumnia (Art. 283) del Código Penal, los mismos que determinan:

> Artículo 281 ter. (DISCRIMINACIÓN). La persona que arbitrariamente e ilegalmente obstruya, restrinja, menoscabe, impida o anule el ejercicio de los derechos individuales y colectivos, por motivos de sexo, edad, género, orientación sexual e identidad de género, identidad cultural, filiación familiar, nacionalidad, ciudadanía, idioma, credo religioso, ideología, opinión política o filosófica, estado civil, condición económica o social, enfermedad, tipo de ocupación, grado de instrucción, capacidades diferentes o discapacidad física, intelectual o sensorial, estado de embarazo, procedencia regional, apariencia física y vestimenta, será sancionado con pena privativa de libertad de uno a cinco años.
> I. La sanción será agravada en un tercio el mínimo y en una mitad el máximo cuando:
> a) El hecho sea cometido por una servidora o servidor público o autoridad pública.
> Artículo 282°. (DIFAMACIÓN). El que de manera pública, tendenciosa y repetida, revelare o divulgare un hecho, una calidad, o una conducta capaces de afectar la reputación de una persona individual o colectiva, incurrirá en prestación de trabajo de un mes a un año o multa de veinte a doscientos cuarenta días.
> Artículo 283°. (CALUMNIA). El que por cualquier medio imputare a otro falsamente la comisión de un delito, será sancionado con privación de libertad de seis meses a dos años, y multa de cien a trescientos días.

A su vez, la víctima presentó una denuncia disciplinaria ante el Colegio Médico de Bolivia y otras tres ante la Comisión Interamericana de Derechos Humanos (El Diario, 2014).

En el caso de la Difamación se exige que la conducta sea concretada en forma pública y reiterada, afectando a la reputación de la víctima, es decir su reputación debe ser dañada, en este entender, el ex Ministro Calvimontes, incurrió en revelar los padecimientos[14] de G.C.M. en una conferencia de prensa ante los medios de comunicación, por ende la noticia se hizo de conocimiento público y masivo, generándole afectación; no obstante, la conducta no se verificó de manera reiterada, considerando que el tipo penal exige que no se lo haga una sola vez, sino varias. En cuanto a la Calumnia basta la imputación falsa de la comisión de un delito para su consumación, en el caso analizado, se sindicó a la víctima de ser doblemente peligroso al haber dejado su tratamiento para la tuberculosis ganglionar y por ser portador del

[14] Respecto a la tuberculosis, en una entrevista brindada al Programa Todo A pulmón, cargada en YouTube en fecha 31 de octubre de 2014, antes de la revelación efectuada por el ex Ministro Calvimontes, G.C.M. manifestó padecer dicha enfermedad, la información fue consultada en https://www.youtube.com/watch?v=3DMhvU4hnHA el 15 de noviembre de 2019.

VIH SIDA, alegando el abogado patrocinante de la víctima que su defendido fue acusado de ser autor del delito descrito en el Artículo 216 (Delitos contra la salud pública) numerales 1 y 10 del Código Penal, que señala:

> Artículo 216. (DELITOS CONTRA LA SALUD PÚBLICA): Incurrirá en privación de libertad de uno a diez años, el que:
> 1) Propagare enfermedades graves o contagiosas u ocasionare epidemias.
> (…)10) Transmitiere o intentare transmitir el VIH conociendo que vive con esta condición.

En lo atinente al tipo penal de Discriminación, la revelación del estado de salud de G.C.M., le generó un trato diferenciado y perjudicial en cuanto a sus derechos y consideraciones sociales, manifestándose en rechazo, intolerancia, falta de aceptación y desprecio en lugares públicos y en su comunidad. Al respecto, G.C.M. manifestó:

> (…) la conferencia ha sido un acto malicioso, un acto doloso, un acto planificado (…) en sentido de sepultarme destruirme, físicamente, moralmente, socialmente (…) la familia me ve en otro sentido, los amigos, la mayor parte de mis amigos, aunque ya un poco la gente se informó que esta cosa es injusta, ilegal (…) también esta frustrada mi vida, yo podía haber tenido todo un proyecto de vida, ahora en lo futuro por este tabú social tal vez se me restrinjan muchos de mis derechos (…). (NTN24, 2014)
> (…) en la calle la gente me veía como algo distinto y no faltaba la gente que escupía al suelo (…) mis amigos en vez de darnos la mano, ahí nomás quedaba, otros para evitar problemas se alejaban, han sido momentos difíciles (…) en el mes de junio el Fiscal Calani logró la documentación de forma ilegal de la Caja Petrolera y como panfletos en ese momento había circulado mi situación de salud (…) todos los senadores, diputados, especialmente diputados tienen (…) mucha gente ya sabía (…). (Cusi, 2014)
> (…) No puedo ni trabajar, no puedo ni ir a un médico, no puedo tener atención (…) me han marcado como en las calles de La Paz o de Bolivia, como las cebritas, no puedo hacer nada en el futuro. (Unitel, 2017)
> (…) revela mi situación de salud que soy portador el VIH SIDA, esa situación para mi significó muerte (…) mucha gente que se informó prácticamente se alejaron (…) ha sido difícil para mí ganarme siquiera un cliente, todo el mundo se alejaba porque decían que solo por darme la mano podía transmitir el VIH SIDA (…). (Cusi, 2019)

Así también en un medio radial, G.C.M. rompió en llanto al hablar de su delicada y complicada situación (Cusi, 2016). Aún en la comunidad de Jilatiti Qullana de la que es originario G.C.M., fue víctima de discriminación, al acudir a lavarse las manos en un pequeño rio y ser acusado por los comunarios de contaminar el agua con su enfermedad (Urgente.bo, 2018). Todos estos hechos, generaron una grave afectación psicológica, económica, social y del estado de

salud físico (Correo del Sur, 2017) de la víctima, quien cursó un cuadro depresivo, cargando con el estigma del rechazo de una sociedad aún conservadora respecto a su enfermedad, ya que fue aislado y sometido a discriminación en el ámbito social, laboral, círculo de amistades y comunidad.

Si bien los abogados y autoridades adecuaron estos actos a los tipos penales vigentes, también denotan la revelación y uso arbitrario de un dato personal sensible referido al estado de salud, información considerada de especial protección y preservada en concreto por la legislación boliviana en el Artículo 9 de la Ley N°3729, dado su alto potencial discriminatorio y de afectación de derechos, verificándose en el caso analizado un tratamiento de datos al margen del conocimiento y el consentimiento de su titular. Así también debe considerarse que el detrimento por la revelación de un dato sensible es más gravoso que por la comisión de los ilícitos de difamación o calumnia, por lo tanto, amerita una sanción mayor, y una investigación en el marco del ejercicio de una Acción Penal Pública.

- **Medidas adoptadas por las autoridades en favor de la víctima**

El entonces Defensor del Pueblo, Rolando Villena, reclamó una disculpa pública al ex Ministro de Salud Calvimontes y planteó su enjuiciamiento como resultado de la enfermedad de G.C.M., por vulnerar la intimidad y privacidad del paciente consagradas en la Constitución y por violar las leyes y los Convenios Internacionales que garantizan su confidencialidad. Por ende, emitió el Comunicado Público de fecha 22 de diciembre de 2014, demandando al Comité de Lucha contra el Racismo y toda forma de Discriminación y a la autoridad que corresponda en su condición de servidor público, el inicio de las acciones legales pertinentes, y la petición de disculpas públicas (Defensoría del Pueblo, 2015, p.89). Asimismo, mediante una nota de 29 de diciembre de 2014, la citada instancia gubernamental solicitó al entonces Viceministro de Descolonización Félix Cárdenas, procesar al ministro de Salud Juan Carlos Calvimontes por sus declaraciones en relación a la salud de G.C.M. (Periódico Digital Radio Fides.com, 2014). Al margen de lo señalado, no se evidenció ninguna actuación para precautelar los derechos de la víctima.

- **Influencia de las Tecnologías de Información y Comunicación**

Si bien la revelación de la enfermedad de G.C.M. fue a través de los medios de comunicación convencionales (Televisión y prensa escrita), la red Internet jugó un papel preponderante, coadyuvando a viralizar la noticia, y además a que los individuos se expresen ya sea en favor o en contra del caso en cuestión.

La red Internet ha permitido la creación de variados espacios virtuales que promueven y estimulan la acción comunicativa de las personas, aunado a ello la expansión del ciberespacio que ha ido evolucionando y penetrando a pasos agigantados en el quehacer comunicacional del ser humano. En la transferencia de datos que se da del mundo real al mundo virtual a través de Internet, se traspasa todo tipo de informaciones, fronteras, valores e intereses. El carácter de interactividad que poseen las TIC rompe el modelo lineal de comunicación, ya que los usuarios no solo consumen el contenido de los medios, sino que lo comparten con otros, lo reproducen, lo redistribuyen y lo comentan. En consecuencia, las Tecnologías de Información y Comunicación, generaron que circule abundante información de fácil acceso a lo largo del tiempo, posibilitando que el padecimiento de G.C.M. sea conocido por un sinnúmero de personas; cabe agregar que la información publicada en la red Internet es atemporal porque una vez cargada puede ser consultada en cualquier momento, de lo que emana una revictimización para el afectado.

El modus operandi acerca de las conductas que vulneran datos personales, revelan situaciones que escapan al derecho penal tradicional y quedan sin protección los contenidos inmateriales de la información personal, hechos que en su conjunto ameritan la promulgación de normas específicas.

En suma, salvaguardar la información personal en la vía penal contribuirá a optimizar el ejercicio y tutela del derecho a la autodeterminación informativa, coadyuvando con la prevención, persecución y sanción de ilícitos que agravien a los titulares de los datos personales, con lo que a partir de instancia procedimental podrán adoptarse las medidas investigativas y otras pertinentes para su protección, evitando además la revictimización de los afectados. Así también, con la persecución penal de estas conductas, se evitará la comisión de otros ilícitos para los cuales habitualmente se utilizan estos datos.

- **CONCLUSIONES**

Los resultados plasmados en el Marco Práctico producto del trabajo de campo, ponen de manifiesto el rol fundamental de las Tecnologías de Información y Comunicación en la sociedad actual, que al presente forman parte del desarrollo nacional en el sector público y privado, siendo su globalización un fenómeno insoslayable. Estas innovaciones están presentes para facilitar la vida del ser humano, y en Bolivia su uso es cada vez más recurrente; empero, en ocasiones son la llave para la comisión de ilícitos que lesionan la información personal, afectando derechos y libertades de los individuos, entre éstos el derecho de

autodeterminación informativa; aspectos reflejados coincidentemente en los resultados de la encuesta, la entrevista y el estudio de caso.

También es concurrente la percepción de falta de seguridad y medidas de tutela adecuadas de datos personales en las entidades públicas y privadas, que en su mayoría no brindan una protección apropiada. Por otra parte, se evidenció según la encuesta que las conductas que habitualmente vulneran el derecho a la autodeterminación informativa son: el uso y el acceso no autorizados de datos.

Sobre el particular, los expertos entrevistados expresan que estas transgresiones incluyen la recolección, la difusión, el acceso y la mercantilización de estos datos, así como la comisión masiva de delitos en tanto a derechos sensibles de información que está en la red y se utiliza para fines delictivos, destacando el error humano por desconocimiento que repercute en la vulnerabilidad de los datos personales.

En lo concerniente a la existencia de un artículo en el Código Penal boliviano que tipifique atentados contra los datos personales, de la aplicación de los tres citados instrumentos se corroboró que las únicas referencias se encuentran contenidas en los Artículos 363 bis (Manipulación informática) y 363 ter (Alteración, acceso y uso indebido de datos informáticos), que al presente resultan insuficientes dado el dinamismo de la sociedad actual en torno a las TIC, así lo han revalidado los expertos entrevistados. Lo anterior, conforme a los resultados de la encuesta y estudio de caso, genera que los abogados y autoridades consideren subsumir las conductas que transgreden datos e información personal, en tipos penales tales como: falsedad material, falsedad ideológica, uso de instrumento falsificado, difamación, calumnia, injuria, revelación de secreto profesional, violencia familiar o doméstica, amenazas, extorsión y discriminación.

Así también, los resultados permiten inferir que es necesaria y factible la incorporación al Código Penal de nuevos tipos penales para la tutela de los datos personales de carácter general, aquellos de carácter sensible y los que conciernen a menores de edad; incluyendo como sujeto activo a cualquier persona, servidores públicos y responsables de las bases de datos. Al respecto, uno de los entrevistados, argumenta que como sujeto activo debiera incluirse a cualquier persona y en su caso, a aquellos que poseen conocimientos específicos en el ámbito informático; otro de los expertos plantea que esta categoría debería comprender a todas las personas que estén a cargo de administrar archivos correspondientes a datos personales ya sea en entidades públicas o privadas; en tanto que el tercer experto postula

englobar únicamente a los servidores públicos que tienen a su cargo el tratamiento de datos personales, atendiendo el alto grado de responsabilidad aparejado a sus funciones.

En lo atinente a las conductas a incluir en los tipos penales que se propone, el criterio mayoritario arrojado por la encuesta señala: acceso, uso, alteración y revelación ilícitos; bajo la figura dolosa y con penas de reclusión, días multa e inhabilitación especial. En cuanto a los entrevistados, uno de ellos propugna analizar adecuadamente las conductas que no se encuentran previstas en la norma sustantiva penal, así como insertar conductas tanto culposas como dolosas y hacer énfasis en las medidas preventivas; mientras que el otro entrevistado adopta la postura de contemplar el apoderamiento, la utilización o la modificación de datos personales sin estar autorizado, e incluir únicamente la forma dolosa y las penas de cárcel y multa pecuniaria. Por último, el tercer entrevistado plantea incluir el tratamiento de datos personales como conducta ilícita, bajo la figura dolosa, y la sanción de reclusión para servidores públicos.

A su turno, los resultados del estudio de caso, ponen de manifiesto la afectación de los datos personales sensibles por conductas tales como su obtención, acceso, utilización, revelación y difusión. En suma, se colige que la ausencia de tipos penales orientados a la tutela de datos personales, incide como limitante del ejercicio del derecho a la autodeterminación informativa, como facultad para controlar el flujo de la información personal.

Finalmente, los resultados de los instrumentos aplicados al unísono develan que, con la inclusión de tipos penales de protección de datos personales en el Código Penal, operará una mejora de la tutela del derecho de autodeterminación informativa, constituyendo una arista adicional a las existentes para su salvaguarda. De lo anterior se colige que es factible establecer tipos penales que engloben dichas conductas, vinculadas fundamentalmente pero no de manera excluyente a los avances tecnológicos, posibilitando así su persecución penal, su sanción y la reparación del daño en favor de las víctimas, aspecto que incidirá en la optimización de la tutela del derecho de autodeterminación informativa.

El actual Código Penal, no contempla en sentido estricto disposiciones específicas respecto a la protección de datos personales, este hecho hace que muchos delitos sean tipificados en torno a las figuras penales existentes que en ciertos aspectos difieren de los hechos perpetrados, factor que imposibilita una calificación jurídico legal que individualice atentados de esta naturaleza, por lo que es imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de una extensión extralegal del ilícito penal, ya que con ello se

vulnera el principio de legalidad expresado en la máxima “nullum crimen nulla poena sine lege”, quedando dichos hechos en la impunidad.

En materia penal la tipicidad y legalidad son principios ineludibles, es por ello que las nuevas formas de delincuencia requieren de una regulación específica, evitando el riesgo de caer en la atipicidad o en la analogía, ello no implica ampliar más allá de lo necesario el repertorio de delitos, sino únicamente en los casos que así lo ameriten atendiendo a la trascendencia e incidencia de las conductas reprochables y las características del bien jurídico y los derechos afectados.

Así las cosas, un ordenamiento jurídico penal que considere la tutela de la información y el dato, incidirá en optimizar la tutela del derecho de autodeterminación informativa, entendido como la faceta positiva del derecho a la privacidad que permite ejercer al individuo un control sobre sus datos personales públicos y privados, beneficiando a la sociedad boliviana en su conjunto, como corolario de la realidad imperante, en un escenario de ostensible transición a la ciudadanía y economía digital, que posibilita que los actos jurídicos con el Estado y entes privados, se lleven a cabo de manera virtual, surtiendo los mismos efectos que los actos presenciales o convencionales, pero que en contraposición, generan un incremento de las transgresiones por parte de delincuentes que se aprovechan de los datos personales para beneficio propio.

Se vulneran datos personales, cuando se publica información sensible en redes sociales (Los Tiempos, 2019), cuando se venden datos personales con fines comerciales (Página Siete, 2019), cuando terceros se apropian de la identidad de una persona sin su consentimiento para hacerla aparecer como deudora de grandes sumas de dinero o como autor de ilícitos que jamás cometió (El Deber, 2017; Opinión, 2017; Opinión, 2019); igual ocurre cuando las entidades públicas para cumplir los fines del Estado, capturan de manera física o virtual información sensible sin advertir que la calidad de la información que entregan los ciudadanos amerita un tratamiento especial por tratarse de datos personales (ATB Digital, 2018; Los Tiempos, 2018b; Contraloría General del Estado, 2019; Correo del Sur, 2019). También cuando se utiliza información para hacer figurar a personas como integrantes de partidos políticos y agrupaciones ciudadanas sin serlo (La Razón, 2018; El Deber, 2018); se transgrede el derecho de autodeterminación informativa. A su vez, estos datos son empleados en ilícitos como la pornografía, para perpetrar secuestros o realizar transferencias ilegales de cuentas bancarias y cometer estafas (ATB, 2017; Los Tiempos, 2018a; Aguilera, 2018), siendo estos solo algunos de tantos casos producto de la violación de datos personales, que se presentaron en la realidad boliviana.

De lo expuesto, se concluye que las Tecnologías de Información y Comunicación están en constante desarrollo y su penetración en las actividades del Estado, entes privados y la sociedad es progresiva, experimentándose a diario en la realidad nacional hechos que transgreden la información y los datos personales con graves secuelas para sus titulares, por lo que de acuerdo a los resultados del trabajo de campo, es viable la reforma del Código Penal para la incorporación de tipos penales orientados a su protección, con lo que se propenderá a optimizar la tutela del derecho de autodeterminación informativa.

CAPÍTULO IV
LEGISLACIÓN COMPARADA

Este acápite presenta un enfoque sobre las medidas adoptadas por la legislación comparada, respecto a la protección de datos personales en el ámbito de la tutela del derecho penal. Para el efecto, se incluye a Argentina, Colombia y España, países que han implementado en diversas áreas, sólidas medidas para garantizar el respeto y óptimo ejercicio del derecho a la autodeterminación informativa y han incorporado tipos penales específicos para la protección de datos personales.

4.1 Argentina

La Ley N°25.326 de Protección de datos personales promulgada el 30 de octubre de 2000, incorporó el concepto de dato personal como objeto de tutela jurídica y reglamentó la Acción de Hábeas Data, acogida en la reforma constitucional de 1994; a su vez, modificó el Código Penal incluyendo por disposición de su Artículo 32, los Artículos 117 bis y 157 bis, posteriormente reformados por la Ley N°26.388 de 24 de junio de 2008, que modificó el citado cuerpo legal incorporando delitos informáticos.

El Artículo 117 bis, contenido dentro del Título II Delitos contra el honor, fue derogado por el Artículo 14 de la citada Ley N°26.388, “pasando su tipo penal a acumular los tipos penales del Art. 157 bis” (Rebollo y Saltor, 2013, p. 159), principalmente a causa de las observaciones a su ubicación sistemática; mientras que la redacción del citado Artículo 157 bis, contenido en el Titulo V Delitos contra la libertad, Capítulo III Violación de secretos y de la privacidad quedó como sigue:

> Artículo 157 bis. Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
> 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
> 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

El numeral 1 del citado Artículo, respecto al acceso a un banco de datos personales refiere: “de cualquier forma”, de lo que se colige que no contempla únicamente un acceso de índole

informático. La violación de sistemas de confidencialidad y de seguridad son medios por los que se puede acceder ilegítimamente al banco de datos, pero no son los únicos. Al señalar la redacción del tipo el “acceso”, no tiene cabida la tutela en la fase de recolección de datos personales, siendo únicamente para datos ya incorporados en las bases de datos.

El sujeto activo es indeterminado es decir puede ser cualquier persona, mientras que el sujeto pasivo, es el titular de los datos personales; igualmente, resulta comprendido en esta categoría como afectado el titular del banco de datos cuyo acceso ilícito es pasible de generarle perjuicio, en vista de que se espera que adopte medidas de seguridad efectivas en relación a la preservación y procesamiento de datos. Es un delito doloso, ya que el agente debe obrar a sabiendas de que su acceso es ilegítimo. De acuerdo a Riquert (2013), en el caso del numeral 1, al tratarse de un delito de pura actividad, la lesión del bien jurídico protegido se concreta con el acceso, “(…) no siendo necesaria la verificación de otro resultado autónomo, como podría ser que el agente se apropie de datos que integran el banco” (p.14).

El numeral 2, tipifica proporcionar o revelar la información a otra persona, cuando por disposición de la ley estuviere obligado a guardar secreto; en ese contexto, quedan excluidas las bases de datos de uso público no sujetas a confidencialidad; asimismo, cabe señalar que no se refiere expresamente a archivos o bancos de datos en soportes digitales, por lo que su protección se extiende a datos contenidos en otro tipo de soportes y/o formatos. El sujeto activo, es la persona obligada a preservar el secreto por disposición de la ley, quien se encuentra en posición de garante, desde esta perspectiva es un sujeto de índole determinado o calificado, que comprende a las personas que tengan una obligación de dicha naturaleza, ingresando en este ámbito los encargados y responsables de las bases de datos. El sujeto pasivo corresponde al titular de los datos personales.

En cuanto a la acepción de revelar, ésta importa: mostrar, exponer o dejar ver, mientras que proporcionar se refiere a facilitar o dar, los cuales pueden concretarse por cualquier medio informático o no. El inciso tipifica una conducta de carácter doloso ya que se proporciona o revela ilegítimamente una información que por disposición de la Ley es reservada, y se encuentra a cargo y bajo la responsabilidad de una persona que por sus funciones conoce esta prohibición, en la que el carácter ilegítimo representa una falta de consentimiento. El obligado al secreto sólo podrá revelarlo, sin incurrir en delito, previa autorización judicial, o ante la existencia de razones fundadas en motivos de seguridad pública, defensa nacional o salud pública.

.

El numeral 3, reprime la inserción de datos, no especificando la veracidad o falsedad de los mismos; e igualmente que en los incisos 1 y 2, constituye una figura dolosa. Al señalar: “hiciere insertar” refiere la participación de otra persona, que no necesariamente intervendría dolosamente, pudiendo obrar bajo el influjo de un engaño, configuraría por ende un supuesto de autoría mediata (Terragni, p. 555). Observan De Langhe y Rebequi (citados por Riquert, 2013, p.11) que el término “ilegítimamente” conlleva que basta la incorporación del dato, sea falso o verdadero para consumar el ilícito. El sujeto activo es indeterminado, en tanto que el pasivo es el titular de los datos personales.

Cabe imprimir que todas las anteriores conductas se consuman por el solo hecho de concretarse, no siendo requerida la producción de otro resultado autónomo; por consiguiente, los tres incisos involucran ilícitos de carácter formal o de mera actividad, y el objeto lo constituye el dato personal (Mallo, 2014).

En lo atinente al bien jurídico protegido por este tipo penal en sus tres numerales, Aboso (2012, p.780) señala que es la intimidad y en especial los datos personales almacenados en un sistema informático, en similar sentido Terragni (citado en Riquert, 2013) plantea:

> (…) no se trata sólo de evitar la revelación de secretos, sino que comprende en general a la intimidad pero no únicamente en su inteligencia como prerrogativa excluyente de terceros respecto de determinados ámbitos de la vida privada, sino también en cuanto se la concibe como un derecho de control sobre la información y los datos de la propia persona, incluso sobre los ya conocidos, para que sólo puedan utilizarse conforme a la voluntad de su titular. (p.10)

La reiterada señalización del término ilegitimidad, ha sido objeto de críticas, porque enfatiza la falta de consentimiento, y resulta redundante, al señalar que se lo hace a sabiendas, es decir, careciendo de este derecho (Riquert, 2013, p.12).

Riquert (2013, p.14) también menciona concursalidades, dentro del mismo Capítulo, entre el primer numeral del Articulo analizado y el Artículo 153 bis (Acceso ilegítimo simple), que sanciona con la prisión de quince días a seis meses, el acceso por cualquier medio a un sistema o dato informático de acceso restringido, sin autorización o excediendo la que se posea. De similar manera, identifica que el numeral 3 puede concurrir con las falsedades documentales.

En lo que atañe a la pena, se ha previsto para los tres numerales del Artículo 157 bis, la prisión de un mes como mínimo, a dos años como máximo y cuando el autor fuere un funcionario público, adicionalmente la inhabilitación especial de 1 a 4 años, como agravante. Aunque la

disposición analizada no hace referencia expresa a los datos sensibles y de menores de edad, puede aplicarse a esta categoría de datos personales, considerando que gozan de especial protección conforme a la Ley N°25.326 y que el numeral 2 del Artículo 157 bis, protege los datos personales cuyo secreto debe preservarse por disposición de la ley.

Arocena (2012, p.986) señala que a través de la inclusión del tipo penal citado, se han llenado lagunas de punición y que la Ley N°26.388 ha logrado su cometido respetando básicamente el principio de subsidiariedad del derecho penal pues las nuevas figuras delictivas se presentan como herramientas indispensables para solucionar problemas a los que las disposiciones de las restantes ramas del ordenamiento jurídico (derecho administrativo, derecho civil, etc.) no pueden dar adecuada respuesta.

En líneas generales, se califica como positiva la reforma por la que se incluyó el tipo penal con anterioridad glosado, ya que no obstante del marco legal constitucional, y las leyes vigentes, repetidamente se identificaron en la República de Argentina casos de robo de identidad, sustracción de información personal o venta masiva de datos personales, ameritando la intervención del derecho penal que no puede quedar al margen de estos fenómenos.

Es de destacar que Argentina, se adhirió al Convenio sobre la Ciberdelincuencia de 23 de noviembre de 2001 (Convenio de Budapest), mediante Ley N°27.411 de 15 de diciembre de 2017, factor que constituye un hito sustancial para la mejora del sistema penal en las áreas de persecución e investigación de delitos informáticos y en materia de cooperación internacional. Producto de lo anterior, se gestionó modificar la ley sustantiva y adjetiva penal, considerando la evidencia digital, y que la evolución del perfil del ciberdelito avanza de forma dinámica, exigiendo la actualización permanente de los métodos para combatirlo; en consecuencia, fue consensuado un proyecto legislativo actualmente en conocimiento de las instancias respectivas del Congreso de Argentina.

Asimismo, en correspondencia con la adhesión al citado Convenio, mediante Resolución N°1291/2019 de 25 de noviembre de 2019 se creó la Unidad 24/7 de Delitos Informáticos y Evidencia Digital en la órbita de la Dirección Nacional de Asuntos Internacionales del Ministerio de Justicia y Derechos Humanos.

4.2 Colombia

A través de la Ley N°1273 de 5 de enero de 2009, el legislador colombiano, modificó el Código Penal, creando un nuevo bien jurídico a tutelar, denominado: “de la protección de la información y de los datos”, por medio de esta reforma, se adicionó el Título VII BIS, el cual contempla un artículo que tipifica la violación de datos personales, estableciendo además circunstancias agravantes, tal como se cita a continuación:

> Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
> (…) Artículo 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:
> 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
> 2. Por servidor público en ejercicio de sus funciones.
> 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
> 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
> 5. Obteniendo provecho para si o para un tercero.
> 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
> 7. Utilizando como instrumento a un tercero de buena fe.
> 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Respecto al Artículo 269F, éste sanciona diversas acciones (obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear) relacionadas con el procesamiento y manejo de datos personales o códigos personales sin autorización, contenidos en ficheros, archivos, bases de datos o similares. No distingue si los mismos serán únicamente de carácter digital o contenidos en medios informáticos o electrónicos, por lo que se colige que también comprende una protección a bases de datos o archivos en soportes físicos u otros catalogados como tradicionales. Como condicionante, señala el provecho propio o de un tercero, entendido como beneficio o ventaja para que se

consume el ilícito. Por sus características, es un delito de resultado ya que requiere que el sujeto agente haya realizado una o más conductas descritas y obtenido el provecho señalado (Suárez, 2019, p. 47), el cual puede ser de cualquier naturaleza y no únicamente económico.

El bien jurídico tutelado en este delito es la información y los datos (Riascos, 2012, p. 368), sobre el particular, Sánchez (2016, pp. 59-60), postula que este bien está concebido de diversas formas: como un valor económico, intrínseco e inmaterial de cada persona y acoge la confidencialidad, integridad y disponibilidad de la información y de los sistemas informáticos en que ésta se almacena o transfiere; resaltando que además simultáneamente protege variados intereses jurídicos.

La incorporación de la información y del dato como un bien jurídico, denota el grado de preeminencia tal que ameritó la asignación de una específica protección del derecho penal en la Era Digital, caracterizada por la exacerbación de los adelantos tecnológicos, siendo estos bienes cualificados como valores inmateriales e intangibles; no obstante, pasibles de ser determinados o determinables económicamente, acarreando su vulneración consecuencias jurídico-penales.

El tipo penal es doloso (Suárez, 2019, p. 50) toda vez que el agente actúa a sabiendas de que no está facultado para realizar las acciones descritas. El sujeto activo es indeterminado, porque la ley no requiere una característica específica, en consecuencia puede ser cualquier persona; en cuanto al sujeto pasivo, este es el titular de los datos personales. Así también pueden serlo el Estado, o las personas naturales o jurídicas, de derecho público o privado, según fuesen administradores de agencias de información comercial, operadores de bases o bancos de datos, u otros que pudiesen resultar afectados.

El objeto material son el código personal y el dato personal (Suarez, 2019, p. 50). En cuanto a los códigos personales, Riascos (2012, p. 400) expresa que estos son medidas de seguridad de acceso a la información instaladas por el titular de los datos para guardar la confidencialidad o secreto de la información que le concierne, por ejemplo, las contraseñas, claves o passwords utilizados por la persona para acceder a un programa o sistema informático, que son secretos y sirven de autenticación para el ingreso de su titular.

En lo atinente a la sanción, el tipo penal impone la pena de prisión de 48 a 96 meses, es decir una privación de libertad de 4 a 8 años y multa de 100 a 1000 salarios mínimos legales mensuales.

Sobre la figura analizada, Riascos (2012) señala:

> (…) abarca todo el procedimiento o tratamiento de datos personales que son una especie del género datos informáticos y por cuanto prevé varios verbos rectores que afectan a las diferentes etapas o fases de dicho procedimiento (desde la recolección, almacenamiento, registro, transmisión o circulación de datos). (p.398)

Asimismo, el citado autor reprocha la variedad de verbos rectores consecutivos y alternativos en la estructura del tipo, manifestando que si bien abarcan diferentes posibilidades, pueden llevar a equívocos en la utilización de los mismos, dando lugar a incriminaciones indebidas, y que habrá momentos en que las mismas se solapen a través de los dispositivos informáticos y se desnaturalice el tipo penal. De igual manera, sugiere excluir el término “sin estar facultado para ello” por “con fines ilícitos” y la eliminación de la frase “con provecho propio o de un tercero”, ya que de acuerdo al Artículo 269H numeral 5, se incluye este factor como agravante para los tipos básicos del Título VII, existiendo una incoherencia o una falta de técnica legislativa (Riascos, 2012, pp. 401-402).

Otro punto importante a considerar es que el Artículo 269H añade el incremento de la pena, de la mitad a las tres cuartas partes, de efectivizarse las siguientes circunstancias agravantes:

- **La calidad del sujeto pasivo.** El estado o instituciones del sector financiero nacionales o extranjeros, también pueden fungir como sujeto pasivo en este tipo de ilícitos, cuando la afectación recae sobre sus redes o sistemas informáticos o de comunicaciones.
- **La calidad del sujeto activo.** Cuando el delito es cometido por un servidor público en el ejercicio de sus funciones.
- **La deslealtad del sujeto activo.** Se sanciona más drásticamente a quien ha sido depositario de la confianza y se aprovecha de esta para la comisión del ilícito.
- **La revelación de información en perjuicio**. Revelar información personal y consecuencia de ello generar un perjuicio. Aunque no se describe la naturaleza del mismo, se asume que puede ser tanto moral como económico.
- **La obtención de provecho.** La pena se agrava cuando se obtiene un beneficio para sí o un tercero, esta circunstancia no es aplicable al Artículo 269F, que ya establece este tipo de ventaja en su configuración.
- **La seguridad pública.** Los sistemas informáticos pueden ser utilizados para amedrentar a la sociedad o generar riesgos para la seguridad o defensa nacional.

- **La instrumentalización de un interviniente.** Cuando el sujeto activo utiliza a otra persona para que actúe como cómplice, o cuando instrumentaliza a alguien para colaborar en la comisión del delito y también a la víctima para que lleve a cabo la conducta típica.
- **La posición de garante.** Cuando el sujeto activo se aprovecha de su posición de garante respecto a la información y datos, para realizar el ilícito es pasible de sufrir adicionalmente la pena de inhabilitación para el ejercicio de la profesión relacionada con sistemas de información hasta por tres años. Este numeral comprende a los responsables o encargados de las bases de datos.

Cabe manifestar que la tutela brindada por los citados Artículos, se orienta a los datos de carácter personal de manera genérica, no efectuando distinción respecto a los datos sensibles y de menores de edad; no obstante, se deduce que la salvaguarda de igual forma incluye esta especie de datos.

Este marco jurídico se ha convertido en una importante contribución e instrumento efectivo para enfrentar los “delitos informáticos” en Colombia, en particular los inherentes a los datos personales, posibilitando la persecución penal contra aquellos delincuentes que incurran en las conductas tipificadas en dicha norma.

Por último, señalar que mediante Ley N°1928 de 24 de julio de 2018 el Congreso de Colombia aprobó el Convenio sobre la Ciberdelincuencia suscrito en Budapest, Hungría en 2001 adhiriéndose al mismo, con lo que inició una nueva faceta de lucha contra la delincuencia informática, forjando una política de ciberseguridad que le permite acceder a capacitación y colaboración internacional para contrarrestar este flagelo de carácter global.

4.3 España

El Código Penal Español fue aprobado mediante la Ley Orgánica N°10/1995 de 23 de noviembre de 1995, incluyendo tipos penales relacionados con la tutela de los datos personales, a decir de Gómez (2008) este aspecto en su momento representó una novedad de dicho cuerpo legal (p. 329).

En lo sucesivo el Código Penal ha experimentado diversas modificaciones siendo la última efectuada mediante Ley Orgánica N°1/2015 de 30 de marzo de 2015, bajo la motivación de ofrecer respuesta a la delincuencia informática y observando la transposición de la Directiva N° 2013/40/UE de 12 de agosto de 2013, cuyo objeto, conforme a su Artículo 1 radica en

establecer normas mínimas relativas a la definición de infracciones penales y sanciones aplicables en el ámbito de los ataques contra los sistemas de información, facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes; documento de aplicación obligatoria de los miembros de la Unión Europea y que en sus Considerandos 5, 29, 30 y Artículo 9, destaca la preminencia y exhorta a tutelar el derecho fundamental de protección de datos personales y en caso de su afectación imponer las respectivas sanciones.

Es así que el ya citado Código Penal, en su Título X, Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, Capítulo I, Del descubrimiento y revelación de secretos, con relación a la protección de datos personales, prevé:

> Artículo 197
> 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
> 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.
> 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.
> Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.
> 4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:
> a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o
> b) Se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.
> Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.
> 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual,

o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.

7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

(…) Artículo 197 ter. Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:

a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o

b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 197 quater

Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

Artículo 197 quinquies

Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.

Artículo 198

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

> Artículo 200. Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

El Artículo 197, numeral 1, prevé el tipo básico de descubrimiento y revelación de secretos, que tutela el derecho fundamental a la intimidad personal, según Rodríguez (2007, p.494) "(…) superando la idea tradicional del concepto de libertad negativa, materializado en el concepto de secreto que imperaba en el Código Penal derogado, art. 497". Por su parte, el numeral 2, se encuentra orientado específicamente a la protección de datos personales, en ese entendido para Gómez (2008) el bien jurídico protegido es la libertad informática o habeas data: "(…) como afirmación de la propia libertad y dignidad de la persona frente al poder informático, reconociéndole al individuo facultades de control sobre los datos personales informatizados (…)" (p. 330), considerada como el derecho a controlar el uso de los datos que se encuentran en un programa informático o en otro tipo de archivo.

Constituye un tipo de carácter doloso, porque el sujeto activo opera sin autorización, para apoderarse, acceder, utilizar, alterar o modificar, datos de carácter personal o familiar reservados registrados en ficheros o soportes informáticos, electrónicos o telemáticos o cualquier otro tipo de archivo, o registro público o privado, es decir no se limita únicamente a datos insertos en soporte digital, sino también en otros formatos. En este contexto, Anarte (2002), señala:

> Así se deriva de que además de sobre datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos, las conductas puedan recaer sobre datos registrados en cualquier otro tipo de archivo o registro. Esto puede interpretarse sin duda a favor de que el Código acoge algunos de los rasgos de las fases más avanzadas de la libertad informática y en ese sentido que parece lógico afirmar que el precepto brinda una "protección penal de datos personales" (p. 236).

Respecto al término "reservados" el mismo autor señala:

> Más bien parece que, por mucho que la condición de dato "personal" o, mejor, de "carácter personal" (y la de automatizado) generalmente conlleve la condición de reservado, este precepto mantiene una diferencia entre ambas condiciones, que permite separar el régimen jurídico-penal, que muestra así su naturaleza de ultima ratio, de la tutela dispensada en especial por la LOPRODA, respecto de todos los datos de carácter personal. (Anarte, 2002, p. 237)

Sobre el particular, el término reservados originó una controversia doctrinal inclinándose algunos autores (Morales Prats, Romeo Casabona, Rueda Martín, Fernández Teruelo, Gómez

Navajas, Puente Aba, González Rus, Carbonell Mateu y González Cussac), por asentir que independientemente del vocablo, la tutela de este numeral alcanza todo tipo de datos personales, en este sentido Gómez (2008), expresa:

> Es importante resaltar que los datos reservados protegidos en el artículo 197.2 del CP no pertenecen a lo que se ha dado en denominar el núcleo duro de la privacy (SSTS de 10 de diciembre de 2004 y 11 de julio de 2001, Ar. 1056), es decir, no son datos de los considerados «sensibles». Para MORALES PRATS el término «reservados» no tiene sentido porque todos los datos personales automatizados quedan protegidos por el artículo 197.2 del CP, dado que una vez introducidos en el fichero automatizado pueden ser manipulados. (p. 341)

Sin embargo, otro sector doctrinal (Orts Berenguer y Roig Torres, Queralt Jiménez, Anarte Borrallo y Doval Pais y Tomás-Valiente Lanuza), asume la posición de que la protección comprende a los datos concernientes a la intimidad más estricta. Finalmente, el Tribunal Supremo español en gran parte de sus fallos, se decantó por adoptar la interpretación más amplia (Gonzáles, 2015, p. 58), considerando que los datos personales sensibles se encuentran particularmente tutelados por el numeral 5 del Artículo 197.

Como condición para que se consume el ilícito debe operar un perjuicio de cualquier índole, no especificándose la naturaleza del menoscabo ocasionado, por lo que constituye un delito de resultado. El sujeto activo es indeterminado, mientras que el sujeto pasivo resulta ser un tercero en la primera parte del artículo. En su segunda parte, el numeral 2 tipifica el acceso por cualquier medio y la alteración o utilización en perjuicio del titular o un tercero de estos datos; en ambos supuestos el tercero puede ser el titular de la base de datos o del fichero que resguarda los datos o inclusive otra persona o institución que resultare afectada.

Respecto al sujeto pasivo, se ha identificado una falta de precisión en la redacción, ya que no existe claridad al determinar quién puede ostentar esta calidad, pues el Artículo 197, numeral 2, en su primera parte refiere únicamente como tal a un tercero, mientras que en la segunda señala al titular de los datos o un tercero, lo cual llevaría a concluir que el titular no puede ser incluido como sujeto pasivo en la primera parte de dicho numeral (Gómez, 2008, pp. 332-333).

Con relación al empleo en la redacción de los términos “modificar” y “alterar” Gómez (2008), sostiene:

> Se castiga, asimismo, en el primer inciso del artículo 197.2 del CP, la modificación de datos reservados, mientras que en el inciso 2.º del artículo 197.2 del CP se castiga la alteración de

> datos, sin que se alcance fácilmente a ver qué diferencia hay entre una y otra conducta. (p. 337)

Para ambos casos se impone la pena de prisión de uno a cuatro años y multa de doce a veinticuatro meses. Cabe añadir que, la protección penal se circunscribe a la tutela de datos ya registrados o archivados y, por tanto, no se extiende a las fases de creación de los ficheros automatizados y de recogida de datos personales. El numeral 3 del Artículo 197, constituye un tipo agravado, relacionado con los numerales 1 y 2. En su primera parte la acción típica, consiste en difundir, revelar o ceder a terceros, datos o hechos descubiertos o imágenes captadas, imponiendo las penas de prisión de dos a cinco años y en la segunda parte, prisión de uno a tres años y multa de doce a veinticuatro meses, a quien realice estas conductas sin haber tomado parte en su descubrimiento, conociendo su origen ilícito.

La segunda parte, se califica como delito autónomo porque el sujeto activo del mismo no ha intervenido en el tipo básico (Rodríguez, 2007, p.691); no obstante conocer el origen ilícito de los datos, hechos o imágenes. Dicha determinación, responde a razones de política criminal, para evitar la impunidad de ciertas conductas ajenas a la vulneración directa del derecho fundamental, pero que igualmente atentan contra el mismo.

A su turno, el numeral 4, se encuentra referido a la cualificación del autor e impone una pena privativa de libertad de tres a cinco años, cuando los hechos descritos en los numerales 1 y 2 se cometan por los encargados o responsables de las bases de datos, archivos o registros, o cuando se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima, por lo tanto, constituye un tipo agravado.

Y si los datos reservados se hubieran difundido, cedido o revelado a terceros, se imponen las penas en su mitad superior. Por lo expuesto, se evidencia que este apartado, recoge los principios de responsabilidad y consentimiento en el tratamiento de datos personales, que al ser vulnerados originan el ilícito. Así también, la tutela de este numeral, comprende a la cesión o transferencia de datos y el deber de confidencialidad que deben observar los encargados y responsables del tratamiento de datos personales.

En dicho sentido, Gómez (2008), infiere:

> El fundamento de la agravación se basa, pues, en la condición profesional del sujeto activo, que tiene acceso autorizado a los datos pero que, precisamente por ello, está especialmente llamado a velar por la reserva de éstos. Ello limita considerablemente el ámbito de aplicación del tipo cualificado, pues esa persona debe tener encomendada esa responsabilidad,

> otorgándole una posición de garante de discreción con respecto a los archivos y registros en los cuales constan los datos reservados. (p.349)

En cuanto a los datos sensibles, el numeral 5 del Artículo 197 le otorga protección a aquellos datos que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o cuando la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, imponiendo las penas previstas en su mitad superior, es decir se está frente a un tipo agravado en función a la cualidad del dato y de la víctima.

Mientras que el numeral 6, impone la sanción prevista en los incisos 1 al 4 del Artículo 197, en su mitad superior, si los hechos se realizan con fines lucrativos, imponiendo otra agravante cuando además se trate de datos sensibles, sancionando esta conducta con la pena de prisión de cuatro a siete años.

Por su parte, el numeral 7 del Artículo 197, determina la pena de prisión de tres meses a un año o multa de seis a doce meses, cuando sin autorización de la persona afectada se difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella, obtenidas con su asentimiento cuando la divulgación menoscabe la intimidad personal, estableciéndose que si el agente es el cónyuge o pareja, aún sin convivencia, o la víctima fuera menor de edad o persona con discapacidad, o el hecho fuere perpetrado con fines de lucro, se impondrá la pena en su mitad superior. Esta conducta comprende la denominada pornovenganza, consistente en la difusión de imágenes o grabaciones audiovisuales con contenido sexual, en las que se actúa por revancha, exigiendo en ocasiones a la víctima un monto pecuniario a cambio, hostigándola sexualmente, o llegando a comercializar las imágenes y videos obtenidos, vulnerando el principio de consentimiento que rige en materia de protección de datos personales.

Al respecto, Gonzales (2015), asevera:

> Esta agravación responde, en términos de injusto, a las mayores posibilidades de comisión del delito por parte de aquellos sujetos, por lo fácil que les resulta o les puede resultar acceder a fotografías y videos íntimos de quien es o ha sido su pareja y que han sido realizados en común. No puede pasarse por alto, además, que la tipificada es una conducta que se desata cada vez con mayor frecuencia en el seno de rupturas sentimentales abruptas, las cuales crean un terreno propicio para traicionar la expectativa de intimidad de la otra parte, con lo cual razones de prevención general también pueden haberse tenido en cuenta a la hora de incluir este tipo agravado. (p.71)

El Artículo 197 ter, adelanta la intervención del derecho penal a conductas preparatorias de los ilícitos previstos en los numerales 1 y 2 del Artículo 197 o del Artículo 197 bis, cuando sin estar debidamente autorizado, el agente produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros: un programa informático para cometer estos delitos; una contraseña, código, o similares para acceder a la totalidad o parte de un sistema de información, imponiendo la sanción privativa de libertad de seis meses a dos años o alternativamente una multa de tres a dieciocho meses.

A su turno el Articulo 197 quater, establece la aplicación de las penas superiores en grado cuando los hechos descritos en el Capítulo se hubieran cometido en el seno de una organización criminal, configurando así otra agravante. El Artículo 197 quinquies, contempla la responsabilidad penal de las personas jurídicas por cualquiera de los delitos comprendidos en los Artículos 197, 197 bis y 197 ter., en este caso el sujeto activo lo conforman las personas de existencia moral.

Además de la multa de seis meses a dos años, el citado Artículo faculta a los jueces y tribunales a imponer las penas establecidas por el apartado 7 del Artículo 33, en sus incisos b) al g), los cuales refieren:

> b) Disolución de la persona jurídica. La disolución producirá la pérdida definitiva de su personalidad jurídica, así como la de su capacidad de actuar de cualquier modo en el tráfico jurídico, o llevar a cabo cualquier clase de actividad, aunque sea lícita.
> c) Suspensión de sus actividades por un plazo que no podrá exceder de cinco años.
> d) Clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años.
> e) Prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito. Esta prohibición podrá ser temporal o definitiva. Si fuere temporal, el plazo no podrá exceder de quince años.
> f) Inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años.
> g) Intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exceder de cinco años.

Cabe señalar que los tipos descritos con anterioridad por sus características son de carácter doloso, mediando en estos la voluntad final de realizar la acción típica.

Por su parte, el Artículo 198, prevé la responsabilidad específica de la autoridad o funcionario público, cuya conducta puede adecuarse a cualquier tipo descrito en el Artículo 197, 197 bis

y 197 ter, en este supuesto, además de la imposición de las penas previstas en los citados Artículos en su mitad superior, le corresponderá la inhabilitación absoluta[15] de seis a doce años. De lo señalado se infiere que puede obrar como sujeto activo un funcionario público, operando esta particularidad como circunstancia agravante y ameritando la imposición de una sanción adicional de prohibición, en atención a que por sus específicas labores, se encuentra en posición de garante de derechos de terceros, teniendo la posibilidad de entrar en conocimiento de datos personales de los mismos y utilizarlos ilícitamente, por lo cual este tipo penal es de índole dolosa.

El Código Penal Español, también otorga protección a los datos de personas jurídicas cuando se descubran, revelen o cedan datos de las mismas, sin el consentimiento de sus representantes, así lo dispone en su Artículo 200, por el cual las regulaciones del Capítulo son aplicables a este tipo de entes en lo que fuere pertinente. Así también, España se adhirió al Convenio sobre Ciberdelincuencia de Budapest, mediante Instrumento de ratificación de 20 de mayo de 2010, lo cual sin duda constituye un gran paso en el ámbito de la investigación y sanción de delitos informáticos, aportando así con herramientas legales y procedimentales para la lucha contra el cibercrimen cuyo carácter es fundamentalmente transfronterizo.

Del análisis de la legislación comparada, se deduce que los datos personales en los países señalados se encuentran protegidos en la vía penal, ya sea desde la perspectiva del bien jurídico que involucra la intimidad, la privacidad (en su faceta positiva o negativa) o desde la salvaguarda de la información y el dato, habiéndose introducido tipos penales específicos para su tutela, en atención a la gravedad de las consecuencias que acarrea su vulneración, siendo aplicables en última ratio, es decir, al no ser posible acudir o garantizar el derecho a través de otras vías. Adicionalmente, Argentina, Colombia y España se encuentran adscritos al Convenio de Budapest, aspecto que incide positivamente en la adopción de disposiciones sustantivas y procedimentales de orden interno y transnacional en materia de cibercrimen, con el fin de contrarrestar la criminalidad que se vale de medios tecnológicos para cometer conductas punibles atentatorias del derecho de protección de datos personales o autodeterminación informativa.

En este sentido, estos países asumieron el compromiso de garantizar que prime en sus ordenamientos jurídicos penales la confidencialidad e integridad de los sistemas informáticos, redes y datos, bajo el reconocimiento de que la protección de la información y los datos

[15] De acuerdo al Artículo 41 del Código Penal Español, la pena de inhabilitación absoluta produce la privación definitiva de todos los honores, empleos y cargos públicos que tenga el penado, aunque sean electivos. Produce, además, la incapacidad para obtener los mismos o cualesquiera otros honores, cargos o empleos públicos, y la de ser elegido para cargo público, durante el tiempo de la condena.

personales es sustancial en la Era Digital y que su uso ilícito amerita la atención del derecho penal por atentar contra bienes jurídicos y transgredir una vasta gama derechos fundamentales.

A continuación, se presentan los contenidos sintetizados de la legislación comparada analizada, incluyendo al Estado Plurinacional de Bolivia:

Tabla N°19

Legislación comparada

PAÍS	TIPO PENAL		SUJETO ACTIVO	SUJETO PASIVO	CONDUCTA	ELEMENTOS DESCRIPTIVOS Y NORMATIVOS	OBJETO	SANCIÓN	AGRAVANTE
	Datos personales	Datos pers. sensibles							
ARGENTINA	Acceso y revelación de datos personales Art. 157 bis num. 1 y 3	Datos cuyo secreto se está obligado a preservar por disposición de la ley Art. 157 bis num. 2	Cualquier persona Persona obligada a preservar secreto Funcionario público	Titular de los datos	Acceder Proporcionar Revelar Insertar	-A sabiendas e ilegítimamente -Violando un sistema de confidencialidad y seguridad -De cualquier forma	Dato personal en banco de datos o archivo	Prisión de 1 mes a dos años	Inhabilitación especial de 1 a 4 años
BOLIVIA	Manipulación informática Art. 363 bis	-	Cualquier persona	Titular de la información - tercero	Manipular	-Beneficio indebido -Perjuicio de tercero -Resultado incorrecto -Evitar proceso -Procesamiento o transferencia	Datos informáticos	Reclusión de 1 a 5 años y multa de 60 a 200 días	-
	Alteración, acceso y uso indebido de datos informáticos Art. 363 ter		Cualquier persona	Titular de la información	Apoderar Acceder Utilizar Modificar Suprimir Inutilizar	-Perjuicio del titular -Computadora o soporte informático	Datos en cualquier soporte informático	Prestación de trabajo hasta un año o multa de hasta 200 días	
COLOMBIA	Violación de datos personales Art. 269F	-	Cualquier persona Servidor público Resp. de la Información Persona con relación de confianza	Titular de los datos	Obtener Compilar Sustraer Ofrecer Vender Intercambiar Enviar Comprar Interceptar Divulgar Modificar Emplear	-Sin estar facultado -Provecho propio o de un tercero	Dato personal o código personal en archivos, bases de datos o semejantes	Prisión de 48 a 96 meses y multa de 100 a 1000 salarios mínimos	De la mitad a tres cuartas partes -Redes o sistemas estatales o financieros -Servidor público -Confianza depositada -Revelar información en perjuicio -Obtener provecho para sí o tercero -Fines terroristas -Utilizando un tercero de buena fe -Responsable de los datos adicionalmente inhabilitación hasta por 3 años
ESPAÑA	Datos de carácter	-Ideología -Religión -Creencias	2.Cualquier persona	Titular de los datos o tercero	Apoderar Utilizar	-Sin autorización -En perjuicio de tercero o del titular	Datos personales en cualquier tipo de archivo	Prisión de 1 a 4 años y multa de 12 a 24 meses.	

	personal o familiar Art. 197 num. 2, 3, 4, 6, 7	-Salud -Origen racial -Vida sexual -Victima Menor -Víctima discapacitada Art. 197 num. 5			Modificar Acceder Alterar				
			3.Cualquier persona	Titular de los datos	Difundir Revelar Ceder	-A terceros	Datos Hechos Imágenes	Prisión de 2 a 5 años	
						-Conocimiento del origen ilícito y sin tomar parte de su descubrimiento		Prisión de 1 a 3 años y multa de 12 a 24 meses	
			4.Respons. o encargado de la información	Titular de los datos	Apoderar Utilizar Modificar Acceder Alterar Difundir Revelar Ceder	-Responsables de los ficheros,soporte informáticos, electrónico, telemáticos, archivos o registros -Utilización no autorizada	Datos personales en cualquier tipo de archivo.	Prisión de 3 a 5 años	En su mitad superior si se hubieren difundido cedido o revelado
			5.Cualquier persona	Titular de los datos	Descritos en los apartados anteriores	-Datos que revelen ideología, religión, creencias, salud, origen racial, vida sexual. -Víctima menor de edad -Persona con discapacidad necesitada de protección	Datos personales sensibles Datos personales de menores Datos personales de victima con discapacidad		Penas previstas en los apartados anteriores en su mitad superior
			6.Cualquier persona	Titular de los datos	Hechos descritos en los apartados anteriores	-Fines lucrativos	Datos personales descritos en los apartados anteriores		Penas previstas en los apartados del 1 al 4 en su mitad superior Prisión de 4 a 7 años para datos personales sensibles
			7.	Titular de los datos	Difundir Revelar	-Sin autorización -A terceros	Imágenes	Prisión de 3 meses a 1 año o multa de 6 a 12 meses	Mitad superior si es el cónyuge o análogo

			-Cualquier persona -Cónyuge o análogo		Ceder	-Con anuencia de la víctima -Menoscabo grave a la intimidad -En domicilio o lugar fuera del alcance	Grabaciones audiovisuales		Victima menor Victima con discapacidad Fines lucrativos
	Art. 197 quater		Org. Criminal	Titular de los datos	Hechos descritos en el Capítulo	-En el seno de una organización criminal	Descritos en el Capítulo		Penas superiores en grado
	Art.197 quinquies		Persona jurídica	Titular de los datos	Delitos Art. 197, 197 bis y ter		Descritos en los Art. 197, 197 bis y ter	Multa de 6 meses a 2 años Además de las establecidas en el Artículo 33, apartado 7 incisos b al g	
	Art. 198		Funcionario público	Titular de los datos	Delitos Art. 197, 197 bis y ter	-Sin mediar causa legal -Prevaliéndose de su cargo	Descritos en los Art. 197, 197 bis y ter	-	Penas en su mitad superior Inhabilitación absoluta por 6 a 12 años
	Art. 200		Descritos en el Capítulo	Persona jurídica	Descubrir Revelar Ceder	-Sin el consentimiento de sus representantes	Descritos en el Capítulo	Descritos en el Capítulo	Descritos en el Capítulo

Fuente: elaboración propia (2019)

CAPÍTULO V
PROPUESTA

5.1 Introducción

El presente apartado desarrolla la propuesta de la investigación, consistente en un proyecto de Ley a efectos de incorporar tipos penales en el Código Penal del Estado Plurinacional de Bolivia, orientados a la protección de los datos personales, para con ello contribuir a optimizar la tutela del derecho de autodeterminación informativa. El citado derecho, entendido como la facultad del individuo de ejercer un control sobre sus datos e información de carácter personal, ya sea de naturaleza pública, privada o íntima que lo identifican o lo hacen identificable, tiene su génesis en respuesta a las nuevas necesidades derivadas de la revolución tecnológica, es así que la investigación partió de advertir la ausencia de los citados tipos penales dentro del esquema estructural del Código Penal del Estado Plurinacional del Bolivia y, en segunda instancia, al determinar la necesidad de su creación.

Al efecto, se consideran principios y preceptos constitucionales y otros particularmente orientados a la temática analizada; del mismo modo, los resultados emanados de la encuesta, la entrevista y el estudio de caso, a los cuales se arribó producto del trabajo de campo.

5.2 Objetivo

La propuesta tiene el objetivo de incorporar tipos penales referentes a la protección de datos personales, datos personales sensibles y datos personales de menores de edad, en el Código Penal del Estado Plurinacional de Bolivia.

5.3 Alcance

El alcance de la propuesta es a nivel nacional puesto que se plantea la incorporación de artículos en el Código Penal, orientados al conjunto de los estantes y habitantes del Estado Plurinacional de Bolivia.

5.4 Bases jurídicas y técnicas de la propuesta

La propuesta se sustenta en derechos, así como principios de corte constitucional y otros inherentes a la protección de datos personales y al ámbito del derecho penal, de acuerdo a los fundamentos que a continuación se exponen.

5.4.1 Derechos y bienes jurídicos tutelados

El derecho a la autodeterminación informativa o derecho a la protección de datos personales, se encuentra desarrollado en el núcleo de la Acción de Protección de Privacidad consagrado en el Artículo 130 de la Constitución Política del Estado y afianzado por el Tribunal Constitucional boliviano en su labor interpretativa, como expresión jurisprudencial contenida en las Sentencias Constitucionales Nrs. 0127/2010-R de 10 de mayo de 2010 y 1978/2011-R de 7 de diciembre de 2011, así como Sentencias Constitucionales Plurinacionales Nrs. 2175/2012 de 8 de noviembre de 2012, 0089/2014-S2 de 4 de noviembre de 2014, 0080/2014-S2 de 4 de noviembre de 2014, 0332/2015-S1 de 6 de abril de 2015, 0819/2015-S3 de 10 de agosto de 2015 y 0426/2015-S3 de 20 de abril de 2015, entre otras, que reconocen su carácter de derecho humano y fundamental para acceder a los bancos de datos públicos y privados con el fin de tener conocimiento de la información almacenada, hacia donde fluyó la misma, para qué fines y ejercer un control sobre sus datos personales.

Así también, debe considerarse que la propia Norma Fundamental, en su Artículo 13 parágrafos II y IV, señala: “Los derechos que proclama esta Constitución no serán entendidos como negación de otros derechos no enunciados (…) los derechos y deberes consagrados en esta Constitución se interpretarán de conformidad con los Tratados internacionales de derechos humanos ratificados por Bolivia”.

En concordancia, los Artículos 256, parágrafos I y II y 410 parágrafo II de la citada Norma Suprema, establecen que los tratados e instrumentos internacionales en materia de derechos humanos, firmados, ratificados o a los que se hubiera adherido el Estado, que declaren derechos más favorables a los contenidos en la Constitución, se aplicaran de manera preferente sobre ésta; asimismo, la interpretación de los derechos fundamentales se efectúa de acuerdo a los tratados internacionales de derechos humanos cuando éstos prevean normas más favorables. En consecuencia, estos instrumentos de orden internacional forman parte del bloque de constitucionalidad.

De lo señalado se destaca el principio de progresividad, el bloque de constitucionalidad y la cláusula abierta, como institutos jurídicos de la Constitución boliviana, que permiten la evolución permanente del subsistema garantista, lo cual también hace viable la protección del derecho de autodeterminación informativa o protección de datos personales, siendo que todo sistema democrático se funda en el respeto de los derechos humanos y debe orientar su accionar a cautelar y mantener su vigencia. Bajo dicho razonamiento, el citado derecho ha

sido reconocido en el Estado Plurinacional de Bolivia, gracias a la labor del Máximo Intérprete de la Constitución, ameritando mecanismos efectivos para su tutela.

La autodeterminación informativa o protección de datos personales, es el derecho cuya optimización primordialmente se pretende con la presente propuesta, a través de la protección penal de la información y los datos. Por su carácter no solo sustantivo sino transversal e instrumental para el ejercicio y tutela de otros derechos, adquiere preminencia considerando que, a través de su eficaz salvaguarda, se protegerán los mismos, a contrario sensu, su vulneración acarreará el menoscabo de dichos derechos, entre estos a manera enunciativa, mas no limitativa, se encuentran los siguientes:

Tabla N°20

Derechos tutelados a través de la autodeterminación informativa

DERECHO	ARTÍCULO DE LA CONSTITUCIÓN POLÍTICA DEL ESTADO
No ser discriminado	14 parágrafo II
Vida	15
Integridad física	15
Integridad psicológica	15
Integridad sexual	15
Salud	18 parágrafo I y II
Autoidentificación cultural	21 numeral 1
Privacidad	21 numeral 2
Intimidad	21 numeral 2
Honra	21 numeral 2
Honor	21 numeral 2
Propia imagen	21 numeral 2
Dignidad	21 numeral 2, 22
Espiritualidad	4, 21 numeral 3
Religión y culto	4, 21 numeral 3
Acceder a la información	21 numeral 6
Libertad	22
Petición	24
Secreto de las comunicaciones privadas	25
Trabajo digno sin discriminación	46 parágrafo I
Derechos de la niñez y adolescencia	59, 60 y 61

Fuente: elaboración propia (2019)

El derecho a la autodeterminación informativa, al ser considerado como el núcleo de la personalidad, la libertad y la dignidad (Garriga, 2004, p. 41), se encuentra estrechamente vinculado a una multiplicidad de derechos fundamentales, radicando en lo anterior uno de los pilares para prevenir y sancionar su conculcación, es por ello que, en la medida en que el Estado implemente acciones concretas de índole legislativo para su protección como líneas de defensa especializada para los individuos, estas incidirán diametralmente en el resguardo de otros derechos fundamentales, radicando en ello una justificación preponderante, para la incorporación de nuevos tipos penales en la norma sustantiva penal.

A su turno, la tutela de la información y el dato como bienes jurídicos, coadyuvará a salvaguardar otros bienes jurídicos contenidos en la legislación vigente, como el honor, la propiedad, la fe pública, la libertad sexual, la vida y la integridad corporal.

5.4.2 Principios

Toda ley debe fundarse en principios rectores y orientadores que constituyen el horizonte de la misma y a manera de lineamientos inspiran el rol que desempeña dentro de la arquitectura legal del Estado y en beneficio de la sociedad.

Es así que, con relación a la presente propuesta, se consideran principios y valores supremos contenidos en la Constitución Política del Estado, como directrices de las que deriva el ordenamiento jurídico y el orden sociopolítico de una nación, cuya fuerza es vinculante. A su vez, la propuesta se cimenta en principios establecidos en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 20 de junio de 2017 y el Reglamento General de Protección de Datos de 27 de abril de 2016; en razón de que ambos desarrollan fundamentos de carácter técnico y especializado, el primero al constituir un conjunto de directrices en materia de protección de datos personales dirigido a países latinoamericanos; mientras que el segundo, debido a las disposiciones vanguardistas que contiene, que han inspirado a distintos Estados del orbe para elaborar su legislación y al erigirse al presente, como el más alto estándar en la temática analizada.

a) Principios, valores y preceptos constitucionales

Con base en el pluralismo, el Estado boliviano se estructura sobre principios y valores rectores, partiendo del fenómeno de constitucionalización del ordenamiento jurídico, o irradiación de su contenido hacia las normas infra constitucionales, en consecuencia, la

propuesta se inspira en principios ético – morales y valores supremos de orden constitucional, contenidos en el Artículo 8 de la Norma Fundamental, tal como se esgrime a continuación:

- **Suma qamaña (vivir bien)**: es entendido como un estado de bienestar, una relación de equidad entre las personas y la comunidad (Choque, 2007, p. 280), y es un componente que se pretende robustecer con la incorporación de tipos penales orientados a la tutela de la información y los datos personales, de modo tal que no queden impunes conductas nocivas que lesionen estos bienes jurídicos, las mismas que son cada vez más recurrentes en la realidad boliviana.

  Con lo anterior, se pretende contribuir a asegurar el restablecimiento de una convivencia pacífica en sociedad, proporcionando al individuo un mecanismo más para ejercer su derecho a la autodeterminación informativa.

- **Dignidad**: de acuerdo a Yañez (2007, pp. 204-205) implica en primer término, la prohibición de la producción de normas o la realización de actos, que tengan un contenido degradante o envilecedor. En segundo término, impone un mandato de actuación, que le impele al Estado a desarrollar políticas destinadas a promocionar o favorecer el desarrollo de la persona. Para Garriga (2016, p. 59) es el fundamento de los derechos humanos. Es así que, mediante la incorporación de tipos penales referidos a la protección de datos personales, se coadyuvará a preservar el derecho del individuo a un trato que no lesione su condición de ser racional, libre, igual y capaz de autodeterminarse responsablemente.

- **Igualdad**: entendida como valor y principio que reconoce las diferencias y al mismo tiempo sostiene que ellas, no pueden ser soporte para ningún tipo de discriminaciones. El Estado debe asegurar una eficaz igualdad formal y material de la ley, proscribiendo cualquier tipo de discriminación, y en su caso, brindar las facilidades, medios y recursos para que puedan acceder libremente a las oportunidades, quienes en razón de desventajas económicas, sociales, culturales o de cualquier naturaleza, se hallan impedidos de gozar de las mismas. La propuesta se orienta en base a este valor, otorgando a cualquier individuo la posibilidad de obtener la tutela respecto a su información y datos personales en la vía penal; como una herramienta para optimizar su derecho a la autodeterminación informativa.

- **Libertad**: constituye un fundamento necesario para el resto de los valores, como un cimiento de la configuración del orden político y de la paz social. En el caso concreto,

involucra la libertad del individuo de decidir sobre sus datos personales y ejercer un control sobre los mismos; en consecuencia, la obtención y el tratamiento de estos datos sólo debe realizarse con el consentimiento del titular, así también en cumplimiento de un mandato legal o judicial, quedando vedada su obtención, utilización, difusión o cualquier procesamiento ilícito.

- **Respeto:** posibilita lograr una armoniosa interacción social. Toda persona tiene derecho al respeto de sus datos personales, máxime si estos son sensibles, esta información no puede procesarse sin el consentimiento ni conocimiento de la persona interesada, salvo que medie disposición legal o judicial expresa. Toda conducta que vulnere este valor, al generar consecuencias negativas para el titular amerita las sanciones respectivas.

- **Responsabilidad**: la adopción de medidas normativas para la adecuada tutela del derecho de autodeterminación informativa, en observancia de mandatos constitucionales y legales, constituye responsabilidad del Estado Plurinacional de Bolivia. Las entidades públicas, privadas o personas particulares que efectúen el tratamiento de datos e información personal, deben actuar responsablemente, considerando que la vulneración de derechos acarrea consecuencias jurídicas para los titulares de los datos, para los responsables de las bases de datos o para cualquier persona que efectúe el procesamiento de los mismos.

La Constitución Política del Estado, contiene a su vez, preceptos en los que se sustenta la presente propuesta:

> Artículo 9. Son fines y funciones esenciales del Estado, además de los que establece la Constitución y la ley:
> 1. Constituir una sociedad justa y armoniosa (…) sin discriminación.
> 2. Garantizar el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, las naciones, los pueblos y las comunidades, y fomentar el respeto mutuo (…).
> (…) 4. Garantizar el cumplimiento de los principios, valores, derechos y deberes reconocidos y consagrados en esta Constitución.
> (…) Artículo 13.
> I. Los derechos reconocidos por esta Constitución son inviolables, universales, interdependientes, indivisibles y progresivos. El Estado tiene el deber de promoverlos, protegerlos y respetarlos.
> II. Los derechos que proclama esta Constitución no serán entendidos como negación de otros derechos no enunciados.

(…) IV. (…) Los derechos y deberes consagrados en esta Constitución se interpretarán de conformidad con los Tratados internacionales de derechos humanos ratificados por Bolivia.

Artículo 14.

I. Todo ser humano tiene personalidad y capacidad jurídica con arreglo a las leyes y goza de los derechos reconocidos por esta Constitución, sin distinción alguna.

II. El Estado prohíbe y sanciona toda forma de discriminación fundada en razón de sexo, color, edad, orientación sexual, identidad de género, origen, cultura, nacionalidad, ciudadanía, idioma, credo religioso, ideología, filiación política o filosófica, estado civil, condición económica o social, tipo de ocupación, grado de instrucción, discapacidad, embarazo, u otras que tengan por objetivo o resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos de toda persona.

III. El Estado garantiza a todas las personas y colectividades, sin discriminación alguna, el libre y eficaz ejercicio de los derechos establecidos en esta Constitución, las leyes y los tratados internacionales de derechos humanos.

(….) Artículo 21. Las bolivianas y los bolivianos tienen los siguientes derechos:

(…) 2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad.

Artículo 22. La dignidad y la libertad de la persona son inviolables. Respetarlas y protegerlas es deber primordial del Estado.

(…) Artículo 25.

I. Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial.

II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente.

III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice.

(…) Artículo 60. Es deber del Estado, la sociedad y la familia garantizar la prioridad del interés superior de la niña, niño y adolescente, que comprende la preeminencia de sus derechos, la primacía en recibir protección y socorro en cualquier circunstancia, la prioridad en la atención de los servicios públicos y privados, y el acceso a una administración de justicia pronta, oportuna y con asistencia de personal especializado.

Artículo 61.

I. Se prohíbe y sanciona toda forma de violencia contra las niñas, niños y adolescentes, tanto en la familia como en la sociedad.

(…) Artículo 108. Son deberes de las bolivianas y los bolivianos:

1. Conocer, cumplir y hacer cumplir la Constitución y las leyes.

2. Conocer, respetar y promover los derechos reconocidos en la Constitución.

(…) Artículo 109.

(…) II. Los derechos y sus garantías sólo podrán ser regulados por la ley

> Artículo 110.
> I. Las personas que vulneren derechos constitucionales quedan sujetas a la jurisdicción y competencia de las autoridades bolivianas.
> II. La vulneración de los derechos constitucionales hace responsables a sus autores intelectuales y materiales.
> (…) Artículo 113.
> I. La vulneración de los derechos concede a las víctimas el derecho a la indemnización, reparación y resarcimiento de daños y perjuicios en forma oportuna.
> (…) Artículo 116.
> (…) II. Cualquier sanción debe fundarse en una ley anterior al hecho punible.

Es sustancial la importancia que reviste la Constitución en un Estado Constitucional de Derecho, respecto al establecimiento de un sistema de legitimación de la pena y, su relevancia para la reforma del sistema penal en general y para el derecho penal en particular. El poder punitivo del Estado se define y funda en la Norma Suprema, en consecuencia, los principios rectores del sistema penal no son meros límites al Ius puniendi[16], sino auténticos fundamentos o principios constituyentes del mismo, confluyendo en un derecho penal cuya función esencial es garantizar los valores, bienes y derechos que en el texto constitucional se establecen.

Por estas razones, desde una orientación constitucional y partiendo de que la intervención del derecho penal afecta derechos fundamentales y que las libertades sólo pueden limitarse a través de éste, solo los bienes de relevancia constitucional pueden justificar este sacrificio. En este contexto, la propuesta cimentada en la Constitución, se funda en valores supremos, los fines y funciones del Estado, los derechos fundamentales, las cláusulas para interpretar los mismos de conformidad con los Tratados internacionales de derechos humanos ratificados por Bolivia y aquellos preceptos propios del derecho penal.

b) Principios de la protección de datos personales

Los principios relativos a la protección de los datos personales en los que se sustenta la propuesta son los siguientes:

- **Licitud:** el tratamiento de datos personales realizado por entidades públicas, privadas y personas particulares en el Estado Plurinacional de Bolivia debe sujetarse a la

[16] Para la orientación sistemática o dogmática-penal, el rol de la Constitución es, básicamente, limitar el poder del Estado en materia penal y garantizar los derechos del individuo, en cambio desde la perspectiva sustancial o constitucional no solo es un límite sino fundamento del mismo.

Constitución Política del Estado y normativa vigente, debiendo efectuarse únicamente para fines lícitos.

- **Consentimiento**: es la base legal legitimadora del tratamiento de datos de carácter personal, las entidades públicas, privadas y personas particulares que efectúan tratamiento de datos personales, procurarán el consentimiento de los titulares de los datos, el cual debe recogerse en medios que permitan comprobar y demostrar que fue otorgado (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numeral 12 y RGPD, 2016, Artículo 7).

- **Calidad:** las entidades públicas y privadas que efectúen tratamiento de datos personales, deberán adoptar las medidas necesarias para mantener las bases de datos con información exacta, completa y actualizada, de tal manera que no se altere su veracidad. (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numeral 19).

- **Finalidad:** el tratamiento de datos personales debe sujetarse al cumplimiento de finalidades determinadas, explícitas, legítimas y lícitas. Las entidades públicas, privadas y personas particulares efectuarán el tratamiento de datos personales en su posesión únicamente para los fines que motivaron su acopio inicial, salvo que concurran causales previstas por la normativa vigente (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numeral 17).

- **Seguridad:** las entidades públicas y privadas deberán adoptar medidas de índole administrativo, físico y técnico, a efectos de garantizar la confidencialidad, integridad y disponibilidad de los datos personales, con el fin de consolidar adecuados sistemas de seguridad, incluida la protección contra el tratamiento no autorizado o ilícito y contra la pérdida, destrucción o daño accidental de datos personales. Las vulneraciones a la seguridad, darán lugar a la imposición de medidas correctivas y si corresponde sancionatorias (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numeral 21).

- **Protección especial:** los datos personales sensibles como el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos relativos a la salud, vida y orientación sexual, ameritan un especial resguardo. Constituye deber del Estado velar porque ningún tipo de institución o particular efectúe el tratamiento de datos personales sensibles, salvo

en los casos que sea estrictamente necesario para el cumplimiento de atribuciones y obligaciones expresamente previstas en las normas vigentes, o cuando se cuente con un consentimiento expreso y escrito del titular, por razones de seguridad nacional, seguridad pública, orden público, salud pública o salvaguarda de derechos y libertades de terceros (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numeral 9 y RGPD, 2016, Artículo 9).

- **Protección de menores de edad:** los niños y adolescentes merecen una protección específica respecto a sus datos personales, en consideración de que son mayores los riesgos y consecuencias que acarrea para ellos la utilización ilícita de su información personal (Estándares de Protección de Datos Personales para los Estados Iberoamericanos, 2017, numerales 8, 11.1 inciso i, 13 y 16.3; y RGPD, 2016, Considerandos 38, 58, 75; Artículos 6 numeral 1 inciso f), 8 y 12 numeral 1).

c) Principios del Derecho Penal

- **Legalidad:** involucra la necesidad de predeterminar normativamente las conductas ilícitas y sus penas, a través de una tipificación precisa dotada de la adecuada concreción en la descripción que incorpora (lex certa); es asimismo una garantía de orden formal, consistente en la necesidad de una norma que ostente rango de ley, como presupuesto de la actuación punitiva del Estado, exigencia estricta en el ámbito penal. En consecuencia, impone la limitación del ejercicio de la función punitiva solo a las acciones previstas por la ley con carácter previo aprobada por el Órgano Legislativo. En observancia de este principio, la incorporación de tipos penales orientados a la protección de la información y los datos personales, debe regularse por medio de una ley que remoce el Código Penal.

- **Taxatividad:** la pena es aplicable a un tipo de conducta expresamente prevista por la ley con la indicación de sus elementos descriptivos y normativos. Este principio, excluye la aplicación analógica de la ley penal, e impone que a través de la técnica legislativa se propenda a su objetividad. En dicho contexto, los tipos penales que se proponen posibilitarán una persecución penal y si corresponde el establecimiento de sanciones, para aquellas conductas que específicamente deriven de vulnerar la información y los datos personales, incidiendo lo anterior en optimizar la tutela del derecho de autodeterminación informativa.

- **Proporcionalidad de las penas:** las penas deben guardar relación con el daño causado por el delito, por lo tanto, el medio previsto por el legislador tiene que ser adecuado y exigible para alcanzar el objetivo propuesto. Este principio guarda estrecha relación con la libertad como valor y los principios de dignidad y justicia, en razón de que una pena desproporcionada, arremetería con la libertad y dignidad de la persona, consiguientemente sería injusta. Los tipos penales cuya incorporación al Código Penal se propone en el proyecto de ley, se inspirarán en este principio en su construcción, considerando las particularidades del delito y una sanción acorde al mismo.

- **Subsidiariedad:** la gravedad de la sanción penal como castigo, deberá reservarse únicamente para aquellas situaciones en que se haya demostrado que no puede utilizarse una forma de sanción menos grave. Por más reprochable que sea la conducta sólo se incluirán entre los tipos penales cuya creación se propone, aquellas que resulten más lesivas para los datos y la información personal de los individuos, cuya solución no pueda operar en otra vía por ser ineficaz o insuficiente.

5.5 Cumplimiento

El cumplimiento de la propuesta, se encuentra delegado a la Asamblea Legislativa Plurinacional, por ser el órgano llamado por Ley para la sanción de proyectos normativos, en observancia del procedimiento legislativo.

5.6 Factibilidad presupuestaria

El proyecto de ley no generará costo alguno, y coadyuvará a optimizar la tutela del derecho de autodeterminación informativa en Bolivia, como derecho cuyo ejercicio posibilita la protección de otros derechos, en un Estado constitucional y democrático que amerita el resguardo de la información y datos de carácter personal, atendiendo al contexto actual en el que se desenvuelve la sociedad boliviana.

5.7 Fundamentación de la propuesta

Los fundamentos en que se sustenta la propuesta se encuentran conformados por:

- **Fundamento político – social**

La Constitución Política del Estado, en su Artículo 9, numerales 1, 2 y 4 asume como fines y funciones esenciales del Estado, constituir una sociedad justa y armoniosa, con plena justicia social, garantizando el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, naciones, pueblos y comunidades, fomentando el respeto mutuo, así como el cumplimiento de los principios, valores, derechos y deberes reconocidos y consagrados en la misma.

En ese contexto, la Norma Fundamental, en su Artículo 103, parágrafo II, incluye como política estatal la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas Tecnologías de Información y Comunicación, reconociendo la importancia del conocimiento y la tecnología como ejes para impulsar la economía plural, la erradicación de la extrema pobreza y la universalización de los servicios básicos; aspecto refrendado con la incorporación de la política de Soberanía Científica y Tecnológica con Identidad Propia, en el punto cuarto de la Agenda Patriótica del Bicentenario 2025, Ley N° 650 de 19 de enero de 2015; en cuya observancia se ha puesto en vigencia normativa que involucra el uso de las Tecnologías de Información y Comunicación y por consiguiente el tratamiento de datos personales.

Es así que el Estado Plurinacional de Bolivia, a través de sus instancias competentes, viene ejecutando distintas iniciativas, traducidas en políticas, planes, leyes, decretos supremos y reglamentos. Entre estos, destacan la ciudadanía digital y el gobierno electrónico, la primera conocida también como e-ciudadanía o ciberciudadanía, referida al uso de las TIC, para propiciar la participación ciudadana en asuntos políticos, culturales y sociales del Estado, a través de entornos e interfaces de índole digital o electrónico, por medio de Internet y redes sociales. El segundo, entendido como la administración del Estado ejercida mediante las Tecnologías de Información y Comunicación, para desburocratizar y optimizar sus relaciones con los ciudadanos, mejorando los servicios y simplificando los trámites.

Estas operaciones incluyen la adopción de medidas de interoperabilidad, cuya implementación y desarrollo se encuentran a cargo de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación, entidad que también es responsable de la emisión de credenciales para el ejercicio de la ciudadanía digital, habiéndose habilitado a 23.714 ciudadanos (Gobierno del Estado Plurinacional de Bolivia, 2019), cifra que tiende a incrementarse con el transcurso del tiempo.

Como resultado de lo anterior, es cada vez más creciente el número de operaciones realizadas por entidades gubernamentales que incorporan las TIC en su habitual quehacer para la prestación de servicios y concreción de actividades en el marco de sus atribuciones, permitiendo la interacción de los individuos con los órganos estatales por medios digitales, medidas que en su conjunto tienen como fin mejorar la transparencia, eficiencia, eficacia y el acceso a la información.

Por los anteriores fundamentos, los trámites que se materializan a través del entorno virtual tienden a incrementarse, vislumbrándose similar escenario respecto a las instituciones privadas. En correspondencia, es mayor el número de personas que hacen uso de la red Internet, dispositivos digitales y tecnológicos y la cantidad de información y datos personales que circula se multiplica aceleradamente, incluidos los datos personales de niños y adolescentes, que constituyen una población altamente vulnerable; factores que en su conjunto han llevado a la sociedad boliviana a formar parte de la “aldea global” de la Sociedad de la Información. Los usuarios de las herramientas digitales ceden sus datos de carácter personal para fines específicos, ignorando el posterior uso de los mismos. Estos datos manejados de forma responsable son un instrumento útil para facilitar actos cotidianos; empero, empleados equivocadamente pueden convertirse en una fuente de discriminación y coacción de la autonomía del individuo, llegando a confluir en ilícitos.

En este creciente escenario, el tratamiento de datos personales, entendidos como todo dato relativo a una persona que la identifica o la hace identificable, adquiere capital importancia ya que constituyen el reflejo mismo del individuo, y si bien desde tiempos inmemoriales se recopilan estos datos; con la incursión de las TIC su acopio alcanza niveles exorbitantes, suscitando recurrentes vulneraciones en el Estado Plurinacional de Bolivia con perjuicio para los titulares de los datos personales que se traducen en detrimentos a nivel psicológico y económico llegando a afectar el entorno familiar, laboral y social.

La efectiva protección de datos personales, conforma el núcleo del derecho fundamental de autodeterminación informativa, intrínsicamente vinculado a la dignidad humana, incluido por la doctrina en la tercera generación de derechos humanos producto del avance y evolución de la sociedad, en virtud a lo cual los derechos adquieren nuevos matices en respuesta a las necesidades de los individuos propias de la denominada era tecnológica.

En dicho contexto, la propuesta destaca la relevancia actual que tienen la información y el dato en la sociedad boliviana, por su estrecha relación con el derecho de autodeterminación informativa que salvaguarda los datos personales, los cuales actualmente carecen de medios

idóneos para su tutela penal, emergiendo de ello una necesidad, como corolario de la influencia de las TIC en la actividad estatal y privada.

- **Fundamento jurídico**

Los países europeos y latinoamericanos ya desde hace más de una década han sancionado leyes sobre la materia e incorporado en sus respectivos ordenamientos jurídicos, tipos penales para la tutela de los datos personales, siendo al presente Bolivia, un estado carente de esta normativa, necesaria en la era del Big Data y la inteligencia artificial.

El estudio ha puesto de manifiesto la ausencia de tipos penales de protección de los datos personales y la insuficiencia de los tipos penales tradicionales existentes frente a la criminalidad que atenta contra la información personal, con implicancias negativas que se traducen en limitantes del eficaz ejercicio del derecho de autodeterminación informativa, en un escenario en el cual, el derecho penal producto de la evolución tecnológica se ve en la necesidad de ampliar su tutela en beneficio de la sociedad, en un proceso de adaptación jurídica en torno a la realidad imperante.

Las condiciones actuales ameritan un giro que permita al país hacer frente a la salvaguarda de derechos en la Era Digital, y, en razón de que los datos personales se vinculan a la dignidad misma y otros derechos fundamentales del individuo, constituye obligación del Estado su óptimo resguardo. Es así que, al proponer la incorporación al Código Penal de tipos penales para la salvaguarda de los datos personales, se identifican tres aspectos:

1. La insuficiencia de los tipos penales tradicionales para la protección de los datos personales, datos personales sensibles y datos personales de menores de edad.
2. La ausencia de tipos penales de protección de datos personales, datos personales sensibles y datos personales de menores de edad.
3. La necesidad de incorporar tipos penales de protección de datos personales, datos personales sensibles y datos personales de menores de edad, en mérito a la incursión de las TIC y su uso generalizado, así como a causa de las vulneraciones recurrentes suscitadas en la realidad boliviana a las cuales los mecanismos legales vigentes no han dado respuesta efectiva, situación que no sólo incide en la transgresión del derecho de autodeterminación informativa sino en otros vinculados e inherentes.

Con la inclusión de los tipos penales citados precedentemente en la actual norma sustantiva penal, se efectivizará la persecución y sanción de conductas que quebranten la información personal no quedando impunes las mismas.

- **Fundamento económico**

La información y los datos han adquirido connotaciones de valor económico, primordialmente gracias a las TIC y su irrupción omnipresente en diversos segmentos de la vida cotidiana, acelerando el fenómeno de la globalización, comercio electrónico y gobierno electrónico.

Actualmente, constituyen un activo fundamental en los procesos de negocios estatales y sobre todo empresariales, en torno a las actividades de promoción, comercialización de productos y servicios, así como mejora en el relacionamiento con los clientes. El comercio electrónico es considerado como el motor de la economía del Siglo XXI, ligado a la red Internet y a la información. Los motores de búsqueda, las redes sociales digitales, el marketing y los negocios viven o dependen de los datos y en particular de aquellos de carácter personal.

En ese marco, las conductas que atentan contra los datos personales, pueden dar lugar a diversos delitos como amenazas, coacciones y acoso, por ejemplo cuando se intimida con revelar públicamente hechos de la vida privada o que perjudiquen el honor, solicitando a cambio pagos de sumas de dinero. En otros casos, se vinculan a estafas a través de obtener fraudulentamente de los usuarios sus datos personales, como cuentas bancarias, números de tarjetas de crédito, datos de identificación, claves o contraseñas, para usarlos en la concreción de transferencias, compras o solicitud de créditos.

Estos datos pueden ser obtenidos por SMS, llamadas telefónicas, ventanas emergentes, recepción de correos electrónicos, entre algunas de las formas más usuales. También se suscitan casos de robo de identidad o suplantación, cuando se obtiene información personal y se la utiliza para fraudes o delitos. Asimismo, puede efectuarse sin autorización el borrado, daño, deterioro, alteración o supresión de datos que suponen un menoscabo de material informático avaluable económicamente, teniendo en cuenta su vinculación con las actividades empresariales y la pérdida de productividad. En este escenario, se reportan a nivel global millonarias pérdidas económicas por ataques perpetrados a sistemas informáticos; en consecuencia, este tipo de ilícitos generan un impacto monetario de suma consideración.

5.8 Resultados del trabajo de campo

Los resultados del trabajo de campo presentados y analizados con mayor profundidad en el Capítulo III, constituyen otro pilar que determina la factibilidad de la presente propuesta, toda vez que de la aplicación de los instrumentos de la encuesta, entrevista y el estudio de caso, se estableció que la sociedad boliviana, se desenvuelve en un contexto influenciado por las Tecnologías de Información y Comunicación, dentro del cual opera un considerable flujo de datos, en un entorno en el que campea la inseguridad respecto a la recopilación y uso que de los datos personales hacen las entidades públicas, privadas y hasta personas particulares.

Así también el estudio identificó la falta de regulación normativa en materia penal para satisfacer las necesidades crecientes de tutela de los datos personales, razón por la cual usualmente el universo litigante aplica figuras penales tradicionales, tratando de subsumir en éstas, las vulneraciones del citado bien jurídico.

Por su parte, los expertos entrevistados expresaron argumentos coincidentes que aportaron con profundidad al tema de investigación, reseñando factores que inciden en el estado de desprotección de los datos personales en Bolivia, y ratificando el gran influjo de las TIC en el acopio y tratamiento de los mismos. A su vez, esgrimieron criterios en torno a la necesidad de implementar nuevos tipos penales para la protección de datos personales, datos personales sensibles y datos personales de menores de edad, así como los elementos que deberían contener las figuras cuya creación se propone. En suma, los entrevistados coincidieron en que es oportuna la creación de tipos penales para la tutela del derecho de autodeterminación informativa.

Concluyentemente se arribó a un resultado que permite inferir la pertinencia de la incorporación de tipos penales de protección de datos personales, datos personales sensibles y datos personales de menores de edad en el Código Penal del Estado Plurinacional de Bolivia.

5.9 Descripción de la propuesta

El proyecto de ley, se encauza a la incorporación de tipos penales para la protección de datos personales en el Código Penal. En este sentido se propone la creación de dos tipos penales, el primero orientado a la tutela de cualquier género de dato personal y el segundo a los datos sensibles y de menores de edad, tal como se describe a continuación:

Tabla N° 21

Operacionalización de la propuesta – incorporación del tipo penal de protección de datos personales

VARIABLE	DIMENSIONES	CARACTERÍSTICAS	SUSTENTO TEÓRICO/ METODOLÓGICO
Tipo penal para la protección de datos personales	Nombre jurídico	Procesamiento indebido de datos personales	Legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Conducta de acción	Obtener, acceder, utilizar, alterar o tratar	Legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Sujetos en la tipicidad	Activo: Cualquier persona, servidor público, responsable o encargado del procesamiento Pasivo: Titular de los datos personales o un tercero	Marco teórico, legislación comparada, y resultados de la encuesta, entrevista y estudio de caso
	Objeto material	Datos personales, contenidos en bases de datos públicas o privadas de cualquier naturaleza o en dispositivos informáticos, digitales, electrónicos o tecnologías de información y comunicación	Marco teórico, legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Bien Jurídico	Información y datos	Marco teórico, legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Circunstancias jurídicas	-Sin autorización -Fines ilícitos -Ocasionar perjuicio	Legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Sanción	-Reclusión de dos a cuatro años -Reclusión de cuatro a ocho años (agravante)	Legislación comparada
	Agravante	-Servidor público, responsable o encargado del tratamiento	Legislación comparada
	Ubicación en el Código Penal	Capítulo XI Delitos informáticos Artículo 363 quater	Legislación comparada

Fuente: elaboración propia (2020)

Tabla N° 22

Operacionalización de la propuesta – incorporación del tipo penal de protección de datos personales sensibles y de menores de edad

VARIABLE	DIMENSIONES	CARACTERÍSTICAS	SUSTENTO TEÓRICO/ METODOLÓGICO
Tipo penal para la protección de datos personales sensibles y de menores de edad	Nombre jurídico	Revelación de datos personales sensibles y de menores de edad	Legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Conducta de acción	Acceder, utilizar, revelar, difundir o tratar	Legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Sujetos en la tipicidad	Activo: Cualquier persona, servidor público, responsable o encargado del procesamiento Pasivo: Titular de los datos personales sensibles y menores de edad	Marco teórico, legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Objeto material	Datos personales sensibles Datos personales de menores de edad	Marco teórico, legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Bien jurídico	Información y datos	Marco teórico, legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Circunstancias jurídicas	-Sin autorización -Fines ilícitos -Ocasionar perjuicio	Legislación comparada, resultados de la encuesta, entrevista y estudio de caso
	Sanción	-Reclusión de tres a cinco años -Reclusión de cuatro a ocho años (agravante)	Legislación comparada
	Agravante	-Uso de medios o dispositivos informáticos digitales, electrónicos, red Internet o TIC -Con el fin de obtener beneficio económico, la sanción de agravará en un tercio -Servidor público, responsable o encargado del tratamiento	Legislación comparada
	Ubicación en el Código Penal	Capítulo XI Delitos informáticos Artículos 363 quinquies	Legislación comparada

Fuente: elaboración propia (2020)

Cabe señalar que la protección penal no se limita a los datos registrados en bases, ficheros o dispositivos informáticos, electrónicos, telemáticos o digitales, sino que, se extiende la tutela

de los mismos a aquellos que se hallen contenidos en cualquier tipo de archivo o registro público y privado o que curse en poder de personas particulares, incluso si su procedimiento de recopilación y tratamiento es en soportes convencionales o tradicionales.

5.10 Relevancia jurídica de la propuesta

La identificación de la ausencia de tipos penales de protección de los datos personales adquiere relevancia en el ámbito jurídico, en función a que la finalidad a la que se circunscribe el proyecto de Ley, es la optimización de la autodeterminación informativa o protección de datos personales como derecho humano y fundamental, desde la perspectiva del derecho penal, lo cual, a la vez, incidirá positivamente en la defensa y amparo de otros derechos y bienes jurídicos vinculados.

Aunque es evidente el camino que resta aún por transitar hasta lograr un reconocimiento internacional, la incorporación de los tipos penales que se propone, impulsarán una efectiva tutela penal del derecho a la protección de datos personales, en el Estado Plurinacional de Bolivia, permitiendo su persecución penal y la imposición de sanciones en los casos que correspondan, radicando en este factor su relevancia jurídica.

5.11 Desarrollo de la propuesta

Para el desarrollo de la propuesta, se tomaron en cuenta las siguientes etapas:

- Etapa I: Identificación del problema jurídico
- Etapa II: Desarrollo del marco metodológico
- Etapa III: Desarrollo del marco teórico
- Etapa IV: Validación y aplicación de instrumentos
- Etapa V: Presentación y análisis de datos
- Etapa VI: Elaboración del proyecto

5.12 Presentación de la propuesta

EXPOSICIÓN DE MOTIVOS

OBJETO

La protección de los datos personales, como tema de actualidad a nivel global, cobra importancia al encontrarse vinculado al ejercicio del derecho a la autodeterminación

informativa como facultad del individuo para controlar su información personal, es decir, el ejercicio del poder de disposición para decidir los datos que proporciona a entidades públicas, privadas e individuos particulares; conocer quiénes o qué instancias los poseen y para qué, pudiendo oponerse a esa posesión o uso; denominado también derecho a la protección de datos personales, es un derecho humano, fundamental y autónomo, distinto de los derechos a la privacidad e intimidad, con los que, si bien puede guardar cercanía en algunas facetas, tiene sus propias particularidades y características.

La penetración rápida de las Tecnologías de Información y Comunicación, va en incremento; en consecuencia, es difícil imaginar actividades que no se encuentren ligadas a las mismas.

En este escenario la información y los datos son considerados como el petróleo del Siglo XXI para la economía digital, materia prima e insumo, fuerza económica y geopolítica del nuevo milenio. Como secuela de lo anterior, la interceptación masiva de datos refleja apenas una vaga idea del ámbito actual en el que la sociedad se desenvuelve, la ciberdelincuencia crece de forma exponencial, dado que las herramientas y modalidades para delinquir están cada vez más interrelacionadas con las comunicaciones y transacciones personales, profesionales, financieras, gubernamentales y comerciales. El robo de datos, su recolección y venta, aunado a los progresos en hardware y avances en software, son algunos ejemplos que utilizan los criminales desafiando la norma penal y la administración de justicia.

Las habilidades otrora consideradas como avanzadas y altamente especializadas para fungir como hacker hoy en día ya no lo son, y pueden ser realizadas por individuos que dispongan de un cierto nivel de conocimientos y sobre todo de tiempo.

Es por ello que los ciberdelitos abarcan un amplio espectro de actividades criminales relacionadas con datos e información personal que atentan contra la confidencialidad e integridad de los mismos, con ostensibles repercusiones negativas para el ámbito económico y social, como la pérdida de control sobre los datos, restricción de derechos, discriminación, usurpación de identidad, pérdidas financieras, pérdida de confidencialidad de datos sujetos a secreto profesional, daños a la reputación, la intimidad y la privacidad, entre otros. Esta problemática social amerita ser abordada y encarada desde varios aspectos, y en los casos más lesivos le atañe al derecho penal, a través de definir las conductas delictivas para su inclusión en la Ley penal.

El Estado Plurinacional de Bolivia no es ajeno a estos avances tecnológicos, cuya incursión es verificable tanto en la actividad estatal como privada, aspecto ostensible en la

implementación de políticas, planes y la emisión de normativa referente al advenimiento de la ciudadanía digital y el gobierno electrónico, que tienen como corolario el flujo de información incuantificable. Como resultado de lo anterior, a diario se vulneran derechos vinculados a la autodeterminación informativa, que incluyen menoscabos de datos personales sensibles y de menores de edad, con nefastas consecuencias morales y económicas para sus titulares, resultando insuficiente la salvaguarda de los mecanismos legales existentes ya sea por la vía civil, administrativa o constitucional, quedando vedada la posibilidad de su persecución penal en los casos más ofensivos, puesto que no existen figuras en la norma vigente en las cuales con especificidad se subsuman estas conductas, debiendo las autoridades y el universo de litigantes adecuarlas a otros tipos penales previstos.

En ese contexto, se identifica la necesidad de configurar una herramienta de tutela específica para los datos personales en el ámbito penal, como acontece en otros países del orbe.

Por los fundamentos vertidos, el presente proyecto, tiene como objetivo proponer la incorporación de tipos penales de protección de datos personales, datos personales sensibles y datos personales de menores de edad, llenando un vacío legal, con el fin de optimizar la tutela del derecho de autodeterminación informativa.

ANTECEDENTES

El Estado Plurinacional de Bolivia en cumplimiento del mandato contenido en el Artículo 103 parágrafo II de la Constitución Política del Estado, asumió como política la implementación de estrategias para incorporar el conocimiento y la aplicación de nuevas Tecnologías de Información y Comunicación.

En observancia de dicho precepto, la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación N° 164 de 8 de agosto de 2011, fue sancionada con el objeto de establecer el régimen general de telecomunicaciones, tecnologías de información y comunicación, del servicio postal y el sistema de regulación. De similar manera, los Reglamentos a la citada Ley, aprobados por Decretos Supremos Nrs. 1391 de 24 de octubre de 2012 y 1793 de 13 de noviembre de 2013, respectivamente, regulan lo relacionado a la implementación del régimen de servicio de telecomunicaciones, la certificación digital, gobierno electrónico, software libre, correo electrónico y el uso de documentos digitales y la firma digital en el Estado Plurinacional de Bolivia, desarrollando en sus partes pertinentes normativa de protección a los datos personales.

Por su parte, el punto cuarto de la Agenda Patriótica del Bicentenario 2025, Ley N° 650 de 19 de enero de 2015; incorpora la política de Soberanía Científica y Tecnológica con Identidad Propia, como pilar a ser desarrollado por el Estado para alcanzar la meta de una Bolivia libre y soberana.

El Decreto Supremo N°3251 de 12 de julio de 2017 aprueba el Plan de implementación de Gobierno Electrónico y el Plan de implementación de Software Libre y Estándares Abiertos, conforme a su Artículo 4 faculta a las entidades públicas a compartir información a través de mecanismos de interoperabilidad y de acuerdo a determinaciones emanadas del Comité Plurinacional de Tecnologías de Información y Comunicación (COPLUTIC), en coordinación con la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), en el marco de las normas vigentes y disposiciones específicas de los sectores estratégicos.

También faculta al COPLUTIC, para solicitar a las entidades públicas la habilitación de acceso a información a través de la AGETIC y la suscripción de convenios de interoperabilidad entre entes públicos, para garantizar el intercambio de datos.

El Decreto Supremo N°3525 de 4 de abril de 2018, establece la Política de Atención a la Ciudadanía: Bolivia a tu servicio y el Portal de trámites del Estado; regula el archivo digital, la interoperabilidad y la tramitación digital; de acuerdo a su Artículo 2 su ámbito de aplicación comprende las entidades públicas y privadas que presten servicios públicos delegados por el Estado, las entidades territoriales autónomas y otras entidades públicas, con el propósito de brindar mayor transparencia y fluidez en la interacción entre los administrados y el sector público, la transferencia de información entre entidades del Estado y entre estas con la población, para promover la celeridad de los trámites administrativos. Esta normativa en su Artículo 12, dispone que los entes públicos prioricen el uso de las Tecnologías de Información y Comunicación en los trámites a su cargo y enfatiza la figura de la interoperabilidad de datos entre entes públicos.

La Ley de Ciudadanía Digital N°1080 de 11 de julio de 2018, regula las condiciones, responsabilidades, acceso y ejercicio de la ciudadanía digital en las entidades públicas y privadas que presten servicios públicos delegados por el Estado, determinando en su Artículo 5 que los bolivianos y extranjeros residentes en territorio nacional mayores de 18 años de edad y también los menores conforme a la capacidad que les reconoce el ordenamiento jurídico, deben registrarse ante las entidades responsables y obtener credenciales de ciudadanía digital. El mismo Artículo en su parágrafo II delega a la AGETIC, el desarrollo de

lineamientos técnicos de registro para acceder a la ciudadanía digital, y en su parágrafo III, faculta a los entes públicos y privados que presten servicios públicos a compartir los datos que conozcan a través de mecanismos de interoperabilidad. Al presente, ya se encuentra en plena vigencia la ciudadanía digital, habiéndose expedido las respectivas credenciales que habilitan a su ejercicio a un determinado número de ciudadanos, avanzándose paulatinamente en este proceso.

Como consecuencia de la normativa citada, se han incrementado los avances en materia de soportes digitales y la difusión de tecnología, masificándose la creación de bases de datos de carácter personal de diversa naturaleza y características, y se ha multiplicado la utilización de dispositivos tecnológicos y digitales por parte de la ciudadanía en general, factores que develan un exponencial e inminente intercambio de datos personales que opera entre los entes estatales, privados y personas particulares y que incluye los datos personales de menores de edad. Si bien al Estado Plurinacional de Bolivia aún le resta camino por transitar en el ámbito del desarrollo tecnológico en contraste con los países de la región, el escenario legal descrito posibilita una mayor recolección de datos personales e información de los bolivianos y su tratamiento, siendo así que en lo fáctico se han suscitado un sinnúmero de casos que atentaron contra datos personales, datos personales sensibles y datos personales de menores de edad y que a través de su utilización ilícita acarrearon nefastas consecuencias para sus titulares, quedando muchos en la impunidad.

Frente a ello, en un orden con tendencia creciente al uso generalizado de las Tecnologías de Información y Comunicación, emerge como necesario el derecho fundamental y autónomo de autodeterminación informativa, estrechamente asociado a la evolución tecnológica y que permite al ciudadano el control de su información personal, evidenciándose la ausencia de tipos penales en el Código Penal y la insuficiencia de los tipos penales tradicionales existentes y en particular de aquellos descritos en los Artículos 363 bis y 363 ter, como mecanismos de salvaguarda que en los casos más graves, operen como instrumentos para viabilizar o en su caso restituir a los individuos el control sobre su información personal e imponer a los infractores las consiguientes sanciones, en un escenario de avances tecnológicos que ameritan una vanguardista legislación penal, que no puede prescindir de los principios de legalidad, taxatividad y prohibición de analogía, aplicables a dicha esfera del derecho.

MARCO CONSTITUCIONAL Y NORMATIVO

La incorporación de artículos referidos a tipos penales que sancionen conductas que atenten contra la información y los datos personales, tiene asidero en normativa e instrumentos a continuación descritos:

- **Constitución Política del Estado**

La Constitución Política del Estado, en su Artículo 8 asume como principio ético moral el suma qamaña (vivir bien) como un estado de equidad entre las personas y la comunidad, así también instituye los valores de dignidad, igualdad, libertad, respeto y responsabilidad, orientados a forjar una sociedad de bienestar y equilibrio, basada en el desarrollo y reconocimiento de los derechos fundamentales, como cimiento articulador de los ámbitos político, social y jurídico del Estado.

La Norma Fundamental, en su Artículo 9 numerales 1, 2 y 4 adopta como fines y funciones esenciales del Estado, constituir una sociedad justa y armoniosa, con plena justicia social, garantizando el bienestar, el desarrollo, la seguridad y la protección e igual dignidad de las personas, naciones, pueblos y comunidades, fomentando el respeto mutuo y el cumplimiento de los principios, valores, derechos y deberes reconocidos en la misma.

Por su parte, los Artículos 60 y 61 de la Norma Suprema determinan como deber del Estado, la sociedad y la familia el garantizar el interés superior los niños y adolescentes, aspecto que involucra la preeminencia de sus derechos, la primacía en recibir protección y socorro en cualquier circunstancia, el acceso a una administración de justicia pronta, oportuna y con asistencia de personal especializado, prohibiendo y sancionando toda forma de violencia contra este sector vulnerable.

A su turno, el Artículo 21 numeral 2 de la Constitución, consagra como derechos civiles de los bolivianos: “(…) la privacidad, intimidad, honra, honor, propia imagen y dignidad”, en tanto que en su Artículo 130 parágrafo I, establece:

> Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

En ese contexto, el derecho de autodeterminación informativa o derecho a la protección de datos personales, es considerado por la doctrina y legislación comparada como un derecho humano, fundamental y de carácter autónomo. En Bolivia ha sido reconocido en dicho sentido por la jurisprudencia constitucional (SC N° 0127/2010-R de 10 de mayo de 2010, SCP Nrs. 2175/2012 de 8 de noviembre de 2012 y 0080/2014-S2 de 4 de noviembre de 2014, entre otras) y entendido como:

> (…) el derecho que tiene la persona de acceder a los bancos de datos públicos y privados con el fin de tener conocimiento de cuanta información se ha almacenado, hacia donde fluyó la información o datos de la misma y para que fines, por lo que, sin una autorización expresa, tan solo el titular de ese derecho tiene la potestad de disponer la información concerniente a sus datos de carácter personal, de preservar la propia identidad informática, o lo que es igual, de consentir, controlar, o incluso el de rectificar los datos informáticos de carácter personal. (SCP N°0819/2015-S3 de 10 de agosto de 2015)

En consecuencia, el núcleo de este derecho se encuentra contenido en el Artículo 130 de la Constitución Política del Estado, siendo aplicable por imperio del Artículo 13 de la misma, en un entorno en que las Tecnologías de Información y Comunicación han incursionado profusamente en la actividad pública y privada, ameritando este extremo la tutela especializada de la información y los datos. Su óptimo resguardo, en la vía penal a través de la incorporación de tipos penales para la defensa de la información y los datos, como deber del Estado constitucional y democrático, coadyuvará a la protección y ejercicio de derechos conexos como la privacidad, intimidad, honra, honor, propia imagen, dignidad, a no ser discriminado, integridad física, psicológica y sexual, salud, autoidentificación cultural, espiritualidad, religión y culto, acceder a la información, petición, secreto de las comunicaciones privadas, derechos de la niñez y adolescencia, así como otros vinculados, a su vez bienes jurídicos como el honor, la propiedad, la fe pública, la libertad sexual, la vida y la integridad corporal, serán reforzados en su tutela, aspectos que en su conjunto contribuirán a optimizar el derecho a la autodeterminación informativa y alcanzar los fines, funciones, principios y valores del Estado.

- **Declaración Universal de Derechos Humanos, Pacto Internacional de Derechos Civiles y Políticos, Convención Americana sobre Derechos Humanos y Convención sobre los Derechos del Niño**

La Declaración Universal de Derechos Humanos, confiere a la privacidad el reconocimiento de derecho humano fundamental, expresando en su Artículo 12, que: “Nadie será objeto de injerencias arbitrarias en su vida privada su familia su domicilio o su correspondencia, ni de

ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

El Pacto Internacional de Derechos Civiles y Políticos (ratificado por Ley Nº2119 promulgada el 11 de septiembre de 2000) en su Artículo 17 numerales 1 y 2, protege al individuo de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, asimismo de ataques a su honra o reputación, incluyendo el derecho a la protección de la Ley contra esos ataques; disposición concordante con el Artículo 11 numerales 1, 2 y 3 de la Convención Americana sobre Derechos Humanos (ratificada por Ley Nº1430 promulgada el 11 de febrero de 1993), que además añade: "Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad".

A su vez, la Convención sobre los derechos del niño ratificada por Bolivia mediante Ley N°1152 de 14 de mayo de 1990; determina en su Artículo 16 numerales 1 y 2 que ningún menor será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación, gozando del derecho a la protección de la ley contra dichas injerencias o ataques.

Estos instrumentos establecen que son los Estados quienes a través de las medidas pertinentes incluidas aquellas de carácter legislativo, deben hacer efectivos los derechos y libertades en ellos reconocidos y conforman un marco legal internacional para la defensa del derecho de autodeterminación informativa, desde la perspectiva de los derechos a la dignidad, privacidad, honra y reputación.

- **Instrumentos y estándares internacionales**

También existen otros instrumentos que constituyen referentes y guías para el establecimiento de la tutela penal de la información y los datos personales, estos son:

- ✓ Directrices de la Organización para la Cooperación y el Desarrollo Económicos – OCDE (1980) sobre protección de la privacidad y flujos transfronterizos de datos personales, en su Cuarta Parte, promueve la protección de la privacidad y las libertades individuales en relación con los datos personales a través de la aprobación de legislación nacional adecuada; procurando las oportunas sanciones y soluciones en caso de incumplimiento.
- ✓ Convenio N°108 del Consejo de Europa (1981), garantiza el respeto de derechos y libertades fundamentales, en relación al tratamiento automatizado de datos de carácter

personal. Determina en sus Artículos 6, 10 y 11, la protección de datos sensibles, el establecimiento de sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno y que cada Parte, puede conceder una protección más amplia que la prevista en el Convenio.

- ✓ Principios Rectores para la Reglamentación de los Ficheros Computarizados de datos personales adoptados mediante Resolución N°45/95 de la Asamblea General de la Organización de Naciones Unidas – ONU (1990), establece principios relativos a las garantías mínimas que deben contener las legislaciones nacionales en materia de datos personales, destaca los principios de legalidad, seguridad y de no discriminación que incoan a no registrar datos sensibles. En caso de violación de las disposiciones de la legislación interna, determina que se prevean sanciones penales y de otro tipo. Los principios son aplicables también a ficheros manuales (numerales 1, 5, 7 y 8).
- ✓ Convenio sobre la Ciberdelincuencia del Consejo de Europa (2001), más conocido como Convenio de Budapest, exige a las partes que actualicen y armonicen sus legislaciones penales contra la piratería y otras infracciones de la seguridad incluidas las infracciones de los derechos de autor, fraudes informáticos, pornografía infantil y otras ciberactividades ilícitas. En sus Artículos 2 (Acceso ilícito), 3 (Interceptación ilícita), 4 (Ataques a la integridad de los datos) y 5 (Ataques a la integridad del sistema), tipifica conductas que atentan contra la seguridad e integridad de la información y sistemas informáticos.
- ✓ Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico – APEC (2004), incoa a la adopción de medidas legislativas y de seguridad para prevenir daños por el mal uso de la información personal y por su recolección ilegal, y prevé que los remedios para violaciones a la privacidad deben ser proporcionales a la probabilidad, severidad de cualquier daño y sensibilidad de la información (numerales 22, 31 y 38).
- ✓ Agenda de Túnez para la Sociedad de la Información, de la Organización de Naciones Unidas - Unión Internacional de Telecomunicaciones (2005), insta a enjuiciar la ciberdelincuencia, destacando la necesidad de concebir para ello instrumentos eficaces y eficientes, exhortando a garantizar la protección de la información, privacidad y datos personales, mediante la adopción de medidas legislativas pertinentes (apartados 40 y 46).
- ✓ Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Resolución de Madrid adoptada por la Conferencia Internacional de Autoridades de Privacidad y de Protección de Datos (2009), impulsa la promoción de medidas adecuadas para facilitar el acceso de los interesados a los correspondientes procesos judiciales o administrativos, para la obtención de la reparación de los daños y/o perjuicios. Incluye la protección de datos sensibles y el establecimiento de

responsabilidad por daños y perjuicios morales y materiales, como consecuencia de la vulneración de normativa de protección de datos, sin perjuicio de las sanciones penales, civiles o administrativas previstas (apartados 13 y 25).

- ✓ Resolución N° A/RES/68/167 “El derecho a la privacidad en la era digital” de la Asamblea General de Naciones Unidas (2013). Posteriormente actualizada el 2016, mediante Resolución A/C.3/71/L.39 de la Organización de Naciones Unidas (ONU), pone en relieve la recopilación ilícita o arbitraria de datos personales como un acto de intrusión grave, que viola el derecho a la privacidad. Exhorta a los estados a examinar sus procedimientos, prácticas y legislación con miras a afianzar el derecho a la privacidad, su respeto y protección a través de medidas para poner fin a las violaciones, cerciorándose que la legislación nacional se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos (numeral 4). La actualización del 2016, promueve la instauración de una legislación adecuada, con sanciones y recursos eficaces que protejan a las personas contra las prácticas que atentan contra el derecho a la privacidad, la recopilación y el tratamiento ilegales y arbitrarios, retención o el uso de datos personales por particulares, empresas y organizaciones privadas (numeral 5 inciso f).
- ✓ Principios sobre la privacidad y la protección de datos personales, emitidos por la Organización de Estados Americanos – OEA (2015), enuncia principios a ser incluidos en las legislaciones de los estados, entre estos, el principio de protección y seguridad, y el de responsabilidad a efecto de evitar daños a las personas por accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación de sus datos personales, así como la protección de datos sensibles. Asimismo, refiere la incidencia creciente de intrusiones externas (“violaciones de los datos personales”), las cuales suscitan preocupaciones relacionadas con el ámbito penal, por lo que incoa a imponer a los controladores de datos, sanciones que sean proporcionales al grado del perjuicio o riesgo y su indemnización (Principios Seis: protección y seguridad, Nueve: datos personales sensibles y Diez: responsabilidad).
- ✓ Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos Personales (2017), formula directrices, principios y derechos para la protección de datos personales, a desarrollarse en la normativa de los países iberoamericanos, que incluyan procedimientos de reclamación ante la autoridad de control, recurrir a la tutela judicial para hacer efectivos los derechos y, el establecimiento de un régimen de medidas correctivas, sanciones y reparación de daños y perjuicios (numerales 43 y 44).También le asigna particular protección a los derechos de los menores de edad (numerales 8, 11.1 inciso i, 13 y 16.3).

- ✓ Reglamento (UE) N°2016/679, Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, emitido por el Parlamento Europeo y el Consejo de Europa, de 27 de abril de 2016, más conocido como Reglamento General de Protección de Datos (RGPD), que por sus disposiciones vanguardistas, medidas y sanciones estrictas, ha logrado reconocimiento internacional, además de su aplicación extraterritorial, ejerciendo influencia en varias legislaciones alrededor del mundo, al considerarse el estándar más alto en lo que respecta al tratamiento y protección de datos personales. Esta normativa comunitaria europea, en sus Considerandos 149 y 152, establece que los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales para el caso de infracciones graves y aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. Así también en sus Considerandos 38, 58, 75; Artículos 6 numeral 1 inciso f), 8 y 12 numeral 1, le otorga especial atención al resguardo de los datos personales de los menores de edad.

Por último, señalar que es viable la iniciativa legislativa ciudadana, para la presentación del presente proyecto de ley, al amparo de los Artículos 162 parágrafo I numeral 1 y 163 numeral 2 de la Constitución Política del Estado, concordantes con los Artículos 116 inciso a) y 117 del Reglamento General de la Cámara de Diputados.

PRINCIPIOS EN LOS QUE SE SUTENTA EL PROYECTO

La incorporación de tipos penales para tutelar la información y los datos personales, se sustenta en los siguientes principios y valores supremos de orden constitucional, insertos en el Artículo 8 parágrafos I y II de la Constitución Política del Estado: suma qamaña (vivir bien), dignidad, igualdad, libertad, respeto y responsabilidad. En ese entender, el Estado Plurinacional de Bolivia, está constituido sobre la base del respeto mutuo e igualdad entre sus habitantes, teniendo a la dignidad como fundamento para la protección de los derechos.

En función a la responsabilidad que le compete al Estado, a través de la incorporación de nuevos tipos penales en el Código Penal, se efectivizará la persecución y si corresponde, la imposición de sanciones a aquellas conductas que atenten contra la información y los datos personales; en consecuencia, al no quedar estas impunes, se coadyuvará a la construcción de una sociedad armónica que garantice la vigencia de los derechos y el alcance del suma qamaña o vivir bien, como un estado de equilibrio al interior de la colectividad.

Los principios de licitud, consentimiento, calidad, finalidad, seguridad, protección especial y protección de menores de edad, propios del ámbito de la protección de datos personales, incluidos en los numerales 8, 9, 11.1 inciso i), 12,13,16.3, 17, 19 y 21 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 20 de junio de 2017, concordantes con los Artículos 6 numeral 1 inciso f), 7, 8, 9 y 12 numeral 1 del Reglamento (UE) N°2016/679 emitido por el Parlamento Europeo y el Consejo de Europa de 27 de abril de 2016, propenden al establecimiento de un régimen legal de respeto en la recopilación y tratamiento de datos personales, afianzando a los individuos que sus datos no serán utilizados para fines distintos a los que ameritaron su acopio inicial, por lo que en caso de incumplimiento es factible establecer disposiciones penales respecto a las conductas más graves para su salvaguarda; aspecto de mayor consideración en relación a los datos personales sensibles y datos de menores de edad, cuyo tratamiento entraña mayor riesgo de vulneración de derechos y libertades fundamentales.

Bajo ese contexto, toda norma penal debe observar los principios de legalidad, taxatividad, proporcionalidad de las penas y subsidiariedad, en cuyo cumplimiento se describan las conductas prohibidas consideradas como delitos y las sanciones aplicables, sin que pueda forzarse la coincidencia de la conducta con otra similar ya establecida, considerando además la exigencia de proporcionalidad respecto al delito cometido, como búsqueda de la adecuada relación entre la gravedad de la afectación y la importancia del bien jurídico tutelado, reservando la aplicación de la ley penal para aquellos casos más gravosos en los que otros medios jurídicos no han mostrado ser efectivos, factores todos que se erigen en garantías propias del Estado Constitucional de Derecho que a través del derecho penal marca los límites y las reglas del comportamiento de las personas, propendiendo a su mejor convivencia.

En suma, la incorporación de tipos penales que salvaguarden la información y los datos personales, permitirá que estas conductas no queden impunes y en consecuencia operará una optimización de la tutela del derecho de autodeterminación informativa en el Estado Plurinacional de Bolivia.

CONCLUSIÓN

En base a los fundamentos expuestos, se concluye que es viable y necesaria la aprobación del presente proyecto de ley para que sea promulgado con carácter nacional y aplicado en todo el territorio del Estado Plurinacional de Bolivia, con el fin de salvaguardar la información y los datos personales, contribuyendo con ello a optimizar el derecho fundamental de autodeterminación informativa, y como corolario otros derechos vinculados.

PROYECTO DE LEY

LA ASAMBLEA LEGISLATIVA PLURINACIONAL

DECRETA:

LEY DE INCORPORACIÓN DE LOS ARTÍCULOS 363 QUÁTER Y 363 QUINQUIES EN EL CÓDIGO PENAL

ARTÍCULO 1. (OBJETO). La presente ley tiene por objeto disponer la incorporación de los Artículos 363 quater y 363 quinquies, en el Capítulo XI, Delitos informáticos del Código Penal, Ley N° 1768 de 10 de marzo de 1997.

ARTÍCULO 2. (INCORPORACIÓN DE LOS ARTÍCULOS 363 QUÁTER Y 363 QUINQUIES). Incorpórese los Artículos 363 quáter y 363 quinquies, en el Capítulo XI, Delitos informáticos del Código Penal, bajo el siguiente texto:

ARTÍCULO 363 Quáter. (PROCESAMIENTO INDEBIDO DE DATOS PERSONALES). El que sin estar autorizado o con fines ilícitos, obtenga, acceda, utilice, altere o efectúe tratamiento de datos personales contenidos en bases de datos públicas o privadas de cualquier naturaleza o en dispositivos informáticos, digitales, electrónicos u otras tecnologías de la información y comunicación, ocasionando perjuicio al titular de los datos o un tercero será sancionado con reclusión de dos a cuatro años.

ARTICULO 363 Quinquies. (REVELACIÓN DE DATOS PERSONALES SENSIBLES Y DE MENORES DE EDAD).

I. El que sin estar autorizado o con fines ilícitos, acceda, utilice, revele, difunda o efectúe tratamiento de datos personales relativos a la ideología, religión, creencias, salud, origen racial, vida sexual, orientación sexual, biométricos, genéticos, otros datos sensibles o datos de menores de edad, causando perjuicio a su titular, será sancionado con reclusión de tres a cinco años.

II. La sanción se elevará en un tercio cuando los hechos fueren cometidos a través de medios o dispositivos informáticos, digitales, electrónicos, la red internet, otras tecnologías de información y comunicación, o con el fin de obtener un beneficio económico.

III. Si los hechos descritos en los artículos 363 quáter y 363 quinquies, fueran cometidos por servidores públicos, por los responsables o encargados de las bases de datos o archivos respecto a la información a su cargo, la sanción será de reclusión de cuatro a ocho años.

CONCLUSIONES Y RECOMENDACIONES

- **CONCLUSIONES A PARTIR DE LOS OBJETIVOS ESPECIFICOS**

a) Caracterizar los fundamentos teóricos e históricos del derecho a la protección de datos personales.

De la caracterización de las bases teóricas e históricas del derecho a la autodeterminación informativa o protección de datos personales, se infiere que sus orígenes se remontan a Europa, producto de una labor jurisprudencial y doctrinal, vinculado intrínsecamente a las Tecnologías de Información y Comunicación, y consolidado actualmente como un derecho de carácter independiente, autónomo, humano y fundamental, que comprende la facultad de toda persona para disponer y controlar sus datos personales, pudiendo decidir qué datos proporciona a terceros, conocer quién posee estos datos y para qué, así como oponerse a dicha posesión o tratamiento.

En Latinoamérica, emerge como resultado del Habeas Data, respondiendo también su configuración a una construcción jurisprudencial, en un contexto vinculado a las transgresiones a los derechos de la intimidad y privacidad, y de manera secundaria a las TIC, llegando a ser reconocido de igual manera su carácter autónomo y de derecho fundamental.

Al presente, ha adquirido preminencia tal, que ha sido recogido en los textos constitucionales y en leyes penales de diversos países del orbe.

b) Identificar las bases teóricas, doctrinales e instrumentos internacionales, que sustentan la tutela penal de los datos personales.

Es innegable que las Tecnologías de Información y Comunicación, han traído grandes cambios para el desarrollo de la sociedad a nivel personal, estatal y económico, con incontables beneficios para la humanidad; sin embargo, también han abierto nuevas posibilidades y riesgos en torno a derechos fundamentales y libertades de las personas; surgiendo la necesidad de regular y dar respuesta a nuevas cuestiones, intereses y conflictos, poniendo de manifiesto la relación entre el derecho y la tecnología. Es así que ante nuevas conductas que acarrean daños a los derechos de los individuos, el derecho debe mutar para incorporar nuevos tipos penales. Es donde emergen los delitos informáticos y ciberdelitos, con diversas características que los distinguen de los delitos tradicionales, al vincularse a la

tecnología y por su carácter transnacional; tornándose en más difíciles y complejos de combatir. Estos ilícitos entre sus áreas de afectación engloban a los datos personales.

Bajo la aplicación de los principios de legalidad y taxatividad, el delito y la pena deben estar previstos en una Ley como garantía de seguridad jurídica dentro de un Estado Constitucional de Derecho, en virtud de cuya aplicación se señalen los alcances de la norma penal en forma clara, concreta y precisa, principios que la legislación penal debe observar ineludiblemente.

Los instrumentos de carácter internacional como la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y la Convención sobre los derechos del niño, incluyen disposiciones para la protección de datos personales desde la óptica de la salvaguarda de los derechos a la privacidad, la honra, la reputación y la dignidad. Otros instrumentos como las Directrices de la Organización para la Cooperación y el Desarrollo Económicos – OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (1980); el Convenio N°108 del Consejo de Europa relativo al respeto de derechos y libertades fundamentales en relación al tratamiento automatizado de datos de carácter personal (1981); los Principios Rectores para la Reglamentación de los Ficheros Computarizados de datos personales adoptados mediante Resolución N°45/95 de la Asamblea General de la Organización de Naciones Unidas – ONU (1990); el Convenio sobre la Ciberdelincuencia del Consejo de Europa (2001); el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico – APEC (2004); la Agenda de Túnez para la Sociedad de la Información de la Organización de Naciones Unidas y la Unión Internacional de Telecomunicaciones (2005); los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, aprobados mediante la Resolución de Madrid adoptada por la Conferencia Internacional de Autoridades de Privacidad y de Protección de Datos (2009); la Resolución N° A/RES/68/167 “El derecho a la privacidad en la era digital” de la Asamblea General de Naciones Unidas (2013), posteriormente actualizada en 2016, mediante Resolución A/C.3/71/L.39 de la Organización de Naciones Unidas; los Principios sobre la privacidad y la protección de datos personales, emitidos por la Organización de Estados Americanos – OEA (2015); los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de la Red Iberoamericana de Protección de Datos Personales (2017); y así también el Reglamento (UE) N°2016/679, Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, emitido por el Parlamento Europeo y el Consejo de 27 de abril de 2016, contienen disposiciones que a manera de directrices orientan la protección que los Estados deben brindar a la información y datos personales, incluido el establecimiento de sanciones de índole penal.

La protección de datos personales en Bolivia emana de la Constitución Política del Estado, y como obra del Tribunal Constitucional, que ha perfilado su contenido en Sentencias Constitucionales en torno al Recurso de Habeas Data y a la Acción de Protección de Privacidad. Por otra parte, las regulaciones existentes confluyen en una gama de normas que involucran a los datos personales como insumo fundamental de las operaciones del Estado, entes privados y personas particulares, en el contexto de planes y políticas que fomentan el uso de las Tecnologías de Información y Comunicación, vislumbrándose su incidencia en un mayor índice de recopilación, uso, tratamiento y cesión de datos personales en territorio boliviano, que a su vez trasciende fronteras.

Frente a lo señalado, es ostensible la insuficiencia de los tipos penales vigentes y en particular los descritos en los Artículos 363 bis (Manipulación informática) y 363 ter (Alteración, acceso y uso indebido de datos informáticos) del Código Penal, para combatir eficazmente la criminalidad que tiene como objeto los datos personales, los datos personales sensibles y los datos personales de menores de edad, cuya vulneración cada día se traduce en más frecuente y constituye una limitante al ejercicio del derecho a la autodeterminación informativa.

c) Diagnosticar la necesidad de incluir tipos penales orientados a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia.

Los instrumentos de la encuesta, la entrevista y el estudio de caso, develan la actual trascendencia de las Tecnologías de Información y Comunicación en la sociedad boliviana, y su influjo en la comisión de ilícitos vinculados a la información y los datos personales. Así también, producto del Marco Práctico, se corroboró la ausencia en la norma sustantiva penal de figuras que tipifiquen conductas lesivas de estos datos y las limitaciones de los tipos penales existentes, situación que hace patente la necesidad de la inclusión en el Código Penal de estas nuevas formas de criminalidad.

La problemática descrita, requiere de la elaboración de respuestas normativas adecuadas que incluyan la obtención, el acceso, el uso, la cesión, la alteración, la revelación y otros tratamientos ilícitos de datos personales. Los principios de la dogmática penal, entre los que destaca el principio de legalidad representado en el aforismo “Nullum crimen, nulla poena sine praevia lege”, y la prohibición de analogía que proscribe la aplicación extensiva de la norma penal a una conducta analógica a la descrita en el tipo, revelan la imposibilidad de responder con la actual Ley penal a la prevención y sanción de las conductas que lesionen los datos personales, los datos personales sensibles y los datos personales de menores de edad.

d) Comparar la legislación penal de Argentina, Colombia y España en relación a delitos que vulneran los datos personales.

Se efectuó la comparación de la legislación penal de Argentina, Colombia y España, países que desde hace más de una década incluyeron tipos penales específicos para la tutela de los datos personales. En el caso de Argentina su Código Penal incluye regulaciones relativas a la protección de datos personales cuyo secreto se está obligado a preservar por disposición de la Ley, mientras que la norma sustantiva penal de España sistematiza disposiciones orientadas a datos personales de carácter general, datos sensibles y de menores de edad.

Colombia por su parte, también incorporó un tipo penal que tutela datos e información personal.

Las normas penales de los tres países al unísono comprenden sanciones privativas de libertad para este tipo de delitos, así también la pena de inhabilitación para ejercer un cargo público en el caso de Argentina y España, e inhabilitación para el ejercicio de la profesión relacionada con sistemas de información procesada con equipos computacionales en Colombia. Por su parte, España y Colombia imponen además penas de multa. La legislación penal de los países señalados comprende una tutela para datos personales contenidos en cualquier soporte ya sea en medios digitales o informáticos, así como en los medios convencionales o tradicionales, y las conductas que se sancionan se sintetizan básicamente en obtener, acceder, alterar, procesar, revelar, difundir y otros tratamientos que de manera ilícita recaen sobre datos personales causando perjuicio a sus titulares.

Lo descrito, pone de manifiesto la relevancia que se le ha otorgado a la tutela de los datos personales con su incorporación en los Códigos Penales de Argentina, Colombia y España, no solo desde la visión de la protección del derecho a la privacidad, sino también desde la perspectiva del derecho de autodeterminación informativa, considerada como la faceta positiva de la privacidad, aportando en su conjunto al presente estudio, con una visión más concreta respecto a las regulaciones específicas que deben contener los tipos penales para la salvaguarda de los datos personales.

e) Diseñar la propuesta de incorporación de tipos penales referidos a la protección de los datos personales en el Código Penal del Estado Plurinacional de Bolivia.

Respecto a la propuesta, la investigación ha posibilitado sustentar teórica y empíricamente la hipótesis, así como brindar una respuesta al problema formulado, cuyo asidero radica en la

importancia de optimizar la salvaguarda del derecho de autodeterminación informativa a través de la creación de tipos penales de tutela de los datos personales y su incorporación en la norma sustantiva penal boliviana, para responder a las demandas y requerimientos de la sociedad actual, como un deber del Estado, en un escenario en que la protección no alcanza a ser suficiente, al no contemplar figuras penales que tipifiquen y sancionen conductas de esta naturaleza.

En virtud de las deficiencias advertidas y con respaldo emanado de la revisión documental, la aplicación de las técnicas de la encuesta, la entrevista y el estudio de caso, se pone de manifiesto la necesidad de optimizar la tutela del derecho de autodeterminación informativa, que entraña un interés común para la sociedad boliviana, por lo que se elaboró una propuesta consistente en un Proyecto de Ley de incorporación de los Artículos 363 quáter y 363 quinquies en el Código Penal, sustentado en la Constitución Política del Estado, Instrumentos internacionales y principios propios del derecho penal.

- **CONCLUSIONES A PARTIR DEL OBJETIVO GENERAL**

Proponer la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela del derecho de autodeterminación informativa.

La información es considerada como un bien altamente apreciado, configura en sí misma un activo e insumo para una amplia gama de operaciones estatales y privadas, por ende, también objeto y blanco de los delincuentes. Los datos personales, como componentes de la información, constituyen el reflejo del individuo, por ello adquieren una connotada trascendencia para el Estado, empresas privadas (nacionales y transnacionales) y los particulares, toda vez que fácilmente pueden ser utilizados y aprovechados para obtener ganancias por su venta o cesión, sin el conocimiento ni anuencia de sus titulares. A su vez tanto la administración pública como privada, solicitan y tienen en su poder una infinidad desproporcionada de datos personales, en algunos casos exigiendo más datos de los que realmente corresponden para el cumplimiento del fin que ameritó su recolección.

Los datos personales en el Estado Plurinacional de Bolivia son susceptibles de utilización, apropiación, modificaciones y tratamientos no autorizados o divulgación en beneficio de terceros, causando daños morales y económicos, con lo que se transgrede el derecho de autodeterminación informativa, y junto a ello una variedad de derechos fundamentales como la dignidad, la privacidad, la intimidad, el honor, la reputación, el derecho a no ser discriminado

o los derechos de la niñez y adolescencia; entre otros, vulneraciones que también se traducen en afectaciones al patrimonio cuando se trata de datos relacionados al ámbito financiero, empresarial o comercial, verificándose estas conductas de manera frecuente en la realidad boliviana, sin que sean suficientes los mecanismos jurídicos de tutela y resguardo existentes.

Por lo señalado, respecto al objetivo general se concluye que es factible la propuesta de incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, teniendo como base el cumplimiento de los objetivos específicos del presente estudio, que se sintetizan en identificar la ausencia de estos tipos penales en la legislación vigente y la necesidad que de lo anterior emana, como secuela derivada del uso generalizado de las Tecnologías de Información y Comunicación, con lo cual operará una optimización de la tutela del derecho de autodeterminación informativa al contemplar la salvaguarda de la información y el dato personal en sede penal, erigiéndose como un pilar adicional de protección a los ámbitos normativos vigentes.

- **RECOMENDACIONES**

✓ Se recomienda a la Asamblea Legislativa Plurinacional, a través de la Cámara de Diputados (por constituir una iniciativa ciudadana), considerar para su tratamiento la presente propuesta que desarrolla el Proyecto de Ley de Incorporación de los Artículos 363 quáter y 363 quinquies en el Código Penal, el cual, de sancionarse previo cumplimiento del procedimiento legislativo y recaudos de rigor, permitirá el establecimiento de un régimen de protección penal de datos personales en el Estado Plurinacional de Bolivia, para garantizar la tutela óptima y efectiva del derecho a la autodeterminación informativa.

✓ Como secuela del influjo de las Tecnologías de Información y Comunicación, es difícil imaginar que en un futuro inmediato algún tipo de delito no se perpetre o deje evidencia ligada a las mismas. La delincuencia informática y la ciberdelincuencia crecen de forma considerable puesto que las herramientas y modalidades electrónicas están cada vez más interrelacionadas con las comunicaciones, actividades y transacciones personales, laborales, financieras, judiciales, gubernamentales y comerciales, en virtud de lo cual se considera pertinente la actualización del Código Penal en lo inherente a los delitos informáticos y cibercriminalidad, de modo tal que la legislación sea adecuada para prevenir y combatir este tipo de ilícitos, tomando como referencia el Convenio sobre la ciberdelincuencia de Budapest.

- ✓ El Estado boliviano a través de sus órganos competentes, debe diseñar e implementar políticas orientadas a prevenir y combatir los delitos contra la información y los datos personales, a través de campañas dirigidas a entidades públicas, privadas e individuos particulares. Estas medidas también deben considerar la capacitación y actualización de operadores de justicia, personal del Ministerio Público, miembros de la Policía Boliviana, abogados e interesados, para comprender mejor el fenómeno vinculado a las actuales tecnologías y así desempeñarse óptimamente en sus respectivas áreas funcionales.

- ✓ En atención al carácter transnacional de los ciberdelitos en general y a los ilícitos contra los datos personales en particular, dada su alta vinculación a las Tecnologías de Información y Comunicación, las instancias pertinentes del ámbito gubernamental, deben adoptar las medidas necesarias de cooperación y coordinación entre el Estado Plurinacional de Bolivia y otros países, para una eficaz lucha contra este tipo de delincuencia, considerando prioritariamente las gestiones pertinentes y expeditas para la adhesión al Convenio sobre la ciberdelincuencia de Budapest.

Referencias bibliográficas

Organización de Naciones Unidas. (2013). *Estudio exhaustivo sobre el delito cibernético y las respuestas de los estados miembros, la comunidad internacional y el sector privado ante ese fenómeno.*

Aboso, G. (2012). *Código Penal de la República Argentina. Comentado, concordado con jurisprudencia.* Buenos Aires, Argentina: B de F.

Acurio, S. (2017). *Derecho Penal Informático.* Ecuador: Pontificia Universidad Católica del Ecuador. Obtenido de https://www.academia.edu/19803737/Derecho_Penal_Inform%C3%A1tico

Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación. (2019). Juventudes TIC. Estudio sobre las TIC en adolescentes y jóvenes de Bolivia. Recuperado el 23 de diciembre de 2019, de https://www.agetic.gob.bo/pdf/estadotic/libro_juventudes_tic.pdf

Aguilera, J. (25 de julio de 2018). La Policia Boliviana crea la Oficina de Delitos Ciberneticos - Division de Cibercrimen. *Que no me pierda*. (M. Delgado, Entrevistador) Recuperado el 12 de diciembre de 2019, de https://www.youtube.com/watch?v=8OaEYUlKzbM

Aguirre, E., & Alejandro, O. (2013). Código Penal Comentado. Argentina.

Alvarez, M. (2015). *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital.* Madrid, España: Reus S.A.

Anarte, E. (2002). Sobre los límites de la protección penal de datos personales. *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento, 2*, 225-254.

Arocena, G. (2012). La regulación de los delitos informáticos en el código penal argentino. Introducción a la Ley Nacional N° 26.388. *Boletín mexicano de derecho comparado, XLV*(135), 945-988. Recuperado el 15 de mayo de 2019, de https://www.redalyc.org/pdf/427/42724584002.pdf

Asamblea General de las Naciones Unidas. (1948). Declaración Universal de Derechos Humanos de 10 de diciembre de 1948.

Asamblea General de las Naciones Unidas. (1976). Pacto Internacional de Derechos Civiles y Políticos de 23 de marzo de 1976.

Asamblea Legislativa Plurinacional. (2010). Reglamento General de la Cámara de Diputados .

ATB. (14 de febrero de 2017). Delitos informáticos aumentan en Bolivia según la Policía. Recuperado el 5 de diciembre de 2019, de https://www.youtube.com/watch?v=OXvOn0tMsig

ATB. (2018 de junio de 2018). Migración habilitó plataforma virtual para facilitar trámites. Recuperado el 14 de diciembre de 2019, de https://www.youtube.com/watch?v=nMzOCOmSqrs

ATB Digital. (19 de junio de 2018). MAS alista el proyecto de ley de protección de datos personales. Recuperado el 15 de junio de 2019, de https://www.atb.com.bo/tecnolog%C3%ADa/mas-alista-el-proyecto-de-ley-de-protecci%C3%B3n-de-datos-personales

Ávila, W. (2013). Hacia una reflexión histórica de las TIC. *Hallazgos, 10*(19), 213-233.

Bacigalupo, E. (1999). *Derecho Penal, Parte General* (Segunda ed.). Buenos Aires, Argentina: Hammurabi.

Baechler, J. (1978). *¿Qué es la ideología?* Buenos Aires, Argentina: Emece.

Balaguer, M. (2016). *Derecho de la información y de la comunicación* (Segunda ed.). Madrid, España: Tecnos.

Balbín, C. (2011). *Tratado de Derecho Administrativo.* Buenos Aires, Argentina: La Ley.

Barriga, P. (13 de noviembre de 2013). Entrevista a abogada de Paola Belmonte. Recuperado el 12 de noviembre de 2019, de https://anteriorportal.erbol.com.bo/archivos_multimedia/escuche_aqui_la_entrevista_la_abogada_de_paola_belmonte

Barrio, A. (2017). *Ciberdelitos: amenazas criminales del ciberespacio.* Madrid, España: Reus.

Bauzá, M. (2006). El actual derecho de la protección de datos en América y Europa. *Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales*, 41-58.

Belmonte, P. (14 de abril de 2014a). Entrevista a Paola Belmonte y Martin Sotomayor. *Todo A pulmón*. (J. Arandia, Entrevistador) La Paz, Bolivia. Recuperado el 12 de noviembre de 2019, de http://eju.tv/2014/04/paola-belmonte-pens-quitarme-la-vida/

Belmonte, P. (10 de abril de 2014b). Paola Belmonte reaparece en una entrevista con Amalia Pando. (A. Pando, Entrevistador) Recuperado el 12 de diciembre de 2019, de https://anteriorportal.erbol.com.bo/archivos_multimedia/audio_paola_belmonte_reaparece_en_una_entrevista_con_amalia_pando

Blossier, J., & Calderón, S. (2003). Delitos informáticos: camino a la impunidad. *Revista de Derecho Argentina*(54). Recuperado el 23 de marzo de 2019, de http://www.alfa-redi.org/sites/default/files/articles/files/blossiers.pdf

Boletín Oficial de la República Argentina. (2000). Ley N° 25.326 de Protección de los datos personales de 30 de octubre de 2000. Recuperado el 15 de mayo de 2019, de https://www.boletinoficial.gob.ar/

Boletin Oficial de la República Argentina. (2008). Ley N° 26.388 de 24 de junio de 2008. Recuperado el 16 de junio de 2019, de https://www.boletinoficial.gob.ar/detalleAviso/primera/9247892/20080625?busqueda=1

Boletin Oficial de la Republica Argentina. (2011). Ley N° 27.411. Convenio sobre ciberdelito. Aprobación, de 15 de diciembre de 2017. Recuperado el 19 de junio de 2019, de https://www.boletinoficial.gob.ar/

Boletín Oficial del Estado. (1978). Constitución Española. Recuperado el 15 de junio de 2019, de https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf

Boletin Oficial del Estado. (1992). Ley Orgánica N° 5/1992, de Regulación del tratamiento automatizado de los datos de carácter personal, de 29 de octubre de 1992. Recuperado el 22 de abril de 2019, de https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Boletín Oficial del Estado. (1995). Ley Orgánica N° 10/1995 de 23 de noviembre, del Código Penal. Recuperado el 14 de septiembre de 2019, de https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Boletin Oficial del Estado. (1999). Ley Orgánica N° 15/1999 de Protección de Datos de Caracter Personal, de 13 de diciembre de 1999. Recuperado el 15 de marzo de 2019, de https://www.boe.es/eli/es/lo/1999/12/13/15/con

Boletin Oficial del Estado. (2010). Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Recuperado el 5 de octubre de 2019, de https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf

Boletín Oficial del Estado. (2015). Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Recuperado el 15 de diciembre de 2019, de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-3439

Boletin Oficial del Estado. (2019). Código Penal y legislación complementaria (España). Recuperado el 23 de diciembre de 2019, de file:///C:/Users/lenovo/Downloads/BOE-038_Codigo_Penal_y_legislacion_complementaria%20(2).pdf

Bolivia, G. O. (2012). Ley de Servicios Financieros N° 393 de 21 de agosto de 2012. La Paz, Bolivia.

Calderón, A. (2013). Delito informático: reto para los sistemas penales del mundo. En A. Nava, *El derecho en la era digital.* México D.F., México: Porrúa.

Campoli, G. (2003). *Derecho penal informático* (Primera ed.). San José, Costa Rica: Investigaciones Jurídicas S.A.

Carbonell, M. (2006). Nueva interpretación del principo constitucional de legalidad en materia penal. *Iter Criminis, Revista de Ciencias Penales, 3*(6), 29-54. Recuperado el 4 de junio de 2019, de http://blog.uclm.es/cienciaspenales/files/2016/07/10carbonell-_-nueva-interpretacion-del-princpio-constitucional-de-legalidad-en-materia-penal.pdf

Carolina, L., & Wong, V. (2015). Cláusulas de apertura al derecho internacional de los derechos humanos: constituciones iberoamericanas. *Foro Nueva Epoca, 18*(2).

Carrión, H. (2001). Presupuestos para la incriminación de hacking. *Revista de derecho informático*(37). Recuperado el 5 de abril de 2019, de https://delitosinformaticos.com/trabajos/hacking.pdf

Castro, S. (2002). Delitos informáticos:La información como bien jurídico y los delitos informáticos en el Nuevo Código Penal Colombiano. Recuperado el 15 de julio de 2019, de https://www.delitosinformaticos.com/delitos/colombia1.shtml

Cerda, A. (2003). Autodeterminación informativa y leyes sobre protección de datos. *Revista Chilena de Derecho Informático*(3), 47-75.

Choque, M. (2007). Principios para la construcción de una democracia intercultural. En C. Zapata, *Intelectuales indígenas piensan América Latina.* Quito, Ecuador: Abya Yala.

Comisión Económica para América Latina y el Caribe. (2018). Monitoreo de la Agenda Digital para América Latina y el Caribe eLAC2018. Recuperado el 14 de diciembre de 2019, de https://repositorio.cepal.org/bitstream/handle/11362/43444/1/S1800256_es.pdf

Comité interamericano contra el terrorismo - OEA. (2004). Declaración de Montevideo. Recuperado el 14 de marzo de 2019, de http://www.oea.org/es/sms/cicte/documents/sesiones/2004/CuartoPeriodo-DECLARACION%20DE%20MONTEVIDEO.pdf

Comité Jurídico Interamericano. (2015). *Informe sobre Privacidad y Protección de Datos Personales (CJI/doc. 474/15 rev.2) de 26 de marzo de 2015.* Organización de Estados Americanos. Recuperado el 12 de enero de 2019, de http://www.redipd.es/documentacion/otrosdocumentos/common/Informe_CJI-doc_474-15_rev2_26_03_15.pdf

Conferencia Especializada Interamericana de Derechos Humanos. (1969). Convención Americana sobre Derechos Humanos de 22 de noviembre de 1969. Recuperado el 15 de junio de 2019, de https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. (2009). Estándares internacionales sobre protección de datos personales y privacidad, Resolución de Madrid. Recuperado el 10 de mayo de 2019, de https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

Congreso de la República de Colombia. (2009). Ley N° 1273 de 5 de enero de 2009. *Diario Oficial*. Recuperado el 15 de junio de 2019, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Congreso Nacional de Chile. (1999). Ley N° 19.628 Sobre protección de la vida privada. *Biblioteca del Congreso Nacional de Chile*. Recuperado el 20 de marzo de 2019, de Sitio Web: http://bcn.cl/1uv2v

Consejo de Europa. (1981). Convenio N° 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Recuperado el 11 de junio de 2019, de https://rm.coe.int/16806c1abd

Consejo de Europa. (2001). Convenio sobre la Ciberdelincuencia. Budapest.

Contraloría General del Estado. (14 de junio de 2019). *Contraloría General del Estado - Noticias*. Recuperado el 15 de junio de 2019, de https://www.contraloria.gob.bo/portal/Inicio/tabid/55/ctl/verNoticia/mid/1107/articleID/2573/Default.aspx

Correo del Sur. (5 de abril de 2017). Cusi presenta certificado médico que demuestra su estado depresivo. *Correo del Sur*. Recuperado el 12 de noviembre de 2019, de https://correodelsur.com/politica/20170405_cusi-presenta-certificado-medico-que-demuestra-su-estado-depresivo.html

Correo del Sur. (16 de mayo de 2019). Comienza el registro de ciudadanía digital. *Correo del Sur*.

Criado, I., & Gil-García, R. (2013). Gobierno Electrónico, gestión y políticas públicas. Estado actual y tendencias futuras en América Latina. *Gestión y Política Pública, 1*, 3-48. Recuperado el 12 de octubre de 2019, de http://www.scielo.org.mx/pdf/gpp/v22nspe/v22nspea1.pdf

Criales, F., & Torrico, G. (2014). *Diseño metodológica en investigaciones sociales.* La Paz, Bolivia.

Cuervo, J. (1999). Delitos informáticos: protección penal de la intimidad. *Revista de Derecho Informático*. Recuperado el 31 de mayo de 2019, de http://www.informatica-juridica.com/trabajos/delitos-informaticos-proteccion-penal-de-la-intimidad/#INTRODUCCI%C3%93N

Cusi, G. (29 de diciembre de 2014). El Magistrado Cusi en Todo A pulmón. (J. Arandia, Entrevistador) Recuperado el 24 de noviembre de 2019, de https://www.youtube.com/watch?v=c134KrJZ0ag

Cusi, G. (2 de diciembre de 2016). Gualberto Cusi rompe en llanto en una entrevista. (R. Lizárraga, Entrevistador) Recuperado el 11 de diciembre de 2019, de https://www.youtube.com/watch?v=MEL6z4-qiA0

Cusi, G. (12 de diciembre de 2019). Ex magistrado de Bolivia, intervención en la OEA. Recuperado el 20 de diciembre de 2019, de https://www.youtube.com/watch?v=HULMhcTBCOY

Davara, M. (2008). *Manual de Derecho Informático* (Décima ed.). Madrid, España: Aranzadi S.A.

Davinovics, G., & Mayol, A. (2009). Introducción al uso de muestras para la realización de encuestas en la investigación social. En P. Salinas, & M. Cárdenas, *Métodos de investigación social.* Quito, Ecuador: CIESPAL. Recuperado el 12 de octubre de 2019, de https://biblio.flacsoandes.edu.ec/catalog/resGet.php?resId=55376

De la Mata, N. (2007). Los delitos vinculados a las tecnologías de la información y comunicación en el Código Penal: panorámica general. *Cuadernos Penales José María Lidón*(4), 41-84.

Declaración de Cartagena. (2004). Cartagena de Indias, Colombia. Recuperado el 20 de enero de 2019, de http://www.redipd.es/documentacion/common/declaracion_2004_III_encuentro_es.pdf

Declaración de La Antigua. (2003). La Antigua, Guatemala. Recuperado el 12 de enero de 2019, de http://www.redipd.es/documentacion/common/declaracion_2003_II_encuentro_es.pdf

Declaración de Santa Cruz de la Sierra. (2003). Santa Cruz de la Sierra, Bolivia. Recuperado el 20 de enero de 2019, de http://www.redipd.es/actividades/common/xiii_cumbre/Declaracion_Santa_Cruz_de_la_Sierra_Bolivia.pdf

Defensoría del Pueblo. (2015). *XVII Informe a la Asamblea Legislativa Plurinacional 2014.* Recuperado el 15 de diciembre de 2019, de https://www.defensoria.gob.bo/uploads/files/xvii-informe-a-la-asamblea-legislativa-plurinacional.pdf

Del Picó, J. (2018). Estado y religión. *Revista de estudios sociales*(63), 42-54. Recuperado el 15 de marzo de 2019, de https://journals.openedition.org/revestudsoc/1190

Diario Oficial de la República de Colombia. (2018). Ley N° 1928 de 24 de julio de 2018. Recuperado el 15 de diciembre de 2019, de https://dapre.presidencia.gov.co/normativa/normativa/LEY%201928%20DEL%2024%20DE%20JULIO%20DE%202018.pdf

El Deber. (27 de agosto de 2017). La suplantación de identidad arruina la vida de familias enteras.

El Deber. (2018). Indignación de gente que figura como militante de un partido sin haberse inscrito. Recuperado el 12 de junio de 2019, de https://webcache.googleusercontent.com/search?q=cache:zWAxjDhARsEJ:https://eldeber.com.bo/103698_indignacion-de-gente-que-figura-como-militante-de-un-partido-sin-haberse-inscrito+&cd=1&hl=es-419&ct=clnk&gl=bo

El Deber. (2019). El bullying va más allá de las aulas y oprime a los jóvenes en las redes sociales. Recuperado el 11 de diciembre de 2019, de https://eldeber.com.bo/115854_el-bullying-va-mas-alla-de-las-aulas-y-oprime-a-los-jovenes-en-las-redes-sociales

El Día. (1 de junio de 2017). El MAS reprime a Cusi con acciones discriminatorias. *El Día*. Recuperado el 20 de diciembre de 2019, de https://www.eldia.com.bo/index.php?c=&articulo=El-MAS-reprime-a-Cusi-con-acciones-discriminatorias-&cat=150&pla=3&id_articulo=227775

El Diario. (2014 de diciembre de 2014). Formalizan demanda contra Ministro de Salud. *El Diario*. Recuperado el 20 de diciembre de 2019, de https://www.eldiario.net/noticias/2014/2014_12/nt141231/politica.php?n=73&-formalizan-demanda-contra-ministro-de-salud

Federal Bureau of Investigation. (2017). Internet crime report. Recuperado el 3 de mayo de 2019, de https://pdf.ic3.gov/2017_IC3Report.pdf

Federal Bureau of Investigation. (2018). Internet crime report. Recuperado el 11 de mayo de 2019, de https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

Ferrajoli, L. (1995). *Derecho y razón, Teoria del garantismo penal.* Madrid, España: Trotta.

Flores, L. (2015). *Temas actuales de los derechos humanos de última generación.* Puebla, México: Piso 15.

Foro de Cooperación Económica Asia Pacífico (APEC). (2004). Marco de privacidad del Foro de Cooperación Económica Asia Pacífico. Recuperado el 11 de mayo de 2019, de https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

Gaceta Oficial de Bolivia. (2017). Decreto Supremo N° 3404 de 29 de noviembre de 2017. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional Bolivia. (2014). Código niña, niño y adolescente Ley N° 548 de 17 de julio de 2014. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (1975). Código Civil de 6 de agosto de 1975. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (1990). Ley N° 1152 de 14 de mayo de 1990. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (1993). Ley Nº1430 de 11 de febrero de 1993 que ratifica la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica). La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (1997). Código Penal de 10 de marzo de 1997. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (1997). Ley de modificaciones al Código Penal N°1768 de 10 de marzo de 1997. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2000). Ley Nº2119 de 11 de septiembre de 2000 que ratifica el Pacto Internacional de Derechos Civiles y Políticos. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2004). Ley Nº 2631 de 20 de febrero de 2004. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2005). Decreto Supremo N° 28168 de 17 de mayo de 2005. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2009). Constitución Política del Estado de 7 de febrero de 2009. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2010). Ley de protección legal de niñas, niños y adolescentes N° 054 de 8 de noviembre de 2010. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2010). Ley del Órgano Electoral Plurinacional N° 018 de 16 de junio de 2010. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2011). Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación N° 164 de 8 de agosto de 2011. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2012). Reglamento General de la Ley N° 164 aprobado por Decreto Supremo N°1391, de 24 de octubre de 2012 . La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2013). Reglamento a la Ley N° 164 para el Desarrollo de Tecnologías de Información y Comunicación, aprobado por Decreto Supremo N°1793 de 13 de noviembre de 2013. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2015). Decreto Supremo N° 2514 de 9 de septiembre de 2015. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2015). Reglamento a la Ley N° 548, aprobado por Decreto Supremo N° 2377 de 27 de mayo de 2015. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2017). Código del Sistema Penal Ley N° 1005 de 17 de diciembre de 2017. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2017). Decreto Supremo N°3251 de 12 de julio de 2017. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2018). Decreto Supremo N° 3525 de 4 de abril de 2018. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2018). Ley de abrogación del Código del Sistema Penal N° 1027 de 25 de enero de 2018. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2018). Ley de ciudadanía digital N° 1080 de 11 de julio de 2018. La Paz, Bolivia.

Gaceta Oficial del Estado Plurinacional de Bolivia. (2018). Ley N° 1057 de 10 de mayo de 2018. La Paz, Bolivia.

Garriga, A. (2004). *Tratamiento de datos personales y derechos fundamentales.* Madrid, España: Dykinson.

Garriga, A. (2016). *Nuevos retos para la protección de datos personales. En la era del big data y de la computación ubicua.* Madrid, España: Dykinson.

Gobierno del Estado Plurinacional de Bolivia. (9 de octubre de 2019). *Ciudadanía digital*. Obtenido de https://www.gob.bo/ciudadania/servicios-digitales

Gómez, J. (2008). La protección de los datos personales en el Código Penal Español. *Revista Jurídica de Castilla y León*(16), 325-372. Recuperado el 19 de junio de 2019, de https://www.uv.es/limprot/boletin6/gomeznavajas.pdf

Gonzáles Rus, J. (2007). Precisiones conceptuales y político-criminales sobre la intervención penal en internet. *Cuadernos penales José María Lidón*, 13-40.

Gonzales, T. (2015). Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de derecho penal y criminología, 3*(13). Recuperado el 11 de diciembre de 2019, de http://e-spacio.uned.es/fez/eserv/bibliuned:revistaDerechoPenalyCriminologia-2015-13-7010/pag_51.pdf

Hernandez, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación* (Sexta ed.). México D.F., México: McGraw-Hill.

Herrán, A. (2003). *El derecho a la protección de datos personales en la sociedad de la información.* Bilbao, España: Universidad de Deusto.

Ibarra, E. (2013). Derecho de protección de datos personales; regulación de la videovigilancia en México. En A. Nava, *El derecho en la era digital.* México DF, México: Porrúa.

Instituto Boliviano de Comercio Exteriror. IBCE. (1 de junio de 2017). El MAS reprime a Cusi con acciones discriminatorias. Recuperado el 11 de noviembre de 2019, de https://ibce.org.bo/principales-noticias-bolivia/noticias-nacionales-detalle.php?id=77101&idPeriodico=5&fecha=2017-06-01

Jescheck, H. (1993). *Tratado de derecho penal, parte general* (Cuarta ed.). Granada, España: Comares.

Jimeno, J. (2019). *Derecho de daños tecnológicos ciberseguridad e insurtech.* Madrid, España: Dykinson.

La Época. (4 de septiembre de 2019). Uno de cada tres jóvenes ha sido víctima de acoso cibernético. Recuperado el 11 de diciembre de 2019, de https://www.la-epoca.com.bo/2019/09/04/uno-de-cada-tres-jovenes-ha-sido-victima-de-acoso-cibernetico/

La Patria. (2 de diciembre de 2018). Grooming y sexting, las nuevas amenazas en las redes sociales. Recuperado el 11 de diciembre de 2019, de http://www.lapatriaenlinea.com/?nota=337546

La Razón. (4 de mayo de 2014). Planean tipificar pornovenganza y castigarla con 15 años de carcel.

La Razón. (19 de noviembre de 2018). Ciudadanos denuncian que aparecen como militantes de partidos sin nunca haberse inscrito.

Landa, C. (2013). La constitucionalización del derecho peruano. *Derecho PUCP*(71), 13-36.

Ley Fundamental de la República de Alemania. (1949). Recuperado el 24 de marzo de 2019, de https://www.btg-bestellservice.de/pdf/80206000.pdf

Los Tiempos. (30 de diciembre de 2014). Cusi presenta demanda contra Ministro. *Los Tiempos*. Recuperado el 11 de diciembre de 2019, de https://www.lostiempos.com/actualidad/nacional/20141230/cusi-presenta-demanda-contra-ministro

Los Tiempos. (16 de febrero de 2018a). Patrullaje Cibernético de la Policía detecta siete delitos en tres semanas. Recuperado el junio 17 de 2019, de https://www.lostiempos.com/actualidad/cochabamba/20180216/patrullaje-cibernetico-policia-detecta-siete-delitos-tres-semanas

Los Tiempos. (31 de agosto de 2018b). Conoce los trámites que puedes realizar de manera online. Recuperado el 14 de diciembre de 2019, de https://www.lostiempos.com/actualidad/pais/20180831/conoce-tramites-que-puedes-realizar-manera-online

Los Tiempos. (24 de abril de 2019). Nuestros datos expuestos a empresas y Estado: en debate una ley para la protección. Recuperado el 14 de diciembre de 2019, de https://www.lostiempos.com/especial-multimedia/20190422/nuestros-datos-expuestos-empresas-estado-debate-ley-proteccion

Martinez, I. (2013). Delitos contenidos en la Ley Federal de Datos Personales en Posesión de los Particulares. En A. E. Nava Garcés, *El derecho en la era digital.* México DF, México: Porrúa.

Martínez, V. (2015). Acercamiento al concepto de etnicidad:notas sobre algunos debates y las potencialidades del cruce de categorias de etnicidad y género. *Intersticios de la política y la cultura. Intervenciones Latinoamericanas, 4*(8), 65-82.

Mata, R. (2003). *Delincuencia informática y derecho penal.* Managua, Nicaragua: Hispamer.

Medinaceli, K. (2017). *El tratamiento de los datos sanitarios en la historia clínica electrónica: Caso boliviano.* Madrid, España: Agencia Estatal Boletín Oficial del Estado.

Mendoza, J. (2016). Delito Vs. contravenciones tributarias. *Análisis tributario*, 41-46. Recuperado el 12 de diciembre de 2019, de https://www.ait.gob.bo/DOCUMENTOS/REVISTA/Articulos/Delito%20Vs%20Contravenciones%20Tributarias.pdf

Menéndez, J., & Gayo, M. (2014). *Derecho e informática: ética y legislación.* Madrid, España: Bosch.

Miguel, J. C. (2016). *Protección de datos y seguridad de la información* (Cuarta ed.). Bogotá, Colombia: Ediciones de la U.

Muñoz, F., & García, M. (2010). *Derecho Penal - Parte General* (Octava ed.). Valencia, España: Tirant lo Blanch.

Murillo, P. (1990). *El derecho a la autodeterminación informativa.* Madrid, España: Tecnos.

Murillo, P. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Alpizcueta: cuadernos de derecho*(20), 43-58.

Murillo, P., & Piñar, J. (2009). *El derecho a la autodeterminación informativa.* Madrid, España: San José.

Nava, A. (2013). Ciberdelito y ciberseguridad. En A. Nava, *El derecho en la era digital.* México DF, México: Porrúa.

Nava, A. (2018). *Delitos informáticos* (Cuarta ed.). México D.F., México: Porrúa.

NTN24. (26 de diciembre de 2014). Polémica en Bolivia por declaraciones de ministro de Salud contra el magistrado Gualberto Cusi. Recuperado el 15 de Diciembre de 2019, de https://www.youtube.com/watch?v=RyN-UNjwL3I

ODIB. (5 de junio de 2019). 7 Principales riesgos en Internet que amenazan niños, niñas y adolescentes. Recuperado el 12 de diciembre de 2019, de https://www.odibolivia.org/2019/06/05/7-principales-riesgos-en-internet-que-amenazan-ninos-ninas-y-adolescentes/

Oficina Internacional del Trabajo. (1997). *Protección de los datos personales de los trabajadores.* Recuperado el 18 de junio de 2019, de https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_112625.pdf

Ojeda, Z. (2015). El derecho a la protección de datos personales desde un análisis histórico - doctrinal. *Tla-melaua, 9*(38), 58-70. Recuperado el 20 de mayo de 2019, de http://www.scielo.org.mx/pdf/tla/v9n38/1870-6916-tla-9-38-00058.pdf.

Opinión. (12 de noviembre de 2013). Presentadora acusa de extorsión a instructor.

Opinión. (6 de abril de 2015). Preparan ley para regular salas de internet y evitar ciberacoso. Recuperado el 21 de diciembre de 2019, de https://www.opinion.com.bo/articulo/el-pais/%EF%BB%BFpreparan-ley-regular-salas-internet-evitar-ciberacoso/20150406002000517712.amp.html

Opinión. (26 de mayo de 2017). Detectan 6 casos de suplantación al sacar carnet. *Opinión*.

Opinión. (19 de junio de 2018). Agetic prevé elaborar una norma para proteger los datos personales. Recuperado el 12 de mayo de 2019, de https://www.opinion.com.bo/articulo/el-pais/agetic-prev-eacute-elaborar-norma-proteger-datos-personales/20180619170500617324.amp.html

Opinión. (30 de noviembre de 2019). SEGIP identifica ocho casos de suplantación de identidad al mes. Recuperado el 12 de diciembre de 2019, de https://www.opinion.com.bo/articulo/cochabamba/segip-identifica-casos-suplantacion-identidad-mes/20191130000047739062.html

Organización de Estados Americanos (OEA). (2015). Principios de la OEA sobre la privacidad y la protección de datos personales. Recuperado el 5 de mayo de 2019, de http://www.oas.org/es/sla/ddi/docs/cji-doc_474-15_rev2.pdf

Organización de Naciones Unidas - Unión Internacional de Telecomunicaciones. (2005). Agenda de Túnez para la Sociedad de la Información. Recuperado el 23 de junio de 2019, de https://www.itu.int/net/wsis/outcome/booklet-es.pdf

Organización de Naciones Unidas. (1989). Convención sobre los derechos del niño. Recuperado el 19 de junio de 2019, de https://www.un.org/es/events/childrenday/pdf/derechos.pdf

Organización de Naciones Unidas. (1990). Principios rectores para la reglamentación de los ficheros computarizados de datos personales adoptados mediante Resolución N°45/95 de la Asamblea General de la ONU. Recuperado el 12 de mayo de 2019, de https://docplayer.es/9568094-Principios-rectores-para-la-reglamentacion-de-los-ficheros-computadorizados-de-datos-personales.html

Organización de Naciones Unidas. (2013). El derecho a la privacidad en la era digital. Resolución N° A/RES/68/167. Recuperado el 20 de marzo de 2019, de https://undocs.org/es/A/RES/68/167

Organización de Naciones Unidas. (2016). El derecho a la privacidad en la era digital. A/C.3/71/L.39. Recuperado el 15 de octubre de 2019, de https://www.acnur.org/fileadmin/Documentos/BDL/2017/10904.pdf

Organización de Naciones Unidas. (2017). Deliberaciones de la primera reunión del Grupo de Expertos encargado de realizar un estudio exhaustivo sobre el Delito Cibernético, celebrada en Viena del 17 al 21 de enero de 2011. Recuperado el 11 de julio de 2019, de https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/UNODC-CCPCJ-EG-4-2017-2/V1701129_S.pdf

Organización para la Cooperación y Desarrollo Económicos - OCDE. (2002). *Guías de la OCDE para la seguridad de los sistemas de información y redes.* Recuperado el 20 de junio de 2019, de https://www.anacom.pt/streaming/1946922.pdf?categoryId=45842&contentId=132698&field=ATTACHED_FILE

Organización para la Cooperación y el Desarrollo Económicos - OCDE. (1980). Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Recuperado el 25 de mayo de 2019, de https://www.oecd.org/sti/ieconomy/15590267.pdf

Ossio, F. (2010). *Protección de datos personales ¿Habeas Data o Sistema de Data Protection?* La Paz, Bolivia: Editora M.V.

Página Siete. (23 de diciembre de 2014). Ministro de Salud vulnera la ley al revelar la enfermedad de Cusi.

Página Siete. (21 de marzo de 2019). Bolivia, ante la encrucijada de proteger sus datos personales. Recuperado el 12 de diciembre de 2019, de https://www.paginasiete.bo/sociedad/2019/3/21/bolivia-ante-la-encrucijada-de-proteger-sus-datos-personales-212575.html

Parlamento Europeo y Consejo . (s.f.). Directiva N° 2013/40/UE de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco N° 2005/222/JAI del Consejo. *2013*. Recuperado el 23 de septiembre de 2019, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013L0040

Parlamento Europeo y Consejo. (1995). Directiva N° 95/46/CE de 24 de octubre de 1995. Recuperado el 11 de junio de 2019, de https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A31995L0046

Parlamento Europeo y Consejo. (2016). Reglamento (UE) N° 2016/679 Relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos de 27 de abril de 2016. Recuperado el 15 de mayo de 2019, de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32016R0679

Parlamento Europeo, Consejo y Comisión. (2000). Carta de derechos fundamentales de la Unión Europea. Recuperado el 15 de agosto de 2019, de https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Pérez Luño, A. (1991). Las generaciones de derechos humanos. *Revista del centro de estudios constitucionales*(10), 203-217.

Pérez Luño, A. (1996). *Manual de informática y derecho.* Barcelona, España: Ariel.

Periodico Digital Radio Fides.com. (29 de diciembre de 2014). Caso Cusi: Defensor pide a viceministro de Descolonización procesar a Calvimontes. *Periodico Digital Radio Fides.com*. Recuperado el 15 de noviembre de 2019, de http://www.radiofides.com/index_old.php/noticia/politica/caso-cusi%3A-defensor-pide-a-viceministro-de-descolonizacion-procesar-a-calvimontes

Pinedo, I. (2013). Protección de datos sanitarios:la historia clínica y sus accesos. *Revista CESCO de derecho de consumo*(8), 306-318. Recuperado el 20 de marzo de 2019, de Dialnet-ProteccionDeDatosSanitarios-4524537.pdf

Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Nuevo Foro Penal, 13*(88), 72-112.

Puig, M. (2008). *Derecho penal, Parte General* (Octava ed.). Barcelona, España: Reppertor.

Real Academia Española . (2018). *Diccionario de la lengua española.* Recuperado el 30 de junio de 2019, de https://dle.rae.es/?id=Bskzsq5|BsnXzV1

Rebollo, L., & Saltor, C. (2013). *El derecho a la protección de datos en España y Argentina. Orígenes y regulación vigente.* Madrid, España: Dykinson.

Recalde, M. (2015). *El modelo sindical argentino:régimen jurpidico.* Córdoba, Argentina: Villa María.

Red Iberoamericana de Protección de Datos. (2017). Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 20 de junio de 2017. Recuperado el 16 de abril de 2019, de http://www.redipd.org/noticias_todas/2017/novedades/common/Estandares_Esp_Con_logo_RIPD.pdf#Testo%20en%20espa%C3%B1ol

Reunión de Ministros de Justicia o de Ministros o Peocuradores Generales de las Américas. (2004). Resolución N° AG/RES. 2040 (XXXIV-O/04) de 8 de junio de 2004. Recuperado el 15 de junio de 2019, de http://www.oas.org/juridico/spanish/ag04/agres_2040.htm

Riascos, L. (2012). Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. *Derecho y realidad*(20), 335-429.

Rincon, J. (2015). *El delito en la cibersociedad y la justicia penal internacional (Memoria para optar al grado de doctor).* Madrid, España.

Riquert, M. (2013). Código Penal comentado. Argentina.

Rivera, J. (2010). La justicia constitucional en el nuevo modelo de Estado boliviano. En E. Ferrer, A. Bogdandy, & M. Morales, *La justicia constitucional y su internacionalización. ¿Hacia un ius constitucionale commune en América Latina?* (págs. 645-679). México D.F., México: UNAM.

Robledo, J. (2005). *Diseño de muestreo. Nure investigación.* Recuperado el 22 de septiembre de 2019, de 214-Texto%20del%20artículo-845-1-10-20150603.pdf

Rodriguez, L. (2007). *Código Penal. Comentado y con Jurisprudencia.* Madrid, España: La Ley.

Romeo Casabona, C. (2002). La intimidad y los datos de carácter personal como derechos fundamentales y como bienes jurídicos penalmente protegidos. *Estudios jurídicos en memoria de José María Lidón*, 513-536. Recuperado el 15 de junio de 2019, de https://dialnet.unirioja.es/servlet/libro?codigo=6563

Roxin, C. (1997). *Derecho Penal, parte general, Tomo I.* Madrid, España: Civitas.

Serrano, M. (2003). *El derecho fundamental a la protección de datos. Derecho español y comparado.* Madrid, España: Civitas.

Soto, Y. (2017). Datos masivos con privacidad y no contra la privacidad. *Bioetica y derecho, 40*, 101-114. Recuperado el 14 de octubre de 2019, de http://scielo.isciii.es/pdf/bioetica/n40/1886-5887-bioetica-40-00101.pdf

Suárez, A. (2019). Delitos informáticos. En *Lecciones de derecho penal parte especial* (págs. 15-72). Bogotá, Colombia: Universidad externado de Colombia.

Tantaleán. (2016). Tipología de las investigaciones jurídicas. *Derecho y cambio social, 13*(43). Recuperado el 15 de septiembre de 2019, de Dialnet-TipologiaDeLasInvestigacionesJuridicas-5456267%20(4).pdf

Tejero, R. (2010). El movimiento de datos de salud en el ámbito sanitario. En *Biomedicina y derecho sanitario* (págs. 615-651). Madrid, España: Ademas comunicación.

Téllez, J. (2009). *Derecho Informático* (Cuarta ed.). McGraw-Hill/Interamericana Editores.

Torres-Parodi, C., & Bolis, M. (2007). Evolución del concepto etnia/raza y su impacto en la formulación de políticas para la equidad. *Revista Panamericana Salud Pública, 22*(6), 405-416.

Torrico, G., & Pareja, F. (2019). *Alicia en el universo de las TIC.* La Paz, Bolivia.

Tribunal Constitucional . (2006). Sentencia Constitucional N°0030/2006-R de 11 de enero de 2006. Sucre, Bolivia.

Tribunal Constitucional. (2004). Sentencia Constitucional N°0965/2004-R de 23 de junio de 2004. Sucre, Bolivia.

Tribunal Constitucional. (2010). Sentencia Constitucional N° 0189/2010-R de 24 de mayo de 2010. Sucre, Bolivia.

Tribunal Constitucional. (2010). Sentencia Constitucional N°0127/2010-R de 10 de mayo de 2010. Sucre, Bolivia.

Tribunal Constitucional. (2011). Sentencia Constitucional N° 1978/2011-R de 7 de diciembre de 2011. Sucre, Bolivia.

Tribunal Constitucional Español. (2000). Sentencia N° 292/2000 de 30 de noviembre de 2000. Recuperado el 19 de junio de 2019, de https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

Tribunal Constitucional Federal Alemán. (1983). Sentencia de 15 de diciembre de 1983. Recuperado el 15 de enero de 2019, de http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/

Tribunal Constitucional Federal Alemán. (2008). Sentencia de 27 de febrero de 2008.

Tribunal Constitucional Plurinacional. (2012). Sentencia Constitucional Plurinacional N° 2175/2012 de 8 de noviembre de 2012. Sucre, Boliva.

Tribunal Constitucional Plurinacional. (2014). Sentencia Constitucional Plurinacional N° 0089/2014-S2 de 4 de noviembre de 2014. Sucre, Bolivia.

Tribunal Constitucional Plurinacional. (2014). Sentencia Constitucional Plurinacional N°0080/2014-S2 de 4 de noviembre de 2014. Sucre, Bolivia.

Tribunal Constitucional Plurinacional. (2015). Sentencia Constitucional Plurinacional N° 0332/2015-S1 de 6 de abril de 2015. Sucre, Bolivia.

Tribunal Constitucional Plurinacional. (2015). Sentencia Constitucional Plurinacional N° 0426/2015-S3 de 20 de abril de 2015. Sucre, Bolivia.

Tribunal Constitucional Plurinacional. (2015). Sentencia Constitucional Plurinacional N°0819/2015-S3 de 10 de agosto de 2015. Sucre, Bolivia.

Tribunal de Justicia de la Unión Europea. (2014). *Sentencia de 13 de mayo de 2014.* Recuperado el 14 de junio de 2019, de http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

Unitel. (31 de mayo de 2017). Entrevista a Gualberto Cusi. Recuperado el 11 de noviembre de 2019, de https://www.youtube.com/watch?v=WM05meQlNd0&t=479s

Urgente.bo - Revista Oxígeno . (2018). Resucité de una muerte cruel (23 de agosto de 2018). Recuperado el 12 de septiembre de 2019, de https://urgente.bo/noticia/resucit%C3%A9-de-una-muerte-cruel

Viega, M. (2003). Protección de datos y delitos informáticos. Ponencia presentada al III Congreso Internacional de Derecho. Bolivia, 10 al 13 de septiembre de 2003 y publicada en el Libro de Memorias de dicho Congreso.

Villabella, C. (2015). Los métodos en la investigación jurídica. Algunas precisiones. En *Metodologías: enseñanza e investigación jurídicas. 40 años de vida académica. Homenaje al doctor Jorge Witker* (págs. 921-953). Mexico D.F., México: Instituto de investigaciones jurídicas.

Villamor, F. (2007). *Derecho Penal Boliviano. Parte Especial. Tomo II.* La Paz, Bolivia.

Villarino, M. (2018). *La privacidad en el entorno del cloud computing.* Madrid, España: Reus S.A. .

Vizcardo, S. (2014). *Tipificación de los delitos informáticos patrimoniales en la nueva ley de delitos informáticos N° 30046.* Recuperado el 9 de junio de 2019, de file:///C:/Users/lenovo/Downloads/11870-Texto%20del%20art%C3%ADculo-41319-1-10-20160607%20(1).pdf

Witker, J. (2011). *La investigación jurídica: bases para las tesis de grado en derecho* (Segunda ed.). México D.F., México: Publi - Lex.

Yañez, A. (2007). *Ratio Decidendi.* Sucre, Bolivia: Gaviota del Sur.

Zaffaroni, E. (1985). *Manual de derecho penal. Parte general.* Buenos Aires, Argentina: Ediar.

ANEXOS

ANEXO 1

CUESTIONARIO

UNIVERSIDAD ANDINA SIMÓN BOLIVAR

MAESTRIA EN DERECHO PENAL Y DERECHO PROCESAL PENAL

CUESTIONARIO

El presente cuestionario tiene por objetivo establecer la pertinencia de la incorporación de tipos penales para la protección de datos personales en el Código Penal. Su criterio es muy importante para generar una propuesta a los fines señalados. La información proporcionada será utilizada únicamente en el ámbito académico y de manera confidencial. Lea cuidadosamente y seleccione una sola respuesta, marcando la casilla correspondiente.

I. DATOS PERSONALES

Rango de edad: 26-30 ☐ 31-35 ☐ 36-40 ☐ 41-45 ☐ 46-50 ☐ 50 o más ☐

Sexo: Femenino ☐ Masculino ☐

II.DATOS DE INTERES

1. Los datos personales son cualquier tipo de datos que identifican de forma directa o indirecta a un individuo, como el nombre y apellidos, cédula de identidad, dirección, orientación sexual, historial médico y datos biométricos, entre otros.

1. Si ☐
2. No ☐

2. ¿Con que regularidad comparte sus datos personales por medio de las Tecnologías de Información y Comunicación? (dispositivos digitales, internet, redes sociales, entre otros)

1. Frecuentemente ☐
2. Ocasionalmente ☐
3. Casi nunca ☐

3. Desde su percepción, los datos personales proporcionados a las entidades públicas del Estado Plurinacional de Bolivia se encuentran:

1. Adecuadamente protegidos ☐
2. Regularmente protegidos ☐
3. Desprotegidos ☐

4. Desde su percepción, los datos personales proporcionados a las entidades privadas del Estado Plurinacional de Bolivia se encuentran:

1. Adecuadamente protegidos ☐
2. Regularmente protegidos ☐
3. Desprotegidos ☐

5. ¿Cuáles considera que son las formas más recurrentes en que se vulnera el derecho a la protección de datos personales en el Estado Plurinacional de Bolivia?

1. Acceso no autorizado ☐

2. Uso no autorizado ☐
3. Alteración de datos ☐
4. Revelación no autorizada ☐

6. ¿Existe un artículo en el Código Penal que tipifique atentados contra los datos personales?

1. Si ☐
¿Cuál? ……
2. No ☐

7. ¿Se debería incorporar un tipo penal para la protección de datos personales en el Código Penal?

1. Si ☐
2. No ☐

8. ¿Se debería incorporar un tipo penal para la protección de datos personales sensibles y datos de menores de edad en el Código Penal?

1. Si ☐
2. No ☐

9. ¿Cuáles deberían ser las principales conductas a incluir en los tipos penales para la protección de datos personales?

1. Acceso ilícito ☐
2. Uso ilícito ☐
3. Alteración ilícita ☐
4. Revelación no autorizada ☐
5. Acceso, uso, alteración y revelación ilícitos ☐

10. Considera pertinente incluir como sujeto activo a:

1. Cualquier persona ☐
2. Servidores públicos ☐
3. Responsable de la base de datos ☐
4. Cualquier persona y servidores públicos ☐
5. Cualquier persona, servidores públicos, responsable de la base de datos ☐

11. Los tipos penales contra los datos personales, deberían incluir la forma:

1. Culposa ☐
2. Dolosa ☐

12. Los delitos contra los datos personales deberían sancionarse con una pena de:

1. Presidio ☐
2. Reclusión ☐
3. Reclusión y días multa ☐
4. Reclusión e inhabilitación especial ☐
5. Reclusión, días multa e inhabilitación especial ☐

13. Con la incorporación de tipos penales orientados a la protección de datos personales en el Código Penal boliviano, se contribuirá a que la tutela del derecho de autodeterminación informativa:

1. Mejore ☐
2. Continúe igual ☐
3. Desmejore ☐

ANEXO 2

GUÍA DE ENTREVISTA

UNIVERSIDAD ANDINA SIMÓN BOLIVAR

MAESTRIA EN DERECHO PENAL Y DERECHO PROCESAL PENAL

GUÍA DE ENTREVISTA

El presente guía tiene por objetivo establecer la pertinencia de la incorporación de tipos penales para la protección de datos personales en el Código Penal, en el marco de la realización de una tesis de Maestría. Su criterio como experto es muy importante para generar una propuesta a los fines señalados.

Nombre y apellidos:

Profesión:

Especialidad:

Institución donde ejerce su actividad laboral:

1. ¿Cuál es la importancia de los datos personales?
2. ¿Cuál es la incidencia de las Tecnologías de Información y Comunicación en la recolección y difusión de datos personales?
3. ¿Considera que las entidades públicas y privadas brindan una efectiva protección de los datos personales de los bolivianos?
4. Desde su experiencia, ¿cuáles son las formas más recurrentes en que se vulnera el derecho a la protección de datos personales o autodeterminación informativa en el Estado Plurinacional de Bolivia?
5. ¿El Código Penal contempla previsiones para la tutela de los datos personales?
6. ¿Las disposiciones existentes en el Código Penal son suficientes para sancionar conductas que atenten contra los datos personales?
7. ¿A su criterio, se debería incorporar tipos penales que sancionen los hechos más graves que atenten contra datos personales, datos personales sensibles y de menores de edad en el Código Penal?
8. ¿Cuáles deberían ser las conductas punibles en los tipos penales para la protección de datos personales?
9. ¿Quiénes deberían ser incluidos como sujetos activos en los ilícitos contra los datos personales?
10. Los tipos penales contra los datos personales, ¿deberían contemplar la forma culposa o dolosa?
11. ¿Qué tipo de sanción debería corresponder a los ilícitos que atentan contra los datos personales?
12. ¿Con la incorporación de tipos penales orientados a la protección de datos personales en el Código Penal, se lograría mejorar la tutela del derecho de autodeterminación informativa?

¿Autoriza usted el uso de la información otorgada en la presente entrevista, únicamente para los fines académicos de esta investigación?

Muchas gracias!

ANEXO 3
MATRIZ DE ESTUDIO DE CASO

UNIVERSIDAD ANDINA SIMÓN BOLIVAR

MAESTRIA EN DERECHO PENAL Y DERECHO PROCESAL PENAL

MATRIZ DE ESTUDIO DE CASO

Relación y contexto de los hechos	
CATEGORÍAS	**DESCRIPCIÓN**
Conductas que vulneraron el derecho de autodeterminación informativa	
Calidad de los sujetos que realizaron las conductas	
Tipo de dato afectado	
Medios utilizados	
Finalidad	
Principales derechos vulnerados	
Tipos penales que se aplicaron	
Observaciones	

ANEXO 4

FORMULARIOS DE VALIDACIÓN DE INSTRUMENTOS

UNIVERSIDAD ANDINA SIMÓN BOLIVAR
MAESTRÍA EN DERECHO PENAL Y DERECHO PROCESAL PENAL
VALIDACIÓN DE INSTRUMENTO: CUESTIONARIO

Marque en cada casilla, el criterio que corresponda evaluar

Objetivo: Proponer la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela del derecho de autodeterminación informativa.

Criterios a evaluar	Ítem 1		Ítem 2		Ítem 3		Ítem 4		Ítem 5		Ítem 6		Ítem 7		Ítem 8		Ítem 9		Ítem 10		Ítem 11		Ítem 12		Ítem 13	
	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
Claridad en la redacción de la pregunta																										
Claridad en la redacción de las opciones de respuesta																										
Inducción a respuesta (sesgo)																										
Redacción adecuada a la población en estudio																										
Contribuye con el objetivo de la investigación																										
Contribuye a evaluar el objeto de estudio																										

Consideraciones generales	**SI**	**NO**
La secuencia de los ítems es lógica		
La cantidad de los ítems es adecuada		

Consideraciones finales (agregar observaciones que considere importantes para el diseño del instrumento)

1.

2.

Nombre:……**Fecha**:…… ……**Firma**:……

UNIVERSIDAD ANDINA SIMÓN BOLIVAR
MAESTRÍA EN DERECHO PENAL Y DERECHO PROCESAL PENAL
VALIDACIÓN DE INSTRUMENTO: GUÍA DE ENTREVISTA

Marque en cada casilla, el criterio que corresponda evaluar

Objetivo: Proponer la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela del derecho de autodeterminación informativa.

Criterios a evaluar	Ítem 1		Ítem 2		Ítem 3		Ítem 4		Ítem 5		Ítem 6		Ítem 7		Ítem 8		Ítem 9		Ítem 10		Ítem 11		Ítem 12	
	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO	SI	NO
Claridad en la redacción de la pregunta																								
Inducción a respuesta (sesgo)																								
Redacción adecuada a la población en estudio																								
Contribuye con el objetivo de la investigación																								
Contribuye a evaluar el objeto de estudio																								

Consideraciones generales	**SI**	**NO**
La secuencia de los ítems es lógica		
La cantidad de los ítems es adecuada		

Consideraciones finales (agregar observaciones que considere importantes para el diseño del instrumento)
1.
2.

Nombre:……..**Fecha**:……**Firma**:……

UNIVERSIDAD ANDINA SIMÓN BOLIVAR
MAESTRÍA EN DERECHO PENAL Y DERECHO PROCESAL PENAL
VALIDACIÓN DE INSTRUMENTO: MATRIZ DE ANÁLISIS DE CASO

Marque en cada casilla, el criterio que corresponda evaluar

Objetivo: Proponer la incorporación de tipos penales referidos a la protección de datos personales en el Código Penal del Estado Plurinacional de Bolivia, para optimizar la tutela del derecho de autodeterminación informativa.

Criterios a evaluar	**Ítem 1**		**Ítem 2**		**Ítem 3**		**Ítem 4**		**Ítem 5**		**Ítem 6**		**Ítem 7**		**Ítem 8**		**Ítem 9**	
	SI	**NO**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**	**SI**	**NO**
Pertinencia en la inclusión de las categorías																		
Claridad en la redacción de las categorías																		
Claridad en la presentación de las categorías (organización)																		
Inducción a sesgo																		
Contribuye con el objetivo de la investigación																		
Contribuye a evaluar el objeto de estudio																		

Consideraciones generales	**SI**	**NO**
La secuencia de los ítems es lógica		
La cantidad de los ítems es adecuada		

Consideraciones finales (agregar observaciones que considere importantes para el diseño del instrumento)

1.

2.

Nombre:.....**Fecha**:.....**Firma**:.....