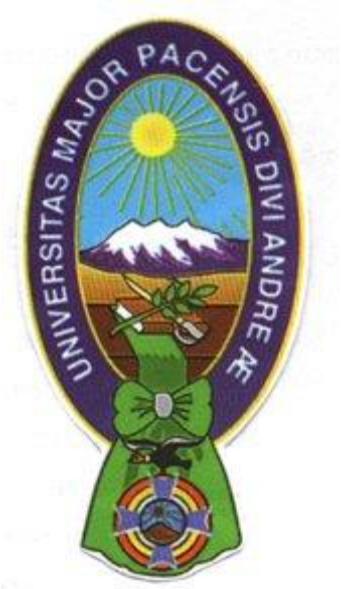
# UNIVERSIDAD MAYOR DE SAN ANDRES

## FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

## CARRERA DE DERECHO

## INSTITUTO DE INVESTIGACIONES Y SEMINARIOS




**TESIS DE GRADO**

# "LA DIFUSIÓN DE INFORMACIÓN ADMINISTRATIVA EN INTERNET Y LA REGULACIÓN DE PROTECCIÓN DE DATOS PERSONALES"

(TESIS PARA OPTAR EL GRADO LICENCIATURA EN DERECHO)

POSTULANTE: GISELLE ANDREA MOYA ROMERO

TUTOR: DR. FRANZ REMY CAMACHO

LA PAZ – BOLIVIA

2013

## DEDICATORIA

A Dios por estar a mi lado durante este proyecto y durante toda mi vida, a mi mami Lourdes mi papi Rodolfo por apoyarme y sacarme adelante en la vida, a mi hermana Janny por ser un ejemplo de vida profesional.

**AGRADECIMIENTOS**

A mis padres, familia, tutor y a la facultad de Derecho y Ciencias Políticas, Carrera Derecho.

## *RESUMEN ABSTRACT*

*El avance en relación a la tecnología y a la información, genera un tema interesante en nuestros días y los que siguen, puesto que en nuestras vidas, la tecnología ganó gran aceptación, convirtiéndose en un mecanismo mediante el cual, trabajamos, nos comunicamos, nos relacionamos, etc.*

*La presente investigación aborda un tema que es fundamental, la protección de los datos personales ante tales avances tecnológicos, pero, en relación a lo que la administración pública difunde como información mediante internet y sus sitios web.*

*La tecnología aunque beneficia en muchos aspectos nuestra vida, conlleva una serie de peligros mediante ciertas aplicaciones, que de alguna manera vulnerannuestra vida privada, y, al no existir una reglamentación para que el gobierno y sus instituciones relacionadas trabajen con sistemas de seguridad de información, nos enfrentamos a unalesión a nuestros derechos fundamentales.*

*Esta investigación analizóantecedentes sobre lo referido en nuestro país, demostrando un riesgo para nuestros derechos fundamentales, por lo que surge la propuesta de una ley que garantice la protección de los datos personales en internet abordando la difusión de información mediante sitios web.*

*Se demuestra de esta manera que el derecho y las telecomunicaciones deben ir de la mano, vale decir que las leyes deben surgir a la par de la realidad de nuestro país procurando de esta manera que el derecho ampare cualquier situación que vulnere derechos fundamentales ante el avance tecnológico, dentro de sus alcances.*

# INDICE GENERAL


| | |
|---|---|
| Dedicatoria | I |
| Agradecimientos | II |
| Resumen Abstract | III |
| DISEÑO DE INVESTIGACIÓN | 1 |
| 1. Enunciado del tema de la Tesis | 1 |
| 2. Identificación del Problema | 1 |
| 3. Problematización | 3 |
| 4. Delimitación del tema de la Tesis | 4 |
| 4.1. Delimitación Temática | 4 |
| 4.2. Delimitación Temporal | 4 |
| 4.3. Delimitación Espacial | 4 |
| 5. Fundamentación e Importancia del tema de la Tesis | 5 |
| 6. Objetivos del tema de la Tesis | 6 |
| 6.1. Objetivo general | 6 |
| 6.2. Objetivos específicos | 6 |
| 7. Marco de Referencia | 7 |
| 7.1. Marco Histórico | 8 |
| 7.2. Marco Teórico | 10 |
| 7.3. Marco Conceptual | 12 |
| 7.3.1. Administración Pública | 12 |
| 7.3.2. Difusión | 13 |
| 7.3.3. Información | 13 |
| 7.3.4. Digitalización | 13 |
| 7.3.5. Red internet | 13 |
| 7.3.6. Cesión Administrativa de Datos | 14 |
| 7.3.7. Publicación masiva | 14 |
| 7.3.8. Almacenamiento de Datos | 14 |
| 7.3.9. TratamientoInformático | 14 |

7.3.10. Almacenamiento Electromagnético de Datos Personales 15
7.3.11. Web 15
7.3.12. Ciberespacio 16
7.3.13. Intranet 16
7.3.14. ProcesoInformático 16
7.3.15. Telemática 16
7.3.16. Teleinformática 17
7.3.17. DerechoInformático 17
7.3.18. Software 17
7.3.19. Hardware 17
7.3.20. Navegador 17
7.3.21. Derechos Fundamentales 18
7.3.22. Datos Personales 18
7.3.23. Derecho a la Intimidad 18
7.3.24. Derecho al Acceso de Datos Personales 18
7.3.25. Derecho a la Información 19
7.4. MarcoJurídico 19
8. Hipótesis de Trabajo 19
8.1. Variables 19
8.1.1. Variable Independiente 19
8.1.2. Variable Dependiente 20
8.2. Unidades de Análisis 20
8.3. Nexo Lógico 20
9. Métodos y Técnicas a utilizarse en la Tesis 20
9.1. Métodos 20
9.1.1. Métodos Generales 20
9.1.2. Métodos Específicos 22
10. Técnicas utilizadas en la Tesis 22
10.1. Análisis Documental 22

**DESARROLLO DEL DISEÑO DE LA PRUEBA**


INTRODUCCIÓN 23

**CAPITULO I**

**MARCO HISTÓRICO** 25

1.1. Antecedentes históricos 25

1.2. Antecedentes e historia de los archivos y registros 25

1.2.1. Los archivos en la antigua Grecia y Roma 25

1.2.2. Los archivos en Egipto y otros pueblos 27

1.2.3. Los archivos en la Edad Media 29

1.2.4. Los archivos en la Era Imperial y la Edad Contemporánea 32

1.2.4.1. Los archivos públicos en la Revolución Francesa 34

1.2.4.2. La destrucción de los archivos de una memoria contemporánea 36

1.2.4.3. Los archivos contemporáneos 38

1.3. Antecedenteshistóricos en el entorno nacional 39

1.3.1. Breve reseña de los quipus 39

1.3.2. Los archiveros de los incas 42

1.3.3. Archivos en la época colonial 45

1.3.3.1. El escribano en la Colonia 47

1.3.3.2. El secreto de información 48

1.3.3.3. La corrupción del escribano 48

1.3.3.4. El libro becerro y el arca de las tres llaves 49

1.3.3.5. Las ordenanzas militares 50

1.4. Antecedentes de la identificación personal 51

1.4.1. La dactiloscopia 51

1.4.2. La cedula de identidad 52

1.4.3. La identificación personal 53

1.4.4. Evolución informática de la identificación personal en Bolivia 53

1.5. Evolución de la tecnología de almacenamiento de datos 54

1.5.1. Discos magnéticos rígidos 55

1.5.2. Computadores personales 56

1.5.3. UnidadZip 57
1.5.4. Discos compactos 58
1.5.5. DVD 58
1.6. Reseña histórica del habeas data o el derecho a la intimidad 59
1.6.1. Derecho a la intimidad y habeas data en Bolivia 62
1.7. Evolución del concepto de protección de datos 70

**CAPITULO II**
**MARCO TEÓRICO** 72
2.1. Noción de archivo 72
2.2. Archivo informático 72
2.3. Acceso a los archivos 74
2.4. Operaciones sobre los archivos 74
2.5. Organización de archivos 75
2.5.1. Archivos de texto 75
2.5.2. Archivo indizado 75
2.5.3. Identificación de archivos 76
2.5.4. Almacenamiento de archivos 77
2.5.5. Protección legal de los datos personales en archivos 77
2.6. Los datos 78
2.6.1. Los datos de carácter personal 78
2.7. El registro informático 79
2.8. Información 80
2.8.1. Derecho a la información 81
2.8.1.1. El derecho de la información como ordenamiento 81
2.8.1.2. El derecho de la información como ciencia 82
2.8.2. Acceso a la información 83
2.8.2.1. Acceso a la información pública 84
2.8.2.2. Acceso a la información y protección de datos personales 84
2.8.2.3. Sociedad informatizada 87

2.8.3. Seguridad de la información 88
2.8.4. Información clasificada 88
2.8.5. Información sensible de las personas 89
2.9. Derecho de acceso 90
2.10. La intimidad 90
2.10.1. Derecho a la intimidad 92
2.11. Habeas data 93
2.11.1. Etimología del habeas data 93
2.11.2. Concepto de habeas data 94
2.11.3. Objetivo del habeas data 94
2.11.4. Clasificación del habeas data 94
2.11.4.1. Habeas data informativo 95
2.11.4.2. Habeas data aditivo 95
2.11.4.3. Habeas data rectificador 96
2.11.4.4. Habeas data reservador 96
2.11.4.5. Habeas data cancelatorio, de supresión o exclusorio. 97
2.11.4.6. Habeas data impropio o publico 97
2.11.4.7. Habeas data impugnativo 98
2.11.4.8. Habeas data bloqueador 98
2.11.4.9. Habeas data disociador 98
2.11.4.10. Habeas data asegurador 98
2.11.5. Utilidades del habeas data 99
2.12. Acción de Protección de Privacidad 100
**CAPITULO III**
**MARCO CONCEPTUAL** 102
3.1. Datos personales 102
3.2. Datos sensibles 102
3.3. Datos no sensibles 103
3.4. Base de datos 103
3.5. Banco de datos 104

3.5.1. Base de datos públicos y privados 104
3.6. Autodeterminación informativa 105
3.7. Archivos informativos 105
3.8. Derecho a la honra 105
3.9. El honor 106
3.10. Derecho al honor 106
3.11. La reputación 106
3.12. Garantías constitucionales 106
3.13. Principio constitucional de garantía 107
3.14. Derecho objetivo 108
3.15. Derecho subjetivo 108
3.16. Petición 108
3.17. Derecho de petición 108
3.18. Privacidad 109
3.19. Derecho a la privacidad 109
3.20. Derecho a la imagen 111
3.21. Derecho a la identidad 112
3.22. Derechos humanos 113
3.23. Persona 113
3.23.1. Persona individual 113
3.23.2. Persona colectiva 114
3.24. Defacement 114
3.25. Bug 114
3.26. Hacker 115
3.27. Spam 115
**CAPITULO IV**
**MARCO JURIDICO** 116
4.1. Convenios y tratados internacionales de protección a los Derechos Humanos 116

4.1.1. Convención Americana sobre Derechos Humanos o Pacto de SanJose de Costa Rica 116
4.1.2. La Declaración Universal de los Derechos Humanos 118
4.1.3. Declaración Americana de los Derechos y Deberes del Hombre 119
4.1.4. Pacto Internacional de Derechos Civiles y Políticos 120
4.2. Ámbito Nacional- Legislación Boliviana 121
4.2.1. Nueva Constitución Política del Estado Plurinacional de Bolivia 121
4.2.1.1. El Código Civil 122
4.2.1.2. El Código Penal 123
4.2.1.3. Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación 124
4.2.1.4. Código Niño Niña Adolescente 124
4.2.1.5. Ley Nº 1488 de Bancos y Entidades Financieras 126
4.2.1.5.1 Recopilación de normas para Bancos y Entidades Financieras por la Autoridad de Supervisión del Sistema Financiero ASFI 127
4.2.1.6. Ley de Imprenta 128
4.2.1.7. Estatuto del Funcionario Público Administrativo 129
4.2.1.8. Decreto Supremo 28168 Acceso a la Información Pública 130
4.3. Legislación comparada 131
4.3.1. Argentina 131
4.3.2. Colombia 133
4.3.3. Perú 134
4.3.3.1. Ley de protección de Datos Personales ley N° 2973 135
4.3.4. Uruguay 137
4.3.5. Unión Europea 138
4.3.5.1. Alemania 142
4.3.5.2. España 145
4.4. La Red Iberoamericana de Protección de Datos Personales 146
4.4.1. Países miembros de la red iberoamericana de protección de datos personales 147

**CAPITULO V**

**MARCO PRÁCTICO** 149

5.1. Propuesta normativa 149

5.1.1. Derecho y la tecnología 149

5.1.2. Motivos que inducen a desarrollar una legislación de protección de datos personales en internet 151

5.1.3. Necesidad y mecanismos de protección de los datos personales en registros públicos 157

5.1.3.1 Mecanismos 157

5.1.3.1.1. Agencia de Protección de Datos de Carácter Personal y el Registro General de Protección de Datos Personales Públicos 157

5.1.4. Propuesta de Ley 159

Exposición de motivos 159

PROYECTO DE LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SUJETOS A ADMINISTRACIÓN PÚBLICA EN INTERNET 162

CONCLUSIONES 176

RECOMENDACIONES 177

BIBLIOGRAFIA IV

ANEXOS

# DISEÑO DE INVESTIGACIÓN

## 1.- ENUNCIADO DEL TEMA DE LA TESIS

### “LA DIFUSIÓN DE INFORMACIÓN ADMINISTRATIVA EN INTERNET Y LA REGULACIÓN DE PROTECCIÓN DE DATOS PERSONALES”

## 2.- IDENTIFICACIÓN DEL PROBLEMA

La introducción de nuevas tecnologías de la información en el mundo actual globalizado y la utilización de la Red Internet como medio masivo de comunicación, tienen incidencia notable en el campo de la publicidad de la actividad administrativa, y se expresa en aspectos relativos a los derechos de acceso a los archivos administrativos o a la protección de datos personales que existen sobre ellos.

Las existencia de modernas redes de comunicación electrónica de las que el Internet es un paradigma indudable, permiten reflexionar sobre la creación de una regulación jurídica de la actividad de información y comunicación de las Administraciones Publicas ante el avance tecnológico, con miras a crear una norma del estado sobre la administración digital, es decir regular jurídicamente el acceso a datos y documentos por vía telemática y la relación de ambos aspectos con el respeto a la protección de determinados derechos ciudadanos.

Ciertos derechos relacionados con la información en poder de la Administración Pública, como son los de autodeterminación informativa y de acceso a archivos administrativos pueden ser de caracteres personales. El derecho debe adecuarse con prontitud a los fenómenos sociales que ha de regular, fenómenos como la Red Internet suponen un verdadero cambio y reto a la vez en el modo en que se producen las relaciones humanas.

La Red Internet y otros medios telemáticos de difusión de información, ayudan a satisfacer necesidades de mejor accesibilidad a la misma, sin que, éste deba afectar el normal funcionamiento de la actividad en este caso administrativo. Hoy en día la mayor parte de los datos que obran en los archivos y registros públicos se encuentran digitalizados, ya sea por razones de organización, espacio, modernización, etc. en este caso será necesario también normar jurídicamente su protección y tratamiento a excepción de que se trate de un documento o datos que solo puedan ser consultados previa acreditación de una determinada posición jurídica.

Cabe recalcar nuevamente que la protección de los datos personales dentro de un sistema informático de determinada administración o institución pública debe contener una serie de formalidades en cuanto a mecanismos de seguridad generando plena confiabilidad a momento de realizar la toma y registro de ciertos datos, precautelando la integridad del dato personal ante posibles ataques de manipulación informática.

Las ventajas que ofrece la red internet como medio de comunicación deben ser debidamente resaltadas en contraposición a los mecanismos basados en la presencia física del ciudadano en las oficinas administrativas a fin de valorar la versatilidad administrativa. En efecto la red internet ofrece mayor accesibilidad a la información debido a que evitan al administrado mayor desplazamiento innecesario a la oficina pública, largas colas de espera, en su caso la posibilidad de almacenar en su propio equipo información o datos y documentos, por tanto el ejercicio del derecho de acceder por parte del ciudadano a esta información digitalizada, por el ente administrativo no se encuentra condicionado en la medida en que la oficina administrativa virtual siempre se encuentra abierta permanentemente y permite una mayor flexibilidad en las relaciones con la Administración Publica que supera las rigidez horaria propia de la burocracia.

La implementación de sistemas telemáticos de comunicación con los administrados permite una mejor organización de los medios personales de manera que, en lugar de llevar a cabo una tarea material de escasa complejidad como es la de proporcionar acceso a los documentos y archivos puedan dedicarse a tareas de mayor importancia. La información por vía telemática, garantiza una mayor rapidez en el acceso, por cuanto la misma puede encontrarse a disposición desde el mismo momento en que se

genere y su consulta se autorice por el órgano competente, lo que en última instancia garantizaría asimismo la plena actualización de los datos así obtenidos.

Los inconvenientes a que puede enfrentarse la Administración Pública para evitar una imagen distorsionada de la realidad, cuando ofrezcan la información en línea, son el riesgo evidente de que se sobrecarguen sus sitios al ofrecer tal cantidad de información, o la posibilidad de que los datos encontrados en la misma sea manipulada o de lo contrario alterada con otro fin a la cual ha sido creada, por lo que será necesario también adoptar medidas técnicas para garantizar la integridad de la información ante los peligros que acechan en una red abierta como la internet, debiendo condicionarse el acceso debido a limitaciones subjetivas basadas en la existencia de una determinada relación entre el sujeto activo del derecho y el objeto el mismo, esto es que los datos o información que se desee conocer sean previamente autorizados, mediante una determinada regulación jurídica. Por último la necesaria publicación de la información administrativa y en especial aquella que venga referida a personas identificadas o identificables en datos de carácter personal y su respectiva regulación constituye un verdadero desafió dadas las enormes posibilidades de recogida y sistematización que presenta la internet, de ahí que deben adoptarse medidas que permitan una oportuna difusión de la información, y al mismo tiempo impidan o limiten la libre recogida de datos.

En definitiva abordaremos el problema de la protección de la intimidad y de los datos personales previstos constitucionalmente frente al abuso y manipulación de páginas o sitios de internet, garantizando de esta manera la participación activa del administrador proporcionando de manera obligatoria la seguridad necesaria, para que este tipo de hechos no afecten a los titulares de los datos personales.

## 3.- PROBLEMATIZACIÓN

- ¿Existirá una regulación jurídica que contemple las medidas de seguridad y el tipo de control que ejerce el estado, sobre los registros públicos en relación a la protección de los datos personales?

- ¿Podrá ser que una adecuada regulación de la difusión de información administrativa prevenga la vulneración de datos personales?
- ¿Existirá una vulneración de datos personales en la red internet?
- ¿Cuál es la clasificación de los datos personales para el acceso a todos los registros públicos en Bolivia?
- ¿El acceso a la información pública mediante internet podrá generar algún peligro para los datos de carácter personal que puedan estar inmersos dentro de los sistemas que se encargan de publicarlos?
- ¿Cuál podrá ser la estructura que debe contener la regulación para la protección de datos personales y qué derechos deberán estar comprendidos en el ámbito de la privacidad e intimidad en los registros públicos?

# 4.- DELIMITACIÓN DEL TEMA DE LA TESIS

## 4.1.- DELIMITACIÓN TEMÁTICA

La delimitación temática especifica se la considera al estudio y análisis de la difusión e información administrativa por la red internet y la necesidad de regular la protección de los datos personales, el tema de investigación requiere de un conjunto de elementos teórico conceptuales de carácter jurídico relacionados básicamente con el Derecho Informático, Derecho Civil, y especialmente el Derecho Constitucional, por tanto es de carácter jurídico.

## 4.2.- DELIMITACIÓN TEMPORAL

El estudio de la problemática procesal se efectuó en el espacio comprendido en los años 2008 a la actualidad, tiempo susceptible de información de datos sobre actos de acceso administrativo, que en su momento serán de gran utilidad.

## 4.3.- DELIMITACIÓN ESPACIAL

Con respecto al espacio geográfico tomare en cuenta a l territorio boliviano, como

modelo de investigación consideraré a la ciudad de La Paz, porque en ella se encuentran las instituciones y entidades administrativas gubernamentales que tienen entera relación con la problemática en sus sitios web.

## 5.- FUNDAMENTACIÓN E IMPORTANCIA DEL TEMA DE LA TESIS

En los tiempos actuales, y como efecto de la globalización y el uso de nuevas tecnológicas o sociedades de la información, conllevan a una modernización sin precedentes, por lo que se trata de buscar el camino para que la relación entre derecho y nuevas tecnologías de la comunicación se convierta en una coexistencia pacífica y armónica, quizá no tanto en el ámbito del Derecho Sustantivo, sino como una vez más en el del Derecho Constitucional, en el que debemos encuadrar el tema que nos ocupa.

Es necesaria una orientación normativa sobre la articulación en nuestra legislación sobre el derecho de acceso a los documentos administrativos que, es una expresión del principio de transparencia de la acción administrativa, frente a la protección o divulgación por difusión de información administrativa por la red internet, así como frente a la protección de los datos personales ante injerencias usando el internet como un medio para realizar manipulaciones indebidas.

Es necesario delimitar la regulación de derechos de acceso a la información, y la de acceso a los documentos públicos, y una consideración imprescindible a la protección de los datos personales que a través del titular de los datos, se podrá desplegar un seguimiento sobre los datos relativos a su persona consintiendo cabalmente tal derecho en la posibilidad de conocimiento de los datos, que, afectándole, obren en poder de otro sujeto, no necesariamente de la Administración Pública.

El derecho de acceso a los documentos administrativos, tiene por objeto obtener determinada información que puede o no ser personal, pero en el caso que lo sea, estará vinculada a una tercera persona. Cuando el acceso a los documentos

administrativos afecte informaciones personales, deberá ser regulado, puesto que tenemos el derecho a mantener la reserva de nuestra información personal cualquiera que sea la forma de tutela que tal derecho adopte, intimidad o protección de datos, y ésta deberá ser mediada por la Administración Pública titular de los documentos cuyo conocimiento se pretende, instaurándose así un vínculo trilateral en el marco de un procedimiento administrativo típico. Pero a medida en que este acceso a la información es mediado, se debe otorgar protección y garantías durante el desenvolvimiento de este procedimiento, lo que llevará indirectamente a una participación activa del Estado, al exigir por norma un adecuado sistema de protección informático.

# 6.- OBJETIVOS DEL TEMA DE LA TESIS

## 6.1.- OBJETIVO GENERAL

Explicar mediante la investigacion cientifico – doctrinal en la normatividad del derecho o la ciencia jurídica, mas concretamente en el Derecho Informatico el Derecho Civil y el Derecho Constitucional, los limites de la difusión de información administrativa en internet en cuanto ala protección de los datos personales, el resguardo de la información, la eficiencia de estos nuevos medios tecnologicos, y el acceso a la información administrativa.

## 6.2.- OBJETIVOS ESPECÍFICOS

- Demostrar la necesidad de implementar una regulación jurídica para la protección de datos personales en toda información administrativa realizada por medios masivos como la red internet.
- Demostrar que ante la ausencia de normativa legal de protección a los datos personales en la difusión de información administrativa en internet, urge una necesidad de regular este aspecto especialmente como una garantía de los derechos constitucionales.
- Analizar la difusión masiva de información administrativa por los entes públicos y si estos son responsables ante vulneraciones de los datos personales que se

encuentran registrados en sus sistemas de información.

- Determinar los lineamientos jurídicos regulatorios de algunos países con relación al nuestro en cuanto a la protección de datos personales.
- Demostrar la necesidad de reglamentar la protección de datos de carácter personal dentro de las páginas web de administraciones públicas en internet frente a la difusión de información que realizan estos.

## 7.-MARCO DE REFERENCIA

Frente a una nueva sociedad de la información y el avance de nuevas tecnologías infotelemáticas de la comunicación, la difusión de información por medios masivos como la red internet es evidente, de tal manera que la administración pública no puede quedar al margen. Por lo que siendo que se encamina hacia la informatización y digitalización de la información, para posibilitar el empleo de la informática a objeto de transformar sustancialmente la organización y el funcionamiento de su actividad pública, se presenta en el camino retos y obstáculos para perfeccionar la aplicación de las comunicaciones electrónicas y de los llamados medios de información, no viendo la posibilidad también de establecer sistemas de conservación y protección de la información administrativa, como un medio para crear vehículos seguros de transmisión y recepción de información para los ciudadanos. Contemplar el uso de medios técnicos, electrónicos, informáticos y telemáticos, compatibles entre sí, para que tanto los órganos administrativos como las personas que demanden ante ellos servicios de información obtengan un servicio rápido eficiente y altamente confiable, es un paso hacia la modernización, empero en esa tarea de informatizar la información, la administración pública debe precautelar los datos personales especialmente protegidos y que este servicio de información no afecte los derechos de los ciudadanos.

Dentro de una sociedad donde la información y la tecnología ingresa a un contexto internacional globalizado de vertiginoso avance, es un hecho notorio la progresiva incorporación de la misma, en ramasy actividades de nuestra vida: economía, sociedad, derecho, administración.

## 7.1.- MARCO HISTÓRICO

Debemos considerar el desarrollo de la tecnología desde los inicios y el cambio que producirá en las sociedades futuras el uso masivo de la Internet. Una nueva infraestructura en las comunicaciones ha surgido a lo largo y ancho del mundo. La infraestructura anterior, animada por la Revolución Industrial, fue el transporte; las de la sociedad post industrial han sido el cable, la banda de amplia frecuencia, la televisión digital, la fibra óptica, el fax y el correo electrónico, por ejemplo. Hoy día Internet y la red mundial (World Wide Web) han crecido en menos de cinco años a un ritmo sin precedentes en la historia de las comunicaciones; ningún adelanto previo había invadido tan rápidamente las conciencias y había asegurado tan amplia acogida pública.

Internet se originó hace unos veinte años a partir de la iniciativa por parte del Ministerio de Defensa de los Estados Unidos para enlazar la investigación militar por medio de una red interactiva llamada Arpanet. Las computadoras, no la red, eran las responsables de garantizar la comunicación; en suma, toda computadora podía "hablar" con cualquier otra. Más o menos al mismo tiempo, las redes de zonas restringidas (LAN) se desarrollaron; en lugar de conectar sus equipos a enormes computadoras centrales a tiempo parcial, como había sucedido antes, las empresas y las organizaciones conectaron toda la red de zona restringida a la Arpanet. Los siguientes pasos se dieron cuando la Fundación Nacional para la Ciencia de Estados Unidos (NSF) creó cinco centros con supercomputadoras en las universidades más importantes y decidió desarrollar su propia red.

En noviembre de 1991 el Congreso de los Estados Unidos creó la Red Nacional de Investigación y Educación (NREN), para llevar el servicio a las instituciones educativas y científicas. Es importante destacar que la NREN es una red interna de redes lógicas y autónomas, y no un sistema gestionado centralmente, por lo cual tenía la flexibilidad y la capacidad de desarrollarse y ampliarse de acuerdo con la necesidad de los usuarios. Los siguientes pasos lógicos consistieron en llevar Internet directamente al hogar

gracias a empresas privadas por una cuota mensual. Internet es entonces, simplemente, una red de redes a disposición del que cuente con un navegador.

Hoy día están vinculadas sesenta millones de computadoras, y decenas de millones de usuarios en más de cien países. Al ritmo actual de crecimiento, muy pronto estarán conectados cien millones de equipos. Todo individuo que "navegue" en la red, es decir, que busque sitios específicos para obtener información distinta, puede sentirse abrumado por semejante avalancha. Internet y la nueva infraestructura de comunicaciones difieren radicalmente de las de la década anterior. En la actualidad disemina la circulación de las noticias, del chisme y del rumor y por ello enfatiza la novedad y el escándalo. Pone al alcance los recursos culturales de la humanidad con una minuciosidad nunca antes conocida. Multiplica a los grupos afines a través de las fronteras nacionales. Transforma la naturaleza de los "guardabarreras"; quienes determinan o modifican los gustos de los individuos pertenecientes a un círculo de ideas afines, los cuales adoptan o rechazan nuevos estilos, productos y pasatiempos cómo las redes sociales que incluso imponen una moda.

En los últimos doscientos años la tecnología ha sido el agente de cambio de la vida moderna y sus estructuras sociales, ha transformado la naturaleza de las ocupaciones, las relaciones de la gente y se ha constituido en el medio del crecimiento económico. Sin embargo, se suele emplear el término tecnología de un modo indiscriminado, a pesar de los profundos cambios en el carácter de ésta y en sus distinciones. Para casi todas las personas la tecnología implica máquinas o modalidades mecánicas —mecanismos que desde luego aún existen—, pero la nueva tecnología de las comunicaciones y computadoras —que constituye el fundamento de la sociedad post industrial— es una tecnología intelectual, con raíces y modalidades de aprendizaje muy distintas comparadas con las de la tecnología anterior. Hoy la ciencia jurídica no puede quedar rezagada ante estos avances de la tecnología y corresponde normar y regular la incidencia de estos medios masivos de comunicación en la protección y tutela de los derechos de las personas, mediante la generación de mecanismos jurídicos para este cometido.

## 7.2.- MARCO TEÓRICO

Dentro de la presente investigación se tomará en cuenta el siguiente Marco Teórico:
La privacidad es un término que va más allá de la intimidad, que es ya un término más conocido y usado en la sociedad en general. La privacidad se compone por un sinfín de facetas del individuo, que tratadas de manera conjunta, máxime por medios informáticos, pueden llegar a constituir un perfil que el mismo individuo, titular de esos datos aislados, desconoce, y, por tanto, no controla.
La transformación tecnológica propia del día a día, propicia a que la intimidad o la privacidad de información o datos personales, sea vulnerada, por lo que la reacción propia del autor idealiza una protección de sus datos, que es un derecho fundamental ,inevitable, para que la información se encuentre, resguardada, y no pueda ser robada o extraída, para usos ilegales.

Existe un principio del consentimiento, por el que el titular de los datos es el único que tiene derecho a decidir quién, cómo cuándo y para qué se tratan sus datos. Este principio no se encuentra detallado, sino que se define sólo en relación con la fase en la que los datos se transfieren a un tercero, es decir, cuando se produce la cesión o comunicación de datos a terceros, en la que el titular pierde, en su caso, aún más el control sobre su información personal. Por lo que es necesaria la existencia de una regulación jurídica que determine el uso y acceso de la información administrativa y la protección de los datos personales lo cual permita que los sujetos obligados – los terceros autorizados-no difundan, distribuyan o comercialicen los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones u obtenidos de manera indiscriminada, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

La información, o los datos que se recaban o que se registran en un sistema de datos personales, deben ser exactos, mantenida al día, apropiada para el fin para el que fue almacenado y obtenida por medios légales.

El principio de seguridad en el tratamiento de datos personales tiene una premisa, la cual tiene un fin en específico:

- Evitar el desvío de la información, mal intencionadamente o no, hacia sitios.
- Evitar el conocimiento de personas ajenas, un tercero.
- Garantizar la integridad de los datos personales evitando su alteración, pérdida, transmisión y manipulación, generando de esta manera un principio de respeto a los derechos del afectado, asegurando confidencialidad.

La normativa prevé la existencia de ciertos derechos de los titulares de dichos datos en los que se concretan ciertos principios, como instrumento propicio para controlar el tratamiento que, de sus datos personales, haga el responsable del sistema de datos personales, y, en su caso, instarle a modificar o suprimir aquellos datos cuyo tratamiento no resulte procedente, así como a conocer qué información se está tratando sobre su persona.

En consecuencia los datos constituyen un antecedente que una persona tiene de sus actos, tanto personales, académicos, familiares, económicos, políticos, sociales y jurídicos, por cuanto por Dato debemos entender, que es aquel producido naturalmente en el cotidiano que hacer de la sociedad, se recolectan, almacenan con el objeto de protegerlos y usarlos en la elaboración de un producto llamado información.

Estos datos constituyen una representación de la persona y establecen lo que le interesa transmitir, una información o un mensaje almacenados en registros archivos o bases de datos que generen información, existiendo una diferencia entre datos personales íntimos y datos personales de alcance público. El Dr. José Alfredo Arce, señala: que dato es: “una representación de una porción de la realidad social expresada en términos que forman parte de un código preestablecido de manera que pueda ser interpretado y que está destinado a ser información”. Así pues los Datos Públicos, son aquellos que tienen menor importancia y que son de fácil obtención, es decir que se encuentran casi a disposición de todos, ejemplo: Nombre, domicilio, número de cédula de identidad, teléfono, registro de contribuyentes etc.; en cambio datos privados o reservados, son los denominados también información sensible, referida a cuestiones intimas del individuo, raciales, religiosas, costumbres sexuales,

opiniones, estado de salud, etc., cuyo conocimiento o divulgación puede provocar discriminación al titular de esos datos y son los que requieren de mayor protección.

El acceso a datos es la facultad que tiene una persona de requerir que se ponga en su conocimiento la existencia de datos personales en determinados registros, bases de datos, ficheros automatizados, etc. y para que dicho requerimiento resulte efectivo y de la manera más eficaz, deberá obtener dicha información, dentro de límites determinados, soporte electrónico, papel, visualizaciones, pantallas u otros medios, siendo los registros anotación o inscripciones de información que por ser relevantes deben ser conservadas adecuadamente, como por ejemplo los nacimientos, defunciones y los matrimonios.

Frente al avance de la tecnología debemos tener en cuenta que nuestros datos ya han comenzado a circular de manera indiscriminada o no, y nosotros no tenemos conocimiento de donde se encuentran, quien los almacena, los usa, los traslada o los hace públicos sin nuestro conocimiento, todo esto es a consecuencia de la falta de información sobre lo que puede ocurrir si nosotros mismos no protegemos nuestros datos personales o peor aún, nuestros datos personales no son precautelados por el estado el cual nos tiene en desamparo ante los abusos que una red abierta como el internet puede ocasionar a nuestra persona o familia, como sujetos de derecho y base social.

## 7.3.- MARCO CONCEPTUAL

### 7.3.1.- ADMINISTRACIÓN PÚBLICA

Es una organización que el Estado utiliza para canalizar adecuadamente demandas sociales y satisfacerlas, a través de la transformación de recursos públicos en acciones modificadoras de la realidad, mediante la producción de bienes, servicios y regulaciones.

### 7.3.2.- DIFUSIÓN

Es la acción y efecto de difundir (propagar, divulgar o esparcir). El término, que procede del latín diffusio, hace referencia a la comunicación extendida de un mensaje.

### 7.3.3.- INFORMACIÓN

Es un conjunto organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente, asimismo permite resolver problemas y tomar decisiones, ya que su uso racional es la base del conocimiento.
Por otro lado, otra perspectiva nos indica que la información es un fenómeno que aporta significado o sentido a las cosas, ya que mediante códigos y conjuntos de datos, forma los modelos del pensamiento humano.

### 7.3.4.- DIGITALIZACIÓN

Es la operacion mediante la cual se convierte una imagen en una serie de códigos binarios que representan cada uno de los puntos de su estructura y que, de esta forma, puede ser almacenada en un ordenador. Asi pues, se trata de la conversión de una imagen analgica en un conjunto de valores numéricos digitales. Los dispositivos caractersticos para esta operacion son: los escaners, las tabletas graficas y las videocamaras. En todos estos casos, la información puntual recibida llega a la memoria del ordenador y se va utilizando despues para el tratamiento y salida subsiguiente.

### 7.3.5.- RED INTERNET

El término genérico "red" hace referencia a un conjunto de entidades (objetos, personas, etc.) conectadas entre sí. Por lo tanto, una red permite que circulen elementos materiales o inmateriales entre estas entidades, según reglas bien definidas de tal manera que la red internet es la interconexión de redes informáticas que permite a las computadoras conectadas comunicarse directamente. El término suele referirse a una interconexión en particular, de carácter planetario y abierto al público, que conecta redes informáticas de organismos oficiales, educativos y empresariales. También

existen sistemas de redes más pequeños llamados intranet, generalmente para el uso de una única organización.

### 7.3.6.- CESION ADMINISTRATIVA DE DATOS

Es toda revelación de datos realizada por persona distinta del interesado en el margen de la via adminstrativa. Este concepto es muy amplio, puesto que revelación abarca tanto la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma que facilite el acceso a los datos de un fichero a un tercero, distinto del interesado.

### 7.3.7.- PUBLICACIÓN MASIVA

Acción y efecto de publicar mediante cualquier medio de difusión de información de manera extensiva o en algún medio de consulta frecuente de información.

### 7.3.8.- ALMACENAMIENTO DE DATOS

Es la acción de guardar física o virtualmente archivos e información de todo tipo. Más específicamente en la informática, las unidades de almacenamiento serán todos aquellos dispositivos, internos o externos, que almacenan la información de un sistema dado. Los dispositivos diferirán entre sí en forma, tamaño y uso, pero en conjunto todos contribuyen a la conservación de datos relevantes para el usuario en formato digital.

### 7.3.9.- TRATAMIENTO INFORMÁTICO

Son las operaciones que las personas hacemos con la información. Estas operaciones pueden ser muy variadas, por ejemplo: lectura, escritura, copia, traducción, transmisión, ordenación, clasificación, comparación, archivo, cálculo, análisis, síntesis.

Por otra parte este tratamiento de la información, omnipresente en todas las actividades humanas, lo podemos realizar nosotros directamente o con la ayuda de

determinados instrumentos y máquinas: máquinas de escribir, calculadoras, ordenadores.

### 7.3.10.- ALMACENAMIENTO ELECTROMAGNÉTICO DE DATOS PERSONALES

Se trata de aquellos dispositivos que son capaces de guardar datos personales por medio de bobinas electromagnéticas (cabezas), en su superficie (cintas ó discos), ya que cuentan con una gran cantidad de partículas magnéticas recubiertas de una película de pintura especial que las protege. Estos dispositivos tienen mecanismos que producen fricción y calor, por lo que con el tiempo sufren desgaste, además si son expuestos a campos electromagnéticos intensos, humedad ó movimiento brusco pueden sufrir la pérdida de datos.

### 7.3.11.- WEB

Es un vocablo inglés que significa “red”, “telaraña” o “malla”. El concepto se utiliza en el ámbito tecnológico para nombrar a una red informática y, en general, a Internet.
El término, de todas formas, tiene varios usos. Además de nombrar a Internet en general, la palabra web puede servir hacer mención a una página web, un sitio web o hasta un servidor web.

Una página web es un documento que incluye un archivo HTML con texto, imágenes, videos, animaciones Flash, etc. Al conjunto de páginas web que suelen formar parte del mismo dominio o subdominio de Internet se lo conoce como sitio web. Dentro del sitio web, todas las páginas guardan alguna relación entre sí y están vinculadas mediante vínculos (también conocidos como enlaces, hipervínculos, hiperenlaces o links).

El servidor web, por otra parte, es un programa creado para transferir páginas web a través de la implementación del protocolo HTTP. Por extensión, se denomina servidor a la computadora donde se ejecuta dicho tipo de software.

### 7.3.12.- CIBERESPACIO

El auge de las comunicaciones entre ordenadores –cuyo máximo exponente es la macrored mundial Internet- ha creado un nuevo espacio virtual, poblado por millones de datos, en el que se puede «navegar» infinitamente en busca de información. Se trata, en una contracción de cibernética y espacio, del ciberespacio.

### 7.3.13.- INTRANET

Es una red de ordenadores privada basada en los estándares de Internet, utiliza tecnologías de Internet para enlazar los recursos informativos de una organización, desde documentos de texto a documentos multimedia, desde bases de datos legales a sistemas de gestión de documentos. Las Intranets pueden incluir sistemas de seguridad para la red, tablones de anuncios y motores de búsqueda. Una Intranet puede extenderse a través de Internet. Esto se hace generalmente usando una red privada virtual.

### 7.3.14.- PROCESO INFORMÁTICO

En la informática, un proceso es un concepto manejado por los sistemas operativos, que está compuesto por las instrucciones de un programa destinados a ser ejecutadas por el microprocesador, su estado de ejecución, en un determinado momento dado su memoria de trabajo y otras informaciones.

### 7.3.15.-TELEMÁTICA

Conjunto de métodos técnicas y servicios que resultan del uso conjunto de la informática y las telecomunicaciones asimismo es la transmisión de datos a distancia entre y por medio de ordenadores. Comunicación de datos mediante equipos informáticos transmisión de datos entre personas utilizando el ordenador de por medio.

### 7.3.16. TELEINFORMÁTICA

Utilización de los medios de comunicación para intercambiar información a través de las computadoras, con los sistemas informáticos que requieran para ello.

### 7.3.17.- DERECHO INFORMÁTICO

Conjunto de normas positivas referidas al tratamiento automatizado de la información en sus múltiplesaspectos. Es aquel estudio que se realiza a todos esos fenómenos informáticos vinculados con las esferas del derecho.

### 7.3.18.- SOFTWARE

Serie de programas de computación que se distribuyen conjuntamente.Está formado por una serie de instrucciones y datos, que permiten aprovechar todos los recursos que el computador tiene, de manera que pueda resolver gran cantidad de problemas. Un computador en sí, es sólo un conglomerado de componentes electrónicos; el software le da vida al computador, haciendo que sus componentes funcionen de forma ordenada.
El software es un conjunto de instrucciones detalladas que controlan la operación de un sistema computacional.

### 7.3.19.- HARDWARE

Elementos físicos de la arquitectura de un ordenador, desde la CPU hasta el monitor, pasando por todos los periféricos que pueden ser acoplados al ordenador.

### 7.3.20.- NAVEGADOR

Aplicación que permite visualizar la información que contienen las páginas web de internet, escritas generalmente en formato HTML.

### 7.3.21.- DERECHOS FUNDAMENTALES

Se entienden por derechos fundamentales aquellos derechos de los cuales es titular el hombre por el mero hecho de ser hombre. Es decir, que son poseídos por todo hombre, cualquiera que sea su raza, condición, sexo o religión. Tiene las siguientes denominaciones: derechos humanos, derechos del hombre, derechos de la persona humana. Se emplea, en fin, el término derechos fundamentales. Los derechos fundamentales constituyen para los ciudadanos la garantía de que todo el sistema jurídico y político se orientará hacia el respeto y la promoción de la persona humana.

### 7.3.22.- DATOS PERSONALES

Son cualquier información concerniente a personas físicas identificadas o identificables (nombre, apellidos, dirección, dirección de e-mail, documentos de identidad, etc.).

### 7.3.23.- DERECHO A LA INTIMIDAD

Es aquel derecho que tiene toda persona de hacer conocer o no cierta información que le pertenezca a solo y exclusivamente ella, es decir que, de la misma forma en que el hombre nace libre físicamente, tiene la libertad de dar a conocer de sí mismo, a la sociedad lo que su voluntad le sugiera. Esta consideración encuentra una explicación bipolar, ya que por un lado puede tratarse de la inseguridad que representa el almacenamiento, ensayo, recopilación o transmisión de datos, en las redes internas de las empresas publicas o privadas, así como de la misma red mundial, o bien, a pesar de la seguridad, debido al ingenio que poseen personas que por diversas razones se aplican en la manipulación de sistemas informáticos ajenos, ya sea por una u otra de las alternativas, la intimidad de las personas se ve conculcada.

### 7.3.24.- DERECHO AL ACCESO DE DATOS PERSONALES

El derecho de acceso consiste en la facultad de una persona de conocer o interesarse por conocer los datos personales suyos en posesión de un responsable o titular de datos personales**.** Mediante el derecho de acceso, el particular solicita, siguiendo un

procedimiento, información al titular o responsable del fichero de datos, sobre qué datos tiene y cómo los han obtenido.

#### 7.3.25.- DERECHO A LA INFORMACIÓN

El derecho a la información es una garantía individual de carácter social, y para ello se debe definir la información, que es el intercambio de ideas, la comunicación de acontecimientos, pensamientos, sentimientos, etcétera. La comunicación de la información puede ser masiva o de "*difusión*" o puede ser comunicación interpersonal.

### 7.4.- MARCO JURÍDICO

En el marco jurídico, para el estudio del tema, se tomaran en cuenta los siguientes preceptos jurídicos:

- Nueva Constitución Política del Estado
- Leyes y tratados internacionales relativos al tema de investigación.

## 8.- HIPÓTESIS DE TRABAJO

"La regulación jurídica de la protección de datos de carácter personal en la difusión de información por la administración pública en la red internet,mediante sus sitios web, como supuesto de comunicación del Estado, protegerá los derechos del ciudadano en el marco del respeto evitando una violación a los derechos fundamentales y convenios internacionales".

### 8.1.- VARIABLES

#### 8.1.1.- VARIABLE INDEPENDIENTE

"Una apropiada regulación Jurídica de los datos personales en la difusión de información por la administración pública, en la red internet como supuesto de comunicación del Estado".

### 8.1.2.- VARIABLE DEPENDIENTE

"…protegerá los derechos del ciudadano en el marco del respeto evitando una violación a los derechos fundamentales y convenios internacionales".

## 8.2.- UNIDADES DE ANÁLISIS

- La necesidad de adecuar la legislación nacional para lograr una respuesta eficaz ante los cambios introducidos por las nuevas tecnologías de la información y la comunicación en las prácticas administrativas, especialmente en la difusión masiva publica de información en sitios web o digitalización de datos o documentos públicos, procurándoles la mayor protección posible.
- El impacto, tecnológico es ineludible por ende es necesario adecuar el derecho a este avance tecnológico.
- Determinar la necesidad de incorporar mecanismos jurídicos que regulen en el marco de aplicación de los recursos tecnológicos de comunicación, el respeto a los datos personales a la intimidad de los ciudadanos.

## 8.3.- NEXO LOGICO

El elemento o vínculo en la hipótesis empleada está dado por las palabras: "Protegerá" y "Evitando".

# 9.- MÉTODOS Y TÉCNICAS A UTILIZAR EN LA TESIS

## 9.1.- MÉTODOS

### 9.1.1.- MÉTODOS GENERALES

**MÉTODO DIALECTICO:**Al presenciar desde hace unos años el avance casi diario de las tecnologías de información y comunicación, convirtiéndose su uso en una realidad indelegable en nuestras vidas, procura una relación estrecha con la problemática de nuestro tema, lo que conlleva a utilizar de manera general el método denominado dialectico.

“Al interpretar de una manera comprensiva la realidad relacionándola con la problemática”[1], estamos frente a este método.

El cumplimiento y demostración de la hipótesis y del objetivo general, depende esencialmente de tomar en cuenta la realidad en la que esta sumergida el tema, siendo en este cado el avance se la tecnología, desencadenando una serie de vacíos jurídicos con los cuales ante una desmedro de nuestros derechos podríamos hacerlos valer, por lo que analizando el problema de la inexistencia de una norma en el ordenamiento jurídico vigente que vele por un interés que debe ser protegido mediante una ley específica, estamos frente a una investigación dialéctica. Si bien existen tratados internacionales a la pare de nuestra constitución, no es suficiente tenerlos como referencia sino que es menester establecer la importancia de la protección de un derecho del ser humano.Para su interpretación se seguirán reglas argumentativas universales de la ciencia jurídica. En consecuencia únicamente se recurrirá a la doctrina de manera subsidiaria, cuando, por insuficiencia, ausencia u obscuridad de la norma, sea así necesario. Por lo que adoptamos una sola estrategia de investigación, la documental, realizando una lectura analítica y critica de las fuentes doctrinales, normativas, informativas y documentales en general, con relación al tema de investigación para concluir con una propuesta de norma interna.

**MÉTODO DEDUCTIVO:** Este método me permitirá analizar de manera general la problemática del avance tecnológico por la que atraviesa la sociedad y el estudio global de incidentes relacionados con el mismo en correlación a los datos de carácter personal, para luego deducir y determinar cuál sus repercusiones para llegar a proteger nuestros derechos como titulares de dichos datos.De tal manera que se partirá de principios y teorías generales por medio de razonamiento lógico, para conocer el fenómeno en lo general permitiendo que puedan deducirse varias suposiciones o presupuestos, partiendo de premisas y conceptos preestablecidos.

[1] Arturo Vargas Flores, GuiaTeoricoPractico para la elaboración de Perfil e Tesis, pag. 96, La Paz Bolivia.

### 9.1.2.- MÉTODOS ESPECÍFICOS

**MÉTODO ANALÍTICO:** Como un método explicativo sistemático de la circunstancia y el objeto de estudio, que permite separar el fenómeno de la esencia, consiste en la descomposición de un todo en sus elementos, y su armado posterior de forma sistemática. Respondiendo a una premisa teórica preestablecida.

**MÉTODO EXEGÉTICO:** Que consistirá a su vez en un análisis semántico y gramatical de la normatividad existente sobre el tema,encontrandola verdadera intervencion que ha motivado al legislador para poner en vigencia determinada norma juridica, tomando como base accesoria el derecho comparado.

**MÉTODO TELEOLÓGICO:** Mediante la aplicación de este método se encuentra un interés que jurídicamente debe ser protegido, permitiendo determinar cuáles son los derechos que innatamente nos pertenecen como seres humanos, esbozándolos en una norma específica que precautelará dichos interés

**MÉTODO LÓGICO JURÍDICO:**Al tratarse de un tema desarrollado con principios y conocimientos jurídicos, aplico la lógica jurídica para llevar a cabo la investigación de una manera ordenada, importante desarrollo para seguir un proceso de investigación jurídica.

## 10.- TÉCNICAS UTILIZADAS EN LA TESIS

Para esta etapa emplearemos:

### 10.1.- ANÁLISIS DOCUMENTAL

Para la utilización de esta técnica se procederá a la discriminación de fuentes de información bibliografía y hemerográfica clasificándola dependiendo de su relevancia en fuentes primarias y secundarias, asimismo dependiendo de su dosificación e interpretación a la que se pretende llegar en el presente trabajo de investigación.

# DESARROLLO DEL DISEÑO DE LA PRUEBA

## INTRODUCCIÓN

Los últimos años del siglo veinte y comienzos del siglo actual coincidieron con un cambio radical en la sociedad: la aparición de una nueva era, un nuevo tipo de sociedad, una nueva cultura, que se convirtió en una verdadera revolución. No se trataba ya de computadoras ni de un nuevo software, no se trataba de un tendido de fibra óptica, ni del desarrollo de redes privadas en las empresas, ni la aparición de bases de datos que permitían almacenar toda la información deseada. Es todo ello y mucho más, tanto que no se puede fijar sus límites.

El internet, permitió al mundo que se unan ciertos elementos como, la voz, la imagen y el dato, permitiendo el tránsito de los mismos, movimiento que recibió el nombre de Revolución Digital. Y al mismo tiempo despertaron incertidumbre a los usuarios, temiendo por su parte, la libre visibilidad e inimputable uso de sus datos personales, lo que se resume en una transgresión a la intimidad de las personas, puesto que ellas mismas debían ser las que otorguen una vía libre o permiso si vale el termino, para la utilización o manipulación de sus datos. Todo ello basado en la protección que nos brinda, a cada ciudadano, la misma ConstituciónPolítica del Estado, siendo la principal fuente de protección a los miembros del estado, teniendo como derechos fundamentales los de la privacidad e intimidad, no solo de la persona misma sino también del entorno familiar.

La interacción entre la tecnología y los datos personales refleja una inmensa capacidad para el procesamiento y almacenaje de los mismos, por lo tanto existe la tendencia a la protección del dato de carácter personal y a la autodeterminación respecto a la información que otorga cualquier individuo.

Asimismo es factible que la vida privada se refiera a aquellos aspectos que ofrecen algún nexo con cuestiones de la vida social del individuo vinculados a la esfera laboral, profesional o comercial o meramente personal tal es el caso de los datos que se encuentran bajo la manipulación de entes públicos quienes sin prever el peligro de

infiltración de redes, registran datos que bien podrían ser utilizados, manipulados o ser de conocimiento de personas malintencionadas,para fines, para los cuales, ningún dato personal fue creado.

En este sentido no se introdujo ningún aporte en nuestra legislación sobre la protección de datos personales en internet lo que significa ya un problema en cuanto a la vulneración de derechos fundamentales.

Es por esto que es necesario investigar los límites de la difusión de información administrativa publica y su grado se seguridad dentro sus sistemas informáticos,revisando casos específicos de vulneración de sistemas de información cuyo acceso permita el descubrimiento de ciertos datos.

El objetivo será probar la necesidad de una regulación jurídica, especifica en cuanto a protección de datos de carácter personal, cuyo registro se encuentra en sistemas informáticos administrativos.

# CAPITULO I

# MARCO HISTÓRICO

## 1.1. ANTECEDENTES HISTÓRICOS

El propósito no es profundizar el conocimiento de los archivos yregistros sino citar los mismos como valiosas fuentes del derecho de protección a los datos carácter personal a fin de poder concluir con la importancia del mismo dentro nuestrosderechosfundamentales.

En un principio se analizara los orígenes del archivo y los registros, puesto que en ellos intervienen ciertos datos, de igual manera será importante analizar la identificación personal, pasando por el Habeas Data o Acción de Protección de Privacidad al derecho de protección de datos personales.

## 1.2. ANTECEDENTES E HISTORIA DE LOS ARCHIVOS Y REGISTROS

### 1.2.1. LOS ARCHIVOS EN LA ANTIGUA GRECIA Y ROMA

En Grecia se emplearon las tablillas de arcilla con escritura silábica, pero también se privilegió el uso de soportes duros e imperecederos como el mármol para la inscripción de documentos importantes. El Testamento de *EpíttetaSpartana* es un interesante ejemplo de esta forma cultural de registrar la memoria, sobre todo porque contiene el primer reglamento de archivo y conservación. Fue impresa en cuatro piezas de mármol, divididas en ocho columnas de escritura, al final de lascuales se halla la regla de guardar el documento en el archivo y su inscripción en materia dura (mármol o metal) en sitio seguro y perdurable. En tanto los textos piadosos se custodiaban en los templos de Cibeles y Delos y ya en esta época se erige el Archivo de Estado en el Metroon de Atenas.

A partir del siglo IX a.C. el papiro fue aceptado como único instrumento para salvar la memorial del pueblo. Al igual que en Egipto, las funciones de los archivos y las

bibliotecas estaban delimitadas. El archivo del rey consignaba inventarios y listas de alimentos y animales. Era obligatorio el registro de leyes y los tratados o convenios entre polis por escrito, para evitar cambios de opinión de los firmantes. Muy pronto se establecieron los archivos públicos que fortalecían el poder del pueblo al posibilitar la verificación de una mentira.

El interés por los documentos de archivo y las obras de biblioteca generó un intenso movimiento de los coleccionistas. Hacia 86 a.C. Apelicón de Teos adquirió los textos acromáticos de Aristóteles y muchos escritos, pues era rico vanidoso y ladrón. Robó los originales de las antiguas resoluciones de la Asamblea de Atenas.

El Imperio Romano fue grande en muchos sentidos. Llevo su visión civilizatoria a un amplio y extendido territorio, impuso normas de convivencia y relacionamiento, desarrolló el derecho romano y fue el centro del cristianismo, al que paradójicamente combatió con sañaen sus inicios. Roma continúo el uso del papiro y el pergamino, y señalo a los templos para su conservación. Por ejemplo, el templo de Júpiter, construido por Tarquino el Soberbio, último de los reyes etruscos, guardaba en su interior los Libros Sibilinos, estudiado por los sacerdotes flámines.

Hacia el 83 a.C. se observa un avance notable, pues ya existían funcionarios responsables del tratamiento documental, entre ellos el *Tabularius,* archivista del Imperio instituido por Antonio Pio en su afán de reorganizar sus oficios, otorgándole la función de custodiar dos tipos de archivo: el *Tabularium* o archivo de documentos públicos y el *Secretarium*, archivo imperial, secreto por antonomasia.

El *Tabularium*del Capitolioera el más importante del Imperio. El edificio destinado al archivo fue construido el 676 d.C. por Quinto Lutecio Cátulo y su custodia fue entregada al *Cuestor*, magistrado romano responsable, entre otras funciones, de los almacenes del municipio, dando origen así a los primeros archivos civiles. Estos repositorios eran conocidos con el nombre de *Tablinas.* Uno de ellos fue establecido en el templo de la Libertad, destruido en un incendio el año 23 a.C. y reconstruido 20 años después; tenía una sección destinada al *Tabularium Castrense* que guardaba documentación de todo género, relativa al Comando de Ejercito y Marina de Guerra.

El *Tabularius* era a su vez secretario de la curia municipal, por tanto tenía a su cargo la custodia del archivo, la redacción de ciertos documentos - inventario de bienes de los pupilos o de las sucesiones, testamentos de los ciegos – y cumplía a cabalidad el servicio fedatario. El Jefe de la Oficina Provincial Romana, equivalente al actual Registro Civil, llevaba la lista de habitantes según anotaciones o rudimentaria partidas de nacimientos y defunciones.

Durante la administración de Adriano se amplió la presencia de los Caballeros en los cuadros de mayor responsabilidad de la administración central, quienes se hicieron cargo de la *ab epistulislatinis, ab epistulisgraecis*, y la *a studiis* de donde surge la *a memoria*, es decir la oficina responsable del control de los archivos oficiales. También se emplearon las tablas de bronce como soporte de ciertos documentos. Estos se encontraban en la colonia Capitolina y eran el registro más hermoso y antiguo del Imperio que comprendía decretos y decisiones del pueblo y del senado romanos y que se remontaban casi a la fundación de Roma.

Ese desarrollo se vio truncado en la primera década del sigloIV d.C. a consecuencia de la invasión de los Galos, que destruyeron Roma y con ella sus archivos y documentos relativos a la historia de los primeros siglos de la ciudad[2].

## 1.2.2. LOS ARCHIVOS EN EGIPTO Y OTROS PUEBLOS

En Egipto se privilegió el uso de papiro obtenido del *cyperospapyrus*. Fue Ramsés II, conquistador de los hititas, quien llego a establecer uno de los primeros repositorios para conservar los papiros en el templo Ramesseum. El temprano desarrollo de sus archivos se viabilizo por la necesidad de información de los faraones y la alta burocracia egipcia, que instruyó la creación de un extenso sistema documental centralizado que comprendía: Archivo Real de Documentos Públicos, Archivos Estatales y 40 repositorios legales y provincias que remitían copias de los diarios del gobernador a una especie de Archivo Central.

[2] Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.29.

Los archivos se diferenciaron de las bibliotecas, que fueron especializándosemás y que eran conocidas como “Lugar de la cura del alma”, porque contenían colecciones de papiros farmacológicos, y “Casa de vida” porque custodiaban las fuentes esotéricas temidas y veneradas del templo de Ramsés.

Esta biblioteca, cuyas obras solo podían ser leídas por un grupo de sacerdotes, cuyo miedo a los castigos divinos era superior al deseo de obtener triunfos gracias a la aplicación de sus conocimientos, fue objeto de persecución por Akhetanón, quien, en su afán de consolidar su religión monoteísta, arrojo todas estas fórmulas a las llamas. Duendes, espectros,espíritus, monstruos, demiurgos y Osiris mismo, con toda su cohorte, fueron consumidos por el fuego y reducidos a cenizas. Este crimen de lesa cultura fue castigado por sus sucesores, quienes mandaron borrar incluso su rostro de las piedras, su nombre, y restituyeron de memoria el contenido de muchos de los papiros antiguos.

En el Imperio nuevo de Egipto se designó un alto funcionario estatal en el cargo de Inspector de Archivos, el *Visir*, brazo derecho de los faraones con sede en Tebas y Memphis, lo que denota la importancia de su rango, pues era responsable de la gestión de la mano de obra, del patrimonio real y nacional, del ejercito de la justicia suprema, así como la percepción de los impuestos, designación de magistrados y el control de los archivos.

Lo propio aconteció con el pueblo hebreo, cuyo sacerdote principal escribió los diez mandamientos en tablas de piedra. Una vez establecidos en Jerusalén, custodiaron los textos oficiales religiosos en el templo, dentro de un arca para su conservación. Se afirma que Yahvé ordeno a Besalel construir el Arca de la Alianza en madera de acacia negra de unos dos codos y medio de largo, codo y medio de ancho, y codo y medio de alto. En los años 66 o 77 d.C. cuando las tropas romanas combatían contra judíos rebeldes, los rollos sagrados fueron escondidos en varias jarras cilíndricas, en once cuevas. Se trata de libros divididos en bíblicos, apócrifos y sectarios, escritos en hebreo, arameo y, excepcionalmente, en griego, casi todos hechos en papiro, con cubiertas de piel y al menos uno en cobre, escritos con tinta con una base de carbón.

En India, los principales archivos estaban a cargo de los sacerdotes, mientras que en china las Leyes eran custodiadas en el templo por las castas sacerdotales, porque se les atribuía carácter sagrado.

El desarrollo de los archivos en China estuvo muy asociado a un tratamiento historiográfico. Hacia 213 a.C. ShiHuandi creo una biblioteca imperial dedicada vindicar los escritos legalistas, defensores de su régimen; para ello ordeno confiscar el resto de los textos sagrados del budismo fueron escondidos en el interior de una serie de grutas en Mogao, oasis en medio del desierto de Gobi, a lo largo de la llamada Ruta de la Seda. Recién durante la dinastía Han la historiografía china logro restituirse gracias a que numeroso eruditos había conservado en la memoria obras enteras. A diferencia de otras regiones y excepcionalmente en China se avanzó hacia la investigación con el establecimiento temprano del Buró de Historiografía[3].

### 1.2.3. LOSARCHIVOS EN LA EDAD MEDIA

Con la caída del Imperio Romano de Occidente, Europa se transforma todos sus órdenes. Con fuerza, surge un nuevo concepto de civilización protagonizado por pueblos emergentes que fueron calificados como bárbaros, cuando en realidad eran portadores de culturas y cosmovisiones diferentes.

Entre los siglos VII y XI, las grandes transformaciones sociales, políticas y económicas provocaron la desaparición de los archivos escritos implantándose la oralidad como medio de transmisión de la información y la legalización de las relaciones comerciales, que se practicaban mediante el trueque de bienesy servicios, al extremo que todos los procedimientos del gobierno se desarrollaban oralmente. Empezó una era de desestructuración de los sistemas archivísticos antiguos que se prolongaría a lo largo de la Edad Media.

[3] Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.30.

Los escasos archivos que sobrevivieron quedaron bajo la custodia de los curas, quienes destinaron recintos sagrados para albergar la memoria histórica. Notable fue en esta época la labor de los monjes copistas, gracias a cuyo esfuerzo recibimos como legado numerosos documentos. Paulatinamente fueron generándose nuevas formas de documentar las acciones administrativas de las cortes federales. Aquellos escasos archivos oficiales se transportaban a grupa de mula, detrás de las cortes de reyes y señores feudales, que eran esencialmente trashumantes. Efectivamente por aspectos de seguridad, “los reyes llevaban el archivo del reino consigo a todas partes a fin de que los mismo guardias, destinados para la seguridad de sus personas pusiesen también a cubierto un tesoro tan precioso”.

Los archivos ambulantes de la Edad Media se explican por la misma naturaleza itinerante de las cortes de los reyes. Los responsables de su gestión debían cumplir con la función de registro, conservación, custodia y servicio de los documentos que retenían en sus arcas, los cuales tenían fundamentalmente función utilitaria como prueba en algún litigio, tales como títulos de derechos, sobre posesiones y rentas, privilegios pontificios, contratos matrimoniales, testamentos, actas de investidura y homenaje, tratados de paz, treguas o alianzas. Al no ser considerados como documentos de valor histórico, su información era fácilmente desechada, por ejemplo, en épocas de carestía de pergaminos se borraba la información antigua y se sobrescribía la nueva.

Se guardaba el archivo en una arquera o caja de madera sin forrar y con tapa llana asegurada por varios goznes o bisagras por un lado, y uno o más candados o cerraduras por el opuesto, dando origen a la larga tradición del arca de las tres llaves que se introduce a América. En estas Arcas sin guardar un orden cronológico,amontonados unos sobre otros iban los documentos de acá para allá, con gran merma y deterioro, hasta que la Iglesia, en sus monasterios y catedrales, se hizo depositaria de ellos. Este curioso método se mantuvo hasta que sobrevino la trágica derrota de Felipe II en Francia, frente a Ricardo de Inglaterra en la que se perdieron todos sus registros, al ser secuestrados sus archivos ambulantes o itinerantes con tremendas consecuencias para la administración del reino. Como resultado de esta pérdida, el soberano francés: mandó crear el *Tresor des Chartes* en Paris, con el fin de

proteger los documentos que contenían los privilegios y derechos del reino. Durante la segunda mitad del siglo XIII fue instalado en un depósitoanexo a la *Sainte-Chapelle de Palais*, donde permaneció hasta 1783.

A partir del siglo XII se observa el ascenso de los burgos o pequeñas ciudades y los incipientes municipios donde se mandaron a organizar los archivos de la ciudad para custodiar los originales, dejandoen los monasterios las copias. Instruyeron el uso del papel en lugar del pergamino, nuevo insumo que se introduce en España al caer en manos de Jaime I, el Conquistador, la ciudad de Játiva, con sus fábricas de papel, que tenían allí los musulmanes, que había importado de la lejana China, a través de Asia y África.

En el siglo XIII, los registros o copias de la documentación eran emitidos por la *Chancileria,* organismo especializado en la extensión de documentos reales. Al término de ese largo periodo de reorganización del mundo conocido se formaron varios archivos oficiales fundamentalmente como efecto de la introducción del papel y la conquista de nuevos territorios de las emergentes potencias europeas. Paulatinamente se fue sepultando la cultura oral, incapaz de retener la magnitud y calidad de la información que debían administrar los reyes y burócratas para controlar vastos territorios, mientras las urbes emergían a lo largo y ancho de Europay sus colonias dotadas de administraciones que empleaban el testimonio y el registro escrito cada vez con mayor frecuencia.

Los archivos y los almacenes de alimentos fueron el blanco de los rebeldes de todos los tiempos. En aquella época de violencia social durante la revuelta sangrienta de los ciompifloretinos asaltaron el palacio del Podestá, principal magistrado de la ciudad, quemando los archivos de justicia y saqueando los depósitos de granos en Or San Michele. Paradójicamente, era también tiempo de siembra archivística, pues en esa época se descubre la importancia estratégica de la información. En el siglo XIV, el Rey de Aragon, Don Pedro IV, El Ceremonioso, nombra, a Pedro Passeya como custodio del Archivo Real. El archivo nunca más estaría sometidoal riesgo de un precario traslado, no siendo en adelante suficiente una arqueta, sino uno o varios armarios con susanaquelesinteriores para conservar los documentos, que tampoco podrán seguir

siendo trasladados de un sitio a otro. El hombre empieza a comprender el poder del archivo, la trascendencia de su misión y su eficacia[4].

### 1.2.4. LOS ARCHIVOS EN LA ERA IMPERIAL Y LA EDAD CONTEMPORÁNEA

Se institucionalizo la cultura del papel a la par de la consolidación de la monarquía y la emergencia de las ciudades, con el correspondiente incremento del comercio. El valor del documento escrito se revitalizó, surgiendo nuevamente la necesidad de crear y desarrollar los registros y archivos administrativos. A partir de ese momento, las ciudades consignan escrupulosamente los nacimientos, defunciones, matrimonios, así como las transacciones económicas y bancarias.

Con el advenimiento del Imperio Español y los descubrimientos geográficos hubo mayorcelo en la conservación de los documentos de las nuevas posesiones territoriales. En 1524, Carlos I de España ordeno la transferencia de los Archivos Reales de Castilla al Archivero de Simancas para garantizar una conservación apropiada de los materiales documentales del reino y otros registros necesarios para operaciones diarias de administración y gobierno.

En 1612 se organizaron los Archivos Secretos del Vaticano, designándose un archivista para su custodiay conservación, aunque no se abrirían al público sino más tarde. Fue mucho después del establecimiento de los archivos oficiales que se publicó el primer Manual para la Conservación de los Archivos, inmerso en la obra *Des Archives*, de Baldassare Bonifacio en 1632, seguido de la edición de la obra *Des Archives Comentarius*, escrito en 1620 por Albertino Barisoni y publicado en 1637.

Los registros administrativos y comerciales fueron reconocidos como la única fuente para la resolución de disputas y el cumplimiento de contratos. El principal uso de estos papeles se refiere a fines de tipo legal y propósitos financieros, lo que determina que su control esté sobre todo a cargo de la iglesia y el rey, aunque a principios del

[4] Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.31.

renacimiento, en vista de la importancia de los archivos para la vida de la sociedad, estos empiezan a ser considerados como propiedad estatal.

En el Siglo XVII, los archivos jugaron un papel importante en la política expansionista europea. El ejércitoinglés, por ejemplo, controló los archivos capturados en las colonias africanas, empleándolos para justificar la propiedad de los territorios conquistados. Posteriormente, siguiendo la tradición inglesa, los ejércitos ingleses se encargaron de centralizar los archivos de los países europeos invadidos.

En Japón, los samuráis (1660-1789), caracterizados por desarrollar una sofisticada cultura marcialy militar, demostraron sus facultades creadoras y su gran capacidad de trabajo en el campo de la ciencia y de la filosofía, sobresaliendo particularmente en el campo de la historia, iniciando una especie de historiografía objetiva, impulsando para este propósito la fundación de archivos y bibliotecas.

Durante el siglo XVIII, los archivos cobran mayor importancia y se construyen edificios especiales para conservar los papeles oficiales. Siguen esa tendencia en 1713, el Electorado de Hannover; en 1731, el Reino de Turín; en 1761, el Archivo de Versalles (Francia); en 1778, Florencia; en 1781, Milán, etc. En 1785 se establece el concepto de centralización de archivos, cuando el Imperio Español ordena el establecimiento del Archivo de Sevillas de las Indias, destinado a concentrar en un solo edificio todos los papeles de las colonias españolas. Este fue un paso fundamental en la construcción de la teoría archivística.

El crecimiento inusitado de los archivos sin responder a un sistema universal o una técnica capaz de poner orden a los papeles, provoca una primera situación de crisis generalizada, caracterizada por una anarquía que hacía imposible su uso. Para ejemplificar esta situación basta observar el caso de Francia que, en vísperas de la revolución burguesa, mostraba la existencia de una impresionante infraestructura archivística conformada por 1.200 repositorios, de los cuales 400 se hallaban en París,

carentes de reglas de administración, organización francamente pobre y acceso sumamente restringido[5].

### 1.2.4.1. LOS ARCHIVOS PÚBLICOS EN LA REVOLUCIÓN FRANCESA

En 1789, en Francia, la revolución burguesa impuso el principio de igualdad civil, jurídica y fiscal, propugnada por los diputados del Tercer Estado. En el fragor de esa lucha contra los privilegiados, en el área rural se produjo el asalto de los campesinos a los castillos y la consecuente quema de los archivos que custodiaban los títulos de propiedad señorial de la tierra, vista la destrucción de la memoria como una forma simbólica de sepultar la sujeción al antiguo régimen.

La ilustración francesa introdujo un concepto y una práctica que revolucionaron el conocimiento. Consecuente con sus ideales, las primeras mediadas determinaron declarar los archivos franceses como propiedad del pueblo, al principio como una medida para conocer y censurar el manejo de la administración imperial de los decapitados reyes. Una medida lógica, entonces, resulta la inclusión del derecho a la información, como una emanación natural del derecho a la libertad de culto y de palabra, que garantiza la Declaración de los Derechos del Hombre y del Ciudadano en 1789.

Con el triunfo revolucionario bajo el lema de *legalité, fraternité, egalité*, entre las más importantes medidas dictadas se encuentra la designación del Comité para el Establecimiento de los Archivos Públicos que recomendó la creación de los Archivos Nacionales (cristalizada 1794) para hacer accesibles a los ciudadanos de la republica todos los papeles del gobierno y la monarquíarecientemente derrotada, calificándolos, como propiedad pública, iniciando en los hechos la era delos archivos modernos centralizados. Con este afán, se llega a tocar extremos impensables, como la instrucción de Napoleón a sus ejércitos (1810) de centralizar en Paris los archivos de los países invadidos por Europa.

[55] Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.36 -42.

En 1821, bajo la influencia de la RevoluciónFrancesa, se crea la *Ecole des Chartes*en Paris con el propósito de capacitar especialistas en el manejo de fuentes históricas, ejemplo que siguen Viena en 1854 y San Petesburgo en 1877.

La atención republicana francesa hacia los archivos del *AncienRegime* del depuesto y posteriormente decapitado Luis XVI, produce una verdadera revolución enlas técnicas archivísticas. Al principio, los archivos eran organizados temáticamente, método adoptado de la bibliotecología por los archivistas que provenían de la profesión bibliotecaria, provocando en poco tiempo la desorganización de los fondos del archivo.

En 1840, Natili de Wally introduce reformas estructurales con la aquiescencia de la alta burocracia republicana, instruyendo la aplicación en todos los archivos, como principio fundamental, el *respect des fonds*, es decir el respeto a los fondos organizados en las instituciones, sin mezclarlos ni desglosarlos para organizar materias, algo que luego sería sistematizado como el respeto al principio de procedencia y a la estructura organizacional del ente productor.

Nueve años más tarde, los Archivos de Francia fueron concentrados en el Hotel Soubiese, en seis secciones que contenían 5.436 legajos de piezas relativas a las órdenes militares. Los países europeos, entre ellos España, otorgaron mucha importancia a sus archivos administrativos y militares. Caso aparte constituye Inglaterra que ya en el siglo XVII había establecido la política de justificación de la propiedad de los territorios conquistados, apoyándose en la posesión y control de los archivos capturados en las colonias. En 1838, mediante acta parlamentaria, ordena el establecimiento de la *Public Record Office*, es decir archivos públicos en calidad de Archivo Nacional con el fin de conservar los papeles del gobierno y del reino.

En general, la poderosa influencia de la ilustración marca el florecimiento del nacionalismo en Europa, con un notable incremento de los estudios de identidad nacional e historia local, regional y estatal; de tal forma que a medida que los nuevos estados van surgiendo a la vida independiente genera una tendencia a construir

edificios para albergar sus archivos oficiales, donde reside la fuente primaria para la reconstrucción histórica.

Los archivos, como había sucedido en 1500 en Europa, empiezan a ser utilizados por la sociedad civil, obligando su apertura al gran público por medio de servicios bibliotecarios, como sucedió en el caso de los archivos Secretos del Vaticano abiertos al uso público por bula papal de Leon XIII en 1880.

El concepto de propiedad Estatal, o más bien fuente común para la memoria colectiva, va pergeñándose cada vez con mayor precisión. Los archivos son considerados de gran importancia como ramas especializadas de los servicios públicos, que es un avance conceptual muy significativo.

La larga tradición archivística francesa, que en 1840 eclosiono en el descubrimiento del principio de *provenance,* a quienes corresponde también el honor de haber establecido el *registraturprinzip*, o principio del orden original. A partir de entonces, la historia de la archivística no sería la misma. Al finalizar el siglo XIX, los archiveros alemanes S. MullerJ.A. Feith y R, Fruin elaboran y publican el Manual para la Administración y la Organización de los Archivos que recoge y sistematiza los principios de procedencia y del orden original.

### 1.2.4.2. LA DESTRUCCIÓN DE LOS ARCHIVOS DE UNA MEMORIA CONTEMPORÁNEA

En 1900, coincidente con la apertura de un nuevo siglo, se produce la proliferación del uso del papel, con la consecuente sobre producción de registros oficiales y el crecimiento inusual de los archivos. Había llegado el tiempo de poner orden a las tareas del archivo, cuya responsabilidad lo asumieron los historiadores, bibliotecarios y archivistas reunidos en unCongreso Internacional de Archivistas, en Bruselas en 1910, rompiendo la resistenciade los historiadores en los Estados Unidos, sacralizando el principio francés de *repect des fonds* para llevar adelante la organización de los archivos, que se sobrepone a la tendencia de organizar las series documentales por materias.

Ocho años más tarde, la revolución soviética, de indenegables alcances estructurales para el mundo de entonces, ordena la nacionalización de los documentos del antiguo régimen zarista y dispone su administración en una agencia central para la Administración de Registros, que en la práctica llego a ser el mayor sistema archivístico centralizado en el mundo entero.

Durante la Segunda Guerra Mundial ciertos archivos tuvieron un dramático desarrollo como sucedió en el ghetto de Varsovia, cuyos supervivientes escondieron sus registros y documentos en cajas de metal enterradas, para garantizar su sobrevivencia y testimoniar los 63 días de heroica resistencia delghetto contra el exterminio nazi. Conocidos como los archivos clandestinos de Emmanuel Rigelblum.

En la postguerra, los archivos centrales del Ministerio del Interior de Polonia concentraron los archivos del ejército del interior y del Gobierno Polaco en el exilio. El Instituto para el Estudio de la Polonia Clandestina, con sede en Londres, cuenta con un importante archivo sobre el exterminio nazi en Polonia y la resistencia de los partisanos. En el otro extremo, la temida SS nazi de Hitler sostuvo archivos secretos en los Lebensborn, hogares diseñados por Himmler para cuidar de las mujeres solteras que esperaban hijos de innatos alemanes cuyas características raciales correspondían al ideal ario de los nazis cuyos nacimientos se registraban cuidadosamente en expedientes estrechamente custodiados, que se mantenían separados de las actas municipales de nacimiento. Ante la inminencia de la derrota, la mayor parte de estos expedientes fueron destruidos por la misma SS, pero unos miles se salvaron y permitieron conocer escabrosos detalles de esos experimentos.

La manía destructora de los nazis fue una característica de su régimen. El 27 de febrero de 1933, incendiaron el Reichstag con todos sus archivos. Al retirarse de Varsovia, arrasaron con los archivos de la biblioteca pública[6].

[6] Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.42-43.

### 1.2.4.3. LOS ARCHIVOS CONTEMPORÁNEOS

En la postguerra se legisla sobre el derecho de acceso a los archivos. Esa medida se extiende pronto al conjunto de países que forman la Organización de las Naciones Unidas. En 1948, la Declaración Universal de los Derechos Humanos incluye el derecho a investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, recogido inmediatamente por el Consejo Internacional de Archivos quienes en un afán realizan esfuerzos para hacermás fácil el acceso a los archivos y seguirá calando hondo en los archivistas profesionales en el futuro, como se observa en las conclusiones del Coloquio sobre los Archivos para el siglo XX (1979) que abogaban por el acceso competo de la información.

Francia se ha continuado, mostrándose como vanguardista en la organización y desarrollo de los archivos, habiendo construido entre1956 y 1985 un total de 64 edificios para albergar los archivos nacionales y departamentales. En la ciudad de Paris se encuentra la sede del Consejo Internacional de los Archivos, creado en 1950, cuatro años más tarde después de la constitución de la UNESCO, organismo que inicia en 1979el Programa de Administración de Registro y Archivos (RAMP), para promover en largo plazo, primero mediante publicaciones, una efectiva administración y uso de los archivos, particularmente en los países de desarrollo.

De lo público los archivos pasaron, nuevamente, al terreno de la restricción. Principalmente ciertos archivos de las grandes potencias que introdujeron el concepto de archivos clasificados, cuyas características salieron a la luz con el Libro Azul sobre el Estudio de Objetos Voladores no Identificados, a cargo de la FuerzaAérea de los Estados Unidos, la misma que manejo muchos de sus archivos como secreto.

Actualmente, la legislación de los Estados Unidos, es muy rígida con la administración de los archivos clasificados. Se ha observado los extremos de la legislación a raíz de la Guerra contra Irak, que fuera sustentada a partir de información clasificada que a la postre resultó ser falsa. En uno de esos episodios se ha señalado que la revelación de información clasificada se castiga con una pena de hasta diez años de cárcel y

remarcaron que la identificación de un agente de inteligencia puede poner en riesgo su vida y la de otros.

Los archivos clasificados pueden igualmente, desaparecer sin provocar traumas en la administración. Así se observócuando el primer ministro de Inglaterra informo de que los servicios secretos han retirado oficialmente su anterior afirmación de que Sadam Hussein podía desencadenar un ataque con armas químicas en 45 minutos.

El goce pleno del derecho de petición marcó con fuerza la organización de los archivos contemporáneos. La infraestructura documental se abre al servicio público atravesando las fronteras institucionales y las administraciones nacionales. Más aun, los archivos son empleados para fines ajenos a la Administración que los generó, es decir, sirven como fuente primaria para la investigación científica y la búsqueda de raíces y el origen de las personas comunes.

El archivo devino de ser un instrumento de la administración, en una poderosa herramienta para la transformación del conocimiento y el desarrollo sostenible de los pueblos y naciones. Los organismos internacionales desarrollaron un gran esfuerzo para hacer accesibles los archivos a sus titulares, es decir los hombres y mujeres de cada Nación y Estado. A la postre, los archivos se transformaron en instituciones culturales y científicas, cuando sus documentaciones fueron transferidas desde las instituciones productoras hasta los archivos históricos[7].

La conciencia sobre el valor de los documentos es ahora generalizada.

## 1.3. ANTECEDENTES HISTÓRICOS EN EL ENTORNO NACIONAL

### 1.3.1. BREVE RESEÑA DE LOS QUIPUS

GunnarMendoza señala en 1967, estos instrumentos eran: “atadijos de cuerdecillas que mediante la combinación de nudos y colores componían un sistema de anotación

[7]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.43-46.

con el cual se lleva la cuenta cronológica y estadística del imperio incaico, deben considerarse como documentos archivísticos, sin que su condición física sea un impedimento para ello".

Un *quipu* o el conjunto de ellos conforman un archivo de uso más bien administrativo y contable con fines prácticos de control, conducción y desarrollo del imperio. De manera excepcional se lo empleaba para la transcripción de mensajes cortos de los incas.

Su soporte físico respondía a una lógica mnemotécnica compleja, de registro numérico y contable. Su origen se remontaría al periodo Wari-Tiwanaku (1580 a.C.), pero fueron sistematizados durante el periodo Inca. Estos archivos, de carácter descentralizado, se encontraban a cargo de los *quipucamayoc* o funcionarios especializados, quienes registraban sus datos en ramales de grandes cuerdas anudadas, es decir, hilos torcidos de diversos colores, grosores y significados, en los que se anotaba minuciosamente las cosas que se gastaban y lo que las provincias contribuían, para que se supiese lo que daban y contribuían.

Como se puede ver, los conceptos de *quipu*varían. Algunos autores lo describen simplemente como nudo, otros autores se refieren a ellos como cuerdas, registros fabricados en lana de camélido o fibra vegetal. Pero ambos coinciden en que conforman un sistema complejo de registro como lo señalaron algunos cronistas.

El registro de los *quipus* estaba destinado a llevar la cuenta de los ingresos o tributos, los egresos o toda salida de depósitos, los silos del Inca, los registros diarios del ganado y finalmente las producciones de cultivos. El tributo no era entregado sino era pagado en oro o plata. Esto significaba que abarca la totalidad de bienes y productos empleados en el incario, desde lo significativo hasta lo superfluo, aspecto que les permitía tomar en cuenta también que un par de alpargatas no se podían esconder. Era tal su importancia que Guamán Poma de Ayala afirma que el Imperio Incaico estaba gobernado por medio de los *quipus.*

Estamos ante un registro de tipo semiótico, cuya codificación se basa en los colores de los hilos de los *quipus* que identificaban diversos asuntos o cuentas, por ejemplo, el amarillo al oro, el blanco a la plata y el colorado a la gente de guerra;así como en la forma y disposición de los nudos.

Los *quipus* registraban informaciones jerarquizadas sobre productos de distinta naturaleza. Por ejemplo, armas: lanzas, arcos , flechas, porras, hachas, hondas; productos manufacturados; animales; productos agrícolas; datos demográficos precisando los nacimientos y defunciones, asimismo se realizaba el registro de mujeres y hombres, edad, y como eran agrupados, por pueblos o provincias.

La labor de registrar los datos demográficos estaba a cargo de los jefes de las comunidades de 100 habitantes, que tenían una doble función, protectores y fiscales, de manera que conocían detalladamente los acontecimientos del grupo a su cargo y, sin duda, estaban enterados de los asuntos de guerra. Según el jurista español Santillán, el *RunayPchacac*, era uno de los cuatro visitadores o Jueces de Inca, responsable de controlar el desarrollo demográfico, la salud, la alimentación y tranquilidad en el territorio de su jurisdicción. Por tanto debía cuidar de dar cuenta a sus superiores, de grado en grado.

Esos datos demográficos eran de mucha utilidad para fines castrenses porque tenían un riesgo detallado de la cantidad de gente apta para la guerra a la falta o perdidas ocurridas en batallas y encuentros con los ejércitos rivales.

En ese sentido, los datos recogidos por los *quipucamayoc*eran importantes para determinar, tanto la paga de los tributos como para saber la gente que había para la guerra y la que podía quedar por defensa del pueblo.

El historiador peruano Porras Barrenechea infiere una actividad historiográfica en el *quipucamayoc*, quien era cultor de la historia oficial inca; pero curiosamente, los *amawtas* no aparecen en su estudio. Según este autor, el *quipucamayoc*tenía una grave responsabilidad, que afectaba a la colectividad y al espíritu nacional.

Debíaconservar intacta la memoria de los grandes reyes por el recitado métrico del cantar, ayudado por el instrumento mnemotécnico de los quipus.

El estudio de la estructura de los *quipus* o registros contables aporta mayores precisiones respecto a sus alcances. Los archivos de los quipus se elaboraban en todas las *markas*, de tal forma que en cada provincia existían tantos contadores como autoridades. Los *quipucamayoc*, basándose en esos registros, cerraban sus cuentas trimestralmente hasta completar estadísticas generales anuales[8].

### 1.3.2. LOS ARCHIVEROS DE LOS INCAS

La denominación de los *quipucamayoc* deriva de la raíz *quipo* que, desde el punto de vista de este estudio, es un sinónimo de registro de documento, es decir la unidad documental simple o compuesta. Por tanto, *quipoc* vendría a significar escribano, secretario, archivero o contador según los niveles de responsabilidad funcionaria en la administración inca. Todos ellos tienen en común el manejo o administración del registro oficial, es decir del *quipo*o documento, incluyendo la interpretación de su simbología.

El *quipucamayoc*tenía una función compleja extendida en todo el Tahuantinsuyo. En general, el cargo recaía en aquellas personas que ocupaban la segunda calle de los recuentos de población, es decir, de acuerdo ala clasificación de Guamán Poma, tenían que ser ancianos, viejos, pasados de edad, por lo general de los sesenta años o más, siempre y cuando podían ejercer sus funciones con idoneidad.

Dentro de la jerarquía funcionaria el administrativo de mayor nivel era una especie de Contador y Tesorero Mayor del Tahuantinsuyo denominado *Runa quipocIncaphaciendadchasquicoc,* ocupado en concentrar los datos anuales. Mientras que el menor nivel era el Escribano público de cabildo que asentaba lo que pasaba en cada pueblo del reino. Además existía la figura del Escribano de Quipo, cordel, el *quillcacamayoc* cuya función específica era la de precisamenteauxiliar del

[8]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.62.

*quipucamayoc*.Todos estos funcionarios eran obviamente diferentes a los llamados secretarios (Escribano Colonial).

La extensión del vocablo y la función originaria del *quillqa*fue ampliamente estudiada por Porras Barrenechea, quien afirma que, “de acuerdo a los primeros vocabularios, *quillca* quiere decir pintura y *quillcacamayoc,* pintor” y posteriormente se tradujo *quillca* como equivalente a escritura.

Aquellos secretarios eran gente de absoluta confianza de los incas y muy prácticos en el manejo de los *quipus*. El secretario del Inca, por ejemplo, recogía los registros orales de su propia boca para codificar esa informaciónen *quipus*de colores teñidos(*quillcacamayoc o quillcauataquipoc*). Tal era la destreza de estos secretarios que llevó a Guamán Poma de Ayala a exclamar: “estos tenían tanta habilidad en los cordeles que, ¿qué me hiciera si fuera en letra?”.

Esta aserción permite esbozar una respuesta sobre la extensión del *quipu* a la oralidad. Porras Barrenechea afirma que “el *quipucamayoc*debía conservar la memoria de los grandes reyes por el recitado métrico del cantar”, que vendría a ser la unidad de medida de la memoria oral, constituyéndose en un aporte ciertamente importante.

Los *quipucamayoc* y los *amawtas* pertenecían a la *panaca* o allyu de los Incas, y estaban exentos de pagar tributo o realizar otras obligaciones; por tanto Vivian a expensas del Inca. Eran seleccionados por su excelente memoria y entrenados para usarla. Se afirma que había especialistas en diferentes categorías del contenido de los *quipus.* El método de transmisión del contenido era típico de la endo-educación, pues el *quipucamayoc* enseñaba a su hijo, a su vez, este al suyo y asísucesivamente, de manera que la preservación e interpretación de los valores tanto evidénciales como informativos de los documentos se conservaba indefinidamente como a los *quipus* mismos.

Para garantizar la continuidad del método de conservación, control, sistematización, y difusión de la memoria, los *amawtas* eran responsables de elegir a los sucesores, ya que tenían mucho cuidado en  enseñar a sus hijos y a hombres de sus provincias,

porque así por las bocas de unos lo sabían otros, de tal manera que hoy en día entre ellos cuentan lo que paso a quinientos años como si fueran diez.

El problema de las funciones se complica considerando el testimonio de Garcilazo del Vega, quien afirma que el *quipucamayoc*, era a la vez, escribano e historiador. Su función de escribano lo lleva a registrar los datos estadísticos y los anuales de los sucesos dignos de memoria. Pero como historiador, estudiaba esos datos para conservar en la memorial la tradición de aquellos hechos famosos, porque tenían que dar cuenta de ello cuando se la pidiesen, por tal oficio eran reservados de tributo y de cualquier otro servicio.

No queda entonces claro si el *quipucamayoc*deveníaen *amawta.* Tampoco si el *amawta* podía ser también *quipucamayoc*lo cual es muy probable. Según Gracilazo de la Vega, los *amawtas*sistematizaban la memoria recogida por los *quipucamayoc*. El *amawta* vendría a ser el custodio de la memoria almacenada en los archivos del Cuzco, archivos que se convierten históricos por su naturaleza. Una vez que la información era decodificada y desclasificada, el *amawta*, autorizaba su difusión por medio de los *arawicus.*

A lo largo de la labor de registro de la historia oficial y del establecimiento de la contabilidad, los *quipucamayoc*desarrollaron cinco series de *quipus*, según la tipología de Porras Barrenechea:

1. Recuerdo de los Reinados de los Incas
2. Batallas
3. Leyes
4. Calendario
5. Cambios de Población

Además se constata la utilización de *quipus* de lanas de colores para connotar una temporalidad que haga referencia a los distintos tres arcos cronológicos: todos ellos en

materia de lana, el color pajizo hacía referencia a la Época Preincaica, el morado a la Época de los Caciques y el carmesí a la Época del Inca[9].

### 1.3.3. ARCHIVOS EN LA ÉPOCA COLONIAL

A partir de 1531, en el actual territorio de Bolivia empezó la invasión hispana, seguida por la conquista, la colonización y el sometimiento de los pueblos indígenas. Esta epopeya estuvo vanguardizada por grupos de fieros capitanes ilustrados como Ñuflo de Chávez o Andrés Manso, iletrados como Gonzalo Pizarro y de bastarda cuna como Diego de Almagro. A pesar de esas diferencias todos eran soldados aguerridos, valientes y temerarios.

Se dice que el primero grupo conquistador del Perú no incluía nobles ni procedía directamente de España, sino de la Antillas. Sabemos, además que el soldado no era vecino ni estante fijo en una ciudad, en consecuencia, su estado era semejante al del vagabundo. Junto con ellos llegaron los primeros cronistas, como Fráncico de Jerez y Pedro Pizarro, quienes observaron la prisión y ejecución de Atahuallpa. En cambio, otros registraron paso a paso el proceso de colonización del Perú.

Pedro de Cieza de León fue un cronista soldado español de la conquista quien fue uno de los historiadores mejor informados de la civilización inca a quien le cabe el mérito de haber recogido valiosos registros históricos de boca de vencidos. A partir de estos relatos, legó para la posteridad información sobre dos aspectos: las vicisitudes de la cruenta conquista y los adelantos alcanzados por la alta cultura inca, cuyo desarrollo quedo debidamente registrado en los archivos orales y *quipus* incaicos.

A partir de la conquista del Perú se introduce un nuevo sistema de gobierno, con una fuerte carga ideológicafeudal que entra en contradicción con el antiguo modo de producción inca. Justamente por eso se la conoce como una fase de transición, en la que coexiste un sistema antiguo de documentación e informaciónutilizada por los incas, junto a otro sistema moderno hispano-colonial.

[9]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.66.

En los Andes el *quipu* rebaso su tiempo gracias a la supervivencia de los *quipucamayoc*, quienes continuaron con esta práctica. Incluso fueron empleados por los Caciques en las demandas de anulación de los tributos de los pueblos sometidos, evidenciándose las características de alta confiabilidad de sus registros. Esto significa que los registros del *quipu* fueron reconocidos como prueba legal en los tribunales de la época. Además se afirma que Toledo, el gran reformados del Perú, institucionalizo su uso y el *quipu* habría tenido vigencia plena en 1570.

Incluso los caciques habrían sido autorizados a seguir empleando el *quipu* para optimizar el ejercicio de sus propias funciones de percepción de tributos y concretización del servicio personal de los indios.

Es evidente que los cronistas de la conquista conocieron el sistema contable inca, sistematizado por los *quipus*, en forma de cuerdas anudadas, que también observo Cieza de León, haciendo la descripción del *quipu* y el señalamiento de sus principales funciones, lo que demuestra la coexistencia de dos sistemas oficiales de registro o archivo. Sin embargo, a la postre, destruyeron las bases del sistema documental Inca para imponer el hispano. El primer Concilio de Lima ordeno la destrucción completa de los *quipus* públicos del imperio incaico que estabanconcentrados en Cusco.

La conquista española puede entenderse como una empresa comercial, pero a la vez como una empresa militar, pese a que en la época colonial no existieron ejércitos militares, sino más bien milicias reclutadas por el oprobioso mecanismofeudal de la leva o reclutamiento forzoso, para enrolarlas en las guerras, como hizo Diego de Almagro, quien preparo su entrada a Chile con acopio de recursos, lo que le permitió hacer levas de gente con abundancia de armas y caballos y una lúcida plaga de capitanes, todos ansiosos por conseguir prebenda y exultantes existes.

Esa cruel tradición militar se aplicaba con rigor en las nuevas tierras, a pesar de su prohibición expresa por la Leyes de Burgos de alistar tropas en las Indias, que se estaba despoblando debido a su empleo en las conquistas continentales, por tanto, las tropas debían ser alistadas en España.

Debido a la inexistencia de minas de oro y plata, los conquistadores volcaron su interés en someter a los pueblos indígenas.

De acá surge la pregunta ¿Qué clase de documentos son las crónicas? Sin duda fuentes primariasconstruidas a partir de registros contables (*quipus*), testimonios orales (memoria histórica inca) y registros propios (descripciones y observaciones). Consecuentemente, se trata de los primeros registros oficiales en el cumplimiento de misión militar. La tarea de aquellos cronistas no era simple, pues muchas veces tuvieron que memorizar los acontecimientos para escribirlos después, a pesar de las amenazas a su vida. Por ejemplo Fráncico de Carvajal, el demonio de los Andes, maestre de campo y temerario soldado de Gonzalo Pizarro, amenazó de muerte a toda personaque intentase relatar los hechos que comprometían su intercesión, porque entendió que eran más dignos de la ley de olvido que no de memoria ni perpetuidad.

El valor de los archivos, por entonces, bajo la custodia de los escribanos, era verdaderamente importante[10].

### 1.3.3.1. EL ESCRIBANO EN LA COLONIA

Existían dos tipos de escribanos: el de fe pública, denominado Escribano de Cabildo; y el funcionario extrajudicial que celebraba contratos de los ciudadanos, denominado Escribano Público. Ambos tenían distintos niveles. En Charcas se produjo una fusión de ambas funciones, designándose a uno solo con el título de Escribano de Cabildo y Público. Para la administración interior se designaban otros dos escribanos públicos de provincia y, en las postrimerías de la Colonia, se creó el cargo de Escribano de la Real Hacienda.

Para ejercer el oficio de escribano se requería ser seglar, tener 25 años de edad, someterse a un examen, contar con dos años de práctica, gozar de buena reputación, obtener el título real que lo revistiese de fe pública y adquirir la propiedad del oficio.

[10]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.70.

El oficio de escribano era imprescindible para la administración de la vida cotidiana y el desarrollo de la ciudad, pues sin él no podía celebrarse el Cabildo, órgano de gobierno y decisión. Eso expresa la primerapreocupación de los cabildos para asegurar la presencia de un escribano, pues por su mano iban las peticiones de vecinos, estaba a su cargo todo el papeleo capitular como los títulos de propiedad de solares, charcas y tierras, licencias, etc.

Este funcionario podía ser nombrado por provisión real o por el Cabildo; en realidad se trataba de una regalía, pero el Cabildo tenía la potestad de designar uno cuando se producía una vacante, ya sea por ausencia o muerte[11].

### 1.3.3.2. EL SECRETO DE INFORMACIÓN

En todas las ciudades coloniales, las actuaciones del cabildo eran secretas y el escribano estaba obligado a guardar la confidencialidad por juramento. Por esa razón, el rey instruyo escoger diligentemente a personas que seanhombres de buena casta, limpios, sin tener malas razas, que guarden el secreto conveniente, recomendando si era necesario proceda contra los que hubieren descubierto el secreto con todo el rigor. El cargo era vitalicio y el oficio solía pasar de padres a hijos.

Sus obligaciones eran múltiples, pero en lo quenos concierne, escribía actas firmadas después por las autoridades de los Cabildos cuyos archivos custodiaba celosamente. Otra obligación, inherente a su calidad, era la de custodio de la fe pública, con la función fedataria, por la que daba fe y verdadero testimonio[12].

### 1.3.3.3. LA CORRUPCIÓN DEL ESCRIBANO

La labor del escribano era tremendamente importante para el desarrollo del ayuntamiento. Su rol podía ser esencial, pero con facilidad podía corromperse. Se han visto muchos casos:

[11]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.74
[12]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.74

- Alteración de archivos, injustificadamente a favor de ciertas personas o autoridades.
- Desorden de archivos, que no se sabe si fueron hechos a propósito, puesto que para realizar el trabajo de ordenar los mismos, los escribanos cobraban favores o pesos a cambio.
- Sustracción de algunos archivos, los cuales podían ser encontrados en los mercados a la venta, vale decir, que se negociaban ciertos documentos para recibir pesos a cambio.
- Falsificaciones de cartas de alta importancia y secreto, las cuales incluso eran una prueba de delitos de traición[13].

### 1.3.3.4. EL LIBRO BECERRO Y EL ARCA DE LAS TRES LLAVES

Todas las actuaciones debían asentarse en los libros del Cabildo, ordenanza de 1574 cumplida con todo rigor. Toda nota real, ya sea de despacho, provisión o carta de los superiores, debía copiarse a la letra en el libro de cabildo y el original se guardaba en el archivo de provisiones, para que así, siempre conste a la vista de todos, disponible a todo tiempo a los visitadores y jueces de residencia, quienes debían conocer dichos archivos. Por último se mandaba que el escribano deba tenerlas en cuadernos para dar providencia.

El Cabildo tenía la obligación de llevar las Actas Capitulares de su servicio en forma meticulosa. Para ese propósito, estaba obligado a registrar la Legislación Municipal en el Libro de Becerro. El destino de ese primer libro es incierto, pues algunos afirman que se perdió y otros que este resguardado.

El Libro de Cabildo se conservaba en la sede del Ayuntamiento, en un mueble especialmente diseñado para tal efectos denominado caxón, que era un arca de tres llaves, querespondía a un patrón común, señalado por la legislación indiana: “que la caxa sea grande, de madera buena y gruesa bien varreada de barreras de hierro y con

[13]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.76.

buenas cerraduras y llaves diferentes, que se encuentre en una parte segura y bien custodiada".

Había cuatro tipos de arcas de tres llaves: el primero; destinado a resguardar los acaudales del rey, el segundo; los bienes de difuntos, el tercero; los bienes propios de la ciudad; y el cuarto para los papeles y Archivos del Cabildo, en ese orden de importancia.

Las atribuciones del escribano estaban directamente relacionadas con la administración documentaria del cabildo y el manejo de las escrituras públicas. El Archivo del Cabildo registraba en libro blanco las escrituras de las rentas, los censos, sisas, entradas y salidas. En otros archivos separados el inventario de los propios de la ciudad, el libro de privilegios y el libro de provisiones.

Todo esto es sumamente importante para establecer la forma de organización del archivo y su accesibilidad.

Hacia 1557, se deja el arca de tres llaves y se manda hacer un armario para archivo. El mismo serviría para guardar las escrituras y provisiones que las ciudades tienen o han de tener[14].

### 1.3.3.5. LAS ORDENANZAS MILITARES

Los asuntos de guerra y conquista eran atendidos por la Junta de Guerra que sesionaba dos veces por semana, para ver los negocios y materias de guerra, aunque el Cabildo también intervenía en el manejo de información, que podemos considerar de inteligencia. Los consejos de la Junta de Guerra ocupaban la diestra del Presidente del Consejo. Esta junta conocía todos los asuntos relacionados a las campañas militares en las colonias, tales como las provisiones de los oficios y cargos tocantes a la guerra, así sea de mar como de tierra. También las solicitudes de privilegios de los soldados.

[14]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.77.

El servicio fedatario en esa época experimento serias transformaciones, debido a los numeroso pedidos de privilegio de los soldados, evidenciándose en muchos casos fraudes, lo que motivo al monarca a, mandar que en la Secretarias no se admitan certificaciones de servicios particulares, sin haberse tomado la razón de ellas en las Contadurías de Sueldo.

El territorio de Charcas del Virreynato del Perú se anexo al nuevo Virreinato del Rio de la Plata creado en 1776, donde la nueva organización administrativa imperial se impuso en el contexto de las sublevaciones indígnales. En 1782 se promulgo la Real Ordenanza para el Establecimiento e instrucción de Intendentes de Ejército y provincia en el Virreinatito de Buenos Aires que se debe ver como un completo de las Ordenanzas Generales del Ejército,el 22 de octubre de 1768. Esta normativa incorporo los gobiernos militares y políticos e identificó los documentos militares más importantes. Asimismo regulo la gestión documental mediante la prescripción de responsabilidades para la filiación de las tropas en un archivo que se encontraba en las oficinas de la ContaduríaPrincipal, lo que denota su importancia.

Muy poca documentación ha quedado en los archivos oficiales de esos ejércitos de la época colonial, pese a su larga y épica historia. Se ha identificado la existencia de documentación referida al Ejercito en algunos repositorios como el archivo Histórico de La Paz, donde existen referencias de la documentación militar colonial en Expedientes Gobierno (Grupo Corregidor, 1548-1782), así como en la serie Expedientes Gobierno (Grupo Intendencia 1782-1825)y una pequeña serie denominada Ejercito (1781-1824), esta última transferida por la Biblioteca Central de la Universidad Mayor de San Andrés[15].

## 1.4. ANTECEDENTES DE LA IDENTIFICACIÓN PERSONAL

### 1.4.1. LA DACTILOSCOPIA

La dactiloscopia es una de las ramas de la lofoscopia encargada del estudio, clasificación, archivo y recuperación de las mismas impresiones dactilares que

[15]Luis Oporto Ordoñez, Historia de la Archivística Boliviana, La Paz – Bolivia, Pag.78.

aparecen en las falanges dístales de los dedos de las manos, se reconoce y constituye por ser la ciencia más conocida y aplicada con fines de identificación. Se trata de una manera inequívoca de establecer a ciencia cierta la identificación de una persona a partir de su primera reseña técnica ya sea morfológica, fotográfica y lofoscopica.La identificación por medio de este método ha sido de gran importancia para el reconocimiento de muchas personas por la policía y las autoridades competentes, a menudo funciona como piedra angular en sus registros.

Sus antecedentes históricos se pueden encontrar en las siguientes épocas:
- En la época Prehistórica se encontraron marcas dibujos en las cavernas de los primitivos.
-En la época Empírica se encontraron multitud de impresiones digitales de griegos y romanos, escritos, documentos (huellas para autenticar).
-En la época Científica se encontró que la piel tenía porosidad es decir crestas papilares y bajos relieves (surcos interpapilares), es en esta época que se inventó la dactiloscopia y el primer método de identificación decadactilar, que fue creado por Juan Vucetich en el año de 1895[16].

### 1.4.2. LA CEDULA DE IDENTIDAD

El documento de identidad, también conocido como Cédula de Ciudadanía (CC), Carné de Identidad (CI), Cédula de Identidad (CI) o Documento Nacional de Identidad (DNI) o identificación oficial o simplemente identificación, es un documento privado individual que contiene datos personales de carácter público emitido por una autoridad administrativa competente para permitir la identificación personal de los ciudadanos.

No todos los países emiten documentos de identidad, aunque la extensión de la práctica acompañó el establecimiento de sistemas nacionales de registro de la población y la elaboración de los medios de control administrativo del Estado. La posesión de un documento de identidad es obligatoria en la mayoría de los países

[16]http://prezi.com/4hprytwyfkgi/dactiloscopia/

iberoamericanos, mientras que es rara en los que poseen un sistema jurídico basado en el derecho anglosajón.

Sus orígenes y antecedentes históricos se encuentran señalados en la historia de ciertos países, quienes determinaron plasmar este hecho en libros, de los cuales no se tienen los datos específicos[17].

### 1.4.3. LA IDENTIFICACIÓN PERSONAL

La historia de la Identificación Personal, desde sus inicios siempre estuvo a cargo de la Policía Nacional, tiene sus antecedentes en el Convenio Internacional de Policías de Buenos Aires del 20 de octubre de 1905 el cual facilitaba el registro de las denominadas 'Personas Honradas' en las oficinas de Identificación. En diciembre de 1927 con la creación de la Cédula de Identidad Personal a cargo del Servicio Departamental de Policía, se inicia el registro de todos los habitantes y estantes del país. Reglamentándose en 1928 las características y el uso de la Cédula de Identidad. En 1955 se crea el Servicio Nacional de Identificación Personal, lo que fue ratificado con la Ley Orgánica de la Policía Nacional de 1985[18].

### 1.4.4. EVOLUCIÓN INFORMÁTICA DE LA IDENTIFICACIÓN PERSONAL EN BOLIVIA

Como se menciona en el punto anterior en nuestro país la forma de realizar los registros de la identidad de los ciudadanos se realizaba en forma manual, no digitalizada, durante casi nueve décadas, hace unos años se creó el Servicio General de Identificación Personal,el SEGIP, que trata de una institución descentralizada con personalidad jurídica, jurisdicción y competencia en todo el estado Plurinacional de Bolivia, es creado por Ley Nº 145 del 27 de junio de 2011. Esta institución digitalizó mediante sus sistemas informáticos toda la documentación existente sobre la identidad de los bolivianos, entre sus avances, tenemos:

[17] http://www.caletao.com.ar/pol/temrel/13/dni.htm
[18] http://censoarchivos.mcu.es/CensoGuia/archivodetail.htm?id=52276

- Organizaron los archivos físicos en ambientes aún precarios.
- Digitalizaron toda documentación que respalda nuestra identidad, para que los documentos estén disponibles en tiempo real para el trabajo de los operadores.
- Pasaron de la máquina de escribir manual o el equipo de computación utilizado como máquina de escribir, a la estructuración de un sistema informático, en el que las computadoras adquirieron el carácter de terminales de atención al público.
- Armaron el rompecabezas de múltiples bases de datos incipientes e inadecuadamente estructurados, para construir una única base de datos con 12 millones de registros de Identificación Personal y Licencias de Conducir.
- Conformaron una red nacional y una Base de Datos integrada y centralizada y sistemas en línea.
- Contrastaron la base de datos con la del SERECI.
- Iniciaron ya el proceso de saneamiento masivo de datos.

Es de esta manera que Bolivia ya cuenta con un verdadero sistema de registro de identificación, sin descartar que la misma debe permanecer en constante actualización. De tal forma que la evolución informática de la identificación personal en nuestro país surgió hace unos cuantos años[19].

Una prueba de lo referido lo encontramos en una publicación donde se anuncia que existirá un registro de bolivianos vía internet beneficiando exclusivamente a los que viven en el exterior, permitiendo realizar un pre registro previamente a una cedulación que deberá realizarse personalmente, las expectativas para la culminación del proyecto serán a fin de año, con miras a las siguientes elecciones. (Anexo 1)

## 1.5. EVOLUCIÓN DE LA TECNOLOGÍA DE ALMACENAMIENTO DE DATOS

[19] www.segip.gob.bo/

Los inicios de las unidades de almacenamiento de datos, comenzaron con las tarjetas perforadas, unidades por cierto pocas cómodas, ya que había que recordar el orden de las mismas, (ya que si este se perdía no había forma de recuperar el programa) estas tarjetas se insertaban en una máquina de procesamiento de manera secuencial, donde quedaba alojado en la memoria y listo para ser probado. La forma de lectura era semejante al sistema de lectura braille, la computadora leía por agujeros en las tarjetas. Vale destacar que en ocasiones u dependiendo de la complejidad del programa podía ocupar cerca de 200 tarjetas que había que colocar una por una dentro de la máquina, y al apagar la máquina todos esos datos se perdían.

Años más tarde debido a la necesidad de llevar un orden en estas tarjetas y de no tener que perder tanto tiempo introduciendo una por una, se crea la cinta de tarjeta perforada, mejor conocida como cinta perforada, y de esta manera se hace muchísimo más fácil la portabilidad de este sistema. No paso mucho tiempo cuando se descubre las nuevas tecnologías de las cintas magnéticas y se comienza a aplicar en el almacenamiento de datos para computadoras ya que las misas consistían básicamente en espacios de cinta cubierta de óxido ferroso, donde se colocaba positivo y negativo, dependiendo del caso, el principio era tener una serie de imanes entrelazados en una cinta a los cuales les pedía cambiar la polaridad y esto hacia que se trabajara bajo el mismo principio de las perforados pero sin necesidad de tener orificios , solo trabajándola por ondas magnéticas, esto se lograba con el componente ferroso que se colocaba sobre la cinta; para asegurarse esos datos se crearon distintas formas que a la larga comenzaron a ser obsoletas, ya que el tamaño que tenían antes cintas era demasiado grande[20].

### 1.5.1. DISCOS MAGNÉTICOS RÍGIDOS

Estos discos fueron los inicios de los disco duros, la idea era construir unas unidades en las que los datos permanecieran permanentemente en la computadora sin perderse cuando la misma se apagara, además de poder movilizar los datos de manera

[20]http://www.monografias.com/trabajos93/historia-y-evolucion-dispositivos-almacenamiento/historia-y-evolucion-dispositivos-almacenamiento.shtml

másrápida, por otro lado también quería eliminarse los costos de los grandes carretes y de cinta que ocasionaba tener los dispositivos magnéticos. Efectivamente se logra crear estas unidades pero las cintas no estaban del todo eliminadas, así que se ven en la necesidad nuevamente de innovar, creando así los discos magnéticos removibles, conocidos como Diskettes, inicialmente se crearon de tamaño 5 ¼" que en su momento fue maravilloso poder contar con un avance tan pequeño, donde pudiese almacenarse tanta información como lo eran cerca de 500Kb inicialmente.

Pero, la tecnología existente en cuanto al resto de la computadora se quedó muy pequeña al lado de la creación de estos grandes dispositivos de almacenamiento y se comienza a desarrollar todos los demás dispositivos que conforman al computador, como lo son:

a. CPU
b. Tarjeta Madre
c. Memoria RAM (mayor capacidad), entre otras.

A raíz de esto todas las empresas diseñadoras de estos equipos comienzan a utilizar la técnica de Miniaturización, cuya creación se les atribuye a los asiáticos; Para poder hacer computadoras personales, ya que hasta el momento solo se les daba uso en grandes empresas.

### 1.5.2. COMPUTADORES PERSONALES

Cuando comienzan a venderse los computadoras personales los interesados en el área comenzaron a estudiar el cómo manejar estos equipos, programar, crear nuevas aplicaciones, entre otras. Y un grupo de estas personas se interesó en desarrollar simulaciones, juegos, y ambientes visuales para el computador, como consecuencia de esto, tanto los procesadores como dispositivos de almacenamiento empezaron a quedarse cortos para todos los recursos que consumían estos juegos y nuevas aplicaciones visuales. De igual manera empezó a ser de urgencia poder transportar todo este software de un computador a otro, ya que se presentaba el mismo problema de las tarjetas perforadas, hacía falta cerca de 5 diskettes para poder grabar un

software bien hecho. Así que desarrollan los discos de 3 ½" y las nuevas computadoras salen al mercado con estas nuevas unidades, capaces de almacenar hasta 1.44 Mb sosteniendo el mismo principio de los discos de 5 ¼ " pero con una densidad de "pequeños imanes" mayor en un espacio menor.

Pese a que la evolución de los discos duros está inmersa con la creación de los dispositivos magnéticos de almacenamiento, es preferible considerarlo en un punto aparte ya que su estructura compleja amerita utilizar un espacio reservado para él.

Siempre han tenido el mismo principio de desarrollo, que consiste en que los discos duros se presentan recubiertos de una capa magnética delgada, habitualmente de óxido de hierro, y se dividen en unos círculos concéntricos cilindros (coincidentes con las pistas de los disquetes), que empiezan en la parte exterior del disco (primer cilindro) y terminan en la parte interior (último).

En 1992, los discos duros de 3,5 pulgadas alojaban 250 Megabytes, mientras que 10 años después habían superado 40 Gigabytes (40000 Megabytes). En la actualidad, ya contamos en el uso cotidiano con discos duros de más de 3 terabytes (TB), (3000000 Megabytes).

### 1.5.3. UNIDAD ZIP

El mercado no varió durante años para los dispositivos de almacenamiento, es decir, no salieron nuevos productos ya que se podía trabajar muy bien con los creados hasta el momento, lo que si se hizo en todos los componentes de un computador personal, fue aplicarles mejores técnicas de desarrollo para que fueran más rápidos y de mayor capacidad, casualmente en esos años aparece una nueva unidad de almacenamiento conocida en su momento como unidad ZIP, estas unidades no estaban disponibles para todas las computadoras ya que no era compatible con casi ninguna arquitectura creada hasta el momento, pero la parte importante de estas unidades es que su capacidad era bastante alta, inicialmente fueron de 50 Mb y fueron aumentando con el

tiempo; Sin embargo, no tuvo mucho éxito pese a su gran capacidad para la época, las razones de esto fueron:
No eran 100% compatibles con las computadoras clon, que eran las más vendidas (Y siguen siendo). Sus costos de las unidades eran muy altos, tanto el dispositivo de lectura/escritura, como el de almacenamiento.Siempre fueron planteados como unidad adicional al equipo, situación que no ayudó a su fácil comercialización. Y por último su principio también era el de los diskettes y/o cintas magnéticas, solo eran un poco más grandes que las unidades de 3 ½" sin llegar a los de 5 ¼"

### 1.5.4. DISCOS COMPACTOS

Pasado un tiempo cuando ocurre la aparición del modelo 80586 de Intel cuando se logran ver los primeros resultados de un estudio de años, y eran los Discos compactos, conocidos como Cd´s, en estas unidades se podía almacenar hasta 650 Megabytes, lo que era un gran avance ya que todavía estaban disco duros con menor capacidad vigentes en el mercado, así como también habían de mayor capacidad de los mismos.

### 1.5.5. DVD

Una vez más los desarrolladores de tecnología no descansan, y comienzan a ver que ahora que los discos duros tienen 80 GB. Se presenta de nuevo el problema de hacer soporte de datos, ya que para hacer un soporte de un disco de 70 Gigas, hacen falta 100 cd´s lo cual es demasiado, también se presenta el problema de las películas, ya que el formato de VHS se comienza a considerar obsoleto y malo, entonces se decide sacar un nuevo formato de disco, con una tecnología óptica ya que resulta mucho más económica y confiable que las anteriores. Este nuevo desarrollo es conocido con el nombre de DVD, prácticamente popular debido a que los formatos de películas los comenzaron a hacer para este tipo de dispositivo, ya que al ser de mayor capacidad puede tener una mejor calidad de imagen y sonido la grabación en ellos[21].

[21] http://www.monografias.com/trabajos93/historia-y-evolucion-dispositivos-almacenamiento/historia-y-evolucion-dispositivos-almacenamiento.shtml#ixzz2cNNjGx2V

## 1.6.RESEÑA HISTÓRICA DEL HABEAS DATA O EL DERECHO A LA INTIMIDAD

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

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

Tiempo después, aproximadamente desde 1960 y como reacción al vertiginoso desarrollo tecnológico que se traduce en nuevos sistemas informáticos, tanto en los Estados Unidos como en Gran Bretaña se empiezan a promover proyectos legislativos que, dando un nuevo giro o extensión al concepto de derecho a la privacidad, se refieren a la protección de la libertad y esfera personal frente a posibles excesos del registro informatizado o difusión de datos e informaciones vinculadas a aspectos reservados o íntimos.

Se llegó así, finalmente, a la "PrivacyAct" norteamericana del 31 de diciembre de 1974, a la "Data ProtectionAct" británica de 1984, y a la Ley Orgánica mayo de 1992 española, denominada "Regulación del tratamiento automatizada de datos".

A nivel de los textos constitucionales, la Carta de Portugal de 1976 estableció, en su art. 35º, el derecho del ciudadano a: a) Conocer las informaciones que le conciernen almacenadas en archivos, su finalidad y la posibilidad de rectificarlas o actualizarlas; b) A que la información no sea utilizada para el tratamiento de datos "sensibles", referentes a convicciones políticas, religiosas o a asuntos de la vida privada, salvo que se trate de datos no identificables personalmente, con fines meramente estadísticos; c) A que no se atribuya a los ciudadanos un número nacional único de identificación.
La Constitución Española de 1978 estableció, en su art. 18.4, que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". A su vez, en su art. 105, b), asegura "el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de la persona".

En el ámbito latinoamericano, fue la Constitución Brasileña de 1988, en su art. 5º, inc. LXXII, la primera en abordar estos temas, pero sobre todo también la primera en "bautizar" constitucionalmente al instituto del hábeas data. Dicha norma dispone que: "Se concederá Hábeas Data: a) Para asegurar el conocimiento de informaciones relativas a la persona de quien lo pide, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) Para la rectificación de datos, cuando no se prefiera hacerlo en proceso reservado judicial o administrativo". El nombre Hábeas Data fue tomado de la Ley 824 del Estado de Río de Janeiro.

La Constitución Colombiana de 1991, ha establecido en su art. 15º que todas las personas tienen derecho a la intimidad personal y familiar y a su buen nombre, con la obligación del estado de respetarlos y hacerlos respetar. Agrega luego: "De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

A su turno, la Constitución del Paraguay de 1992, en su art. 1350º, establece expresamente el hábeas data y dispone: "Toda persona podrá acceder a la información y a los datos que sobre sí mismo sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaren ilegítimamente sus derechos".

Como acertadamente señala SAGUÉS la novedad principal de la norma paraguaya (por lo demás bastante completa en su regulación del hábeas data) radica en que no solo comprende dentro de la protección de este instituto los consabidos derechos personales como privacidad, no discriminación, reserva sobre convicciones políticas o religiosas; sino también derechos personales de índole patrimonial, referidos a información o datos sobre bienes.

Más recientemente, la Constitución Argentina, con la reforma aprobada en 1994 regula expresamente en el art. 43º el hábeas data, estableciendo que: "Toda persona puede interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

En definitiva, estos desarrollos doctrinarios y normativos fueron configurando un nuevo término y una suerte de derecho autónomo conocido como "libertad informática", un derecho que "tiene por objeto garantizar la facultad de las personas para conocer y acceder a la información que las concierne, archivada en bancos de datos.

Esto es el hábeas data: un instrumento para controlar la calidad de ellos, corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su posible transmisión".

Siguiendo la doctrina sentada por el Tribunal Constitucional Alemán, puede hablarse de un "derecho a la autodeterminación informativa" consistente en la facultad de disponer sobre la revelación y utilización de los datos personales, que abarca todos las etapas de la elaboración y uso de datos por medios informáticos, es decir, su almacenamiento, registro, calificación, modificación, transmisión y difusión[22].

### 1.6.1. DERECHO A LA INTIMIDAD Y HABEAS DATA EN BOLIVIA

La Constitución política del año 1831 reconoce por primera vez algunos indicios del Derecho a la Intimidad, esta fue plasmada en uno de los artículos del Título Ultimo De las garantías, detallado a continuación:

Artículo 163. Están prohibidas las requisiciones arbitrarias, y el apoderamiento injusto de los papeles y correspondencias de cualquier boliviano. La ley determinará en qué casos, y con qué justificación, puede procederse a ocuparlos.

Durante las constituciones siguientes solo figuraba la inviolabilidad al secreto de cartas, los papeles privados y la correspondencia epistolar. Ya para las reformas a la Constitución de 1995, mediante Ley Nº 2410 del 8 de agosto de 2002 este artículo fue modificado, incorporándose un artículo dedicado solo y exclusivamente al Habeas Data, que a la letra decía:

ARTÍCULO 23º.- Acción de Habeas Data
I. Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético, informático en archivos o bancos de datos públicos o privados que afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución, podrá interponer el recurso de Habeas Data ante la Corte Superior del Distrito o ante cualquier Juez de Partido a elección suya. II. Si el tribunal o juez competente declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos

[22] www.softwarelibre.org.bo/wiki/lib/exe/fetch.php?media=habeas_data

personales cuyo registro fue impugnado. III. La decisión que se pronuncie se elevará en revisión, de oficio ante el Tribunal Constitucional, en el plazo de veinticuatro horas, sin que por ello se suspenda la ejecución del fallo. IV. El recurso de Habeas Data no procederá para levantar el secreto en materia de prensa. V. El recurso de Habeas Data se tramitará conforme al procedimiento establecido para el Recurso de Amparo Constitucional previsto en el Artículo 19º de esta Constitución.

A su vez la Ley Nº 2650 de Reformas a la Constitución Política del Estado del 13 de abril de 2004 modifica este Articulo nuevamente en la cual se regula el "Recurso de Hábeas Data". La mencionada norma sostiene:

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

En el ámbito jurídico boliviano se reconoce expresamente el "Recurso de Hábeas Data", solo a partir de la reforma constitucional de 2002, con unas características, objetivos, fines, competencia y jurisdicción especiales y con un procedimiento breve y sumario seguido para el recurso de amparo constitucional.

El derecho boliviano siguiendo parámetros y pautas iberoamericanas sobre el recurso de Hábeas data estilo argentino, el recurso de amparo tipo español, la acción de tutela al estilo colombiano, edifica constitucionalmente su propio recurso de hábeas data con un ámbito limitado de protección y defensa de derechos fundamentales, los cuales los enuncia taxativamente así: "*la intimidad y privacidad personal y familiar, a su imagen, honra y reputación reconocidos en esta Constitución"*; sin embargo, es amplia la legitimación por activa para incoar dicho recurso ante la "Corte Superior del Distrito" o ante cualquier "Juez de partido", a elección de "*Toda persona que creyere estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos…"*

A diferencia del recurso de Hábeas Data Argentino que además de reconocer constitucionalmente el derecho de acceso y conocimiento de los datos o informaciones de la persona humana o de sus bienes y el derecho de solicitar la supresión, rectificación, confidencialidad o actualización de los mismos, siempre que se presente una "falsedad o discriminación" por quienes manejen, almacenen, administren, registren o utilicen "*registros o bancos de datos públicos o privados destinados a proveer informes",* el recurso de Hábeas boliviano amplia el marco de posibilidades para ejercer las facultades del derecho de Hábeas Data, no solo para el acceso y conocimiento de la información, sino para la eliminación, rectificación y actualización de los datos personales. En efecto, éste recurso constitucional se justifica ejercerlo por toda persona cuando "*creyere estar indebida o ilegalmente impedida*" para ejercer las facultades o derechos constitutivos del Hábeas data: acceso, rectificación, eliminación y actualización de la información de la persona concernida.

Si bien este compás más amplio de legitimación del recurso pudiera parecer un tanto ambiguo, por lo menos en el término "*indebido*", ya este tiene diferentes significados, pues se entiende indebido aquello que "no es obligatorio ni exigible", también lo que es "ilícito, injusto o falto de equidad", según el diccionario. Esto traería problemas de interpretación y aplicación de la norma constitucional en forma directa por parte de los jueces de la República Boliviana, así como de la jurisdicción constitucional en el obligado recurso de revisión que tiene que realizar en todos los casos en los que el

conflicto jurídico sea la vulneración o quebrantamiento del Hábeas Data. Quizá el término pueda “cerrárselo”, sin violar la constitución, por parte del legislador boliviano cuando desarrolle y reglamente legislativamente el artículo 23, constitucional. Entiéndase “cerrar” a los efectos de una mejor interpretación jurídica unívoca del término “indebido” con parámetros conceptuales que precisen que sería lo indebido para los destinatarios de la norma y como esos conceptos relacionados en eventualidades concretas puede vulnerar, quebrantar o violar el Hábeas Data. Esa labor interpretación de la norma constitucional no sólo debe dejarse a la jurisprudencia del Tribunal Constitucional, cuando revisa los recursos de hábeas data avocados, tramitados y decididos por los “jueces de partido”, sino que la debe hacer el legislador que es el “intérprete auténtico” y primario de la Constitución.

El recurso constitucional de Hábeas Data en Bolivia, respecto de la determinación del objeto de protección y garantía, hace una descripción amplia de los medios electrónicos (“magnéticos”, “archivos o bancos de datos”) o manuales y mecánicos (“físicos”, “información en archivos”), por los cuales se puede atentar, amenazar o desconocer las facultades o derechos del titular o concernido de los datos personales. La relación pormenorizada de los medios por los que se puede vulnerar el Hábeas Data, si bien parece exagerado para el texto constitucional, no así el texto normativo que se dicte en virtud de aquél, no debe soslayarse, pues algunos textos constitucionales que regulan el Hábeas Data creen sólo suficiente con mencionar a los medios electrónicos, telemáticos o informáticos para identificar los objetos con los cuales se puede vulnerar el Hábeas Data y se echan de menos los medios mecánicos, manuales, escriturarios o tradicionales por los que se ha creado, almacenado, registrado o actualizado información de las personas o de sus bienes, los cuales siguen ocupando un amplio sector de la información tanto pública como privada en cualquier Estado del mundo.

Los archivos de información escriturarios son tan antiguos como la historia misma del ser humano. En cambio, los archivos de información electrónica, son relativamente nuevos, pues sólo éstos sobrevinieron con la entrada en escena de los computadores, faxes, equipos de transmisión de datos o bits de información, etc., es decir, con el llamado “*poder informático*”: la informática, la telegestión y la teletransmisión de datos,

en manos públicas y privadas. Bien es cierto, que el Hábeas Data nace en la mayoría de países europeos, americanos, asiáticos y australianos como una manifestación del "*poder informático*", no deberá desconocerse que la información como un bien jurídico tutelado en todas las constituciones mundiales no sólo se recolecta, almacena, registra y actualiza en archivos, registros o bancos de datos electrónicos, sino desde tiempos inmemoriales en medios escriturarios, mecánicos o manuales. Con una u otra forma de recolección o almacenamiento de información personal o datos se puede vulnerar el Hábeas Data, si se realiza contrariando el ordenamiento jurídico vigente.

La norma constitucional que instituye el recurso de Hábeas Data Boliviano, resulta igualmente parecida a una norma legislativa con ese fin, cuando relaciona la jurisdicción y competencia del "recurso", así como en trámite procedimental de iniciación, terminación y revisión oficiosa del mismo. En efecto, estos aspectos que deberían ser objeto de la norma legislativa reglamentaria del recurso, la Constitución Boliviana lo reglamenta pormenorizadamente, creemos para que el legislador sigas estos parámetros constitucionales sin tratar de deformar o vaciar de contenido la norma. Esta serie de prevenciones constitucionales es casi una regla en el constitucionalismo latinoamericano y por eso nuestras constituciones antes que otra cosa, parecen verdaderos códigos reglamentarios de la vida institucional, política, jurídica, económica y social de los Estados.

Si bien, el artículo 23 de la Constitución Boliviana, en el inciso V, aclara que el recurso de Hábeas Data se tramitará conforme al procedimiento establecido para el recurso de Amparo constitucional, en los incisos I a III, se establecen reglas y parámetros constitucionales específicos para el recurso de Hábeas Data. Así, se dice que el Tribunal o Juez competente, que lo será la "Corte Superior de Distrito" o cualquier "Juez de Partido" a libre escogencia de la persona concernida o titular de los datos personales a quien se le impide ejercer las facultades de acceso, conocimiento, rectificación, eliminación o actualización de datos, si "*declara procedente el recurso, ordenará la revelación, eliminación o rectificación de los datos personales cuyo registro fue impugnado*".

Por su parte, el Tribunal Constitucional Boliviano conocerá de “oficio” las decisiones en las que se pronuncien los Jueces de partido o la Corte Superior de Distrito sobre el Hábeas Data, en el plazo improrrogable y limitado de “veinticuatro horas”. La revisión del Tribunal sin constituirse en una segunda instancia de éste recurso, tiene la virtualidad de no suspender los efectos jurídicos y materiales del “fallo” producido por los jueces y/o la Corte Superior de Distrito, vale decir, que el fallo se cumple o ejecuta pese a la revisión del Tribunal Constitucional.

El recurso de Hábeas data boliviano tiene identidad propia y se puede considerar como un recurso autónomo y una garantía constitucional para proteger y defender los datos o informaciones de una persona o ciertos derechos fundamentales (Intimidad, imagen, honra y reputación). Sin embargo, en cuanto al trámite procedimental, salvo las pautas constitucionales previstas en el artículo 23 y a las que nos hemos referido *ut supra*, se rige por el trámite previsto para el recurso de amparo constitucional previsto en el artículo 19 de la Constitución, con lo cual el recurso de Hábeas Data, procedimentalmente se convierte en una especie de recurso de amparo constitucional. En tal virtud, su naturaleza jurídica es mixta, pues en lo sustantivo el recurso de Habeas Data es un derecho y garantía fundamental autónoma y desde el ámbito adjetivo es un instrumento procesal de defensa de derechos constitucionales al estilo de un “*amparo informativo*” del derecho constitucional argentino.

Finalmente, el inciso V del artículo 23, sostiene que “*el recurso de Hábeas Data no procederá para levantar el secreto en materia de prensa*”. Creemos que esta excepción a la procedencia del Hábeas Data en Bolivia quedó expresamente normada en atención a la alta sensibilidad y vulnerabilidad que despertaba en aquél país el derecho a la información y opinión públicas y la libertad de expresión o de prensa, y en particular a la libertad periodística, no solo por la poco estabilidad de los regímenes democráticos y políticos sino por los casi insolutas dificultades sociales, económicos y legislativos en los que vive el país.

El profesional de las comunicaciones boliviano *Camacho Azurdy*, al comentar el complejo proceso social, político, jurídico y legislativo referido a la *“discusión del derecho de acceso a la información*” pública y privada en el país, hace un análisis de

los instrumentos constitucionales, legislativos e internacionales sobre el derecho de la información consagrado en la Constitución Boliviana desde 1967, así mismo analiza los mecanismos sociales y jurídicos nacionales e internacionales implementados por su país contra los diferentes y sofisticados medios de corrupción empleados en el sector público ("soborno, malversación o peculado, tráfico de influencias, abuso de funciones o del cargo, enriquecimiento ilícito, blanqueo del producto del delito, encubrimiento, obstrucción de la justicia") y privado.

Relata el autor citado, como solo hasta finales de Abril de 2002, el proyecto de la primera ley anticorrupción que tuvo pleno consenso entre los partidos oficialismo y la oposición, "*La Ley de Transparencia de la Administración Pública"* –más conocida como Ley de Transparencia o de acceso a la información pública— fue sancionada el 4 de septiembre de ese año y "*cuatro días después, este proyecto fue vetado por el entonces Presidente de la República, Gonzalo Sánchez de Lozada por fallas procedimentales…*". Así Bolivia se volvió a quedar sin una normatividad específica que salvaguardara derechos y libertades constitucionales de sus habitantes.

Como sostuviera en 1997, el profesor universitario Benjamín Miguel H., en el ámbito del Seminario Internacional sobre el Hábeas Data realizado en la Universidad chilena de Talca, el país para la fecha no tenía mayores informaciones sobre el Hábeas Data y por ello en la reforma constitucional de 1994, nada quedó plasmado en la Constitución sobre el tema, pero sí algunos derechos y libertades constitucionales correlativos a éste como el derecho de amparo, el Habeas Corpus, la libertad de conciencia, la intimidad y la prohibición a la interceptación de las comunicaciones. Por si fuera poco, aun conociendo del tema, tampoco lo hubieran podido incorporar en forma expedita a la Constitución porque en Bolivia los procesos de reforma constitucional son "muy estrictos", pues en "*unalegislatura hay que declarar la necesidad de la reforma, transcribiendo textualmente el proyecto; luego hay que esperar la renovación de éste Poder del Estado, para luego por 2/3 entrar a discutir la reforma. Pero en esta segunda fase solo puede aprobarse o rechazarse el proyecto primitivo. Esto ha permitido que las constituciones no se reformen a medida de los gobiernos, los cuales son siempre transitorios*".

En la Reunión la "Sociedad Interamericana de Prensa (SIP) en el año de 2002, el pleno evidenció que "no se halla plenamente garantizado el derecho de acceso a la información pública en ningún país de América Latina, a pesar de estar contemplado en la mayoría de las Constituciones como una garantía constitucional…" Por su parte y en aquella época, en Bolivia, se presenta y discute "*el anteproyecto de Ley de Necesidad de reforma constitucional elaborado por el Consejo ciudadano para la reforma de Carta Magna que se debatió en el Congreso Nacional, se considera que el recurso de Hábeas Data viola la libertad de prensa y el derecho del secreto de imprenta porque obliga a los periodistas a dar a conocer la fuente de una información que puede ser considerada como violatoria de los derechos y garantías indicadas en la CPE…El 31 de Julio de 2002, el Congreso aprobó la esperada y polémica Ley de Necesidad de Reformas de la Constitución, en la que lamentablemente no se contempla el derecho de acceso a la información pública… En esta dirección, la Carta Magna pone en vigencia, por primera vez en la historia del país, el recurso jurídico de Hábeas Data que, según ésta, deberá ser tratada por las cortes de justicia conforme y bajo la misma modalidad del Hábeas corpus y el amparo constitucional*…".

En el 2003, en Santa Cruz de la Sierra en la XIII Cumbre Iberoamericana de los Jefes de Estado y de Gobierno, se suscribió una Declaración que lleva el nombre de la ciudad, en la cual se reafirmó la voluntad de todos los países asistentes para "*combatir la corrupción en los sectores públicos y privados y la impunidad, que constituyen una de las mayores amenazas a la gobernabilidad democrática*"; además agregaban, "*que, conforme con los respectivos ordenamientos jurídicos, el acceso a la información en poder del Estado promueve transparencia y constituye un elemento esencial para la lucha contra la corrupción y es condición indispensable para la participación ciudadana y el pleno goce de los derechos humanos*".

En la Declaración de Santa Cruz de la Sierra, concordantemente con lo anterior, en el *"punto 45 se hace referencia a la protección de los datos personales como un derechofundamental y se destaca la iniciativa de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenida en la*

*Declaración de La Antigua, por la que se crea la Red Iberoamericana de Protección de Datos…".*[23]

## 1.7. EVOLUCIÓN DEL CONCEPTO DE PROTECCIÓN DE DATOS

A partir del Siglo XVIII los derechos humanos comenzaron a estar presentes, y con su reconocimiento en las normativas constitucionales, fueron alcanzando su consolidación como prerrogativas inherentes a todo ser humano.

Esto es, los derechos individuales y en particular, el reconocimiento de la libertad personal. En este concepto se incorporó el derecho a la intimidad de la persona como prerrogativa objeto de tutela, ya no solo en los instrumentos internacionales, sino además, en sede constitucional de cada país.

Sin embargo, en la situación actual este derecho ha ido variando considerablemente. En virtud de que el desarrollo tecnológico ha redimensionado las relaciones del hombre con sus semejantes, así como en su marco de convivencia. Hoy, no podemos negarlo, la informática se ha convertido, en el símbolo emblemático de la cultura contemporánea.

Por ello el reconocimiento del derecho a la intimidad – en sus diversas manifestaciones- luego de lograr su consolidación como un derecho fundamental, ha ido alcanzando nuevos matices.

Ahora, con el tratamiento, la recolección, el almacenamiento de informaciones que antes solo podía formar parte de la vida íntima de cada ser humano – o bien, era conocido por un mínimo sector-, ha ido variando paulatinamente su entorno y su estructura. Esto es, los datos personales de toda persona se han convertido en una práctica habitual del contorno y almacenamiento por parte de los sectores tanto públicos como privados.

[23] www.informatica-juridica.com/.../La_vision_constitucional_del_habeas_data.asp

Es por ello que el derecho a la intimidad ha tenido que ir re direccionando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora supone un reconocimiento de un derecho de control y acceso de sus informaciones, es decir de toda aquella información relativa a su persona.

Por tal motivo, el uso y control sobre datos concernientes a cada persona, debe serle reconocido ya no solo como una mera prerrogativa, sino además como un derecho fundamentalmente protegido y garantizado por mecanismos de protección idóneos[24].

[24]http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm

# CAPITULO II

# MARCO TEÓRICO

## 2.1. NOCIÓN DE ARCHIVO

El archivo de forma general se trata de un espacio dedicado a la recopilación de cierta información que requiere ser encontrada en determinado caso o situación de manera sencilla y ordenada, su función principal es mantener la información tal y como se la almaceno pudiendo ser modificada, actualizada, corregida, etc.

## 2.2. ARCHIVO INFORMÁTICO

Los archivos en informática es información almacenada de manera digital en algún medio especialmente diseñado para este fin, como discos duros, memorias flash o USB (más conocidas como pendrive). Poseen una identificación o nombre creado por el usuario, y además de ésta contienen una abreviación que corresponde e identifica al tipo de archivo, por ejemplo un archivo de Word, la abreviación es ".doc", y para uno de Excel, esta es ".xls", etc...

Reciben este nombre pues en sus inicios la información de tipo digital como lo son los programas informáticos, se almacenaban usando tarjetas perforadas y se guardaban en carpetas rotuladas, tal como se haría en cualquier oficina con la información "de papel". La gran ventaja está en que al guardar la información en la computadora se facilita su organización, se optimiza enormemente el espacio (una biblioteca completa cabe hoy en día en la palma de la mano), y resulta todo más ágil.

Cada archivo tiene un número determinado de bytes (“paquetes" de información) el que indica el tamaño o peso de la información que contiene. Siempre el número de bytes será positivo y su máximo dependerá del sistema que presente la computadora que lo almacena. Lo que ocurre es que en la informática, por increíble que parezca, la información consiste básicamente en combinaciones de ceros y unos, que son

interpretados luego por cada programa; estas secuencias de números conforman cada "byte" de información.
Los archivos de una computadora están sujetos a diversos cambios según su usuario lo estime; puede moverlos, modificarlos, aumentarlos, reducirlos, renombrarlos y borrarlos.

Los archivos son almacenados en discos duros que giran dentro de la computadora y que son capaces de registrar información de acuerdo a su capacidad de almacenamiento. Estos discos duros permiten un acceso instantáneo a los archivos almacenados en ellos. Cuando las computadoras son muy grandes los archivos pueden ser guardados en lo que se conoce como cintas magnéticas. En el caso de que no se quiera ocupar espacio en el disco duro de la computadora, pueden ser guardados en discos compactos para grabar o memorias transportables y de esta manera poder ser abierto en una computadora distinta a la que creó el archivo.

Los medios de almacenamiento mencionados están quedando rápidamente obsoletos, conforma avanza la tecnología; se estima que en unos pocos años la capacidad de los dispositivos USB, como los famosos pendrives, será de tal magnitud que prácticamente no habrá límite en la cantidad de cosas que se puedan guardar en ellos, y los discos duros con piezas móviles pasarán al olvido.

Como se dijo anteriormente cada archivo recibe un nombre, y es almacenado en un directorio específico, como un sistema de carpetas en una oficina tradicional. El nombre de un archivo no se puede repetir con otro que esté guardado en el mismo directorio, si se intenta hacerlo, inmediatamente la computadora protestará. En las computadoras más antiguas el nombre del archivo tenía que tener un número limitado de caracteres, pero las más modernas permiten nombres largos e incluso cualquier combinación de letras y dígitos. Los archivos son almacenados en carpetas, directorios o catálogos, sin importar el número que cada uno de estos almacene.

Pese a la comodidad que implica tener guardados archivos en una computadora, siempre existen temores en cuanto a la protección que este almacenamiento brinda. Por esta razón se han creado diversos sistemas informáticos cuyo objetivo es proteger

a los archivos frente a accidentes o daños intencionados. Por ejemplo, existen algunos que restringen el acceso a un determinado archivo y así se controla quién los ve, modifica, borra o mueve[25].

## 2.3. ACCESO A LOS ARCHIVOS

Se refiere al método utilizado para acceder a los registros de un archivo. Existen distintas formas de acceder a los registros:

**Secuenciales**; los registros se leen desde el principio hasta el final del archivo, de tal forma que para leer un registro se leen todos los que preceden.
**Directo**; cada registro puede leerse de forma directa solo con expresar su dirección en el fichero por él número relativo del registro o por transformaciones de la clave de registro en él numero relativo del registro a acceder.
**Por Índice**; se accede indirectamente a los registros por su clave, mediante consulta secuencial a una tabla que contiene la clave y la dirección relativa de cada registro, y posterior acceso directo al registro.
**Dinámico;** es cuando se accede a los archivos en cualquier de los modos anteriormente citados.

La elección del método está directamente relacionada con la estructura de los registros del archivo y del soporte utilizado.

La mayoría de los sistemas de archivos modernos permiten asignar permisos (o derechos de acceso) a los archivos para determinados usuarios y grupos de usuarios. De esta manera, se puede restringir o permitir el acceso de un determinado usuario a un archivo para su visualización de contenidos, modificación y/o ejecución (en caso de un archivo ejecutable)[26].

## 2.4. OPERACIONES SOBRE LOS ARCHIVOS

[25] http://www.misrespuestas.com/que-es-un-archivo.html
[26] http://tecnoboard.bligoo.com.ve/western-digital-ya-adapata-sus-discos-duros-a-windows-8

Las operaciones generales que se realizan sobre los archivos son:

**Creación**. Escritura de todos sus registros.

**Consulta.**Lectura de todos sus registros.

**Actualización**. Inserción supresión o modificación de algunos de sus registros

**Clasificación**. Reubicación de los registros de tal forma que queden ordenados según determinados criterios.

**Borrado**. Eliminando total del archivo, dejando libre el espacio del soporte que ocupaba.

## 2.5. ORGANIZACIÓN DE ARCHIVOS

La mayoría de las computadoras organizan los archivos en jerarquías llamadas *carpetas, directorios* o *catálogos*. (El concepto es el mismo independientemente de la terminología usada.) Cada carpeta puede contener un número arbitrario de archivos, y también puede contener otras carpetas. Las otras carpetas pueden contener todavía más archivos y carpetas, y así sucesivamente, construyéndose una estructura en árbol en la que una *carpeta raíz* puede contener cualquier número de niveles de otras carpetas y archivos. A las carpetas se les puede dar nombre exactamente igual que a los archivos. El uso de carpetas hace más fácil organizar los archivos de una manera lógica.

### 2.5.1. ARCHIVOS DE TEXTO

Son utilizados para almacenar documentos que consisten en texto, en ellos, cada registro es un solo símbolo o código de control. El leer estos archivos recibimos la información en orden secuencial en el que aparece cuando lo vemos en un monitor. Los archivos de texto son una secuencia de líneas separadas por marcas de fin de línea[27].

.

### 2.5.2. ARCHIVO INDIZADO

[27] http:/si.ua.es/es/documentos/documentacion/.../teoria-de-bases-de-datos.pdf

Es la aplicación de incluir índices en el almacenamiento de los archivos; de esta forma nos será más fácil buscar algún registro sin necesidad de ver todo el archivo.

Un índice en un archivo consiste en un listado de los valores del campo clave que ocurren en el archivo, junto con la posición de registro correspondiente en el almacenamiento masivo.

Los índices tienen fundamento especificado a continuación:
a.- La colocación de un listado al inicio del archivo: para la identificación del contenido.
b.- La presentación de un segundo índice: para reflejar la información de cada punto principal del índice anterior.
c.- La actualización de los índices: Cuando se insertan y eliminan archivos, es preciso actualizar los índices para evitar contratiempos actualizando un archivo.
d.- La organización de un índice: Nos evita examinar archivo por archivo para recuperar algún registro buscado; por lo tanto ahorraríamos tiempo si tenemos una adecuado organización de los índices[28].

### 2.5.3. IDENTIFICACIÓN DE ARCHIVOS

En los sistemas informáticos modernos, los archivos siempre tienen nombres. Los archivos se ubican en *directorios*. El nombre de un archivo debe ser único en ese directorio. En otras palabras, no puede haber dos archivos con el mismo nombre en el mismo directorio.El nombre de un archivo y la ruta al directorio del archivo lo identifica de manera particular entre todos los demás archivos del sistema informático, de tal manera que no puede existir dos archivos con el mismo nombre y ruta.

Cuando una computadora permite el uso de carpetas, cada archivo y carpeta no sólo tiene un nombre propio, sino también una *ruta*, que identifica la carpeta o carpetas en las que reside un archivo o carpeta.

[28]http://www.slideshare.net/favi_hola/indizacion-y-operaciones

Muchos (pero no todos) sistemas informáticos usan extensiones en los nombres de archivo para ayudar a identificar qué contienen.

### 2.5.4. ALMACENAMIENTO DE ARCHIVOS

En términos físicos, la mayoría de los archivos informáticos se almacenan en discos duros —discos magnéticos que giran dentro de una computadora que pueden registrar información indefinidamente—. Los discos duros permiten acceso casi instantáneo a los archivos informáticos.

Hace unos años solían usarse cintas magnéticas para realizar copias de seguridad. También se usaban otros medios de almacenamiento como discos compactos grabables, unidades Zip, etcétera.

No obstante en la actualidad han cobrado mucho auge las memorias flash, dispositivos con mucha capacidad de almacenamiento que tienen la ventaja de ser pequeños y portátiles; suelen usarse para guardar archivos en dispositivos pequeños como teléfonos móviles o reproductores de audio portátiles[29].

### 2.5.5. PROTECCIÓN LEGAL DE LOS DATOS PERSONALES EN ARCHIVOS

La protección de datos personales se ubica dentro del campo de estudio del Derecho Informático. Se trata de la garantía o la facultad de control de la propia información frente a su tratamiento automatizado o no, es decir, no sólo a aquella información albergada en sistemas computacionales, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

En algunos países la protección de datos encuentra reconocimiento constitucional, como derecho humano y en otro simplemente legal; ninguna de estas figuras prevé nuestra legislación.

[29] http://www.archivonorma.com/old/index.php?secc_id=10&flag=5&tips_id=270

## 2.6. LOS DATOS

### 2.6.1. LOS DATOS DE CARÁCTER PERSONAL

Los datos de carácter personal están referidos legalmente como cualquier información numérica, alfabética, grafica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Se considera que una información hace referencia a una persona física identificada cuando nos indica directamente a que persona se refiere sin necesidad de que tengamos que realizar ningún tipo de averiguación posterior. Un claro ejemplo de ello lo tenemos en los Documentos o Cedulad de Identidad (CI) que está considerado como dato de carácter personal porque la información que contiene identifica perfectamente a una persona física determinada.

Una información hace referencia a una persona física cuando a priori no nos indica a qué persona se refiere pero nos aporta información suficiente para poder llegar a averiguar su identidad. El ejemplo más claro lo tenemos en el ADN, que sabemos que contiene información genética concerniente a una persona concreta pero no sabremos de quién se trata hasta que no lo sometemos al procedimiento adecuado. Esta última se trata de una información concerniente a una persona identificable.

Existen tipos de datos de carácter personal:

- Datos especialmente protegidos: ideología, afiliación sindical, religión, creencia, origen racial o étnico, salud y vida sexual.
- Datos de carácter identificativo: cédula de identidad, dirección, imagen, voz, número de seguro social o mutualidad, teléfono, nombre y apellidos, firma huellas, carnet sanitario.
- Datos relativos a las características personales: datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, lengua materna, características físicas o antropométricos.

- Datos relativos a las circunstancias sociales: características de alojamiento, vivienda, situación familiar, propiedades, posesiones, aficiones y estilos de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.
- Datos académicos y profesionales: formación, titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios u asociaciones profesionales.
- Detalles de empleo: profesión, puestos de trabajo, datos económicos de nómina, historial de trabajo.
- Datos que aportan información comercial: actividades y negocios, licencias comerciales, suscripciones a publicaciones con medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- Datos económicos, financieros y de seguros: ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, datos bancarios, plan de pensiones, jubilación, datos económicos, seguros, hipotecas, subsidios, beneficio, historial de créditos, tarjetas de crédito.
- Datos relativos a transacciones de bienes y servicios: bienes y servicios suministrados por el afectado, bienes y servicios recibidos por el afectado, transacciones financieras, compensaciones o indemnizaciones[30].

## 2.7. EL REGISTRO INFORMÁTICO

En informática, un registro (también llamado fila) representa un objeto único de datos implícitamente estructurados en una tabla. En términos simples, una tabla de una base de datos puede imaginarse formada de filas y columnas o campos. Cada fila de una tabla representa un conjunto de datos relacionados, y todas las filas de la misma tabla tienen la misma estructura.

Un registro es un conjunto de campos que contienen los datos que pertenecen a una misma repetición de entidad. Se le asigna automáticamente un número consecutivo (número de registro) que en ocasiones es usado como índice aunque lo normal y práctico es asignarle a cada registro un campo clave para su búsqueda.

[30] www.cuidatusdatos.com/infodatospersonales.html

## 2.8. INFORMACIÓN

Se trata de un concepto sumamente amplio en que convergen todas las disciplinas, debido a esto sólo se podrá conocer lo que es la información desde algunos de sus puntos de vista en particular, obviando por un momento las demás visiones al respecto..

Por lo general, desde el sentido común, se comprende que la información es todo aquel conjunto de datos que nos permiten saber sobre determinada cosa, evento, fenómeno, etc. Por ejemplo, dentro de la información podemos encontrar datos que describan físicamente un objeto, así como también su origen, sus usos, su historia, etc.

Podemos obtener información también sobre ciertos sucesos, por ejemplo, a través de las noticias. En este caso la información estaría dada por los antecedentes del caso, los personajes involucrados, el contexto en el que sucedió, que fue aquello que aconteció, entre otras.

La información no siempre se definirá de la misma manera. Como vemos, se trata de un concepto tan amplio que se aplica de manera diferente para cada caso incluso, desde una misma disciplina. Sin embargo, si tomamos en cuenta su concepción más amplia, es posible decir que la real función de la información es el poder aumentar el conocimiento que las personas tienen sobre algo, lo que en algunos casos puede ayudar en la toma de decisiones y en la evaluación de determinados procesos, hechos, personas o cosas.

Cuando hablamos de la "era de la información", nos referimos al hecho de que la informática (las computadoras) ha permitido el almacenamiento masivo de una enorme, casi infinita cantidad de datos, disponibles al instante sobretodo hoy en día debido a la existencia de la Internet; por lo mismo el énfasis en la educación, y por supuesto en la ciencia de la informática está en saber ordenar y obtener datos, más que memorizarlos, como se enfatizaba en el pasado. Nadie puede abarcar todo el

conocimiento disponible en el mundo, por lo que importante hoy en día es saber buscar[31].

## 2.8.1. DERECHO A LA INFORMACIÓN

Hoy en día, en el mundo jurídico y, más específicamente, en el de los derechos humanos es muy común escuchar acerca del derecho a la información, pero no realmente se puede hablar del tema sin saber el real significado y avances. Y es que se suelen confundir con los términos como derecho de la información, libertad de información y derecho de acceso a la información o derecho a la información pública.

En la ciencia del derecho y particularmente en aquellas disciplinas que se encuentran en proceso de formación, reconocimiento y actualización, no es fácil distinguir con claridad el alcance de distintos conceptos, que por ser utilizados en el lenguaje cotidiano, pueden tener distintos significados. Lo que no es permisible en la ciencia del derecho ya que vulnera el principio de seguridad jurídica y desvanece el papel de la doctrina y de la certeza legal. Es por ello que la definición de conceptos y distinción de vocablos que tienen elementos relacionados entre sí, pero que no significan exactamente lo mismo, es un buen punto de partida para comprender de qué se habla cuando se refiere a la noción de derecho a la información.
El derecho de la información es concebido comúnmente por la doctrina desde dos perspectivas: por un lado, al conjunto de normas jurídicas y por otro como una ciencia:

### 2.8.1.1. EL DERECHO DE LA INFORMACIÓN COMO ORDENAMIENTO

La evolución de las relaciones y derechos comunicativos o informativos a lo largo de la historia crearon la necesidad de establecer una serie de leyes que regularan la relación de las ciencias jurídicas y las ciencias informativas, éstas constituyen el cuerpo jurídico del derecho de la información, derecho que está constituido por el conjunto de normas jurídicas que se establecen en torno a las relaciones informativas o que tienen como objeto de regulación lo que se refiere a la información o a la comunicación social.

[31] www.icesi.edu.co/blogs_estudiantes/efrablog/2009/08/

Reflexionar sobre el derecho de la información como ordenación comporta la convicción de que la transmisión de ideas, pensamientos, opiniones y conocimientos o hechos no sólo es muy anterior a la aparición de las nuevas ciencias sociales y, por supuesto, del derecho cuya formalización heredamos del mundo romano, sino que ha estado presente en toda sociedad, y lo seguirá estando en todo grupo social, aun en el supuesto indeseable de que nos hallemos en una caótica comunidad absolutamente desconocedora de la cultura de los derechos y libertades del ser humano.

El derecho de la información es una rama en formación del derecho en busca de su autonomía respecto de las ramas jurídicas clásicas. Esto debido a que "los avances de la técnica y las modalidades de la vida pueden crear indefinidamente nuevas ramas o hacer desaparecer o refundir en una sola, otras ya existentes".

La rama del derecho que se conoce como derecho de la información aparece y se desarrolla fundamentalmente coincidiendo con lo que se denomina la "sociedad de la información", caracterizada, entre otras cosas, por el surgimiento de una serie de medios técnicos de transmisión y de información, que provocan numerosos efectos sobre el comportamiento individual y colectivo y sobre la formación de hábitos culturales —a los que hoy habría que añadir los originados por la expansión de las nuevas tecnologías y por los cambios operados en la sociedad misma— y que, lógicamente, darán lugar a una adecuada y progresiva regulación jurídica.

### 2.8.1.2. EL DERECHO DE LA INFORMACIÓN COMO CIENCIA

El derecho de la información se puede afirmar como ciencia porque constituye una ordenación de conocimientos susceptibles de sistematización, de tratamiento en diversas fases de generalización y de abstracción, cuyo objeto es la información que reconoce y regula. Se puede afirmar que "es aquella ciencia jurídica que acota los fenómenos informativos de todo tipo y los encauza hacia la justicia".

Al ser el derecho de la información susceptible de ser tratado en cuanto ordenamiento o como ciencia, no debemos considerar a estas perspectivas como alternativas que se

contraponen, sino que se complementan, al ofrecer la ciencia opciones para el adecuado desarrollo del cuerpo normativo en materia de información.

De tal modo que se llega a la conclusión de que el Derecho a la información responde a la necesidad del ser humano de expresarse y dequerer saber lo que los demás han expresado; responde un requerimiento queen determinado momento se vuelve un derecho fundamental del hombre,pues, como hombres de libertad, debemos tener el derecho de expresarnos, deinformar y de ser informados, y tal prerrogativa natural deberá estar garantizadapor el Estado y definida por la sociedad, la cual es definitiva en el proceso degeneración y aprovechamiento de la información; ella es la que se asigna a éstavalor y función[32].

## 2.8.2. ACCESO A LA INFORMACIÓN

Este concepto es amplio, y se requiere saber de qué tema se trata específicamente, por ejemplo tenemos el acceso a la información de un gobierno, acceso a la información pública, que es un derecho que tiene toda persona de buscar y recibir información en poder del gobierno. Las Naciones Unidas, en una de sus primeras asambleas generales afirmó que: "la libertad de información es un derecho fundamental y... la piedra angular de todas las libertades a las que están consagradas las Naciones Unidas". En otras palabras, es un derecho instrumental que puede ser utilizado para garantizar el cumplimiento de otros derechos esenciales del ser humano. También todos tenemos derecho a ser informados como por ejemplo, las noticias, una buena fuente de información que le ha servido a muchas personas tanto ahora como les va a servir en el futuro, para conocer lo que ocurre a su alrededor, en su ciudad, país o mundo entero.

También se conoce como Acceso a la Información al área de la informática y la bibliotecología que se refiere a garantizar el acceso libre y gratuito a la información. El

[32] Daniel Soto Gama, Principios Generales del Derecho a la Información, Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, 2010, pag.40

Acceso a la Información también abarca muchos temas, como los derechos de autor, el Código abierto, la privacidad y la seguridad[33].

### 2.8.2.1. ACCESO A LA INFORMACIÓN PÚBLICA

El acceso a la información pública es uno de los derechos que tenemos como seres humanos que vivimos en sociedad, y al vivir en dicha sociedad a lo que se apunta es a la democracia. La importancia de este derecho tiene su base en un  Su importancia para todos los ciudadanos radica en que es un mecanismo para garantizar una especie de fiscalización por parte de la población a través de la informatización de la gestión estatal de sus gobernantes, consiguiendo de esta manera la transparencia del estado para sus gobernados.

El acceso a la información pública es un derecho en expansión y que responde a las aspiraciones de democratización profunda de los pueblos de todas las naciones. Los ciudadanos no se conforman con un ejercicio ritual de la vida política; demandan mayores canales y niveles de participación; exigen una mayor transparencia a los servidores públicos y entienden la complejidad de los procesos comunicativos.

Pero los Gobiernos y toda aquella actividad que lleva a cabo, tiene como resultado cierta información, que no siempre puede ser de conocimiento de toda la población, es en tal caso que se pone en juicio la afirmación de transparencia, empero el acceso a la informaciónpública  prevé principios de máxima apertura informativa, promoviendo el funcionamiento publicado de las gestiones administrativas, acción que debería de ser permanente.Cualquier excepción debería ser puesta en revisión, para su estudio si corresponde o no ser de conocimiento público.

### 2.8.2.2. ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

Considerando el acceso a la información como publica haremos referencia a que en la actualidad, es posible generar una interacción inmediata con casi cualquier institución pública y con los servidores públicos que laboran en y para ellas. La  cada vez más

[33]http://www.uabcs.mx/transparencia/index.php/acceso-a-la-informacion

amplia gama de posibilidades para el flujo de información a través de medios electrónicos también obliga a preguntarse cómo funcionan dos de los derechos fundamentales que están surgiendo aun en nuestro país y nuestro Estado: los Derechos de Acceso a la Información Pública y el de Protección de Datos Personales.

Es un hecho innegable que han tenido una relevancia cada vez mayor en el cotidiano flujo de información, tanto en medios públicos -radio, televisión, periódicos, noticiarios, revistas- como privados -redes sociales y correo electrónico-; razón por la que debe de realizarse una reflexión:

Para empezar el Derecho de Acceso a la Información, busca la realización de un gobierno democrático que permite el escrutinio público de la gestión de todas las instituciones públicas, con independencia del orden de gobierno al que pertenezcan (federal, estatal o municipal) y, en general, de cualquier persona -individual o colectiva; física o moral- que por cualquier concepto reciba recursos públicos, incluyendo a los sindicatos estatales. Tiene como objetivo, promover e incentivar la contraloría ciudadana y el combate a la corrupción.

Con su ejercicio puede accederse a toda la información del gobierno, con excepción de aquella que eventualmente pueda poner en riesgo la seguridad del estado, las negociaciones del gobierno o generar inestabilidad económica o social, por destacar algunas. Sin embargo, para ello la autoridad que estime posible ese riesgo, debe formular un análisis minucioso en el que exponga las razones -objetivas y verificables- del daño que podría generar su conocimiento; así como la justificación legal: es decir, la disposición legal que establece tal imposibilidad.

Y por otro lado, mediante la Protección de Datos Personales se pretende garantizar que la información personal de toda persona que se encuentre en cualquier archivo, expediente o documento de las instituciones públicas del Estado, sea tratada de manera restringida y cuya divulgación, en términos generales, esté prohibida. Además de establecer esa prohibición expresa, se contemplaría la posibilidad de que cualquier persona que haya proporcionado sus datos personales a alguna autoridad con motivo de un trámite o servicio (licencias para conducir; permisos para apertura de un local

comercial; inscripción de una propiedad en DD.RR.), pueda acceder a dichos datos, solicitar su rectificación, cancelación o, incluso, oponerse a su difusión o transmisión.

Tratándose de la protección de datos personales, una ley, establecería carácter de confidencialidad a toda la información de cualquier persona que la haga identificada o identificable, como el nombre, género, estado civil, patrimonio, domicilio, preferencia sexual, ideología política y religiosa, entre otros, dicha consideración sufriría una importante ponderación respecto de quienes prestan sus servicios en el sector público.

Pero, si bien tienen el derecho a ser respetados en sus datos personales, dicho ámbito de respeto se ve sensiblemente disminuido por una razón que, siguiendo la intención de los legisladores de favorecer un gobierno abierto, democrático y honesto, tiende a generar confianza en la población a través de la contraloría ciudadana y el combate a la corrupción[34].

La confianza de las instituciones públicas y su credibilidad descansa fundamentalmente en las personas que las representan, por lo que se afirma que las declaraciones patrimoniales y su transparencia son un instrumento de combate a la corrupción.

En ese sentido, los datos relativos a la fotografía, a la formación profesional, al número de cédula y título profesional, así como las percepciones salariales, por mencionar algunos, revisten un carácter predominantemente público que obedece a la intención de garantizar a la ciudadanía quiénes son sus servidores públicos, cuál su trayectoria profesional, la certeza del perfil académico adecuado que implique los conocimientos necesario para desempeñar un cargo público, y los sueldos que perciben.

Tratándose de una ley, como varios países lo tienen, con el ejercicio de ambos derechos el legislador ha procurado, por un lado, establecer un amplia margen de revisión a las actividades del gobierno y, por otro, y en sentido contrario, garantizar que la información privada de las personas que por cualquier motivo se hayan entregado a

[34]http://www.noticiasnet.mx/portal/oaxaca/150167-acceso-informacion-proteccion-datos-personales

las autoridades sea tratada únicamente para el fin para el cual fue recabada, so pena de incurrir en infracción y ser acreedor a una sanción de tipo administrativo o civil, e inclusive, penal.

Una ley por sí misma no puede garantizar un adecuado ejercicio del acceso a la información pública ni la protección de los datos personales en poder del gobierno. Como todos los derechos, solo sabremos qué tan útiles y efectivas son cuando tomemos la decisión de ejercerlos y defenderlos; es necesario conocer sus contenidos y alcances, y ponerlos a prueba mediante su ejercicio.

### 2.8.2.3. SOCIEDAD INFORMATIZADA

Hoy en día los avances tecnológicos, el lanzamiento de nuevos aparatos electrónicos y el desarrollo de nuevas herramientas que facilitan las practicas diarias en nuestro entorno, han generado un gran impacto al interior de la sociedad, además de brindar eficiencia y comodidad conlleva también a replantear la idea acerca del consumo de todos estos recursos, llevándonos a reflexionar que nos representa, qué importancia tienen y la manera como los estamos utilizando. Una sociedad informatizada o también llamada sociedad de información puede definirse como una fase de desarrollo social que se caracteriza por la capacidad de sus miembros correspondiente estos a ciudadanos, empresas y administración pública, con el fin de obtener, compartir y distribuir cualquier información de manera instantánea, desde cualquier lugar y en la forma que se prefiera. Ante el Derecho, el conflicto tecnológico se agrava cuando se confrontan quienes pretenden una tecnología libre de todo control social, que toman el proceso mismo de la innovación tecnológica como expresión fundamental de la libertad humana, con los grupos humanitaristas que ven en la tecnología un peligro. El desarrollo social y moral del ser humano en estos tiempos de globalización va en paralelo con el desarrollo de las realidades técnicas y científicas y la aparición de nuevos paradigmas. El Internet es el paradigma actual, pueden ser una poderosísima infraestructura de liberación para el hombre. En este contexto tiene sentido hablar de gobierno electrónico, democracia electrónica e inclusión digital[35].

[35]http://informaticajuridicametadocumen.weebly.com/seguridad-informatizada.html

### 2.8.3. SEGURIDAD DE LA INFORMACIÓN

La seguridad como concepto ha evolucionado a lo largo del tiempo, comenzando con el enfoque de seguridad informática, cuyo alcance estaba limitado a la protección de los sistemas e infraestructuras, otorgándoles un gran protagonismo, por encima de otros activos, como la información.

Con la proliferación de las redes de comunicaciones, el abaratamiento del acceso a Internet y la aparición de los dispositivos portátiles, la naturaleza y ámbito de los sistemas a proteger cambió, lo que trajo consigo una evolución del concepto de seguridad, que fue sustituido por la seguridad de las tecnologías de la información y las comunicaciones o seguridad TIC. Este nuevo enfoque supuso una mejora sustancial respecto al anterior, puesto que no solo incorporaba nuevos sistemas e infraestructuras, como aquellas destinadas a las comunicaciones, sino que además, otorgaba más importancia a la información como activo, por encima de otros.

Finalmente, todo ello se integró en un concepto nuevo, mucho más amplio y cuya característica principal es considerar la información como el activo de mayor importancia y en torno al cual se desarrolla toda una metodología con un único objetivo, proteger la información. La seguridad de la información desarrolla el concepto de seguridad en torno al activo más importante de cualquier organización: la información.

### 2.8.4. INFORMACIÓN CLASIFICADA

Este tipo de información sensible está restringida por las leyes o regulada para clases particulares de personas. Se requiere una habilitación formal de seguridad para manejar y acceder a documentos clasificados. Esta especie de sistema jerárquico de discreción es usada virtualmente por todos los gobiernos nacionales.

El propósito de la clasificación de documentos es ostensiblemente proteger información que de ser usada podría afectar la seguridad nacional. Esto formaliza aquello que

constituye un "secreto de estado" y propone distintos niveles de protección basado en el daño que se espera que la información pueda causar en manos equivocadas.

Aunque los sistemas de clasificación varían de país en país, la mayor parte de estos niveles corresponden a las siguientes definiciones británicas (nombradas desde el nivel más alto al más bajo):

- Top Secret ("Alto secreto")

Nivel más alto de clasificación de material en un nivel nacional. Esta información podría provocar un "daño excepcionalmente grave" a la seguridad nacional si estuviera públicamente disponible.

- Secret ("Secreto")

Este material eventualmente causaría "serios daños" a la seguridad nacional si estuviera públicamente disponible.

- Confidential ("Confidencial")

Este material podría "dañar" o "ser perjudicial" a la seguridad nacional si estuviera públicamente disponible.

- Restricted ("Restringido")

Este material podría producir "efectos indeseados" si estuviera públicamente disponible. Algunos países no tienen esta clasificación.

- Unclassified ("Sin clasificar")

Técnicamente no es un nivel de clasificación, pero es usado por los documentos gubernamentales que no poseen una de las clasificaciones presentadas arriba[36].

## 2.8.5.INFORMACIÓN SENSIBLE DE LAS PERSONAS

El contenido de este tipo de información se refiere a situaciones privadas y cuyo conocimiento o divulgación general puede generar perjuicios irreparables a los propietarios de los mismos. Así, por ejemplo toda publicidad respecto a preferencias y comportamientos sexuales, religión, filiación política, gremial, religión, raza, etc., encuadra exactamente en los parámetros de información sensible, por lo que deben ser protegidos evitando que la información sea publicada, salvo que existan actividades

[36]es.wikipedia.org/wiki/Información_clasificada

claras de la persona que determinen que las cuestiones no son “sensibles” para ella o que la misma se encargue de exponerlo públicamente. [37]

## 2.9. DERECHO DE ACCESO

Este derecho otorga la facultad a una persona de conocer o interesarse por conocer los datos personales suyos (no los de un tercero) en posesión de un responsable o titular de datos personales, sean estos públicos o privados. Los países que tienen una La Ley de Protección de Datos, por la misma, reconoce una serie de derechos a los ciudadanos sobre sus datos personales en ficheros de toda titularidad, mediante el derecho de acceso, el particular solicita información al titular o responsable del fichero de datos, sobre qué datos tiene y cómo los ha obtenido[38].

## 2.10. LA INTIMIDAD

Nuestra persona está rodeada de características, estados y situaciones que la conforman. Tenemos un nombre, un estado civil, un determinado patrimonio, un domicilio, estudios realizados, hemos ocupado cargos en entes públicos o privados, somos titulares de documentos de identidad, de cuentas corrientes bancarias, de tarjetas de crédito, etc. Todo ello, una vez volcado a un registro, se convierte en datos mediante los cuales se nos puede llegar a conocer, identificar y/o, en su caso, discriminar.

En consecuencia, el conjunto de datos debe ser considerado parte integrante de la persona. Así como no hay persona sin nombre, patrimonio, ni estado civil, tampoco las hay sin datos.

Así mismo, cabe una distinción entre “titular” de los datos y los "administradores" de los mismos. El titular es el individuo a quien los mismos le pertenecen, mientras que los administradores son quienesposeen los bancos o registros que recopilan y ordenan tales datos. Según una acertada visión, a mi entender, el doctor Bianchi hace una

[37] Juan Ramos M., Nuevo Recurso Constitucional “Hábeas Data” en el Derecho Informático, La Paz Bolivia 1999, pág. 25.

[38] María de los Reyes Corripio Gil Delgado, Regulación Jurídica de los Tratamientos de Datos Personales realizados por el sector privado en internet, Agencia de Protección de Datos, Madrid, 2000.

enumeración de cuatro obligaciones básicas respecto de los administradores de datos, a saber: a) estar legitimados para haberlos obtenido; b) llevar un correcto registro, sin incurrir en falsedades, lo que incluye también su actualización, c) asegurar su confidencialidad y no proveer de información sino mediante autorización del titular o a requerimiento de autoridad competente d) evitar su destrucción o deterioro.[39]

En caso de que incurrieran en violación de alguna de estas obligaciones, la intimidad o privacidad del titular de los datos se vería afectada. En el primer supuesto es obvio que quien está en posesión de datos que no le corresponden tener, afectan la intimidad del titular de los mismos. Cuando alguien se apodera de la información que almacena un banco de datos sin estar legitimado para ello, incurre en el mismo delito que quien entra a un domicilio privado sin autorización. En el segundo supuesto, la errónea, falsa o desactualizado registro por parte del administrador de datos, también supone una falta así el propietario de los mismos que afecta su esfera íntima pues genera, potencialmente, los daños que acaecen cuando se suministra una información equivocada sobre alguien.

En el tercer caso, cualquiera que revele un dato, aún el más elemental, sin el consentimiento de su titular, está poniendo en conocimiento de un tercero, información que tal vez no debe poseer. En ciertas situaciones aún el conocimiento indebido de un dato aparentemente poco trascendente, como por ejemplo el número de la línea telefónica, puede ser invasivo de la privacidad. Siguiendo con el ejemplo del domicilio, el administrador está abriendo la puerta de la casa sin el consentimiento de su dueño. En el cuarto caso su deterioro o pérdida puede afectar la titularidad cuando el registro obra como memoria de actividades.

De modo que la reforma constitucional, al establecer el habeas data, no sólo ha incorporado una nueva forma de amparo, lo que constituye de suyo un hecho importante para el derecho constitucional sustantivo y adjetivo, sino que ha expandido el ámbito de protección de la privacidad del individuo, otorgando una garantía específica que tiende a proteger los datos, que en poder de terceros, existan sobre una

[39] José Alfredo Arce Jofré, Informática y Derecho, La Paz Bolivia 2003, pág. 47

persona. Por lo tanto, lo que el hábeas data protege, esencialmente, es la intimidad o privacidad de una persona.

La confidencialidad de la información encuentra su lugar respecto de los datos sensibles y no respecto de los antecedentes comerciales o bancarios, los cuales, según la jurisprudencia: "no son datos inherentes a la personalidad que se hallen amparados por el principio de confidencialidad, por el contrario el suministro de los mismos no sólo no está vedado, sino que resulta acorde con la protección y el saneamiento del crédito".

### 2.10.1.DERECHO A LA INTIMIDAD

No se trata de la potestad más o menos ilimitada de intimar o relacionarse con los demás, resultando casual de las circunstancias de la vida unas veces y logro de un propósito en otras; como en las más de las relaciones amorosas, sean legales o ilícitas. No constituye un derecho a intimar con los otros; sino más bien a que los demás no intimen con uno, cuando no se desea. Para Osorio y Gallardo, configura este derecho el que todas las personas tienen para que sea respetada su vida privada, a efectos de que nadie pueda entrometerse en la existencia ajena publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otros en sus costumbres o perturbando de otro modo su intimidad. Por otro lado y en una actitud opuesta, nos referimos al acecho permanente de violar este derecho –un violador de derechos- que por lo general no está legislado, aun cuando la jurisprudencia le haya abierto paso reconociendo, en los supuestos más intolerables, el derecho al resarcimiento civil por el daño moral sufrido sobre todo con la gente de notoriedad y por sensacionalismo, así pues se hallan los periodistas y los reporteros de televisión; y esto por considerar mérito y hasta hazaña la captación de cualquier escándalo, aún sin idea de chantaje, las relaciones irregulares en lo amoroso, las pequeñas aflicciones, manías o defectos. Todo ello tiende a explotarse al servicio de la morbosidad sui generis de que adolece un extenso sector público, que sólo se siente elevado cuando son rebajados los otros o que goza, con el refinamiento de *voyeur* cuando sorprende a alguien en su situación incómoda o ridícula. En un orden civil, los regulados sobre

servidumbres de vistas y distancias entre edificios cooperan a resguardar la intimidad. Por el contrario, esta, y la moralidad más aún, se ven seriamente comprometidas con la promiscuidad en el seno de la familia, contra la apetecible independencia personal de cada uno de sus miembros en bastantes aspectos. Todo ello lleva a una sola afirmación: "dentro el derecho a la intimidad se pretende que la vida de cada cual, al menos de espontáneas revelaciones propias, resulte tan impenetrable como el fuero mismo de la conciencia"[40].

## 2.11. HABEAS DATA

### 2.11.1. ETIMOLOGÍA DEL HABEAS DATA

Su nombre se ha tomado parcialmente del antiguo instituto del hábeas corpus, en el cual el primer vocablo significa "conserva o guarda tu", y del inglés "data", sustantivo plural que significa "información o datos". En síntesis en una traducción literal seria "conserva o guarda tus datos". Por su parte los profesores Pierrini, Lorencies, Tornabene, dicen: "habeas data significa "que tengas los datos" o "que vengan los datos" o "que tengas los registros", es decir tomar conocimiento de datos propios en poder de otras"…, más adelante critican otros puntos de vista manifestando: "En el precepto constitucional se sigue el criterio que dio nacimiento al instituto con una concepción más amplia y que responde a las necesidades de los Derechos de Tercera Generación, donde la intervención judicial resulta un hecho secundario -para el caso de negativa de titular de la base- y que se produce a favor del afectado para que pueda tomar conocimiento de los mismos, realizar las incorporaciones, modificaciones, actualizaciones o restricciones y solicitar su eliminación o reserva". El profesor OthonSidovj.J, con relación al origen etimológico, señala que podría manifestarse alguna crítica en su elección, pero "hay que reconocer que la expresión es feliz como composición latina para un derecho de fin del siglo de la informática. "Hábeas", segunda persona del presente subjuntivo de Habeo… habere, significa aquí "tengas en posesión", que es una de las acepciones del verbo, y "data" es el acusativo plural de *datum* que los diccionarios más modernos definen como representación convencional de hechos, conceptos o instrucciones de forma apropiada para la comunicación y

[40] Guillermo Cabanellas, Diccionario Enciclopédico de Derecho Usual, Tomo 3 d e, 1989, pag. 103.

procesamiento por medios automáticos. Entonces: que tengas los registros, los datos…" [41]

## 2.11.2. CONCEPTO DE HABEAS DATA

La acción de Hábeas Data se define como el derecho que asiste a toda persona identificada o identificable a solicitar judicialmente la exhibición de los registros públicos o privados en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que implique discriminación.[42]

## 2.11.3. OBJETIVO DEL HABEAS DATA

El Hábeas Data, es un recurso constitucional moderno que tiene por objeto: "**a)** que una persona pueda acceder a la información que sobre ella conste en un registro o banco de datos; **b)** que se actualicen los datos atrasados; **c)** que se rectifiquen los inexactos; **d)** que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros, y **e)** supresión en los procesos de obtención de información del requisito de la llamada "información sensible". [43]

El procedimiento del recurso constitucional de Hábeas Data, goza de un proceso sumarísimo, rápido, expedito de trámites procesales burocráticos, tiene por objeto evitar el uso abusivo de la información que se tiene sobre una persona, de manera que constituye un capitulo elemental de sus libertades. Y por otra parte, la finalidad inmediata de remediar la hipotética humillación que sufre el individuo por la divulgación de datos que lo registran.[44]

## 2.11.4. CLASIFICACIÓN DEL HABEAS DATA

La Teoría Constitucional y el Derecho Procesal Constitucional, clasifican a este recurso en:

[41] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 1-2.
[42] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 3.
[43] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 3 - 4.
[44] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 35.

### 2.11.4.1. HABEAS DATA INFORMATIVO

Tiene lugar cuando el afectado no tiene conocimiento cierto de los datos y quiere acceder a ellos. Esta clase de hábeas data permite a la persona ejercer su derecho a la autodeterminación informática accediendo a los registros o bancos de datos públicos y privados destinados a proveer información, para que pueda recabar toda la información obtenida, almacenado y registrada en torno a su persona. A su vez, puede presentarse en tres variantes:

a) Exhibitorio, tiene por finalidad el que la persona que lo plantea tome conocimiento de sus datos personales obtenidos, almacenados y registrados en los bancos de datos públicos o privados.
b) Finalista, tienen la finalidad de que la persona que lo plantea puede saber para qué y para quién se registran sus datos personales, es decir, conocer los objetivos y fines para los que se han obtenido, almacenado y registrados sus datos personales en los bancos de datos públicos o privados.
c) Augusto oral, tiene la finalidad de que la persona que lo plantea pueda conocer quien obtuvo, almaceno y registros sus datos personales insertos en el registro o banco de datos[45].

### 2.11.4.2. HABEAS DATA ADITIVO

Su objeto es que se incorporen datos que sean pertinentes, ya sea para actualizar información ya registrada, o para completarla porque los datos archivados omitieron aspectos relevantes. Con esa perspectiva, pueden distinguirse dos sub-categorías de hábeas data aditivo, como ser:

a) Habeas Data Actualizatorio. Si se hubieren operado modificaciones respecto de los hechos o aspectos registrados esos asientos resultarían incorrectos y el afectado tiene derecho a que se deje constancia de su nueva situación.
b) Habeas Data Integrativo. Sería el que se dirige a completar la información registrada. Los datos se consideran incompletos cuando existe otro dato que,

[45] Juan Ramos M., Recursos Constitucionales Habeas Corpus, Amparo Constitucional, Habeas Data y Reformas Constitucionales, La Paz Bolivia, 2005, pag. 75-76.

unido a él, altera significativamente lo que de él puede inferirse o la apreciación que de él se haga[46].

### 2.11.4.3. HABEAS DATA RECTIFICADOR

El objetivo de este tipo es el de corregir información, pero no sólo cuando éstas sean falsas, sino cuando resultan inexactas, imprecisas o incompletas. Para obtener la corrección de datos falsos o erróneos. Al interesado le cabe la carga de acreditar que la información registrada es incorrecta, porque constituye el presupuesto de su pretensión. Así por ejemplo, que a una persona le registren como procesara penalmente por supuestos delitos cometidos, siendo así que ya fue absuelta en sentencia, es decir, no obstante de habérsela declarado absuelta de pena y culpa se le siga manteniendo el registrado de personas procesadas penalmente, en este caso, a través del hábeas data, se logra que se corrija el error de mantener una situación jurídica pasada que ya fue superada y modificada por decisión judicial firme.[47]

### 2.11.4.4. HABEAS DATA RESERVADOR

Este tipo de hábeas data tiende a asegurar que un dato correcta y legítimamente registrado sea proporcionado sólo a quienes y en los casos en que se encuentran legalmente autorizados para ello, y en general se vincula a los casos de datos sensibles. En otros términos es aquel mediante el cual se procura la confidencialidad de datos íntimos que pueden suscitar discriminación, mediante su bloqueo. A través de esta clase de recursos la persona logra que no se divulgue ciertos datos suyos para asegurar su confidencialidad, ya que su divulgación podría generarle graves prejuicios. La finalidad es que los datos legalmente obtenidos sean mantenidos para el uso exclusivo en el fin específico para el cual fueron obtenidos[48].

[46] Juan Ramos M., Recursos Constitucionales Habeas Corpus, Amparo Constitucional, Habeas Data y Reformas Constitucionales, La Paz Bolivia, 2005, pag.76.
[47] Juan Ramos M., Recursos Constitucionales Habeas Corpus, Amparo Constitucional, Habeas Data y Reformas Constitucionales, La Paz Bolivia, 2005, pag.76.
[48] Juan Ramos M., Recursos Constitucionales Habeas Corpus, Amparo Constitucional, Habeas Data y Reformas Constitucionales, La Paz Bolivia, 2005, pag.77.

### 2.11.4.5. HABEAS DATA CANCELATORIO, DE SUPRESIÓN O EXCLUSORIO

El objetivo es eliminar la información del registro en el cual se encuentra almacenada, cuando por algún motivo no debe mantenerse registrada, puede que se trate de datos sensibles. Puede solicitarse la cancelación de información sensible o falsa, o que sin serlo, el responsable del registro carezca de un interés legítimo en almacenarla. A través de él se logra que se borren los datos conocidos como información sensible, concerniente a ideas políticas, religiosas o gremiales, al comportamiento sexual, a ciertas enfermedades o datos racionales, cuyo uso podría generar tratos discriminatorios o lesivos al honor o privacidad del afectado. Por ejemplo, porque los datos sean excesivos o impertinentes de acuerdo con el objetivo y finalidad del registro o base de datos. Hemos visto que una de las situaciones típicas del abuso informativo es que la sumatoria de datos aunque no sean íntimos, pueden producir una lesión a la intimidad que permiten reconstruir el perfil de una persona. La información sensible a la información vinculada con aspectos íntimos de las personas, tales como la orientación religiosa, conducta sexual, enfermedades, origen racial, orientación política racista, etcétera. Sin embargo, el progreso de la informática abrió otros horizontes al incrementarse la posibilidad técnica de imagen manejar enormes volúmenes de información y de interpretarla mediante métodos de prospección. Por ello, ahora se considera que todo dato puede tornarse sensible en la medida en que la sumatoria de datos no sensibles, pero que permitan hacer un seguimiento en la vida de la persona, también puede representar una afrenta a la privacidad. A veces, es la manipulación que se hace de datos que en sí mismos carecen de lesividad, lo que los transforma en información sensible[49].

### 2.11.4.6. HABEAS DATA IMPROPIO O PUBLICO

Esta especie de hábeas data no está legislado expresamente en nuestro derecho, sólo se encuentra en la doctrina y ésta señala que el hábeas data público o impropio para designar la acción tendiente a que una persona tenga acceso a datos registrados en

[49] Juan Ramos M., Recursos Constitucionales Habeas Corpus, Amparo Constitucional, Habeas Data y Reformas Constitucionales, La Paz Bolivia, 2005, pag.77-78.

archivos públicos, que no son relativos al interesado pero éste tiene interés de conocer. Sería una garantía para hacer efectivo el carácter público de los registros oficiales.

Por su parte Óscar Raúl Puccinelli, señala que existen otras clases de hábeas Data y estos son:

### 2.11.4.7. HABEAS DATA IMPUGNATIVO

Las normas sobre protección de datos suelen prever el derecho del registrado a la impugnación a la valoración de datos y a las decisiones automatizadas. Este tipo presenta cierta similitud con el hábeas data correctivo, si por vía de esa impugnación se pretende establecer una conclusión distinta a la que aparece en el registro, y con el exclusorio, si la pretensión es de eliminación total de dicha valoración o decisión.

### 2.11.4.8. HABEAS DATA BLOQUEADOR

Muy emparentado al habeas data reservador y al exclusorio se presenta un tipo ligeramente distinto, el que pretende trabar, de manera definitiva o transitoria, el tratamiento, en especial la transmisión de los datos.

### 2.11.4.9. HABEAS DATA DISOCIADOR

El derecho de disociación, reconocido en las normas sobre protección de datos personales y también, entre otras, en las de secreto estadístico, es similar a los de reserva y de exclusión, pero difiere de ellos en cuanto no necesariamente implica la eliminación de un dato del registro ni su confidencialización, sino su transformación.

### 2.11.4.10. HABEAS DATA ASEGURADOR

Uno de los más importantes principios relativos al tratamiento de datos es el de la seguridad de los datos, pues de nada sirve que se reconozcan los derechos a operar

sobre los bancos de datos si los procedimientos técnicos utilizados para dicho tratamiento permiten fugas de información[50].

### 2.11.5. UTILIDADES DEL HABEAS DATA

Dentro del ordenamiento jurídico de todo Estado de Derecho los recursos constitucionales son de vital importancia para garantizar los derechos de sus ciudadanos. Es así que las "acciones de defensa" a las que se refiere el texto constitucional vigente, en su Primera Parte, Capítulo Segundo, nos remiten a aquellos mecanismos de resguardo de los derechos establecidos por dicha norma suprema. Dentro de esos mecanismos, tenemos a la Acción de Protección de Privacidad, que fue incorporada a nuestra legislación constitucional en la Constitución del año 2004, con el nombre con el cual se la conoce en la mayoría de las legislaciones del mundo, es decir la del "Habeas Data".

Este recurso puede conceptualizarse a decir del autor nacional José Antonio Rivera Santibáñez, como "…una garantía constitucional de carácter procesal para la protección de los datos personales, aquellos que forman parte del núcleo esencial del derecho a la privacidad o a la intimidad de una persona, frente a la obtención, almacenamiento y distribución ilegal, indebida o inadecuada por entidades u organizaciones pública o privadas.

Esta garantía constitucional otorga a la persona, sea natural o jurídica, la potestad y facultad, el derecho a acudir a la jurisdicción constitucional para demandar a los bancos de datos y archivos de entidades públicas o privadas con el fin de que permitan el conocimiento, la actualización, la rectificación o supresión de las informaciones o datos referidos a ella, que hubiesen obtenido, almacenado y distribuido".

El recurso constitucional que nos ocupa merece el reconocimiento de la mayoría de las legislaciones en el mundo por la importancia que reviste actualmente la protección de los datos personales, dado el crecimiento acelerado de la tecnología que permite

[50] Juan Ramos M., Recursos Constitucionales Habeas Corpus, Amparo Constitucional, Habeas Data y Reformas Constitucionales, La Paz Bolivia, 2005, pag.78-79.

almacenar dichos datos en medios magnéticos, electrónicos e informáticos, los cuales pueden ser usados muchas veces en perjuicio de las personas, afectando su derecho a la intimidad, a su privacidad y a su honra y reputación, tal como lo refleja el artículo 130 numeral I de la Constitución vigente. La finalidad del recurso será por tanto la de evitar el abuso informático, sin embargo el abuso no necesariamente deberá ser un requisito previo para la existencia, pues este podrá interponerse también para preservar la confidencialidad y la reserva de ciertos datos inherentes a la dignidad, el honor, la privacidad, etc.

Por todo lo expresado, el recurso como tal puede ser de amplio uso para proteger los derechos inherentes a la personalidad y que se hallen mellados o amenazados por la informática y el manejo que se tiene de los datos personales a través de ella, sin embargo aún no es muy utilizada, esto quizás por su relativa reciente introducción a nuestra legislación constitucional, es así que apenas cuatro acciones de este tipo fueron tramitadas en el Distrito Judicial de La Paz (Distrito que tiene una de las mayores cargas procesales del país), en la Gestión 2009, esto de acuerdo al informe anual presentado.

De todas maneras este último aspecto no resta importancia a la acción de protección privacidad, que se constituye en una garantía muy importante para precautelar derechos que en el pasado no se hallaban debidamente protegidos[51].

## 2.12. ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Aprobada la Nueva Constitución Política del Estado el 25 de Enero del 2009, promulgada el 7 de febrero del mismo año, ciertas instituciones cambian en su denominación, así como el habeas data ahora, se denomina Acción de Protección a la Privacidad, considerada como acción de defensa dentro el Capítulo II del Título IV Garantías Jurisdiccionales y Acciones de Defensa, en la Primera Parte Bases Fundamentales del Estado, Derechos, Deberes y Garantías.

[51] http://www.emba.com.bo/index.php?option=com_content&view=article&id=119%3Aaccion-de-proteccion-de-privacidad-en-el-nuevo-ordenamiento-constitucional&Itemid=114&lang=es

La misma sera interpuesta en el plazo máximos de seis meses de la comisión de la vulneración ante cualquier juez y tribunal competente quien si declarare procedente se ordenara la revelación o eliminación, o rectificación de los datos. Asimismo la decisión final se elevara de oficio ante el Tribunal Constitucional Plurinacional en revisión, si que se suspenda la ejecución.

# CAPITULO III

# MARCO CONCEPTUAL

## 3.1.DATOS PERSONALES

Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional.

Además de ello, los datos personales también describen los aspectos más sensibles o delicados sobre el individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros.

## 3.2. DATOS SENSIBLES

Es toda aquella información de determinado individuo que comprende datos cuyo contenido es de carácter netamente delicado, vale decir que puede avergonzar a su titular o puede causar cierta discriminación por lo que requieren una mejor protección.

Son los siguientes:

- Datos médicos relacionados con la salud (información genética, enfermedades, etc.)
- Raza/etnia
- Género
- Filiación Sindical
- Creencias Religiosas o Filosóficas
- Prácticas Sexuales y orientación sexual
- Filiación Política
- Historia Penal
- Ingresos Económicos

## 3.3.DATOS NO SENSIBLES

Son aquellos datos que al ser de conocimiento de cualquier individuo no equivale a la violación de un derecho individual como es el conocer un dato íntimo y hacer algún mal uso de ello.

## 3.4.BASE DE DATOS

Se entiende por base de datos un conjunto de programas de computador que proveen eficientes métodos de acceso a los datos institucionales, los cuales se organizan y almacenan rigurosamente de acuerdo a las normativas computacionales; dicho de otra manera, desde el punto de vista de los almacenamientos magnéticos, las bases de datos proveen vinculaciones lógicas entre los datos operativos, entregando de este modo la información que ha sido previamente definida y acordada con el usuario final. "Las bases de datos son herramientas estándares de la computación tradicional, herramientas que permiten minimizar el problema de la redundancia de los datos, pues estos se almacenan una sola vez y pueden ser utilizados en diversas aplicaciones computacionales, sin necesidad de volver a ingresarlos nuevamente.[52]

En otra definición tenemos que una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico.Las bases de datos tradicionales se organizan por campos, registros y archivos. Uncampo es una pieza única de información; un registro es un sistema completo de campos; y un archivo es una colección de registros. Por ejemplo, una guía de teléfono es análoga a un archivo. Contiene una lista de registros, cada uno de los cuales consiste en tres campos: nombre, dirección, y número de teléfono.

Dicho de otra manera una base de datos es una gran cantidad de información almacenada de una manera estructurada para su fácil e inmediata búsqueda.

[52] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 28-29.

## 3.5.BANCO DE DATOS

Un banco de datos es aquel conjunto de archivos conexos o relacionados, y organizados en función de su comunicación a una determinada población de usuarios. Por lo tanto, el archivo de datos de un profesional o de una empresa destinado al uso interno no constituye banco de datos, sino que solo se considera base de datos. Pues al decir verdad, los bancos de datos tienen por destino natural el poner su documentación a disposición onerosa o gratuita de un público, seleccionada o no. Se trata de empresas de servicios, sean estas privadas o públicas. [53]

Un banco de datos es una base de datos, simplemente cambia el término, que a medida que pasaron los años, la terminología se estableció en base de datos y no banco de datos.

### 3.5.1. BASE DE DATOS PÚBLICOS Y PRIVADOS

La norma constitucional no debe hacer ninguna diferencia alguna en cuanto a que los registros en cuestión estén en una base de datos pública o privada. La única salvedad está referida a que la base privada debe tener en mira la publicidad de aquellos. De ahí que el profesor Villalva Carlos, plantea que las bases de datos son depósitos electrónicos de datos y de información. Esto implica una organización, un sistema de manejo de bases de datos; un control que permite a los usuarios ingresar al mismo de acuerdo a sus derechos de acceso; una administración o manejo de datos; un diseño de la base de datos y de estructura, así como la selección e implementación del software que permite operarlo. Existe un software específico que organiza y recupera los datos almacenados en una base, lo que facilita el acceso al usuario. Los datos son las materias primas con las que se puede elaborar información. Pueden consistir en un conjunto orgánico, como un ensayo literario o una ley, o estar aislados, como la cifra de un censo. El uso personal que una persona puede realizar debe estar aceptado por la

[53] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 29.

comprobación de que ellos constituyen un aprovechamiento marginal de la producción intelectual. [54]

## 3.6. AUTODETERMINACIÓN INFORMATIVA

La autodeterminación informativa es un derecho fundamental derivado del derecho a la privacidad, que se concreta en 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.

## 3.7. ARCHIVOS INFORMATIVOS

Un archivo informático es un conjunto de información que se almacena en algún medio de escritura que permita ser leído o accedido por una computadora. Un archivo es identificado por un nombre y la descripción de la carpeta o directorio que lo contiene. Los archivos informáticos se llaman así porque son los equivalentes digitales de los archivos en tarjetas, papel o microfichas del entorno de oficina tradicional. Los archivos informáticos facilitan una manera de organizar los recursos usados para almacenar permanentemente información dentro de un computador.

## 3.8. DERECHO A LA HONRA

La honra en es un vocablo con diversas acepciones, entre ellas: estima y respeto de la dignidad; buena opinión y fama adquirida por la de virtud y el mérito; pudor, honestidad y recato de las mujeres. Con independencia del valor social que esas virtudes puedan tener, ofrecen otros de índole jurídica, por cuanto la ley reconoce a todas las personas el derecho de defenderlas e impedir que otros las ataquen. De ahí que los ataques a la honra constituían dos tipos de delitos uno relacionado con las agresiones al honor como la injuria, calumnia y difamación y otra que son las agresiones a la honestidad como el estupro, rapto, violación y corrupción. Tal vez los referidos a la honestidad

[54] Juan Ramos M., Nuevo Recurso Constitucional "Hábeas Data" en el Derecho Informático, La Paz Bolivia 1999, pág. 29-30.

sean los más característicos, aunque han sido los más cambiantes a causa de la evolución de las costumbres. Así las frases de antaño corrientes de que una mujer había sido deshonrada o que había perdido la honra cuando había tenido, siendo soltera, trato carnal con un hombre, hubiese o no perdió su virginidad, carece en el presente de valor por lo menos en un sentido absoluto, y eso hasta el punto de que buena parte de la doctrina y de la legislación consideren que bien protegido en los delitos llamados sexuales no es ni en honor y la honestidad, sino simplemente la libertad sexual. Fácilmente se advierte también el notable cambio que en la estimación social ha sufrido las ideas relativas al pudor y al recato femenino lo que hoy en día ha cambiado por las costumbres de nuestra sociedad moderna[55].

## 3.9. EL HONOR

Cualidad moral que nos lleva al más severo cumplimiento de nuestros deberes respecto del prójimo y de nosotros mismos.

## 3.10. DERECHO AL HONOR

Es un derecho vinculado a la dignidad de la persona, que se interpreta en un doble sentido: SENTIDO INDIVIDUAL, por el que no se admitirá discusión alguna por razón de nacimiento, raza, sexo, opiniones o creencias; SENTIDO COLECTIVO, por el que no se puede permitir el odio o el desprecio público a todo un pueblo o etnia.

## 3.11. LA REPUTACIÓN

Es aquella imagen que cierto individuo crea sobre su propia persona de acuerdo a los actos que lleva a cabo en la cotidianeidad, donde los terceros la juzgan en base a dichos actos.

## 3.12. GARANTÍAS CONSTITUCIONALES

[55] Manuel Ossorio, Diccionario de Ciencias Jurídicas, Políticas y Sociales, Buenos Aires Argentina, 2002, pág. 482.

Son aquellas en las que ofrece la constitución en el sentido de que se cumplirán y respetarán los derechos que consagra, tanto en lo que se refiere al ejercicio de los de carácter privado, de los de índole pública[56].

## 3.13. PRINCIPIO CONSTITUCIONAL DE GARANTÍA

Es aquel que ofrece la Constitución en el sentido de que se cumplirán y respetaran los derechos que ella consagra, tanto en lo que se refiere al ejercicio de los de carácter privado como al de los de índole pública[57].

Tratándose de derechos públicos se sustentan, fundamentalmente, en la protección de los intereses de la sociedad y los derechos de los gobernados, donde el estado, en su carácter de sujeto pasivo de las garantías, está obligado a velar por dichos intereses con apego a las normas constitucionales y legales, además de constituirse en garante del interés social al establecer normas tendientes a protegerlo.

El término garantía es sinónimo de seguridad, salvaguarda, protección. Desde el punto de vista jurídico han sido varias las definiciones que se le han dado a las garantías constitucionales, Un concepto un poco más amplio es el que las considera como el conjunto de medidas técnicas e instituciones que tutelan los valores recogidos en los derechos y libertades enunciadas por la Constitución, que son necesarios para la adecuada integración en la convivencia política de los individuos y grupos sociales.

Las garantías jurisdiccionales son las que abren la posibilidad de demandar ante órganos, la preservación o el restablecimiento de los derechos humanos. Son las que se ofrecen a los ciudadanos para que en un caso concreto en que se vulnere un derecho, se pueda acudir a ellas y obtener la debida protección. La vía jurisdiccional será, a través de sus órganos o instituciones,la que con función esencial tutelará y/o fiscalizará los derechos humanos.

[56] Manuel Ossorio, Diccionario de Ciencias Jurídicas, Políticas y Sociales, Buenos Aires Argentina, 2002, pág. 452.
[57] Manuel Ossorio, Diccionario de Ciencias Jurídicas, Políticas y Sociales, Buenos Aires Argentina, 2002, pág. 453.

## 3.14.DERECHO OBJETIVO

En cualquier rama jurídica, el hipotético u ordenador, el normativo como recomendación doctrinal o como expresión positiva. Tiene por fuentes la ley, la costumbre, los principios generales del Derecho, la jurisprudencia y la doctrina. Se caracteriza este derecho por ser general, irrenunciable y sin efecto retroactivo, por lo común. Se subdivide en natural y positivo: aquel, el dictado por la razón a los hombres, el teórico, que unos estiman inmutable y otros variable según los tiempos y circunstancias; este otro, el conjunto de disposiciones legales y reglamentarias establecida expresamente por el legislador. Se distingue entre el Derecho escrito (ley reglamento decreto) y no escrito (costumbre, tradición, uso, practica)[58].

## 3.15. DERECHO SUBJETIVO

Conjunto de facultades que corresponden al individuo y que este puede ejercitar para hacer efectivas las potestades jurídicas que las normas legales le reconocen[59].

## 3.16. PETICIÓN

Con independencia de su acepción genérica como acción de pedir, jurídicamente puede significar el escrito o su parte final, en que se formulara ante un juez algún pedimento. Pero su mayor importancia jurídica está referida al derecho político, y dentro de él, al constitucional, porque la petición no es otra cosa que el derecho reconocido constitucionalmente a favor de todos los habitantes del país para dirigirse a las autoridades públicas y reclamar u observar ante ellas alguna cosa o más propiamente, algún derecho que les interese[60].

## 3.17. DERECHO DE PETICIÓN

[58] Guillermo Cabanellas, Diccionario enciclopédico de derecho usual, Tomo 3 d e, 1989, pág. 142.
[59] Manuel Ossorio, Diccionario de Ciencias Jurídicas, Políticas y Sociales, Buenos Aires Argentina, 2002, pág. 329.
[60] Manuel Ossorio, Diccionario de Ciencias Jurídicas, Políticas y Sociales, Buenos Aires Argentina, 2002, pág. 752.

Es aquel derecho  que tiene toda persona individual o jurídica, grupo, organización o asociación para solicitar o reclamar ante las autoridades competentes -normalmente los gobiernos o entidades públicas- por razones de interés público ya sea individual, general o colectivo; sobre cualquier derecho que se cree fue vulnerado o merece ser tomado en cuenta.

## 3.18. PRIVACIDAD

Privacidad es aquello que una persona lleva a cabo en un ámbito reservado (vedado a la gente en general). Un sujeto, por lo tanto, tiene derecho a mantener su privacidad fuera del alcance de otras personas, asegurándose la confidencialidad de sus cosas privadas. Es el ámbito de la vida personal de un individuo que se desarrolla en un espacio reservado y debe mantenerse confidencial.

## 3.19. DERECHO A LA PRIVACIDAD

El derecho a la privacidad ha evolucionado para proteger la libertad de individuos a realizar acciones determinadas y someterse a ciertas experiencias. Esta autonomía personal ha crecido hasta convertirse en un derecho fundamental protegido por la Constitución.

El derecho a la intimidad o privacidad es la potestad o facultad que tiene toda persona para mantener en reserva determinadas facetas de su personalidad, esto tiene como uno de sus elementos esenciales la inviolabilidad de la vida privada, referida al escenario o espacio físico en el que se desenvuelve, como es el domicilio, los medios relacionales de comunicación y correspondencia y los objetos que contienen manifestaciones de voluntad o de conocimiento no destinadas al acceso de personas ajenas, lo que involucra escritos, fotografías y otros documentos.

Debe entenderse que el derecho a la inviolabilidad de correspondencia no se reduce al ámbito de la correspondencia escrita, es decir, la carta postal, sino que se extiende a

cualquier medio o sistema de comunicación privada, dado que actualmente se cuenta con múltiples formas como telefonía fija y móvil y correo electrónico.

Entonces, la inviolabilidad de correspondencia y de todas las formas de comunicación privada que garantiza la Constitución está destinada a resguardar esencialmente los siguientes bienes jurídicos: 1) La libertad de toda persona para comunicarse con otras, sin que se produzcan interrupciones o interferencias ilegales o arbitrarias; y 2) La reserva o el secreto de aquello que se escribe o habla entre quienes se hayan comunicado.

La CPE Plurinacional de Bolivia, aprobada en enero de 2009, en su Capítulo dedicado a los Derechos Civiles y Políticos, establece en el artículo 21, numeral 2, que las bolivianas y bolivianos tenemos los siguientes derechos: “A la privacidad, intimidad, honra, honor, propia imagen y dignidad”.

Asimismo, y reforzando el alcance de este derecho, el artículo 25 establece que: “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. IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal”.

Esta disposición constitucional regula básicamente lo siguiente:
a) El derecho a la inviolabilidad del domicilio, que básicamente significa que nadie puede introducirse o ingresar en él sin el consentimiento del propietario o habitante, excepto en los casos expresamente previstos por la misma Constitución. Asimismo, debe considerarse que el carácter domiciliario de un recinto se da por el hecho de que, en su interior, una o más personas desarrollan actividades en la esfera de la vida

privada, es decir, a ese ámbito de la existencia de la persona donde los demás no pueden introducirse ilícitamente.

b) El carácter inviolable de la correspondencia y los papeles privados, determinando la prohibición de su incautación, excepto en los casos expresamente establecidos por Ley, y previa orden escrita y motivada de autoridad judicial competente. Esto implica que toda persona tiene el derecho de mantener en reserva su correspondencia y sus papeles privados, este derecho alcanza a toda forma de comunicación, escrita, oral o audiovisual, considerando que ahora existen medios sofisticados para una comunicación pronta y oportuna.

c) La invalidez como medio probatorio de los documentos privados violados o sustraídos, lo que implica que la persona que sustraiga o se apodere ilegítimamente y/o el funcionario público que incaute un documento privado sin el consentimiento o conocimiento del dueño, o sin una orden judicial expresa, no podrá presentar como prueba dicha documentación y, en caso de ser presentada, la misma no podrá surtir efectos probatorios válidos en el proceso.

d) La prohibición de interceptar conversaciones o comunicaciones privadas implica que ninguna persona particular o funcionario público, cualquiera sea su rango de autoridad, puede ni debe, bajo pena de incurrir en delito sancionado por la Ley Penal, interceptar conversaciones o comunicaciones privadas. Esto significa que ninguna autoridad judicial puede ordenar la intercepción de este tipo de conversaciones.

## 3.20. DERECHO A LA IMAGEN

El ser humano en su individualidad, es único e irrepetible, y construye su imagen dentro de la sociedad como cualidad física innata, y como representación de su propia estima y valoración internalizada.

La propia imagen entonces, trasciende el plano de la subjetividad del reconocimiento de uno mismo, en tanto se erige como carta de presentación en función de las distintas relaciones sociales, familiares, profesionales etc.

Esa proyección de la imagen en la sociedad se objetiviza posibilitando la “construcción del otro”, y la “percepción del otro” sobre nosotros mismos en un juego dialéctico de externalización, objetivación e internalización.

La imagen es un valor simbólico de significación en el campo social tanto público como privado, contribuye a las relaciones de reconocimiento entre los miembros de la comunidad, y como emanación de la personalidad humana es merecedora de una adecuada tutela jurídica.

Toda persona tiene derecho a la protección de su imagen, la que conforma conjuntamente con la intimidad y el honor una triada que relaciona al sujeto individual con la sociedad.

En sentido jurídico, tiene un doble aspecto: positivo y negativo. Así, el aspecto positivo sería el derecho a obtener, reproducir y publicar la propia imagen, y a autorizar a terceros que lo hagan. El aspecto negativo consistiría en el derecho a prohibir la mera obtención o la reproducción y publicación de la propia imagen por un tercero que carece del consentimiento del titular para ello; en este aspecto negativo se incluye la publicación que altera la imagen con un trucaje o le da un sentido anómalo con un pie de foto no consentido. Hay pues, un derecho del sujeto a difundir y publicar su propia imagen y, asimismo, un derecho a evitar la reproducción de su imagen, y ello, con carácter *erga omnes*, es decir, frente a cualquier tercero.

## 3.21. DERECHO A LA IDENTIDAD

El Derecho a la Identidad es “un conjunto de atributos, de calidades, tanto de carácter biológico como los referidos a la personalidad que permiten precisamente la individualización de un sujeto en sociedad.”

El Derecho a la Identidad del niño o niña es un interés jurídico superior que prevalece sobre los intereses jurídicos de los demás. Estos presupuestos fueron

instituídosjustamente en favor del desarrollo de la personalidad y protección a la dignidad del menor como ser humano.

## 3.22. DERECHOS HUMANOS

Los Derechos Humanos son el conjunto de prerrogativas inherentes a la naturaleza de la persona, cuya realización efectiva resulta indispensable para el desarrollo integral del individuo que vive en una sociedad jurídicamente organizada. Estos derechos, establecidos en la Constitución y en las leyes, deben ser reconocidos y garantizados por el Estado.

Todos estamos obligados a respetar los Derechos Humanos de las demás personas. Sin embargo, según el mandato constitucional, quienes tienen mayor responsabilidad en este sentido son las autoridades gubernamentales, es decir, los hombres y mujeres que ejercen la función de servidores públicos.

La tarea de proteger los Derechos Humanos representa para el Estado la exigencia de proveer y mantener las condiciones necesarias para que, dentro de una situación de justicia, paz y libertad, las personas puedan gozar realmente de todos sus derechos. El bienestar común supone que el poder público debe hacer todo lo necesario para que, de manera paulatina, sean superadas la desigualdad, la pobreza y la discriminación.

## 3.23. PERSONA

En el lenguaje cotidiano, la palabra persona hace referencia a un ser con poder de raciocinio que posee conciencia sobre sí mismo y que cuenta con su propia identidad.

Dentro de los conceptos legislativos en el derecho positivo se declara que "Son personas todos los entes susceptibles de adquirir derechos o contraer obligaciones"[61].

### 3.23.1. PERSONA INDIVIDUAL

[61] Guillermo Cabanellas, Diccionario enciclopédico de derecho usual, Tomo 6 p q, 1989, pag.220.

Se refiere a la persona natural.

### 3.23.2. PERSONA COLECTIVA

Cuando de persona colectiva se habla, conviene puntualizar en que ámbito se desenvuelve lo que de ella se manifiesta. Y es que en esta materia discrepan, y no poco, la sociología y el Derecho. Para este último, con perspectiva estricta, persona colectiva es un ser de existencia legal susceptible de derechos y obligaciones o de ser termino subjetivo en relaciones jurídicas, según las palabras definidoras del civilista Sánchez Román. Constituye pues, otro eslabón en la serie extensa de la sinonimia utilizada por los autores para designar a las personas abstractas[62].

## 3.24. DEFACEMENT

Es una palabra inglesa que significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este. El autor de un defacement se denomina defacer[63].

## 3.25. BUG

Un error de software, comúnmente conocido como bug (bicho), es un error o fallo en un programa de computador o sistema de software que desencadena un resultado indeseado[64].

[62] Guillermo Cabanellas, Diccionario enciclopédico de derecho usual, Tomo 6 p q, 1989, pag223.
[63] es.wikipedia.org/wiki/Defacement
[64] http://es.wikipedia.org/wiki/Error_de_software

## 3.26. HACKER

Un pirata informático, o Hacker es aquel individuo que usa sus habilidades y conocimientos informáticos para invadir sistemas de información ajenos y vulnerables, y por tal motivo son capaces de ingresar a determinado sistema informático y modificar su contenido, extraer información e incluso publicar información que se encuentra en su base de datos[65] .

## 3.27. SPAM

Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

Aunque se puede hacer spam por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de correo basura incluyen grupos de noticias, usenet, motores de búsqueda, redes sociales, páginas web wiki, foros, web logs (blogs), a través de ventanas emergentes y todo tipo de imágenes y textos en la web[66].

[65] es.wikipedia.org/wiki/Hacker
[66] http://es.wikipedia.org/wiki/Spam

# CAPITULO IV

# MARCO JURIDICO

## 4.1. CONVENIOS Y TRATADOS INTERNACIONALES DE PROTECCIÓN A LOS DERECHOS HUMANOS

### 4.1.1. CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS O PACTO DE SAN JOSE DE COSTA RICA

Si bien dentro del registro de esta Convención no señala específicamente lo relacionado a nuestro tema, si hace referencia a la protección de la vida privada de las persona, a la libertad de buscar, recibir y difundir información y a su vez a la libertad de conciencia, pensamiento, religión y opinión. Cada una de estas libertades y la misma protección a la vida privada pueden traducirse en datos personales de diverso carácter, por lo cual deben ser protegidos. A continuación la transcripción de los artículos referentes a lo escrito:

**Protección de la Honra y de la Dignidad**

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. [67]

**Libertad de Conciencia y de Religión**

1. Toda persona tiene derecho a la libertad de conciencia y de religión. Este derecho implica la libertad de conservar su religión o sus creencias, o de cambiar de religión o de creencias, así como la libertad de profesar y divulgar su religión o sus creencias, individual o colectivamente, tanto en público como en privado.

[67]CONVENCION AMERICANA SOBRE DERECHOS HUMANOS SUSCRITA EN LA CONFERENCIA ESPECIALIZADA INTERAMERICANA SOBRE DERECHOS HUMANOS, San José, Costa Rica 7 al 22 de noviembre de 1969. Art. 11

2. Nadie puede ser objeto de medidas restrictivas que puedan menoscabar la libertad de conservar su religión o sus creencias o de cambiar de religión o de creencias.
3. La libertad de manifestar la propia religión y las propias creencias está sujeta únicamente a las limitaciones prescritas por la ley y que sean necesarias para proteger la seguridad, el orden, la salud o la moral públicos o los derechos o libertades de los demás.
4. Los padres, y en su caso los tutores, tienen derecho a que sus hijos o pupilos reciban la educación religiosa y moral que esté de acuerdo con sus propias convicciones. [68]

**Libertad de Pensamiento y de Expresión**

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
a) el respeto a los derechos o a la reputación de los demás, o
b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

[68]CONVENCION AMERICANA SOBRE DERECHOS HUMANOS SUSCRITA EN LA CONFERENCIA ESPECIALIZADA INTERAMERICANA SOBRE DERECHOS HUMANOS, San José, Costa Rica 7 al 22 de noviembre de 1969. Art. 12

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional. [69]

**Derecho de Rectificación o Respuesta**

1. Toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio a través de medios de difusión legalmente reglamentados y que se dirijan al público en general, tiene derecho a efectuar por el mismo órgano de difusión su rectificación o respuesta en las condiciones que establezca la ley.
2. En ningún caso la rectificación o la respuesta eximirán de las otras responsabilidades legales en que se hubiese incurrido.
3. Para la efectiva protección de la honra y la reputación, toda publicación o empresa periodística, cinematográfica, de radio o televisión tendrá una persona responsable que no esté protegida por inmunidades ni disponga de fuero especial.[70]

## 4.1.2.LA DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS

"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". [71]

"Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de cambiar de religión o de creencia, así como la libertad de manifestar su religión o su creencia, individual y colectivamente, tanto en público como en privado, por la enseñanza, la práctica, el culto y la observancia". [72]

[69]CONVENCION AMERICANA SOBRE DERECHOS HUMANOS SUSCRITA EN LA CONFERENCIA ESPECIALIZADA INTERAMERICANA SOBRE DERECHOS HUMANOS, San José, Costa Rica 7 al 22 de noviembre de 1969. Art. 13
[70]CONVENCION AMERICANA SOBRE DERECHOS HUMANOS SUSCRITA EN LA CONFERENCIA ESPECIALIZADA INTERAMERICANA SOBRE DERECHOS HUMANOS, San José, Costa Rica 7 al 22 de noviembre de 1969. Art. 14
[71]DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, Adoptada y proclamada por la Resolución de la Asamblea General 217 de 10 de Diciembre de 1948. Art. 12
[72]DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, Adoptada y proclamada por la Resolución de la Asamblea General 217 de 10 de Diciembre de 1948. Art. 18

“Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión”. [73]

En estos artículos no existe especificación alguna sobre datos personales o su manipulación; lo que en si es de lo que se trata nuestro tema, pero esta demás recalcar que existen ciertas palabras dentro de estos artículos que tienen que ver mucho con los datos de una persona, en este sentido resaltaremos todas las palabras que tengan que ver con ello, siendo estas las siguientes:

- *Injerencia.*- sinónimo de intromisión ajena, vale decir que sin previa autorización o consentimiento del titular podría uno de sus datos hacerse público, dando lugar a un posible ataque a su honra o reputación.
- *libertad de pensamiento, conciencia, religión, opinión y expresión*.- derechos que todo ser humano libre puede tener, creer o difundir traduciéndose en datos que pueden ser de carácter sensible dando lugar a que la persona titular de estos derechos, pueda verse afectada mediante la discriminación.

### 4.1.3. DECLARACIÓN AMERICANA DE LOS DERECHOS Y DEBERES DEL HOMBRE

El Articulo tres de esta declaración dice: “Toda persona tiene el derecho de profesar libremente una creencia religiosa y de manifestarla y practicarla en público y en privado”. El tema de la religión, haciendo una referencia a los datos personales, puede constituirse en un dato, susceptible a ser publicado y puesto a conocimiento del público en general.

El siguiente artículo, el cuarto, se refiere alDerecho de libertad de investigación, opinión, expresión y difusión, que podríamos hacerlo mediante cualquier medio, y al

[73]DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS, Adoptada y proclamada por la Resolución de la Asamblea General 217 de 10 de Diciembre de 1948. Art. 19

ser cualquier medio, este se convierte en un dato, que también podría ser puesto a conocimiento de cualquier persona[74].

El Artículo quinto de esta declaración hace referencia a que “Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar”, dejando en claro que cualquier vejamen contra la honra y la vida privada de las personas debe ser sancionado por el Estado, tratándose sobre nuestro tema; cualquier dato personal o familiar difundido sin consentimiento puede ser vulnerario a este derecho innato al ser humano.

### 4.1.4. PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS

Al igual que los anteriores convenios y declaraciones, se tratan de los mismos derechos y la misma protección que deberían tener los mismos, transcribimos a continuación todos los Artículos relacionados a nuestro tema.

*Artículo 17*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.

*Artículo 18*1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de tener o de adoptar la religión o las creencias de su elección, así como la libertad de manifestar su religión o sus creencias, individual o colectivamente, tanto en público como en privado, mediante el culto, la celebración de los ritos, las prácticas y la enseñanza. 2. Nadie será objeto de medidas coercitivas que puedan menoscabar su libertad de tener o de adoptar la religión o las creencias de su elección. 3. La libertad de manifestar la propia religión o las propias creencias estará sujeta únicamente a las limitaciones prescritas por la ley que sean necesarias para proteger la seguridad, el orden, la salud o la moral públicos, o los derechos y libertades fundamentales de los demás. 4. Los Estados Partes en el

[74]Art. IV de laDECLARACION AMERICANA DE LOS DERECHOS Y DEBERES DEL HOMBRE, “Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio”.

presente Pacto se comprometen a respetar la libertad de los padres y, en su caso, de los tutores legales, para garantizar que los hijos reciban la educación religiosa y moral que esté de acuerdo con sus propias convicciones.

## 4.2. AMBITO NACIONAL- LEGISLACIÓN BOLIVIANA

### 4.2.1. NUEVA CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA

Nuestra Constituciónprevé la protección de los datos personales como la protección de un derecho fundamental dentro de lo que son los derechos civiles y políticos, como específicamente derecho civil, en su art. 21 numeral 2 3 y 5, respectivamente también en su art. 25 numeral primero y segundo:

PRIMERA PARTE BASES FUNDAMENTALES DEL ESTADO DERECHOS, DEBERES Y GARANTIAS

TITULO II DERECHOS FUNDAMENTALES Y GARANTIAS

CAPITULO TERCERO DERECHOS CIVILES Y POLITICOS

SECCION I DERECHOS CIVILES

Art. 21 Las personas y las bolivianas y bolivianos tienen los siguientes derechos:

2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad.

3. A la libertad de pensamiento, espiritualidad, religión y culto, expresados en forma individual o colectiva, tanto en público como en privado, con fines lícitos.

5. A expresar y difundir libremente pensamientos u opiniones por cualquier medio de comunicación, de forma oral, escrita o visual, individual o colectiva.

6. A acceder a la información, interpretarla, analizarla y comunicarla libremente, de manera individual o colectiva.

Art. 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, estos no podrán ser incautados salvo los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente.

Así mismo prevé Garantíasy el medio por el cual se harían valer todos nuestros derechos en caso de cualquier tipo de vulneración a nuestros datos personales:

Dentro de la misma PRIMERA PARTEBASES FUNDAMENTALES DEL ESTADO DERECHOS, DEBERES Y GARANTIAS

TITULO IV GARATIAS JURISDICCIONALES Y ACCIONES DE DEFENSA

CAPÍTULO SEGUNDO ACCIONES DE DEFENSA

SECCION I ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Art. 130. I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar, u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa.

**4.2.1.1.EL CÓDIGO CIVIL**

La protección de datos en este código es previsto como derechos de la personalidad:

TITULO I

DE LAS PERSONAS INDIVIDUALES

CAPITULO III DE LOS DERECHOS DE LA PERSONALIDAD

Art. 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.

Art. 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.

Art. 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 salvan los casos previstos por la ley.

Art. 19 (INVIOLABILIDAD DE LAS COMUNICACIONES Y PAPELES PRIVADOS)

I. Las comunicaciones, la correspondencia epistolar y otros papeles privados son inviolables y no pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente.

II. No surten ningún efecto legal las cartas y otros papeles privados que han sido violados o sustraídos, ni las grabaciones clandestinas de conversaciones o comunicaciones privadas.

El art. 16 en particular, es referido al derecho a la imagen, la cual no es especificada como derecho fundamental en ninguno de los convenios anteriores, pero se debe tomar en cuenta que una imagen puede ser considerada como un dato tratándose de una información relacionada a un individuo, la cual puede ser utilizada, directa o indirectamente para determinar la identidad del sujeto.

**4.2.1.2.EL CÓDIGO PENAL**

El Código Penal actual estipula delitos y sanciones en su Parte Especial, Libro segundo en los siguientes Títulos:

TITULO IX DELITOS CONTRA EL HONOR

CAPITULO UNICO DIFAMACION, CALUMNIA E INJURIA

Art. 282 (DIFAMACION)

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.

Art. 300 (VIOLACION DE LA CORRESPONDENCIA Y PAPELES PRIVADOS)

El que indebidamente abriere una carta, un pliego cerrado o una comunicación telegráfica, radiotelegráfica, dirigidos a otra persona, o el que, sin abrir la correspondencia, por medios técnicos ce impusiere de su contenido, será sancionado con reclusión de tres meses a un año o multa de sesenta a doscientos cuarenta días.

Con la misma pena será sancionado el que de igual modo se apoderare, ocultare o destruyere una carta, un pliego, un despacho u otro papel privado, aunque estén

abiertos, o el que arbitrariamente desviare de su destino la correspondencia que no le pertenece.Se elevara el máximo de la sanción de dos años, cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados.

TITULO XII DELITOS CONTRA LA PROPIEDADCAPITULO XI DELITOS INFORMATICOSArt. 363 Ter.- (ALTERACION, ACCESO Y USO INDEVIDO DE DATOS INFORMATICOS). El que sin estar autorizado se apoderare, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

#### 4.2.1.3. LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Siendo una ley dedicada única y exclusivamente a las telecomunicaciones y tecnologías de información, ésta no prevé la publicación de los datos personales de la que trata nuestro tema, salvo y escasamente en lo siguiente:

Como *principio de Inviolabilidad*. Donde las conversaciones o comunicaciones privadas efectuadas a través del uso de telecomunicaciones y tecnologías de información y comunicación, así como del servicio postal, son inviolables y secretas, no pudiendo ser interceptadas, interferidas, obstruidas, alteradas, desviadas, utilizadas, publicadas o divulgadas, salvo en los casos determinados por Ley.*Como un derecho de las usuarias y usuarios*, exigir la privacidad e inviolabilidad de sus comunicaciones.

TÍTULO III TELECOMUNICACIONES CAPÍTULO ONCEAVO DERECHOS Y OBLIGACIONES DE LAS USUARIAS Y USUARIOS Art 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.

#### 4.2.1.4. CÓDIGO NIÑO NIÑA ADOLESCENTE

TITULO IV DERECHO A LA LIBERTAD, AL RESPETO Y A LA DIGNIDAD

CAPITULO UNICO DERECHOS

Art. 100 (DERECHOS). El niño niña o adolescente tiene derecho a la libertad, al respeto y a la dignidad como persona en desarrollo. Asimismo, como sujeto de derecho, están reconocidos sus derechos civiles, políticos, económicos, sociales y culturales garantizados por la constitución, las leyes, Convención Internacional sobre los Derechos del Niño y otros instrumentos internacionales ratificados por el Estado Boliviano.

En el siguiente artículo se tomara en cuenta los incisos dos y tres:

SECCION I DERECHO A LA LIBERTAD

Art.101 (DERECHO A LA LIBERTAD). Este derecho comprende:

1. Libre tránsito y permanencia en su territorio nacional, salvo restricciones legales;
2. Libertad de opinión y expresión;
3. Libertad de creencias y culto religioso;
4. La práctica deportiva y el esparcimiento sano, según las necesidades y características de su edad;
5. La participación en la vida familiar y comunitaria, sin discriminaciones;
6. La búsqueda de refugio, auxilio y orientación cuando se encuentre en peligro;
7. Acudir a la autoridad competente en caso de conflicto de intereses con los padres o responsables y;
8. Libertad de asociación.

SECCION II DERECHO AL RESPETO Y A LA DIGNIDAD

Art. 105 (RESPETO). Consiste en la inviolabilidad de la integridad física, psíquica y moral del niño, niña o adolescente, abarcando, además, la preservación de la imagen, la identidad, los valores, las opiniones, los espacios y objetos personales y de trabajo. Ningún niño, niña ni adolescente debe sufrir discriminación étnica, de género social o por razón de creencias religiosas. El estado tiene la obligación de garantizar un trato respetuoso de igualdad y equidad a todos los niños, niñas y adolescentes que habitan en el territorio nacional.

Art. 106 (DIGNIDAD). Es deber de todos velar por la dignidad del niño, niña o adolescente, amparados y ponerlos a salvo de cualquier tratamiento inhumano, violento, deshumanizante, vejatorio o represivo, así como denunciar ante la autoridad competente los casos de sospecha o confirmación de maltrato.

### 4.2.1.5.LEY Nº 1488 DE BANCOS Y ENTIDADES FINANCIERAS

Contiene específicamente la prohibición de revelar ciertos datos bancarios en su Título Sexto,Capítulo I, Secreto Bancario:

ARTICULO 86°.-

Las operaciones realizadas por las entidades de intermediación financiera, estarán sujetas al secreto bancario. No podrán proporcionarse antecedentes relativos a dichas operaciones sino a su titular, a quien éste autorice o a la persona que lo representa legalmente, salvo lo establecido en el artículo 87º de la presente Ley.

ARTICULO 88°.-

Quedan obligados a guardar secreto de los asuntos y operaciones del sistema financiero y sus clientes, que lleguen a su conocimiento en el ejercicio de sus funciones, los directores, síndicos, gerentes y suplentes de:

1. Entidades de intermediación financiera.
2. Banco Central de Bolivia.
3. Empresas de auditoria externa.
4. Empresas valuadoras de riesgo.
5. Empresas vinculadas de entidades financieras.
6. Funcionarios públicos relacionados con la actividad de intermediación financiera.

ARTICULO 89°.-

El Superintendente y los empleados de la Superintendencia, aún después de cesar en sus funciones, están prohibidos de dar a conocer información relacionada con los documentos, informes u operaciones de las instituciones financieras o de personas relacionadas con el sistema financiero. El funcionario o empleado que infrinja esta prohibición, será destituido de su cargo, sin perjuicio de las responsabilidades civil o penal que correspondan.

### 4.2.1.5.1 RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS POR LA AUTORIDAD DE SUPERVISIÓN DEL SISTEMA FINANCIERO ASFI

En esta recopilación de normas que la ASFI exige a los bancos y entidades financieras, se puede observar un gran adelanto en seguridad de información ante los avances tecnológicos, a continuación transcribimos los artículos más importantes que serán tomados en cuenta para nuestra investigación:

LIBRO 3°: REGULACIÓN DE RIESGOS

TITULO VII

REQUISITOS MÍNIMOS DE SEGURIDAD

CAPÍTULO II: REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA PARA LAADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN YTECNOLOGÍAS RELACIONADAS

SECCIÓN 1: MARCO GENERAL

Artículo 1° - (Aspectos generales). El crecimiento vertiginoso en los últimos años enTecnologías de la Información y Telecomunicaciones, está cambiando la forma de hacer negociosen un mundo cada vez más globalizado y virtual.

Por tanto, las leyes, normativas, las políticas de estado, la regulación prudencial y las estrategiasde las Entidades Financieras y de las compañías, deben adecuarse a estos tiempos modernos,donde la llamada Economía Digital (e-Business, e-Commerce, e-Government) crece en cifrasexponenciales y nos trae a un tema de educación, cultura, resistencia al cambio que hay queadministrar, para estar insertos en forma eficiente, confiable y segura en este mercado virtual.

En consecuencia con lo anterior, las Entidades Financieras y las empresas que prestan serviciosauxiliares financieros, están viviendo este cambio y deben tomar acciones rápidas y eficientespara enfrentar, analizar, administrar y controlar los riesgos tecnológicos relacionados con lastransferencias de información y transacciones de fondos realizadas por medios electrónicos, paralo cual las políticas, normas y procedimientos de seguridad informática y planes de contingenciastecnológicos deben brindar un ambiente seguro y adecuado que garantice la continuidad operativadel negocio y su permanencia en el tiempo.

Artículo 2° - (Objeto). El presente capítulo tiene por objeto establecer los requisitos mínimosque las Entidades Financieras y las empresas de servicios auxiliares financieros supervisadas porla Autoridad de Supervisión del Sistema Financiero (ASFI) deben cumplir para administrar lossistemas de información y la tecnología que los soporta, y que son utilizados en las operacionesde intermediación financiera, transferencia electrónica de datos, transacciones electrónicas defondos, banca electrónica y cajeros automáticos con el propósito de minimizar el riesgotecnológico, siendo estos requisitos mínimos de carácter enunciativo y no limitativo.

SECCIÓN 2: REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA

Artículo 2° - (Características y criterios de la información). Los datos que administren lasEntidades Financieras y las empresas de servicios auxiliares financieros deben contener un altogrado de seguridad para cumplir con los objetivos de control y criterios básicos de informacióndefinidas por ASFI. Los criterios básicos se describen a continuación:

a) Confiabilidad: Proveer información apropiada y confiable para el uso de las EntidadesFinancieras y empresas de servicios auxiliares financieros tanto interna comoexternamente.

b) Confidencialidad: Protección de información sensible para que no se divulgue sinautorización.

c) Integridad: Se refiere a la exactitud y suficiencia de la información, así como suvalidez de acuerdo con los valores y expectativas de la actividad de la EntidadFinanciera.

d) Disponibilidad: Oportunidad de la información, cuando sea requerida.

e) Efectividad: Adecuada información para desarrollar las actividades de las EntidadesFinancieras y empresas de servicios auxiliares financieros.

f) Eficiencia: Proveer información suficiente a través del uso de los recursos de la mejormanera posible.

g) Cumplimiento: Debida atención a las leyes, regulaciones y acuerdos contractuales quela Entidad Financiera y empresas de servicios auxiliares financieros deben realizar.

### 4.2.1.6. LEY DE IMPRENTA

Tratándose de una ley con más de ochenta años de vigencia no tiene demasiadascaracterísticas puesto que ni especifica títulos y capitos para una sencilla ubicación de los artículos por relación. Se destacan tres principios que se deben respetar en la Ley de Imprenta como la garantía a la libertad de expresión, el secreto de la fuente informativa y la inviolabilidad de imprentas, pero se advierte que son necesarios cambios y adecuaciones que deberán ser debatidos con los trabajadores de la información a momento de realizar cualquier modificación a referida ley. En cuanto a nuestro tema encontramos los siguientes artículos:

Art. 13.- Se delinque contra las personas individuales o colectivas, en los impresos que las injurian directa o indirectamente, sean o no falsas las imputaciones injuriosas.

Art. 27.- Los delitos de calumnia e injuria contra los particulares quedan sujetos a la penalidad del Código y su juzgamiento pertenece a los tribunales ordinarios, a no ser que el ofendido quiera hacer valer su acción ante el Jurado.

#### 4.2.1.7. ESTATUTO DEL FUNCIONARIO PÚBLICO ADMINISTRATIVO

Dentro de los deberes del funcionario público no está establecido el respeto a los datos personales de cualquier individuo a momento de cumplir sus funciones, escasamente encontramos algo relacionado con nuestro tema, pero cabe recalcar que no es suficiente ni especifico, revisemos los incisos f y h:

TÍTULO IISERVIDOR PÚBLICO

CAPÍTULO IIDERECHOS Y DEBERES

ARTÍCULO 8° (DEBERES). Los servidores públicos tienen los siguientes deberes:

a) Respetar y cumplir la Constitución Política del Estado, las leyes y otras disposiciones legales.

b) Desarrollar sus funciones, atribuciones y deberes administrativos, con puntualidad, celeridad, economía, eficiencia, probidad y con pleno sometimiento a la Constitución Política del Estado, las leyes y el ordenamiento jurídico nacional.

c) Acatar las determinaciones de sus superiores jerárquicos, enmarcadas en la Ley.

d) Cumplir con la jornada laboral establecida.

e) Atender con diligencia y resolver con eficiencia los requerimientos de los administrados.

f) Mantener reserva sobre asuntos e informaciones, previamente establecidos como confidenciales, conocidos en razón a su labor funcionaria.
g) Velar por el uso económico y eficiente de los bienes y materiales destinados a su actividad administrativo.
h) Conservar y mantener, la documentación y archivos sometidos a su custodia, así como proporcionar oportuna y fidedigna información, sobre los asuntos inherentes a su función.
i) Cumplir las disposiciones reglamentarias relativas a la seguridad e higiene en el trabajo.
j) Presentar declaraciones juradas de sus bienes y rentas conforme a lo establecido en el presente Estatuto y disposiciones reglamentarias.
k) Declarar el grado de parentesco o vinculación matrimonial que tuviere con funcionarios electos o designados, que presten servicios en la administración.
l) Excusarse de participar en los comités de selección de ingreso de funcionarios de carrera, cuando exista con los postulantes vinculación o grado de parentesco hasta tercer grado de consanguinidad y segundo de afinidad inclusive, conforme al cómputo establecido en el Código de Familia.

#### 4.2.1.8. DECRETO SUPREMO 28168 ACCESO A LA INFORMACIÓN PÚBLICA

En fecha 17 de mayo de 2005 el presidente Carlos Mesa Gisbert en el marco de la transparencia en la gestión pública del Poder Ejecutivo emite esta norma, donde de manera específica se señala en un artículo la protección de datos personales:
ARTÍCULO 19º (PETICIÓN DE HABEAS DATA).
I. Toda persona, en la vía administrativa, podrá solicitar ante la autoridad encargada de los archivos o registros la actualización, complementación, eliminación o rectificación de sus datos registrados por cualquier medio físico, electrónico, magnético o informático, relativos a sus derechos fundamentales a la identidad, intimidad, imagen y privacidad. En la misma vía, podrá solicitar a la autoridad superior competente el acceso a la información en caso de negativa injustificada por la autoridad encargada del registro o archivo público.
II. La petición de Habeas Data se resolverá en el plazo máximo de cinco (5) días hábiles. En caso de negativa injustificada de acceso a la información, la autoridad

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

Este decreto supremo solo cuenta con veintiún artículos dando lugar a que existan vacíos jurídicos en cuanto la reglamentación del manejo de información estatal y administrativo tanto para los órganos estatales como para la población en general, por lo que existe el Proyecto de Ley de Transparencia y Acceso a la Información Pública, la cual puede ser vista en nuestros anexos[75].

## 4.3. LEGISLACIÓN COMPARADA

### 4.3.1. ARGENTINA

Históricamente, el resguardo legal de la intimidad en Argentina estuvo suficientemente garantizado por su Constitución Nacional (arts. 19 y 18) y los Códigos Civil (art. 1071 bis) y Penal (arts. 151 al 157 relativos a la violación del domicilio y de secretos) pues los medios de comunicación tradicionales (como lo eran el correo postal, el teléfono o el fax) no suponían demasiados desafíos para la legislación de la época.Pero todo cambió a comienzos del Siglo XXI ya que con el uso masivo e irracional de los nuevos sistemas electrónicos de comunicación, la intimidad, la identidad y el anonimato de las personas se vieron crecientemente amenazados. Fue por ello que, para dar respuesta a esta nueva realidad, en el año 2000 se sancionó la Ley Nº 25.326 de Protección de Datos Personales con la finalidad de salvaguardar integralmente los datos de carácter personal que se encontrasen en registros o bancos de datos, para así poder garantizar tanto el derecho al honor y a la intimidad de las personas, como el derecho de controlar la información que sobre las mismas se registre.Esta norma creó, sin lugar a dudas, una nueva cultura en el manejo y control de los datos personales pues beneficia con

[75] Ver Anexo 2.

nuevos derechos a los titulares de los datos y exige un estricto código de conducta para la recolección y el tratamiento de los mismos. También le brinda una especial protección a los denominados datos sensibles que son aquellos relativos al origen racial y étnico, a las opiniones políticas, convicciones religiosas, filosóficas o morales, la afiliación sindical, la salud y la vida sexual. De esta forma, los ciudadanos tienen ahora el derecho de autorizar a las personas que quieran utilizar sus datos siempre y cuando éstos los informen previamente sobre la finalidad para los que serán tratados, las medidas de seguridad que emplearán y quiénes serán los destinatarios. También tienen derecho a presentarse ante una empresa u organismo para que les comuniquen si poseen información sobre ellos y la finalidad para la que la utilizan; derecho a negarse a proporcionar datos cuando no sea obligatorio hacerlo; derecho a exigir que los datos inexactos o incompletos sean rectificados o actualizados, suprimidos o sometidos a confidencialidad; derecho a reclamar los daños y perjuicios y a iniciar la acción judicial de habeas data, por mencionar los más importantes.Del mismo modo, se establecieron una serie de obligaciones precisas para quienes utilicen bases de datos con información personal. Ahora, estos usuarios tienen el deber legal de inscribir todas sus bases de datos en un registro especial a cargo de la Dirección Nacional de Protección de Datos Personales, organismo dependiente del Ministerio de Justicia creado para velar por el cumplimiento de la ley y aplicar sanciones.En cuanto a la recolección de los datos, están obligados a pedirle el consentimiento al titular e informarle sobre lo que pretenden hacer con ellos para que, en última instancia, éste pueda decidir sobre la conveniencia o no de proporcionárselos. Asimismo, estos datos deberán ser recolectados en forma lícita y leal y no ser utilizados para finalidades distintas de aquéllas para las que se recogieron, permitiéndole al titular poder acceder a los mismos cuando éste lo requiera para rectificar, cancelar o suprimir los datos que sean erróneos o falsos.Finalmente, y con el fin de evitar la adulteración, pérdida o consulta no autorizada de los datos, los usuarios de los mismos tienen la obligación de adoptar medidas técnicas y organizativas que garanticen fehacientemente su seguridad y confidencialidad.La correcta aplicación de todo este régimen se encuentra bajo la tutela de la mencionada Dirección Nacional de Protección de Datos Personales quien está facultada para sancionar el incumplimiento a la ley con apercibimientos, multas y la posibilidad de suspender o clausurar las bases de datos. La Dirección Nacional de Protección de Datos Personales “DNPDP”tiene a su cargo un Registro de

las Bases de Datos, instrumento organizado a fin de conocer y controlar las bases de datos. Asimismo asesora y asiste a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos. En este sentido, tiene por función investigar si la base de datos denunciada da cumplimiento o no a los principios que establece la ley y las disposiciones reglamentarias.

### 4.3.2. COLOMBIA

El 17 de octubre de 2012 el Gobierno de Colombia sancionó la Ley Estatutaria de Hábeas Data -Ley 1581 de 2012- mediante la cual se desarrolla el derecho constitucional de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.
Las principales características de esta ley son:

- Se crea el régimen aplicable a los datos personales contenidos en bases de datos administradas por entidades públicas o privadas.
- El titular de los datos debe ser informado de su uso y existencia.
- El tratamiento de datos personales (recolección, almacenamiento, uso circulación, supresión y, en general, cualquier operación sobre estos) requiere del consentimiento previo, expreso e informado del titular de los datos (excepto cuando los datos sean requeridos por autoridades públicas o judiciales, exista urgencia médica o se trate del registro civil).
- Los titulares tienen derecho a actualizar y a rectificar los datos.
- Se cataloga a ciertos datos como “datos sensibles”, cuyo tratamiento se prohíbe por regla general. Los datos sensibles son aquellos que pueden generar discriminación si se hace un uso indebido de la información o que afectan el derecho a la intimidad, por ejemplo, la revelación del estado de salud o del origen racial o étnico.

- Con el fin de dar cumplimiento al régimen de protección de datos, se designa a la Superintendencia de Industria y Comercio como Autoridad Administrativa en la materia.
- La delegatura para la protección de los datos personales podrá iniciar de oficio o a petición de parte investigaciones sobre la materia y, además, está facultada para bloquear temporalmente los datos si existe una amenaza a los derechos fundamentales de un individuo. Igualmente, deberá promover y divulgar el ejercicio del Habeas Data y administrar el Registro Nacional de Bases de Datos (el cual deberá reglamentarse en un año).
- Dentro de las sanciones que podrá imponer la Superintendencia se encuentran el cierre temporal o definitivo y la imposición de multas individuales e institucionales de hasta 2.000 salarios mínimos (Aproximadamente USD$650.000).

### 4.3.3. PERÚ

El marco normativo de la protección de datos personales en el Perú, hasta antes de la daciónde la Ley N° 29733, se venía dando por una serie de normas jurídicas de distinto nivel jerárquico, dispersas en todo su ordenamiento jurídico.

A nivel Constitucional, la Constitución Política de 1993 establece losderechos que constituyen la fuente primigeniaque marca e inspira la legislación existente sobreprotección de datos personales. En este acápitenos referiremos no solo a lo expresamentedispuesto por la Constitución Política, sino queharemos referencia a las otras disposicionesque constituyen el bloque de constitucionalidad,como son el Código Procesal Constitucional y las sentencias de su Tribunal Constitucional.

El artículo 2°, inciso 7) de la Carta Constitucionalreconoce los derechos a la intimidad, al honory a la propia imagen, que ya se encontrabanconsagrados en la Constitución Política de 1979.En el mismo artículo 2°, pero en el inciso 6), sereconoce un nuevo derecho, cuando señala quelos servicios informáticos, computarizados o no, públicos o privados, no suministren informacionesque afecten la intimidad personal y familiar.

El Tribunal Constitucional definió este derechocomo el de autodeterminación informativa, ensu sentencia de fecha 29 de enero de 2003, expedienteNº 1797-2002-HD/TC, en el marco de un proceso de hábeas data.

A su vez, el artículo 200º, inciso 3) de la ConstituciónPolítica de 1993, establece la GarantíaConstitucional del hábeas data para proteger losderechos reconocidos en los incisos 5), derechode acceso a la información pública, y 6) derechoa la protección de datos personales, del artículo2º de la Carta fundamental.

La Ley Nº 28237 que aprobó el primer CódigoProcesal Constitucional (cpc) peruano, en vigordesde el 01 de diciembre del 2004, en su artículo61, inciso 2), establece que toda personapuede recurrir al proceso de hábeas data para2) Conocer, actualizar, incluir y suprimir o rectificarla información o datos referidos a su personaque se encuentren almacenados o registradosen forma manual, mecánica o informática,en archivos, bancos de datos o registros de entidadespúblicas o de instituciones privadas quebrinden servicio o acceso a terceros. Asimismo,a hacer suprimir o impedir que se suministrendatos o informaciones de carácter sensible oprivado que afecten derechos constitucionales.

Hasta el 4 de julio de 2011, el único instrumentode tutela del derecho a la protecciónde datos personales en el Perú era la acciónde hábeas data; con la Ley de protección dedatos personales, Ley N° 29733, en adelanteel derecho a la protección de datos personaleses desarrollado legislativamente y se crea unaautoridad de control, que se suma a la tutela jurisdiccionalexistente en el hábeas data, pero yaen el ámbito administrativo y que se espera seamás efectiva y rápida.

**4.3.3.1. LEY DE PROTECCIÓN DE DATOS PERSONALES LEY N° 29733.**

Esta novísima norma de desarrollo constitucionaltiene un título preliminar y siete títuloscomprendidos en cuarenta artículos, así comodoce disposiciones complementarias finales. Acontinuación presentamos esta ley en algunos de sus aspectos relevantes. Esta norma, reciénestá siendo materia de real asimilación y

tomade conciencia por la mayor parte de la academia,de las autoridades y de la sociedad en generalen el Perú.

El objetivo de esta Ley, se encuentra definido de maneradirecta y simple en el artículo 1°. Consiste engarantizar el derecho fundamental a la protecciónde los datos personales, previsto en el artículo2, numeral 6 de la Constitución Políticade 1993. Con esta declaración se "coloca" legalmenteel epígrafe al citado numeral constitucional,definido en algunas oportunidades por lajurisprudencia del Tribunal Constitucional comoel derecho a la autodeterminación informativa.
La ley señala que la garantía del derecho fundamentala la protección de los datos personalesse materializará a través de un adecuado tratamientode los mismos en un marco de respetode los demás derechos fundamentales que enla Constitución se reconocen.

El marco de garantía del derecho que nos ocupase delimita entonces por el respeto a los demásderechos fundamentales que la Carta Políticadel Perú reconoce, en lo cual es bastanteamplia, pues además de la lista contenida enlos veinticuatro incisos del artículo 2°, yla cláusula interpretativa de los derechos, quehace parte de la cuarta disposición final y transitoria,y que remite para la interpretación delas normas relativas a los derechos y a las libertades, a la Declaración Universal de DerechosHumanos, así como a los tratados y acuerdosinternacionales sobre las mismas materias ratificadospor el Perú.

Esta ley realiza una definición precisa de todos aquellos términos que tienen que ver con el tema de protección de datos, en su artículo 2°, definelos siguientes conceptos: banco de datos personales,banco de datos personales de administraciónprivada, banco de datos personalesde administración pública, datos personales,datos sensibles, encargado del banco de datospersonales, entidad pública, flujo transfronterizode datos personales, fuentes accesiblespara el público, nivel suficiente de protecciónpara los datos personales, persona jurídica dederecho privado, procedimiento de anonimización,procedimiento de disociación, titular dedatos personales, titular del banco de datospersonales, transferencia de datos personalesy

tratamiento de datos personales. El artículoconcluye habilitando al reglamento de la leypara realizar un mayor desarrollo de las definicionesexistentes.

Su ámbito de aplicación está definido en suartículo 3°, es de aplicación a los datos personalescontenidos o destinados a ser contenidosen bancos de datos personalesde administraciónpública y de administración privada, cuyotratamiento se realiza en su territorio nacional.La Ley no se aplicará a los datos personalescontenidos o destinados a ser contenidos enbancos de datos personales creados porpersonasnaturales para fines exclusivamente relacionadoscon su vida privada o familiar; así comoa los contenidos o destinados a ser contenidosen bancos de datos de administración pública,solo en tanto su tratamiento resulte necesariopara el estricto cumplimiento de las competencias asignadas por ley en las materias relacionadascon la defensa nacional, seguridad pública,y para el desarrollo de actividades en materiapenal para la investigación y represión del delito.

### 4.3.4.URUGUAY

En Uruguay existe la Ley N° 18.331 (aprobada el 11 de agosto de 2008) sobre Protección de Datos Personales y Acción de Habeas Data. Es una avanzada legislación que indica que "el derecho a la protección de datos personales es inherente a la persona humana". Por ende, ese derecho, es propio de las personas físicas (respecto de sus datos personales contenidos “a través de cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo”) y por extensión, también de “las personas jurídicas, en cuanto corresponda”. El objetivo de esta ley radica en la pretensión regular la totalidad de los bancos de datos personales existentes en poder de personas físicas y jurídicas, públicas o privadas, y por ello deroga expresamente la Ley Nº 17.838 de 24 de septiembre de 2004 sobre “Protección de Datos Personales Para Ser Utilizados en Informes Comerciales y Acción de Habeas Data”, que refería exclusivamente a las bancos de datos personales destinados a brindar (solamente) informes objetivos de tipo comercial.

Esta ley crea una unidad que tiene como objetivo primordial custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios, llamadaLa Unidad Reguladora y de Control de Datos Personales (URCDP)órgano desconcentrado de la AGESIC ("Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento", de Uruguay), por el artículo 31.

Tal fue el éxito de las funciones de mencionada unidad con relación al cumplimiento de la ley de Protección de Datos Personales y Acción de Habeas Data, que precisamente Uruguay fue designado como país anfitrión de la 34ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad, la que se realizó en Punta del Este, el 23 y 24 de octubre de 2012.

En fecha 17 de abril de este año Uruguay finalizó el trámite de adhesión al Convenio Nº 108 ante el Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos. Dicho documento torna a Uruguay como el primer país fuera de la Unión Europea que concluye con todo el proceso de adhesión al mencionado Convenio y su Protocolo Adicional.Esta es la culminación de otro hito fundamental para el país, junto con la adecuación a la Directiva 95/46/CE, para garantizar la protección de los datos personales a nivel nacional e internacional y su transferencia, este texto constituye referencia, a escala europea, en materia de protección de datos personales.

### 4.3.5. UNIÓN EUROPEA

La Directiva 95/46/CE constituye el texto de referencia; a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE). Con ese objeto, la Directiva fija límites estrictos para la recogida y utilización de los datos personales y

solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos[76].

La presente Directiva se aplica a los datos tratados por medios automatizados (base de datos informática de clientes, por ejemplo), así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él (ficheros en papel tradicionales).

La Directiva no se aplicará al tratamiento de datos:
- efectuados por una persona física en el ejercicio de actividades exclusivamente particulares o domésticas;
- aplicado al ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, tales como la seguridad pública, la defensa o la seguridad del Estado.

Esta Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

- La calidad de los datos: los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Además, serán exactos y, cuando sea necesario, actualizados.
- La legitimación del tratamiento: el tratamiento de datos personales sólo podrá efectuarse si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:la ejecución de un contrato en el que el interesado sea parte, oel cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, oproteger el interés vital del interesado, oel cumplimiento de una misión de interés público, ola satisfacción del interés legítimo perseguido por el responsable del tratamiento.
- Las categorías especiales de tratamiento: deberá prohibirse el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas y la pertenencia a sindicatos, así como

[76] www.datospersonales.gub.uy

el tratamiento de los datos relativos a la salud o a la sexualidad. Esta disposición va acompañada de reservas que se aplicarán, por ejemplo, en caso de que el tratamiento sea necesario para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.

- La información a los afectados por dicho tratamiento: el responsable del tratamiento deberá facilitar cierta cantidad de información (identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, etc.) a la persona de quien se recaben los datos que le conciernan.
- El derecho de acceso del interesado a los datos: todos los interesados deberán tener el derecho de obtener del responsable del tratamiento:la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.
- Las excepciones y limitaciones: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos con objeto de salvaguardar, entre otras cosas, la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.
- El derecho del interesado a oponerse al tratamiento: el interesado deberá tener derecho a oponerse, por razones legítimas, a que los datos que le conciernen sean objeto de tratamiento. También deberá tener la posibilidad de oponerse, previa petición y sin gastos, al tratamiento de los datos respecto de los cuales se prevea un tratamiento destinado a la prospección. Por último, deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.
- La confidencialidad y la seguridad del tratamiento: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se

lo encargue el responsable del tratamiento. Por otra parte, el responsable del tratamiento deberá aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.

- La notificación del tratamiento a la autoridad de control: el responsable del tratamiento efectuará una notificación a la autoridad de control nacional con anterioridad a la realización de un tratamiento. La autoridad de control realizará comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Deberá procederse a la publicidad de los tratamientos y las autoridades de control llevarán un registro de los tratamientos notificados.

Las legislaciones nacionales deben prever un recurso judicial para los casos en los que el responsable del tratamiento de datos no respete los derechos de los interesados. Además, las personas que sufran un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales tendrán derecho a obtener la reparación del perjuicio sufrido.

Se autorizará la transferencia de datos personales de un Estado miembro a un tercer país que garantice un nivel de protección adecuado; por el contrario, no se autorizará la transferencia a terceros países que no dispongan de tal nivel de protección, salvo contadas excepciones que se enumeran en el texto.

La Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.

Cada Estado miembro designará una o varias autoridades públicas independientes encargadas de controlar la aplicación en su territorio de las disposiciones adoptadas por los Estados miembros en aplicación de la presente directiva.

Se crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales, que estará compuesto por representantes de las autoridades de

control nacionales, por representantes de las autoridades de control de las instituciones y organismos comunitarios y por un representante de la Comisión[77].

**4.3.5.1. ALEMANIA**

En un primer período, cuando el número y costos asociados al funcionamiento de equipamiento computacional suponían su empleo sólo por grandes reparticiones públicas, tiene lugar la promulgación de la primera legislación en materia de protección de datos. Así, en 1970 se promulga la Datenschutz, ley sobre tratamiento de datos personales del Land de Hesse, en la República Federal de Alemania, mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. A efectos de asegurar el cumplimiento de sus previsiones, la ley creo el Comisario de Protección de Datos, al cual garantizaba independencia para el desempeñode sus funciones, cuales eran velar por la observancia de los preceptos de la propia ley y cuantos otros hicieren referencia al trato de los datos de los ciudadanos.

Posteriormente, cuando ya se contaba con una serie de disposiciones federales y territoriales que regulaban eltema, con pretensiones de generalidad o cierta especificidad, se dicta la Bundesdatenschutzgesetz, Ley Federal deProtección de Datos de la República Federal Alemana de 1977, en la cual se establece una normativa general deprincipios susceptible de ser aplicados subsidiariamente a otros ámbitos o contextos, lo cual explica que acuda con frecuencia al empleo de conceptos jurídicos indeterminados y se cuide de no entrometerse en competencias que excedan las del gobierno federal.

La Ley Federal de Protección de Datos de 1977 contempla las disposiciones generales, cuyo objeto en evitar eldetrimento de intereses dignos de protección de las personas naturales afectadas por el tratamiento automatizadode datos que le conciernen efectuados por el sector público y privado; entre sus disposiciones se

[77] http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm

observan diversas innovaciones, posteriormente acogidas por otras legislaciones, tales como el "comisario de protección de datos", laconcesión a los titulares de datos del "derecho de bloqueo", y la tipificación de ilícitos penales e infracciónales asociados al tratamiento de datos. Además, impone a los entes que procesen datos la adopción de medidas técnicas y de organización necesarias para garantizar la observancia de la ley, las que precisa en anexo a la misma.

La ley, que establece regímenes jurídicos paralelos para el tratamiento de datos por el sector público y privado, fija también un sistema de control que atiende a tal distingo: respecto de los organismos públicos, impone a las diversas entidades de la administración federal la obligación de velar por el cumplimiento de la legislación y dictar disposiciones administrativas que regulen la aplicación de la ley en su respectivo ámbito de competencias y, a su vez, contempla una autoridad de control llamada a velar por la observancia de la misma y otras disposiciones aplicables a la protección de datos: el Comisario Federal de Protección de Datos.

En cambio, en cuanto al tratamiento de datos por entes no públicos, la ley acude al denominado comisario deprotección de datos y las autoridades de tutela estatal. El primero debe ser nombrado por cada entidad que elaboradatos personales y depende de ella, aun cuando no queda sujeto a sus instrucciones en el desempeño de su cometido, cual es velar por la observancia de la legislación relativa a la protección de datos; en tanto que laautoridad de tutela es fijada por los gobiernos de los estados y le compete velar por la observancia de la Ley deDatos y demás disposiciones sobre protección de datos previstas dentro del ámbito de aplicación a los privados,aunque sólo a requerimiento del afectado[78].

El 6 de Mayo de 2013 a través del ministro del interior alemán Wolfgang Schaeuble se dio a conocer que Alemania pretende realizar una reforma de las leyes de protección de datos para hacerlas más estrictas, actuando de esta forma después de las revelaciones de que los datos personales de los alemanes pueden comprarse fácilmente en Internet.Schaeuble afirmó que un grupo de trabajo realizará diferentes

[78] http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewArticle/10661/11413

propuestas con el fin de aumentar las multas para las violaciones de protección de datos y hacer más estrictas las normas sobre el intercambio de información personal y financiera. "Se producirán rápidamente las consultas necesarias para conseguir que las propuestas legales estén listas antes de finales de este año", declaró Schaeuble en una rueda de prensa después de reunirse con los ministros de Justicia, Economía y Protección del Consumidor para tratar este tema, también dijo que en el futuro las compañías sólo serán capaces de almacenar datos personales si los consumidores lo han acordado de forma específica. Las normas que ya existen permiten, por lo general, a los centros de llamadas y a otras compañías intercambiar direcciones personales a no ser que los consumidores digan que se oponen a ello.

La protección de datos y las cuestiones privadas son temas sensibles en Alemania, un país angustiado por el espionaje realizado por la Gestapo, la Policía secreta oficial de la Alemania nazi, y por la Policía secreta de la antigua Alemania del Este, la antigua Stasi.

Algunos defensores de la privacidad han pedido una completa prohibición sobre el intercambio de datos personales, lo que ha provocado duras críticas por parte de las compañías tecnológicas y de telecomunicaciones. "Algunos consumidores quieren recibir en la actualidad anuncios y aceptan que sus datos pasen de unos a otros", declaró August Wilhelm Scheer, miembro de una asociación del sector, Bitkom, al diario 'Handelsblatt'.

Las cuestiones relacionadas con la protección de datos han jugado un papel fundamental en Alemania durante los últimos meses, en un tiempo en el que el Gobierno intenta suavizar las leyes sobre los datos privados para ayudar a la Policía a combatir el terrorismo y el crimen.

La empresa Deutsche Telekom, la mayor compañía de telecomunicaciones de Europa, impactó a sus clientes a principios de este año con las revelaciones que informaban de que realizó registros telefónicos ilegales en 2005[79].

[79] http://www.hoytecnologia.com/noticias/Gobierno-aleman-endurecera-leyes/73950

#### 4.3.5.2. ESPAÑA

Como antecedentes de una ley que regula la protección de datos personales en España, tenemos a la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), que desarrolla lo recogido en el artículo 18 de la Constitución Española de 1978 y establece, por primera vez, la limitación del uso de la informática para garantizar la intimidad personal.

Posteriormente, la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos, establece el marco jurídico en el que se desarrolla la actual legislación española en Protección de Datos de Carácter Personal.

La LORTAD tardó siete años en disponer de su desarrollo reglamentario, que llegó con el Real Decreto 994/1999, de 11 de junio: Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (RMS).

Pocos meses después de la aprobación de dicho reglamento se promulgó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de CarácterPersonal (LOPD), vigente en la actualidad, y que adapta la legislación española a la Directiva europea, desarrollando la protección de datos más allá de los datos informatizados, incluyendo dentro de su ámbito de aplicación los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento automatizado o no, y toda modalidad de uso de los mismos.

Por fin, la LOPD, tras un periodo de ocho años conviviendo con el RMS, ha visto cómo su desarrollo reglamentario ha sido plasmado mediante el Real Decreto 1720/2007, de

21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RLOPD)[80].

## 4.4. LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS PERSONALES

La Red Iberoamericana de Protección de Datos (RIPD), surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos.

Esta iniciativa contó desde sus inicios con un apoyo político reflejado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en Santa Cruz de la Sierra en nuestro país 14 y 15 de noviembre de 2003, conscientes del carácter de la protección de datos personales como Derecho Fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

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

La actividad de la Red durante estos diez años ha sido intensa y fructífera, promoviendo el desarrollo de diez Encuentros, uno por año, y de otros tantos

[80] http://temariotic.wikidot.com/breve-historia-de-la-proteccion-de-datos-personales

Seminarios sobre los más variados temas de interés: protección de datos de los menores: datos de salud; sector financiero (fraude); sector comercial y marketing, en especial la lucha contra el Spam; las nuevas tecnologías y su impacto sobre la privacidad; transferencias internacionales, etc.

Esta trayectoria ha llevado a que la Red se haya consolidado como principal promotor del diálogo e impulsor de iniciativas y políticas en la región, que ha significado que más de 150 millones de ciudadanos latinoamericanos dispongan en la actualidad, junto al tradicional amparo de habeas data, de normas que permitan garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías. Ejemplos significativos del avance normativo producido en la región durante estos diez años de funcionamiento de la Red, se encuentran en países como Argentina (Ley 25326/2008); Uruguay (Ley 18.331/2008); Perú (Ley 29733/2011); Costa Rica (Ley 8968/2011); Nicaragua (Ley 787/2012), y Colombia (Ley 1581/2012), que ha sido la última en incorporarse al grupo de países que disponen de una normativa específica en esta materia.

En definitiva, es interés primordial de las instituciones que en la actualidad constituyen la RIPD, seguir impulsando el desarrollo del Derecho Fundamental a la Protección de Datos de Carácter Personal a través de las entidades con capacidad y competencias para instar a los gobiernos nacionales a que elaboren una regulación normativa en esta materia, a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

Los objetivos y la organización de la Red están recogidos en el Reglamento aprobado con motivo del VI Encuentro Iberoamericano de Protección de Datos, celebrado en Cartagena de Indias, Colombia, del 27 al 30 de mayo de 2008[81].

### 4.4.1. PAÍSES MIEMBROS DE LA RED IBEROAMERICANA DE PROTECCIÓN DE DATOS PERSONALES

[81] http://www.redipd.org/la_red. php

Es interesante mencionar como antecedentes de esta red, a Bolivia, que al tratarse de uno de los países miembros, no tenga una estructura especifica en cuanto a la protección de datos personales, me refiero a estructura; como a una ley referente al tema; una reglamentación; un ente con conocimiento amplio y concreto, que a su vez realice las funciones que otras unidades llevan a cabo en otros países con respecto a los delitos contra los datos personales de las personas. Los países miembros son:

Principado de Andorra.
República de Argentina.
Estado Plurinacional de Bolivia.
República Federativa del Brasil.
República de Chile.
República de Colombia.
República de Costa Rica.
República del Ecuador.
República de El Salvador.
Reino de España.
República de Guatemala.
República de Haití.
República de Honduras.
Estados Unidos Mexicanos.
República de Nicaragua.
República de Panamá.
República del Paraguay.
República del Perú.
República Portuguesa.
República Dominicana.
República Oriental del Uruguay.
República Bolivariana de Venezuela.

# CAPITULO V
# MARCO PRÁCTICO

## 5.1. PROPUESTA NORMATIVA

### 5.1.1.DERECHO Y LA TECNOLOGÍA

Las modernas tecnologías de la información y las comunicaciones (TIC o ITC), a resultas de la convergencia entre las telecomunicaciones y la informática, están provocando cambios significativos en todos los ámbitos (político, económico, tecnológico, sociológico) de las sociedades contemporáneas avanzadas.

En este sentido, las tecnologías de la información y las comunicaciones, en la medida que representan la transformación de los formatos actuales de las más diversas acciones sociales e individuales (en la cultura, la ciencia, la economía, las relaciones laborales, etc.) y, al mismo tiempo, un incremento de las relaciones interpersonales a distancia y del tratamiento de la información personal, plantean problemas originales y complejos que exigen una adecuada respuesta del ordenamiento jurídico, que, obviamente, no ha de pretender el establecimiento de mecanismos de represión y obstáculos para su desarrollo, sino que, por el contrario, ha de tratar de impulsarlas, mediante el establecimiento y aplicación de un marco normativo adecuado que evite "las graves consecuencias" que, como en la informática, pudieran derivar de su desarrollo incontrolado para el ejercicio de los derechos y libertades.

Desde una perspectiva de carácter general, los "tres órdenes de problemas", que, tradicionalmente, se vinieron detectando con la aparición del fenómeno informático, son: los problemas de orden tecnológico, consistentes "en cómo impedir el acceso incontrolado a los sistemas de proceso de datos mediante la concepción y realización de unos dispositivos físicos o lógicos que le impidan"; los de orden deontológico, que exigen "la creación de una mentalidad responsable por parte de los profesionales y la aceptación de unos códigos de ética informática"; y, finalmente, los problemas de orden jurídico, surgidos de la necesidad de creación y establecimiento de "un marco

conceptual que permita sistematizar supuestos de hechos posibles y darles una solución coherente y uniforme", se han incrementado en el "mundo de las telecomunicaciones", en el que "la habitual organización de sus servicios, puede incidir con especial intensidad sobre el delicado mundo de los datos", haciendo que la protección de datos de carácter personal y del secreto de las comunicaciones sean, en la actualidad, algunos de los ámbitos jurídicos en los que las modernas tecnologías de la información y las comunicaciones despiertan un mayor interés para la doctrina.

Por tal motivo, siendo el derecho un instrumento privilegiado de la construcción de este nuevo espacio, resulta evidente que la investigación jurídica debe, en primer lugar, tomar un adecuado conocimiento de los fenómenos técnicos y sociales, para, a continuación, proceder al estudio de las normas que salen al encuentro de esa nueva realidad, pese a que el propio dinamismo del cambio tecnológico impide, en muchas ocasiones, el que podamos tener "una visión completa y acabada de todos y cada uno de los problemas a que puede dar lugar".

No obstante, la toma en consideración del progreso tecnológico y de los nuevos fenómenos sociales que éste provoca, nos permite afirmar, como se ha pretendido por algunos, la puesta en discusión de los fundamentos mismos del ordenamiento jurídico vigente y tampoco establecer una autonomía como disciplina jurídica de las distintas cuestiones derivadas de las tecnologías de la información y de la comunicación (como también, en su momento, sucedió, debido al auge del fenómeno informático, con el denominado "derecho informático").

Nos encontramos, consiguientemente, en este campo (como en otros, derecho de la alimentación, derecho agrario, derechos de la circulación, etc.), ante lo que la doctrina italiana ha definido como "disciplinas informativas", que, como tales, "habrán de nutrirse siempre de principios muy diversos, cualitativamente heterogéneos según corresponde a las disciplinas matrices de la que proceden". Ciertamente, no es posible aplicar los mismos principios técnico -jurídicos, por ejemplo, a la protección de datos, a los problemas derivados de la protección jurídica del software, o a los delitos cometidos por medios informáticos, o, en el concreto sector de las telecomunicaciones, respecto de las distintas importantes funciones que en el mismo se pueden suscitar y en el que

se entrecruzan diversas ramas del ordenamiento jurídico (derecho administrativo, derecho mercantil y derecho comunitario, básicamente).

Por lo tanto, sin perjuicio de reconocer que el desarrollo de las tecnologías de la información y las comunicaciones, que, como en otros muchos ámbitos, siempre ha sido más rápido que el proceso de adaptación del ordenamiento jurídico, el sustentar una autonomía de este ámbito (llámese "derecho de las tecnologías de la información y las comunicaciones"), "derecho informático" (o cualquier otra denominación), requiere una actualización continua y a la par del crecimiento tecnológico, esfuerzo necesario para que la legislación al respecto se mantenga en continua evolución[82].

### 5.1.2. MOTIVOS QUE INDUCEN A DESARROLLAR UNA LEGISLACIÓN DE PROTECCIÓN DE DATOS PERSONALESEN INTERNET

El estudio de un régimen jurídico sobre protección de datos de carácter personal en el sector de las telecomunicaciones, específicamente en el internet, debe partir de justificar la necesidad de una norma encargada de regularespecífica y separadamenteéstos derechos, de los ya agotados derechos fundamentales.

El uso de internet en nuestro país ha sido tan aceptado por la sociedad en general que nuestra vida como seres de sociedad, no podría desarrollarse sin el uso de estas nuevas tecnologías. Pero no solo nosotros hemos crecido con el uso de la tecnología sino que los administradores del estado se permitieron facilidades laborales aplicándolas, ya sea por un sinfín de motivos, como; espacio, orden, facilidad de búsqueda o específicamente, llegando a nuestro tema; almacenaje de datos de carácter personal sometidos a tratamiento, lo que los lleva a crear sistemas informáticos para organizarse de mejor manera. Ahora bien, estos sistemas informáticos facilitaron también a la población, ya que por medio del internet, una persona puede tener conocimiento de ciertas actividades, noticias o procedimientossin

[82] María de los Reyes Corripio Gil-Delgado , El Tratamiento de los Datos de Carácter Personal y la Protección de la Intimidad en el Secreto de las Telecomunicaciones La transposición de la Directiva sobre la Privacidad y las Comunicaciones Electrónicas, Universidad Pontificia ICAI ICADE Comillas Madrid, 2004, pág. 51

necesidad de apersonarse a determinada institución o ente a recabar todo aquello que se encuentra ya plasmado en páginas y sitios web, creados para ese fin, informar.

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

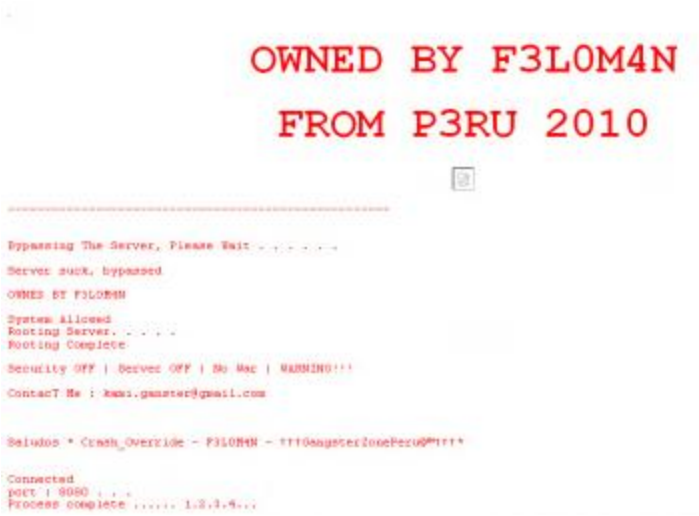
Adentrando en sí a los motivos para crear una legislación de protección de datos personales en internet, se tienen casos de vulneraciones a ciertas páginas de gobierno o relacionados con el mismo, las cuales por la calidad de seguridad aplicadas en las mismas, fueron atacadas por diferentes procedimientos, donde los hackers o piratas por el conocimiento que tienen, operaron, tal y como ocurrió el primero de mayo de la gestión en curso, donde la Presidencia de Bolivia sufrió un ataque cibernético en su páginaweb, su base de datos fue filtrada y pudo extraerse información sobre los datos, identidades y cargos de los funcionarios que trabajan en el Ministerio de la Presidencia, la acción atribuida a Anonymous Bolivia yAnon_0x03, permitióal pueblo boliviano conocer que en Palacio Quemado trabajan 208 empleados, que el Presidente Morales tiene varias secretarias, tres asistentes de despacho, un maestro de ceremonias y tres comunicadores, entre otros colaboradores*, asimismo y más delicado aún*, mediante sus redes sociales, los hackers publicaron también las claves y contraseñas de los correos electrónicos de ciertos ministros, lo que conlleva a una total vulneración de datos de carácter personal (http://pastebin.com/hK8gmuud Anexo 3).Este ataque surgió tras que el Tribunal Constitucional Plurinacional (TCP) de Bolivia declare constitucional la habilitación del presidente Evo Morales y del vicepresidente Álvaro García Linera a una nueva postulación en elecciones generales en 2014.

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

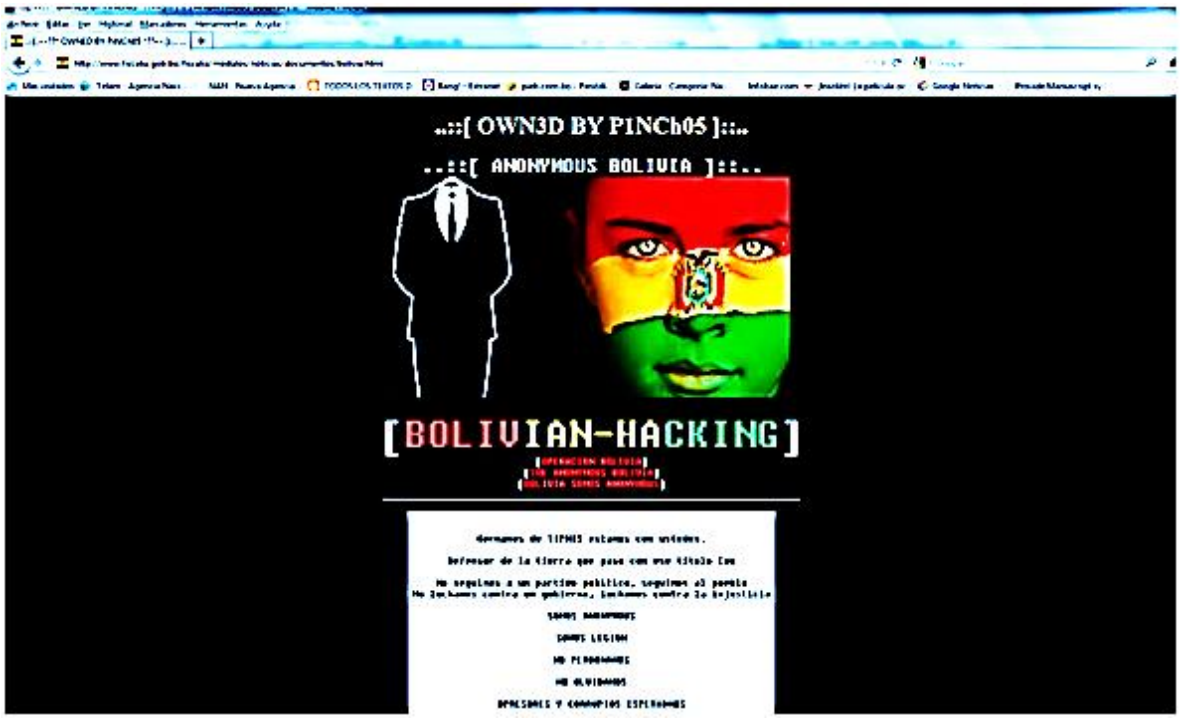
gobiernopara con la sociedad. A continuación desarrollaré, los más recientes antecedentes de los incidentes,publicados en medios de comunicación:

**Incidente YPFB**. En fecha 25 de agosto de 2011, la página HidrocarburosBolivia.com sufrió un ataque cibernético, consistió en que la información de la página fue bloqueada y reemplazada por mensajes de crítica al gobierno sobre diferentes aspectos de la coyuntura social de aquella temporada, cómo críticas a la Ley de Telecomunicaciones, repudio a la carretera por el Territorio Indígena Parque Nacional IsiboroSécure (TIPNIS), causas de los "pinchazos" telefónicos, criticas al servicio de internet en Bolivia, así como la defensa de la libertad de expresión, la Autoridad encargada de las Tecnologías de Información aseveró que los hackersno tuvieron acceso al sistema de información corporativa y que el ataque consistió solo en la técnica *defacement.(*Anexo 4)

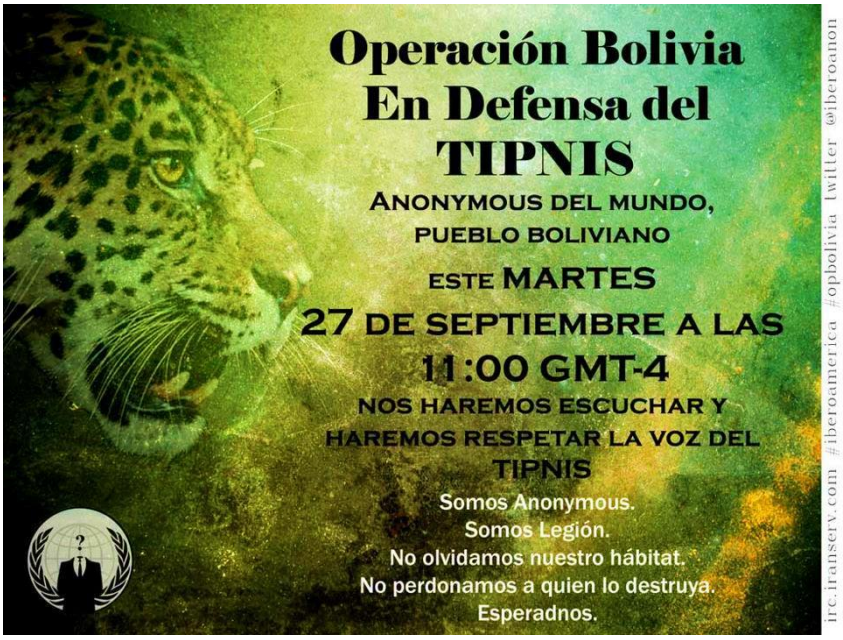
**Incidente Fiscalía**. Varios incidentes se tienen registrados a la página http://www.fiscalia.gov.bo, el año 2008 el ataque se debió a una vulnerabilidad en la versión Apache; el año 2010 fue reportada hackeada nuevamente donde por más de 15 días el enlace apareció con el siguiente mensaje:




Nuevamente, en fecha 28 de septiembre de 2011, al ingresar al link de la página, todo se encontraba normal, pero al abrir la sección de documentos la página torna de color negro con mensajes a favor del TIPNIS, criticando el video donde la ONU nombra al presidente Evo Morales "Defensor mundial de la madre tierra".(Anexo 5)



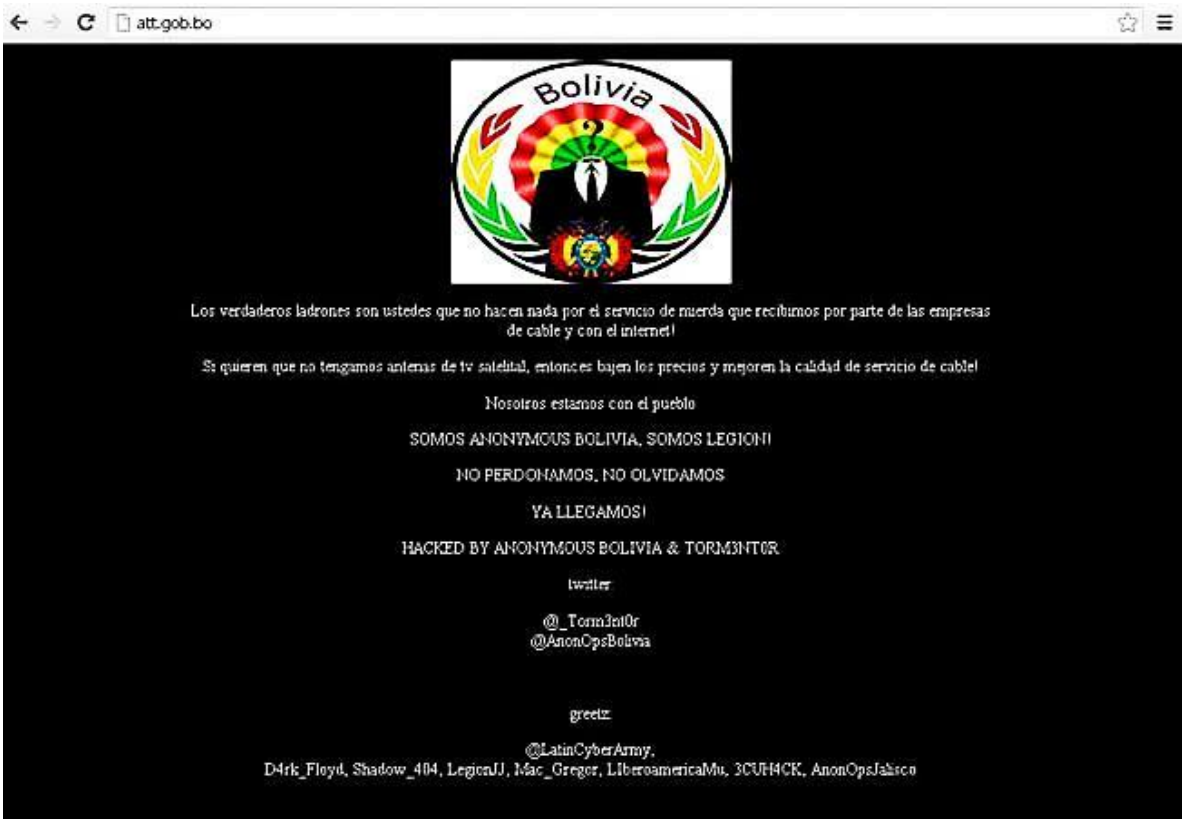

**IncidenteDiprove, Entel, Fiscalía, Presidencia.** Días antes al 27 de Septiembre de 2011, en las redes sociales, se publicó el siguiente mensaje:




Se trató de una operación en repudio a la construcción de la carretera en el TIPNIS, el ataque comenzó a las 11:00, primero impidieron el acceso a la página de la Presidencia, posteriormente atacaron la página de Diprovedejándola expuesta en la

lista de datos de autos "truchos" de DIPROVE. Seguidamente deformaron la página de la fiscalía con la canción "Bolivia" de los Kjarkas de fondo y el mensaje "Pueblo boliviano no estás solo, somos legión, no obedecemos a un partido político, obedecemos al pueblo" En Twitter pasó un mensaje "Gobierno de Bolivia, deberías haberlo esperado" A continuación liberaron 4700 cuentas de correo @entelnet con password y 2900 cuentas wi fi de ENTEL con password también (http://t.co/oDbWsPDfAnexo 6) y para finalizar publicaron una lista de todos los policías de Bolivia con cargos, teléfonos y direcciones domiciliarias (http://pastebin.com/U0Nj2VMKAnexo7).

**Incidente Autoridad de Fiscalización y Regulación de Telecomunicaciones y Transportes de Bolivia ATT.** El golpe dado a la página de la ATT el 22 de Octubre de 2012 se dio posteriormente a que la autoridad dirigida por el ingeniero CliffordParavicini informó que ejecutaría una campaña para poner fin al comercio y uso ilegal de las antenas satelitales, para plagiar el servicio de televisión por cable, como ocurre en muchos puntos de las principales ciudades del país (Anexo 8), ésta es la imagen de la página ATT el día del ataque:




En fecha 6 de Mayo del presente año nuevamente la página de la ATT fue atacada o pretendió ser atacada por ciberdlincuentes -llamados así por el director de la ATT-.Algunos medios se refieren a que la página contenía durante una hora y media daños a la imagen institucional de la ATT como entidad pública, desmereciendo y emitiendo criterios falsos sobre las tareas regulatorias y fiscalizadoras que se van realizando cotidianamente, acción atribuida a un grupo llamado Mas ancho de banda para Bolivia, quienes fueron acusados por los delitos de "instigación pública a delinquir, resistencia a la autoridad, impedir o estorbar el ejercicio de funciones, daño calificado y acceso indebido y no autorizado a soporte informático causando perjuicios al titular de la información". Las autoridades presumen que el ataque cibernético fue gestado por personas inescrupulosas o presuntos usuarios de Internet con el pretexto de una queja contra el operador TELECEL-TIGO, que en días anteriores retiró del mercado su paquete de internet de 300MB por 3 Bs. denominado "servicio para siempre". (Anexo 9).

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

Adentrándonos a uno de los incidentes específicos, nos referiremos a la publicación de las claves de correo electrónico de ministros, con la siguiente afirmación sobre lo que la Ley de Telecomunicaciones refiere acerca del tema: "A los efectos de esta Ley el correo electrónico personal se equipara a la correspondencia postal, estando dentro del alcance de la inviolabilidad establecida en la Constitución Política del Estado. La protección del correo electrónico personal abarca su creación, transmisión, recepción y almacenamiento"[83]. Lo que pretendo dar a conocer con respecto a este Articulo, es que el contenido de un correo electrónico puede ser referente a la vida íntima y privada de las personas, quienes tenemos necesidad de comunicarnos, expresarnos y relacionarnos dentro de nuestro ámbito, ya sea social o laboral, de tal manera que el correo electrónico y su contenido concierne única y exclusivamente a ambas partes, el transmisor y el receptor, no siendo autorizados para su conocimiento el de terceras personas.

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

### 5.1.3. NECESIDAD Y MECANISMOS DE PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL EN REGISTROS PUBLICOS

Existe una imperativa necesidad en crear una ley que se encargue de brindar protección a los datos de carácter personal que se encuentran en internet

[83] Ley General de Telecomunicaciones, tecnologías de Información y Comunicación Art. 89

específicamente en base de datos y archivos desitios web administrativos públicos, que contenga una serie de artículos entendibles, cuyo fin supremo radique en respaldar de una manera minuciosa nuestros datos a momento de que estos sean solicitados para realizar el tratamiento correspondiente, asimismo esta ley permitirá a la ciudadanía recurrir al órgano competente para realizar la respectiva denuncia y seguimiento en el caso que sus datos hayan sido manipulados por medio del uso del internet. Cabe recalcar en este punto que la norma debe ser cambiante o surgir de acuerdo a los fenómenos que se presenten en la sociedad, fenómeno tecnológico trascendente que a la vez de otorgar un sinfín de adelantos para la comodidad y facilidad del ser humano, otorga también modos mediante los cuales ponen en riesgo la privacidad de nuestra información, concerniente solo y exclusivamente a nosotros o a los relacionados en cuanto a tratamientos y procedimientos en los cuales nos vemos inmersos en las actividades llevadas a cabo cotidianamente.

#### 5.1.3.1. MECANISMOS

##### 5.1.3.1.1. AGENCIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y EL REGISTRO GENERAL DE PROTECCIÓN DE DATOS PERSONALES PÚBLICOS

La creación de una Agencia de Protección de Datos de carácter Personal en Internet, dependiente de la Autoridad de Fiscalización y Regulación de Telecomunicaciones y Transportes de Bolivia ATT, vendría a constituirse en un mecanismo indispensable para proteger los datos ingresados para tratamiento en entes públicos.

Para hacer efectiva la ley cabe crear un ente cuya finalidad principal será velar por el cumplimiento de la legislación en materia de protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, oposición, rectificación o cancelación de datos, y más que todo dirigido a su protección. Su objetivo se centrara en garantizar el derecho a la intimidad de los ciudadanos en sus relaciones con la Administración, tutelando los derechos reconocidos en la ley.

Asimismo dentro de la Agencia es necesario crear como un órgano integrado y correlacionado a la Agencia un Registro General de Protección de Datos de Carácter Personal Público, que llevará un detalle de todos aquellos datos concernientes a las

personas a momento de su registro, modificación o eliminación a consecuencia del tratamiento llevado a cabo por el ente público, es decir que este registro general se mantendrá actualizado en cuanto al tratamiento de los datos de carácter personal realizados por los entes públicos, lo que procurara un seguimiento en caso de cualquier tipo de vulneración efectuada.

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

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

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

### 5.1.4. PROPUESTA DE LEY

EXPOSICIÓN DE MOTIVOS

En la actualidad, los datos personales son elementos imprescindibles para llevar acabo cualquier tipo de acto o actividad dentro de nuestra sociedad; con referencia a los actos, éstos podrían ser actos de identificación; como los datos registrados para adquirir cedulas de identidad, licencias, etc.,actos financieros;aquellos datos requeridos por las entidades financieras para créditos u otro tipo de servicios; actos laborales; como aquellos datos registrados de un currículum vitae, entrevistas, o informes de

desempeño; o actos judiciales; que son datos registrados por los ministerios de justicia, fiscalía o juzgados, sobre informes, antecedentes, peritajes de los procesos o casos llevados a su cargo, asimismo dentro de nuestra vida cotidiana requerimos de ciertos servicios como los médicos, para los cuales también se requiere un historial de la salud del paciente, con todos los datos referentes a la intimidad.

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

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

aprovechado por entes públicos quienes para demostrar transparencia y total comunicación sobre su administración con la población, crearon sitios weben base a sus propios sistemas informáticos que se encuentran publicados en Internetdonde publican una serie de eventos, noticias, avances, proyectos, progresos y beneficios para la sociedad. Sin embargo, al encontrarse esta información en Internet, están sujetos a ataques cibernéticos por hackers o piratas informáticos, los cuales se aprovechan de vulnerabilidades que pueda tener el sistema y efectuar ataques a estos sitios; ataques como denegaciones de servicio a los sitios, es decir la no disponibilidad del sistema por un periodo de tiempo, el robo de informaciónconfidencial del sistema, alteraciones indebidas realizadas a los sitios web, etc. Estos ataques informáticos se podrían disminuir, siempre y cuando, cada ente cuente con las medidas de seguridad de información adecuadas.

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

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

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

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

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

Este proyecto vendría a llenar un vacío legal en nuestro ordenamiento jurídico. No se trata de que no exista derecho sobre la materia, el derecho que se aplica hasta ahora, es el constitucional basado en los derechos fundamentales de las personas adquiridos por Convenios y Tratados Internacionales, no especificando que el avance tecnológico pueda afectar a nuestros derechos.

**PROYECTO DE LEY DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SUJETOS A ADMINISTRACIÓN PÚBLICA EN INTERNET**

En conformidad y aplicación del Art. 162, de la Nueva Constitución Política del Estado Plurinacional de Bolivia, en lo referido a la iniciativa legislativa ciudadana,

parágrafo I, inciso 1, me permito elevar a consideración de la Asamblea Legislativa Plurinacional, el presente Proyecto de Ley referido a PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SUJETOS A ADMINISTRACIÓN PÚBLICA EN INTERNET.

**TÍTULO I**

**DISPOSICIONES GENERALES**

**Artículo 1. Objeto**

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

**Artículo 2. Ámbito de aplicación**

1. La presente Ley se aplicaa todo servidor público que tenga en sus registros informáticos cualquier tipo de dato personal susceptible a tratamiento,estos serán protegidos por los cuatro órganos del Estado, en todos sus niveles, ministerios, contralorías, Fuerzas Armadas, Policía Boliviana. Así mismo también quedan obligadaslas entidades que tengan relación con el Estado Plurinacional

Se regirá por la presente Ley todo tratamiento de datos de carácter personal, cuando el tratamiento sea efectuado en territorio boliviano en el marco de las actividades de un establecimiento público, responsable del tratamiento.

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

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley los siguientes tratamientos de datos personales:

a) La base de datos regulada por la legislación de régimen electoral.

b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal sobre la función estadística pública.

c) Los derivados del Registro Civil y del Registro Judicial de Antecedentes Penales o Registro de Antecedentes Policiales de penados y rebeldes.

d) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

**Artículo 3. Definiciones**

A los efectos de la presente Ley Orgánica se entenderá por

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

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

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

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

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

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

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

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

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

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

profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo.

**Artículo 4. Calidad de los datos**

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

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

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

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

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

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

**Artículo 5. Datos especialmente protegidos**

1. De acuerdo con lo establecido en el parágrafo 2, 3, 5 y 6 del artículo 21 de la Constitución, así como con el art. 25 parágrafos I y II, los datos protegidos serán aquellos que tengan que ver con la privacidad, intimidad, honra, honor, propia imagen y dignidad de las personas, al igual que la libertad de pensamiento religión y culto expresados de manera pública y privada,siendo inviolables la correspondencia electrónica o papeles privados contenidos en soporteinformático.

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

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

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

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

5. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal de los apartados 2 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

**Artículo 6. Datos relativos a la salud**

Las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal

relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos.

**Artículo 7. Seguridad de los datos**

1. Toda Institución Pública, deberá contar con un mínimo de seguridad, aplicado en todo sistema del cual dependan los registros de datos e información ingresada para su respectivo tratamiento.

2. El responsable de la base de datos o archivos, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

3. No se registrarán datos de carácter personal en base de datos que no reúnan las condiciones mínimas de seguridad con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

**Artículo 8. Deber de secreto**

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

**Artículo 9. Comunicación de datos**

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

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

**TÍTULO II**

**DERECHOS DE LAS PERSONAS**

**Artículo 10. Impugnación de valoraciones**

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base

únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

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

**Artículo 11. Derecho de acceso**

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

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

**Artículo 12. Derecho de rectificación y cancelación**

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

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

**Artículo 13. Tutela de los derechos**

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

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

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

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

**Artículo 14. Derecho a indemnización**

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

**TÍTULO III**

**ARCHIVOS Y BASE DE DATOS DE TITULARIDAD PÚBLICA**

**Artículo 15. Creación, modificación o supresión**

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

2. Las disposiciones de creación o de modificación de base de datos deberán indicar:

a) La finalidad de la creación de la base de datos o archivos y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica de la base de datos y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Los órganos de las Administraciones responsables de la base de datos o archivos.

f) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

g) Las medidas de seguridad con indicación del nivel alto exigible.

**Artículo 16. Comunicación de datos entre Administraciones Públicas**

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

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

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

**TÍTULO IV**

**AGENCIA DE PROTECCIÓN DE DATOS**

**Artículo 18. Naturaleza y régimen jurídico**

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

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

3. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

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

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

**Artículo 19. El Director**

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

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

**Artículo 20. Funciones**

1. Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

c) Dictar, en su caso y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.

d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.

e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.

f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los archivos y base de datos, cuando no se ajuste a sus disposiciones.

g) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.

h) Recabar de los responsables de la base de datos cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

i) Redactar una memoria anual y remitirla al Ministerio de Justicia.

j) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

2. Las resoluciones de la Agencia de Protección de Datos se harán públicas, una vez hayan sido notificadas a los interesados. La publicación se realizará preferentemente a través de medios informáticos o telemáticos.

Reglamentariamente podrán establecerse los términos en que se lleve a cabo la publicidad de las citadas resoluciones.

**Artículo 21. El Registro General de Protección de Datos**

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

2. Serán objeto de inscripción en el Registro General de Protección de Datos

a) Las Bases de datos de que sean titulares las Administraciones Públicas.

b) Los datos relativos a la base de datos que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de la base de datos de titularidad pública, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

4. Todo registro realizado, será referencia de cualquier modificación, alteración, eliminación, etc. que se haga de cualquier dato personal, suponiendo que esté ha sido vulnerada, lo que establecerá la originalidad y/o fidelidad de dicho dato en las listas de registro.

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

**TÍTULO V**

**INFRACCIONES Y SANCIONES**

**Artículo 22. Responsables**

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

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

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

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

2. Son infracciones leves:

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

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

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

3. Son infracciones graves:

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

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

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

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

4. Son infracciones muy graves:

a) Mantener la base de datos o archivos, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad, estableciendo directrices o guías de implementación de seguridad.

b) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros base de datos que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo. La recogida de datos en forma engañosa y fraudulenta.

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

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

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos ha dicho tratamiento,

con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

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

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

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

**Artículo 24. Infracciones**

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

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

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

**Artículo 25. Prescripción**

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

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

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

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

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

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

**Artículo 26. Procedimiento sancionador**

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

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

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

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de base de datos o archivos de datos de carácter personal, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales base y archivos a los solo efectos de restaurar los derechos de las personas afectadas. Esto contemplara la imposibilidad de incurrir en corrupción, para lo que se apoyara en la lista de origen existente en la Agencia de Protección de Datos Personales, Registro General de Protección de Datos.

DISPOSICIONES ADICIONALES

Primera. Archivos y Base de Datos preexistentes

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

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

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

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

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

## CONCLUSIONES

Como conclusión pensamos que es importante resaltar la preocupación que se tiene por la regulación de este tema en nuestro país, obteniendo una rápida respuesta a la vulneración de nuestros datos personales a través de sitios web de los administradores estatales.

Sin duda alguna, la avasalladora era de la informática deja en su camino vacíos jurídicos ante su crecimiento cotidiano, de tal manera que al exigir una adecuación de los nuevos fenómenos de la vida social a nuestra legislación, no solo exigimos la protección de nuestros derechos fundamentales, sino que generamos la posibilidad de que nuestro país se ponga a nivel con el crecimiento tecnológico, para que de esta manera nuestra legislación sea cada vez más socializada, vale decir que la ley deberá

ir de la mano con los eventos cotidianos de la sociedad que genera reacciones de inconveniencia social.

Del estudio realizado se ha evidenciado que en Bolivia la publicación de información mediante sitios o portales web permite el acceso a sistemas de información internos con relación a la administración pública. Procedimientos llevados a cabo por individuos especialistas con el fin de perjudicar a los titulares de los datos personales, haciéndolos públicos demostrando de esta manera la vulnerabilidad de los mencionados sitios.

Se entiende la importancia de la difusión de información por internet y su gran aceptación, pero tal publicación que tiene base en la creación de sistemas informáticos internos, debe encontrarse obligatoriamente protegida, permitiendo de esta manera una garantía para los titulares de los datos personales que en aquellos sistemas internos pudieran haber sido registrados. Vale decir, que por más que sea información mínima la que se publique en determinado sitio web, debe ser realizado con las más altas normas de protección y seguridad de información, permitiendo de esta manera proteger en sí, el sistema mismo que utiliza determinado ente, órgano o administrador público.

Es importante reglamentar las leyes en materia de protección de datos en internet, para lo cual sería conveniente, que el órgano encargado de la supervisión y control de la ley realice una versiona comentada o que sea más entendible para los ciudadanos, ya que es un tema complejo, sobre todo los términos que se manejan.

## RECOMENDACIONES

El impacto que ha tenido el uso de internet y con ello la difusión de información, hace indispensable el adecuado reconocimiento legal de una protección detallada y a fondo de nuestros datos personales utilizados o registrados en sistemas informáticos de los órganos, entes o administraciones públicas.

Sin embargo, en la realidad muchas veces esta regulación no será suficiente, ya que las personas que van a aplicar la ley necesariamente deben conocer los límites y capacidades de las tecnologías de la informática, para lograr una adecuada valorización de un registro electrónico de datos personales.

Asimismo, debería hacerse una concientización de la importancia del uso de los medios electrónicos en las autoridades, por lo que sería necesario que existiera una capacitación sobre aspectos relativos a las tecnologías de información, tomando en cuenta el registro de datos personales en sistemas informáticos, unificando las normativas con relación a su debida protección.

Los Bancos Financieros, son un ejemplo a seguir en cuanto a seguridad de información, ya que ellos manejan una serie de datos de carácter personal a momento de realizar cualquier servicio, evidentemente, deben conservar el secreto bancario, pero no es más recurrir a una capacitación con actualizaciones informáticas en bancos, para la creación de sistemas de información seguros e impenetrables en el marco Publico.

Así mismo, el proyecto de ley propuesto, podría ser aplicable al ámbito privado también, ayudando de esta manera a empresas privadas con grandes cantidades de información secreta, para que las mismas puedan regirse y a su vez amparase en la mencionada ley.

# BIBLIOGRAFIA


1. ARCE JOFRÉ, JOSÉ ALFREDO

Informática y Derecho, La Paz Bolivia, año 2003.

2. CABANELLAS, GUILLERMO

Diccionario Enciclopédico de Derecho Usual, año 1989.

3. CORRIPIO GIL DELGADO, MARIA DE LOS REYES.

Regulación Jurídica de Tratamientos de Datos Personales realizados por el Sector Privado en Internet.

Agencia de Protección de Datos, Madrid – España, año 2000.

4. CORRIPIO GIL DELGADO, MARIA DE LOS REYES.

El Tratamiento de los Datos de carácter Personal y la protección de la Intimidad en el sector de las Telecomunicaciones

Agencia de Protección de Datos, Madrid – España, año 2001.

5. DAVARA RODRIGUEZ, MIGUEL ANGEL

La Transposición de la Directiva sobre la Privacidad y las comunicaciones Electrónicas.

Año 2004.

6. DERMIZAQUI PEREDO, PABLO.

Constitución, Democracia y Deberes del Hombre

La Paz – Bolivia, año1997.

7. ENCICLOPEDIA JURÍDICA OMEBA.

Editorial Driskill, Buenos Aires Argentina año 1986.

8. OQUENDO LOPEZ, HECTOR ALVARO.

Compilaciones de Derecho Notarial para Bolivia

Editorial Jurídica Cadena, año 2008, 478 págs.

9. ORDOÑEZ OPORTO. LUIS

Historia de la Archivistica Boliviana, año 2006.

10. OSORIO MANUEL

Diccionario de Ciencias Juridicas, Politicas y Sociales

Buenos Aires Argentina, año 2002.

11. PELOSI, CARLOS.

El Documento Notarial

Editorial Astrea, Buenos Aires Argentinas, año 1987, 349 págs.

12. ROMERO, RAUL.

Derechos Reales

Editorial Los Amigos del Libro La Paz – Bolivia, año 1991, 311 págs.

13. RAMOS MAMANI, JUAN.

Derecho Constitucional

Editorial Academia Boliviana de Estudios Constitucionales, La Paz Bolivia, año 2006, 272 págs.

14. RAMOS MAMANI, JUAN

Habeas Data

La Paz – Bolivia, año 2006, 272 págs.

15. RAMOS MAMANI, JUAN

Recursos Constitucionales, Amparo Constitucional, y Habeas Data

La Paz – Bolivia, año 2006.

16. RAMOS MAMANI, JUAN.

Constitución Política del Estado y Derechos Humanos

La Paz Bolivia, Año 2002, 383 págs.

17. SOTO GAMA, DANIEL

Principios Generales del Derecho de la Información

Instituto de Transparencia y Acceso a la información Pública del Estado, México, año 2010.

18. VICEPRESIDENCIA DEL ESTADO PLURINACIONAL

Nueva Constitución Política del Estado Conceptos elementales para su desarrollo Normativo

La Paz – Bolivia, año 2010. 214 págs.

19. VICEPRESIDENCIA DEL ESTADO PLURINACIONAL

Miradas Nuevo Texto Constitucional

La Paz – Bolivia, año 2010. 735 págs.

20. es.wikipedia.org/wiki/Información_clasificada
21. es.wikipedia.org/wiki/Defacement
22. es.wikipedia.org/wiki/Hacker
23. http://www.colegiodenotariosdelapaz.org/index.php?option=com_content&view=article&id=78&Itemid=60
24. http://www.justicia.gob.bo/index.php/noticias/notas-de-prensa/994-ayllon-asegura-que-nueva-ley-del-notariado-permitira-descongestionar-el-sistema-judicial
25. http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm
26. http://www.derechoinformatico.uchile.cl/index.php/RCHDI/article/viewArticle/10661/11413
27. http://www.hoytecnologia.com/noticias/Gobierno-aleman-endurecera-leyes/73950
28. http://temariotic.wikidot.com/breve-historia-de-la-proteccion-de-datos-personales
29. http://es.wikipedia.org/wiki/Error_de_software
30. http://www.redipd.org/la_red. php
31. http://www.emba.com.bo/index.php?option=com_content&view=article&id=119%3Aaccion-de-proteccion-de-privacidad-en-el-nuevo-ordenamiento-constitucional&Itemid=114&lang=es
32. http: www. Alfarediorg. Vista/ data/ revista/ asp.
33. http://es.wikipedia.org/wiki/Spam
34. http: www. Electronet.com/cuarto congr/info
35. http:www.electroinfo.com/datos.asp.
36. http://www.monografias.com/trabajos93/historia-y-evolucion-dispositivos-almacenamiento/historia-y-evolucion-dispositivos-almacenamiento.shtml#ixzz2cNNjGx2V
37. http://censoarchivos.mcu.es/CensoGuia/archivodetail.htm?id=52276

38. http://www.noticiasnet.mx/portal/oaxaca/150167-acceso-informacion-proteccion-datos-personales
39. http://www.caletao.com.ar/pol/temrel/13/dni.htm
40. http://www.monografias.com/trabajos93/historia-y-evolucion-dispositivos-almacenamiento/historia-y-evolucion-dispositivos-almacenamiento.shtml
41. http://www.monografias.com/trabajos93/historia-y-evolucion-dispositivos-almacenamiento/historia-y-evolucion-dispositivos-almacenamiento.shtml#ixzz2cNNjGx2V
42. http:/si.ua.es/es/documentos/documentacion/.../teoria-de-bases-de-datos.pdf
43. http://www.archivonorma.com/old/index.php?secc_id=10&flag=5&tips_id=270
44. http://www.uabcs.mx/transparencia/index.php/acceso-a-la-informacion
45. http://www.slideshare.net/favi_hola/indizacion-y-operaciones
46. www.cuidatusdatos.com/infodatospersonales.html
47. http://prezi.com/4hprytwyfkgi/dactiloscopia/
48. http://tecnoboard.bligoo.com.ve/western-digital-ya-adapata-sus-discos-duros-a-windows-8
49. http://informaticajuridicametadocumen.weebly.com/seguridad-informatizada.html
50. http://www.misrespuestas.com/que-es-un-archivo.html
51. www.segip.gob.bo/
52. www.iidh.ed.cr/comunidades/redelectoral/.../registro%20civil.htm
53. www.icesi.edu.co/blogs_estudiantes/efrablog/2009/08/
54. www.softwarelibre.org.bo/wiki/lib/exe/fetch.php?media=habeas_data
55. www.informaticaJuridica.com/.../La_vision_constitucional_del_habeas_data.asp
56. www.datospersonales.gub.uy