

RETOS REGULATORIOS DE LA PROTECCIÓN DE DATOS EN COLOMBIA

YENNY AMPARO PEÑA REYES

DIRECTORA

Abog. Doris Patricia Reinales Mendoza MBA.

UNIVERSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA DE TELECOMUNICACIONES

MAESTRIA EN TELECOMUNICACIONES Y REGULACION TIC

BOGOTÁ, 2018

DEDICATORIA

Mi familia siempre mi motivo y mi fortaleza para nunca desfallecer en mis sueños y metas. A esos dos ángeles que desde el cielo me guían mi hermano y mi padre que hace poco se fue de nuestro lado, a esa mujer maravillosa que siempre tiene palabras de aliento, mi mamá, a mis hermanas y a un ser maravilloso que Dios puso en mi camino que con su terquedad y para cumplir nuestros sueños tomados de la mano lo hemos logrado Luis Fernando Porras Rozo.

AGRADECIMIENTOS

UNIVERSIDAD SANTO TOMÁS,

Claustro de enseñanza, conocimiento, superación.

PROFESORES,

Continuamente serán fuente de experiencia, paciencia, conocimiento, apoyo, esfuerzo para darnos a conocer siempre cosas nuevas y cumplir esa meta plateada. Pero en especial al Ingeniero **Julio Ernesto Suarez Páez** y a la Doctora **Doris Patricia Reinales Mendoza** que con su dedicación, constancia hizo posible que se llevara a cabo esta investigación.

COMPAÑEROS DE UNIVERSIDAD,

A los 11 fantásticos que pasamos de ser compañeros a ser amigos, por el apoyo brindado, las experiencias vividas, el conocimiento compartido y por conquista de este nuevo sueño.

ADVERTENCIA

La Universidad Santo Tomás no se hace responsable de las opiniones y conceptos expresados por el autor del trabajo de grado, solo velará por qué no se publique nada contrario al dogma ni a la moral católica y porque el trabajo no tenga ataques personales y únicamente se vea el anhelo de buscar la verdad científica.

Capítulo III – Art. 46 del Reglamento de la Universidad Santo Tomás.

TABLA CONTENIDO

ACRÓNIMOS	6
RESUMEN	8
INTRODUCCIÓN.....	12
1 MARCO GENERAL DEL PROYECTO	15
1.1 FORMULACIÓN DEL PROBLEMA.....	15
1.2 JUSTIFICACIÓN	17
1.3 OBJETIVOS	20
1.3.1. General	20
1.3.2. Específicos	20
1.4 ALCANCE	21
1.5 METODOLOGIA.....	21
2 MARCO CONCEPTUAL.....	24
2.1 Definición de Dato	24
2.2 Concepto de Dato Personal.....	25
2.3 Definición Protección de Datos Personales	28
2.4 Clasificación de Los Datos Personales.....	29
2.5 TIPOS DE DATOS QUE HAY.....	31
2.6 Dato Público	31
2.7 Dato Semiprivado	32
2.8 Dato Privado.....	33
2.9 Dato Sensible	33
2.10 Cómo se recolectan Los Datos Personales	37
2.11 Delegatura De La Protección De Datos de la Superintendencia de Industria y Comercio	38

3	ANÁLISIS DE LA REGULACIÓN COLOMBIANA	39
3.1	ANTECEDENTES DE LA REGULACIÓN COLOMBIANA.....	40
3.1.1	Exposición de motivos	42
3.2	LEY 527 DE 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales".....	43
3.3	LEY 1266 DE 2008 "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones" [42]	45
3.4	LEY 1273 DE 2009 "Por medio de la cual se modifica el código Penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"	46
3.5	LEY 1581 DE 2012 "Por la cual se dictan disposiciones generales para la protección de Datos personales".....	47
3.5.1	Análisis de la Ley 1581 de 2012	47
4.	IDENTIFICACIÓN DE PAÍSES QUE CUENTAN CON NORMATIVIDAD SOBRE PROTECCIÓN DE DATOS PERSONALES	54
4.1	España: LEY Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal.	54
4.1.2.	Obligaciones Legales Básicas de La Normatividad	55
4.2	Definiciones Según La Normatividad Española	57
4.3	Chile - Ley N° 19.628 "Sobre protección de la vida privada y Protección de Datos de Carácter Personal" [48].....	61
4.4	Definición de Categoría de Datos Según la Normatividad Chilena.....	64
5.	ESTUDIO DE DERECHO COMPARADO	67
5.1.	Estudio Comparado Ley Orgánica 15/1999 - Ley Estatutaria 1581 De 2012	95

6. RETOS REGULATORIOS.....	105
CONCLUSIONES.....	112
ANEXO A.	115
LISTA DE GRAFICAS.....	125
LISTA DE TABLAS.....	126

ACRÓNIMOS

AEPD: Agencia Española Protección De Datos (País España)

DNI: Documento Nacional de Identidad

EDI: (Electronic data Interchange o EDI). Traducido significa: Intercambio electrónico de informaciones

FMI :Fondo Monetario Internacional

LGT: Ley General Tributaria

LOPD: Ley Orgánica de Protección de Datos de Carácter Personal

LSSI-CE: Ley de Servicios de la Sociedad de la Información y Comercio Electrónico

OCDE: Organización para la Cooperación y el Desarrollo Económicos

OMC: (World Trade Organization). Traducido significa: Organización Mundial del Comercio

ONU:Organización de las Naciones Unidas

RDLOPD: Real Decreto - la Ley Orgánica de protección de datos de carácter personal. (País España)

RFC: (Site Security Handbook). Traducido significa: Manual de Seguridad del Sitio

SERNAC: Servicio Nacional del Consumidor. (País chile)

TIC: Tecnologías de la Información y Comunicación

RESUMEN

“El derecho a la intimidad es clasificado como fundamental” [1], lo cual se relaciona con el derecho a la protección de datos personales, lo que lleva a ejercer un derecho sobre la información personal que se haya recolectado. Es así como se expide en Colombia la Ley 1581 de 2012 “por la cual se dictan disposiciones generales para la Protección de Datos de carácter personal con la cual se puede obtener control, garantía, integridad y confidencialidad para las personas.

El presente trabajo de grado, se ha desarrollado en cinco capítulos, donde se analizarán los aspectos más importantes de la protección de datos a nivel nacional e internacional.

En el primer capítulo se estudian los conceptos más relevantes definidos por la Ley Colombiana y que servirán al lector para contextualizarse en el desarrollo de la investigación.

En el segundo capítulo se realiza un análisis de la normatividad Colombiana en relación a la Protección de Datos personales y financieros como lo define la Ley 1266 de 2008 “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”

En el tercer capítulo se realiza un estudio bibliográfico de los países que se tomarán como referencia para analizar los aspectos principales de la normatividad sobre protección de datos personales en países como España y Chile.

En el cuarto capítulo se realiza un estudio de derecho comparado entre la regulación de Colombia, España y Chile, en este último capítulo se identifican los

retos regulatorios para el ordenamiento jurídico Colombiano y sugerir una mejora en los vacíos regulatorios encontrados para que Colombia sea un país que tenga el nivel adecuado en protección de datos personales.

Se realiza una infografía como aporte adicional a esta investigación en la cual se resaltan aspectos relevantes de la normatividad que las personas deberían conocer tales como a qué se le llaman datos personales, clasificación de los datos, actores en el tratamiento de los datos personales, derechos de los titulares y algunas recomendaciones para proteger los datos.

Palabras clave: Dato personal, seguridad de la información, normatividad, regulación, encargados de la información, titular de la información.

ABSTRACT

"The right to privacy is classified as fundamental" [1], which is related to the right to protection of personal data, which leads to exercising a right over personal information that has been collected. This is how Law 1581 of 2012 is issued in Colombia "by which general provisions are issued for the Protection of Personal Data with which you can obtain control, guarantee, integrity and confidentiality for people.

The present work of degree, is constituted by five chapters.

In the first chapter, the most relevant concepts defined by the Colombian Law are studied and will serve the reader to contextualize in the development of the research.

In the second chapter an analysis of the Colombian regulations is carried out in relation to the Protection of personal and financial data as defined by Law 1266 of 2008 "Whereby the general provisions of habeas data are dictated and the handling of information is regulated contained in personal databases, especially financial, credit, commercial, service and from third countries and other provisions are dictated "

In the third chapter a bibliographic study of the countries that will be taken as a reference is made to analyze the main aspects of the regulations on personal data protection in countries such as Spain and Chile.

In the fourth chapter a comparative law study is carried out between the regulations of Colombia, Spain and Chile, in this last chapter they identify the regulatory challenges for the Colombian legal system and suggest an improvement

in the regulatory gaps found for Colombia to be a country that has the appropriate level in protection of personal data.

An infographic is made as an additional contribution to this research which highlights relevant aspects of the regulations that people should know such as what is called personal data, classification of data, actors in the processing of personal data, rights of the headlines and some recommendations to protect the data.

Keywords: Personal data, information security, regulations, regulation, information managers, information holder.

INTRODUCCIÓN

En el desarrollo de las tecnologías de la información, el manejo de los datos personales toma gran importancia toda vez que la misma información adquiere un especial poder ante los entes públicos y privados; razón por la cual hace que se convierta en un tema de preocupación para las autoridades nacionales e internacionales adecuando las disposiciones legales que actualmente tienen para la Protección de Datos Personales ya que el manejo indebido de la información conlleva al quebrantamiento de los derechos fundamentales, tales como el derecho a la privacidad, a la intimidad y dignidad humana entre los muchos derechos que tiene cada persona.

Es así que las autoridades han creado entes que se encarguen del cumplimiento y velar por la Protección de los Datos Personales. En el caso de Colombia mediante la Ley Estatutaria 1581 de 2012, se designa a la Superintendencia de Industria y Comercio en adelante (SIC), como el organismo encargado de velar por el cumplimiento de la normatividad de la Protección de Datos Personales.

Desde la perspectiva jurídica, la protección de datos personales en Colombia ha tenido un tratamiento diferencial en dos aspectos: el primer aspecto relacionado con la Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la Protección de Datos Personales”, el segundo aspecto tiene que ver con la protección de los datos financieros, Ley 1266 de 2008, “por el cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en la base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”,

La Constitución Política de Colombia con los artículos 15, 20 y 74 garantiza un derecho fundamental; los anteriores derechos se encuentran reglamentados como: la Ley 1712 de 2014 “Por medio de la cual se decreta la ley de Transparencia y de derecho de acceso a la información Pública Nacional y se dictan otras disposiciones”.

La Unión Europea en su articulado de mejores prácticas internacionales en materia de Protección de Datos Personales contemplado en el convenio 108 de 1981 del Consejo de Europa y la Directiva Europea 95/46 de 1995, consideran que los principios mínimos en Protección de Datos que deben tener los países para ser considerados como garantes de la transferencia internacional de datos son: limitación de la finalidad, calidad de datos y proporcionalidad, transferencia, seguridad, acceso, restricción y oposición.

Este proyecto incorpora en su articulado las mejores prácticas internacionales en materia de Protección de Datos contempladas en el Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009, con el objetivo de lograr con esta ley la acreditación de Colombia por parte de la Unión Europea como un país seguro en protección de datos y así poder acceder al mercado europeo sin restricciones atrayendo inversión extranjera y generando nuevos empleos.

En el presente trabajo se pretende abordar la investigación basada en el manejo normativo de Protección de Datos Personales con el fin de establecer cuáles son los retos regulatorios que tiene Colombia para garantizar una efectiva protección de los datos personales.

Dentro de la investigación se realizará un estudio de derecho comparado, donde se analizará la normatividad en Protección de Datos Personales, que desde hace aproximadamente diecisiete años han desarrollado países como España y Chile,

ya que han sido países pioneros en la aplicación de la ley y de las recomendaciones que realiza la Unión Europea. De este estudio se espera determinar las fortalezas y debilidades de la normatividad sobre Protección de Datos Personales en Colombia

El estudio realizado de la normatividad Colombiana podrá identificar si existen vacíos regulatorios, que aspectos de la regulación actual es necesario modificar o actualizar y así realizar recomendaciones que podrán ser aplicables a la normatividad vigente.

1 MARCO GENERAL DEL PROYECTO

1.1 FORMULACIÓN DEL PROBLEMA

La Protección de Datos Personales es un derecho que; empezó a reconocerse de manera autónoma en Europa, y empieza a introducirse en América Latina a través del habeas data en los años 90. Hacia el año 2012, en Colombia se expide la Ley 1581 del mismo año, sin embargo la normatividad sobre dicha materia ha evolucionado significativamente traduciéndose en la aprobación de la ley de carácter general y con sus respectivos entes de control.

Así mismo la Unión Europea en sus mejores prácticas para la Protección de Datos Personales considera algunos principios mínimos como la limitación de la finalidad, calidad de datos, proporcionalidad, transferencia, seguridad, acceso, restricción y oposición, para que un país sea considerado con el nivel adecuado para la transferencia de Datos Personales a nivel Internacional.

Los datos son un insumo fundamental en el uso de las tecnologías y dentro de la sociedad de la información, lo que implica que la normatividad de la Protección de Datos Personales, su manejo y transferencia de dichos datos con terceros países, brinden las garantías necesarias a los usuarios.

Con base a lo anterior, surge la necesidad de realizar un estudio de la normatividad Colombiana y realizar un estudio comparado con la normatividad y las directrices que plantea la unión europea, con el fin de identificar los posibles retos regulatorios de la protección de datos personales y la transferencia de los mismos, en Colombia.

Con este trabajo de investigación se busca identificar los aspectos de la Protección de datos que requieren de una protección legal y dejar sentadas las

bases para quienes se interesen por la regulación, y puedan profundizar sobre la necesidad de modificar la normatividad vigente o expedir una nueva.

Pregunta de la Investigación

¿La normatividad vigente en Colombia garantiza a los usuarios el adecuado uso y Protección de los Datos Personales a nivel internacional?

1.2 JUSTIFICACIÓN

Los datos son un insumo fundamental en la actual sociedad de la información hay quienes afirman que son el nuevo petróleo, por tal motivo día a día se tratan millones de datos personales, es pertinente aclarar que cuando se habla de datos personales, se hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, datos como el nombre, apellidos, fecha de nacimiento, correo electrónico, número de teléfono, características físicas, origen racial, vida sexual, convicciones políticas y religiosas entre otros, los cuales se constituyen en información que permite identificar a una persona de manera directa o indirecta. Los datos pueden ser recolectados de diversas formas, bien sea por entes públicos, privados que los utilizaran para el desarrollo de su actividad.

Lo cual hace que uno de los retos de la sociedad en la actualidad sea la Protección tanto técnica como jurídicamente de datos personales debido al incremento de recolectados, almacenados que sirven de uso para empresas, gobierno, instituciones públicas, privadas lo que con lleva a que se presenten riesgos a la privacidad de las personas, “es por esto que la protección de datos se consideró como un derecho fundamental y se relaciona con la capacidad que tienen los ciudadanos para disponer y decidir sobre el procedimiento y normas adecuadas para evitar que se vulnere la información que se refiera a él.” [2]

Otro elemento relevante para la normatividad es, la transferencia de datos personales a nivel internacional debido a las nuevas vías de comunicación del mundo globalizado. La circulación, la recopilación y el tratamiento de los datos se hacen necesarios para las sociedades modernas pero dicha circulación debe realizarse dentro de los límites propios al reconocimiento de un derecho fundamental.

Plantear la protección de Datos Personales que se transfieren a terceros países es viable, pero no a través de normas nacionales. Se puede plantear a través de la suscripción de acuerdos internacionales, recomendaciones que dicte un organismo internacional al cual estén inscritos varios países. La globalización de la información ha generado la transferencia de datos personales a terceros países, lo cual representa otro riesgo para los titulares de los datos, debido a que en la Ley 1581 de 2012 no se encuentran planteadas reglas para la transferencia internacional de datos, pero se cita en el artículo 5 de la ley 1266 de 2008 en el literal f) se establece *“a otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular”* [3]. Sin embargo, la transferencia queda sujeta a la decisión del encargado de la base de datos lo cual no representa una debida protección ante el usuario.

La protección de datos es un derecho que les permite a las personas realizar un control sobre la información que comparte con otros, como también el derecho sobre la información recolectada para que no sea usada con fines indebidos. Por tal motivo, la protección de datos cada vez es más relevante en la sociedad de la información. El uso de las tecnologías de la información permite realizar esta comunicación de forma masiva e ilimitada.

En algunas ocasiones, la circulación de la información es rigurosamente necesaria para el cumplimiento de finalidades públicas o privadas.

No obstante la circulación de los datos debe respetar los derechos fundamentales de los individuos, conforme con lo estipulado en el artículo 13 de la Ley 1581 de 2012, contenido de sujetos a quienes pueden suministrarse los datos personales.

Es así que en la normatividad vigente para protección de datos personales y la transferencia internacional de los mismos, se encuentra un reto regulatorio debido a que no se brinda la protección adecuada a las personas para realizar este tipo de transferencias de información.

Es así que se propone la revisión de lo que está planteado en la normatividad y realizar el debido cambio logrando que Colombia sea un país garante en la transferencia Internacional de los datos personales.

1.3 OBJETIVOS

1.3.1. General

Identificar los retos regulatorios en la normatividad colombiana con respecto a la protección de datos personales para establecer los vacíos regulatorios mediante un estudio de derecho comparado

1.3.2. Específicos

- Analizar la normatividad colombiana vigente respecto a la protección de datos personales para posteriormente realizar un estudio de derecho comparado que permita identificar los vacíos regulatorios.
- Identificar países que cuenten con regulación de protección de datos personales para realizar el estudio de derecho comparado mediante una revisión bibliográfica.
- Establecer los retos regulatorios de la normatividad Colombiana con respecto a la protección de datos personales basados en el estudio de derecho comparado.
- Realizar una pieza de contenido multimedia que permita socializar la normatividad existente en Protección de Datos personales en Colombia.

1.4 ALCANCE

La importancia que día a día cobra el tratamiento y almacenamiento de la información de los datos concernientes a las personas. Por tal motivo el uso y el control sobre los datos de cada persona cuando se realizan transferencias a terceros países identificando los retos regulatorios en la normatividad Colombiana. La investigación se limitó a identificar que fortalezas y mejoras tiene la regulación de protección de datos emitidos en Colombia y el uso que se realiza a nivel internacional

1.5 METODOLOGIA

La presente investigación se realiza para tener claridad del por qué en los siguientes capítulos se recopilan terminologías que servirá de objeto para el desarrollo de la investigación y para contextualizar al lector, su estudio se convierte en materia prima para el cumplimiento de los objetivos planteados, con el que se llegará a determinar el reto regulatorio en la normatividad vigente.

En este primer capítulo se toma como referente conceptos de la real academia de la lengua, la corte constitucional, la Superintendencia de Industria y Comercio y la Ley 1581 de 2012 de Protección de datos personales.

En el segundo capítulo se realiza un análisis de la normatividad o regulación que se encuentra vigente en Colombia, junto con la exposición de motivos que llevo a que las leyes fueran publicadas y se realice el cumplimiento de las mismas. Para este segundo capítulo se tiene en cuenta las sentencias que llevaron a la aprobación y publicación de las leyes de Protección de Datos personales y financieros como lo dispone en la Ley 1266 de 2008 más conocida como el habeas data (Protección de Datos Financieros).

En el tercer capítulo se identificaron los países de habla Hispana que cuentan con una normatividad en cuanto a Protección de Datos personales por medio de un estudio bibliográfico determinando los países que serán utilizados como referentes para la investigación. Se procede a dar inicio con Perú con la Ley N° 29733 de 2011 “Protección de Datos Personales”, y se determinó que este país que no se tomara para realizar el estudio de derecho comparado debido a que su normatividad se encuentra en proceso de ajustes.

Por su parte se evidencio que Ecuador es un país que aún no cuenta con una ley de protección de dato .En el 2016 presentó ante la Asamblea Nacional de Ecuador el proyecto de Ley Orgánica de la Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales la cual consiste en regular la recaudación de los datos personales que se encuentran en bases de datos públicas y privadas amparando la decisión de las personas sobre los datos su privacidad e intimidad. Al no contar con una normatividad Ecuador es un país que no se tendrá en cuenta para la investigación

Brasil es un país que no cuenta con una normatividad en cuanto a protección de datos este país cuenta con normas específicas que regulan los temas de protección de datos.

Después de realizar este estudio bibliográfico se tomará para la investigación países como España debido a que su normatividad cuenta con una trayectoria aproximada de diecisiete años de estar en vigencia, considerado como un país pionero en Protección de Datos, convirtiéndose en un aspecto de p relevancia para que Colombia lo tome como referente para la creación de la Ley 1581 de 2012, como segundo país se encuentra Chile, país que también cuenta con una amplia trayectoria en su normatividad.

En el cuarto capítulo se profundizará sobre lo anterior, ya que se realizará un análisis de la normatividad expedida en cada uno de los anteriores países el cual permite conocer diferencias y similitudes en los sistemas jurídicos entre países, que para la investigación por la similitud en el sistema legislativo Colombiano se escogieron a los países de España y Chile, el estudio se basa en la normatividad que se tiene para la protección de datos personales. Se realizará el estudio de derecho comparado para evidenciar las similitudes o las diferencias encontradas en dichos países.

En el último capítulo se identifica los retos regulatorios en Colombia, aspectos que se le puede realizar una mejora a la regulación, vacíos regulatorios, recomendaciones para la ley vigente. Esta última fase se realiza por medio de un starfish o también llamada retrospectiva estrella de mar la cual se basa en cinco aspectos que es: Empezar a hacer: Que se debería desarrollar para realizar una mejora teniendo en cuenta el riesgo que de la novedad. Hacer más: Son aquellas que aportan valor para que son la parte positiva del desarrollo que se está realizando. Seguir haciendo: Son las que aportan valor y se deben seguir fortaleciendo como se están realizando, Hacer menos: Son aquellas que no ayudan al objetivo que se tenía planteado lo cual lleva a realizar cambios. Dejar de hacer: Son aquellas que no agregan valor y por lo cual es mejor eliminarlas, adicionalmente se realiza una infografía en la cual se presentan los aspectos más importantes de la ley y recomendaciones.

2 MARCO CONCEPTUAL

Para dar inicio a este capítulo se realizará una breve explicación de diferentes conceptos que se utilizarán de manera reiterada a lo largo del trabajo de investigación, para que sean de fácil comprensión para el lector.

Uno de los conceptos más relevantes, hace referencia al significado de ley, *“la cual es una norma o una regla que nos dice cuál es la forma en la que debe comportarse o actuar la sociedad. La ley indica que es lo permitido y lo que es prohibido realizar en Colombia.”* [4] De esta manera se realiza el preámbulo a los conceptos que se abordarán en la investigación.

2.1 DEFINICIÓN DE DATO

Consultando el origen etimológico de la palabra Dato se puede establecer que proviene del latín “Datum”, cuyo significado es “lo que se da”. En ese orden ideas y para efectos de iniciar el estudio de este concepto se tratará algunos conceptos sobre lo que es un dato: Según el diccionario de la Real Academia de la Lengua las definiciones sobre dato son:

- “m. Información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho. A este problema le faltan datos numéricos.
- m. Documento, testimonio, fundamento.
- m. Inform. Información dispuesta de manera adecuada para su tratamiento por una computadora.”. [5] Otros conceptos al respecto son: “Los datos son la representación simbólica, bien sea mediante números o letras de una recopilación de información la cual puede ser cualitativa o cuantitativa, que facilitan la deducción de una investigación o un hecho.

Los datos indican condiciones o situaciones que por sí solos no aportan ninguna información importante, es en conjunto de la observación y la experiencia que un dato puede tomar cierto valor instruccional. También se dice que los datos son atributos pertenecientes a cualquier ente, pues una utilidad muy significativa de los datos es que se pueden emplear en estudios comparativos.

También se llama datos a aquellos símbolos numéricos obtenidos de algún tipo de estudio para poder realizar cálculos matemáticos que arrojen información sobre un tema en específico, pues abren un gran mundo de posibilidades en el campo de investigaciones científicas, y en cualquier ámbito en general. Por otro lado también se sabe que toda información contenida en la ficha o cédula de identidad de una persona, como el nombre, número de identificación, fecha de nacimiento, estado civil, entre otras, es llamada datos personales.” [6]

2.2 CONCEPTO DE DATO PERSONAL

El dato personal se puede entender como cualquier información referente a personas físicas, que su intimidad está ligada a temas susceptibles como discriminación, su orientación sexual, religiosa, étnica entre otros.

Otras definiciones que establece para dato personal es el que cita la sentencia “C -1011-08” [7] como los datos personales “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal.” [8]

“El dato personal es información sobre las personas, independientemente del medio que se utilice para captarla, almacenarla, manejarla, usarla, registrarla o

comunicarla. Esta señala el marco de acción a partir del cual le corresponde al responsable o encargado adoptar una serie de medidas con miras a garantizar al titular del dato un tratamiento leal y lícito de su información. Desde 1992, la Corte Constitucional ha señalado que el dato personal se caracteriza por:

- Estar referido a aspectos exclusivos y propios de una persona natural
- Permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con mismo y con otros datos
- Su propiedad reside exclusivamente en el titular del mismo, situación que no altera por su obtención por parte de un tercero de manera lícita o ilícita, y
- Su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación” [9]

“El dato personal es la clase de información especial en torno a la cual gira la Ley estatutaria de Protección de Datos Personales, Ley 1581 de 2012. Es definido como cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. La palabra “determinable” es equiparable a la expresión “identificable” a que se refiere el literal a) del artículo 2° de la Directiva 95/46 Unión Europea.” [10]

La Corte Constitucional dejó abiertas las puertas para que eventualmente la ley 1581 de 2012 se aplique al tratamiento de datos de personas jurídicas cuando en una de sus providencias dice: “es legítima la referencia a las personas naturales, lo que no obsta para que, eventualmente, la protección se extienda a las personas jurídicas cuando se afecten los derechos de las personas que la conforman” [11]

De lo anterior se concluye que Dato personal es aquella información que identifica al individuo o que lo puede hacer identificable. Dato personal puede ser: El nombre, DNI (Documento Nacional de Identidad), una fotografía o una grabación de voz, la IP (Internet Protocol), un pin de teléfono, un avatar, la dirección de

email, el Curriculum Vitae (Trayectoria Educativa), la orientación sexual, la condición de consumidor de un producto o de cliente de una empresa, la situación crediticia, un diagnóstico, el historial médico, los hábitos de consumo, la cuenta de banco, la afiliación a un club o red social” [12]

Vale la pena mencionar que la protección de Datos no se refiere solo a datos íntimos, sino a cualquier tipo de dato que identifique o permita la identificación de una persona, está relacionado con las creencias religiosas, la salud, identidad física, económica, cultural, psíquica, social, profesional, títulos académicos, comportamiento sexual, ideas políticas y esté en conocimiento de o tratamiento de terceros.

Es así como algunos documentos internacionales definen el dato personal como se presenta en la tabla 1 a continuación:

DOCUMENTO	DEFINICIÓN DE DATO PERSONAL
“Directrices Organización para la Cooperación y el Desarrollo Económico (OCDE)”	Por "Datos personales" se entenderá toda información correspondiente a una persona identificada o identificable (el sujeto de los datos) (lit. b, núm. 1º) “ [13]
Convenio 108 de 1981	"Datos de carácter personal" Significa cualquier información relativa a una persona física identificada o identificable ("persona concernida") (lit. a), art. 2º)” [14]
Directiva 95 \ 46 \ Unión Europea	"Datos personales": toda información sobre una persona física identificable o identificada (el "interesado"); se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un

	número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológico, psíquica, económica, cultural o social. (lit. a), art 2º)” [15]
Resolución de Madrid de las Autoridades de protección de Datos y privacidad (2009)	[...]Cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados (lit. a) núm. 2º)” [16]
Propuesta de reglamento general de Protección de datos del Parlamento Europeo y del Consejo (2012)	"Datos personales": toda información relativa a un interesado (núm. 2º, art. 4º)” [17]
Directrices Organización para la Cooperación y el Desarrollo Económico (OCDE) de 2013	Se mantiene lo establecido en la versión de 1980” [18]

Tabla 1. Definición De Dato Personal en Documentos Internacionales. Fuente, Angarita Nelson Remolina, Tratamiento de datos personales, (2013) Pág. 135.

Aunque diferentes documentos internacionales se refieran a un concepto de dato personal, todos llegan a un mismo significado global, indicando que es cualquier información de una persona lo cual permita identificarla.

2.3 DEFINICIÓN PROTECCIÓN DE DATOS PERSONALES

El derecho a la protección de datos es la facultad de una persona de controlar y administrar a su voluntad, la información personal que otros tienen de él o de los menores a su cargo. La Ley atribuye a los ciudadanos la titularidad, el control, el

poder de disposición y autodeterminación sobre sus datos personales, supeditando el tratamiento de los mismos al consentimiento e información previa.

La protección de datos, persigue la armonía entre la facultad del ciudadano a disponer de sus datos personales, y el derecho a usar la información que tiene el titular de las bases de datos; asegurando el equilibrio entre uso de datos y garantía de derechos.

2.4 CLASIFICACIÓN DE LOS DATOS PERSONALES

No es igual el tratamiento jurídico de toda la información de una persona. Esto depende de la naturaleza, de los riesgos o perjuicios que pueda ocasionar cada tipo de información, es decir la naturaleza jurídica del dato personal define la forma en que se deban tratar por parte de terceros. La inobservancia de los datos genera diferentes consecuencias de naturaleza civil y penal. Por ejemplo si una entidad bancaria publicados indebidamente los datos de carácter reservados, se incurre en el “delito de divulgación y empleo de documentos reservados, que se encuentran consignado en el artículo 419 en el código penal colombiano”. [19]

Toda clasificación que se desee realizar de datos depende de la sensibilidad de estos. Dicha sensibilidad del dato se define por las características y bajo ciertos parámetros socioculturales, que representara un riesgo para el titular del dato y se materializara en un efecto positivo o negativo. La naturaleza del dato puede convertirse en un factor determinante de los derechos y de la libertad de la persona.

Los protocolos que se deben observar para el tratamiento de determinada información dependerá de la naturaleza del dato, por eso es de gran importancia tener presente la clasificación jurisprudencial o legal de los datos para que a partir de ella el responsable adopte las medidas que debe utilizar para el tratamiento de determinado dato personal.

Dentro de la clasificación de los datos personales pueden tenerse en cuenta los siguientes criterios: grado de confidencialidad de los datos (públicos, privados, sensibles, semiprivados) y el nivel de ocasional de afectación de los datos personales.

En la “sentencia T-261 de 1995” [20] la Corte Constitucional de Colombia se adentró en el estudio de la clasificación del dato personal. Como primera instancia el dato personal es un concepto genérico que hace mención a toda información que concierne a la persona. No todo dato personal es íntimo ni se encuentra en la categoría de privado de la persona. Dentro de la amplia escala de informaciones existen algunos que son públicos y otros íntimos.

“Hay datos personales que específicamente son íntimos y gozan, en consecuencia, de la garantía constitucional en cuanto tocan con un derecho fundamental e inalienable de la persona y su familia, al paso que otros, no obstante ser personales, carecen del calificativo específico de privados, toda vez que no únicamente interesan al individuo y al círculo cerrado de su parentela, sino que, en mayor o menor medida, según la materia de que se trate, tienen importancia para grupos humanos más amplios (colegio, universidad, empresa) e inclusive para la generalidad de los asociados, evento en el cual son públicos, y si ello es así, están cobijados por otro derecho, también de rango constitucional fundamental, como es el derecho a la información.” [21]

Sin embargo en la “sentencia T-729 de 2002” [22] la Corte Constitucional planteó una clasificación de la información con el fin de establecer diferentes niveles de responsabilidad en cuanto a su tratamiento. Para la corte esta clasificación le permite delimitar entre la información que se puede publicar y que no como consecuencia de los derechos a la intimidad y al hábeas data.

2.5 TIPOS DE DATOS QUE HAY

La Corte Constitucional de Colombia clasifica la información en cuatro grandes tipos con el fin de determinar cuáles de estos se pueden publicar en desarrollo del principio de información y cuales no corresponden en protección de intimidad. “Las disposiciones sobre protección de datos, establecen tipologías de datos según el mayor o menor grado de aceptabilidad de la divulgación:

2.6 DATO PÚBLICO

El dato público es aquel que goza de estatus por mandato de la ley o la constitución y por su carácter se puede dar manejo abierto del mismo siempre y cuando se pueda obtener y ofrecer sin restricciones.

Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.

Se define en el “numeral 2° del artículo 3° del Decreto 1377 de 2013” [23] como aquel dato que no sea semiprivado, privado o sensible. Estos datos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas, boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no están sometidas a reserva.

Para la Corte Constitucional de Colombia, el dato público se define “puede solicitarse por cualquier persona de manera directa y sin el deber de satisfacer requisito alguno” [24] Para tratar datos de naturaleza pública, no es necesario contar con la autorización del titular del dato” [25]

Sin embargo aunque los datos de naturaleza pública no requieran siempre de la autorización del titular del dato no simboliza que el tratamiento de este exento de la aplicación de principios de la Ley Estatutaria 1582 de 2012.

Otro aspecto a tener en cuenta es que no debe confundirse la información pública por naturaleza jurídica con aquella que esté a disposición de público o que sea fácilmente accesible, por ejemplo a través de internet. La información no deja de ser privada ni se convierte en pública por el hecho de poder consultarse fácilmente. Como se cita en el artículo 5 del decreto 1377 de 2013, “se estableció que los datos personales que se encuentren en fuentes de acceso público, con independencia del medio por el cual se tenga acceso, entendiéndose por tales aquellos datos o bases que se encuentran a disposición del público, pueden ser tratados por cualquier persona siempre y cuando, por su naturaleza, sean datos públicos.” [26]

2.7 DATO SEMIPRIVADO

El dato semiprivado no fue definido en la Ley Estatutaria 1582 de 2012 ni en el Decreto 1377. Para la recolección, almacenamiento y uso es necesario contar con la autorización del titular. El dato semiprivado es aquel en que para su acceso y conocimiento presenta un grado mínimo de limitación, se deberá tener una orden emitida por una autoridad administrativa para su acceso.

“El dato semiprivado no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios. Este tipo de datos requieren de autorización previa del titular para ser reportados a las bases de datos y circular en términos previstos en la ley 1266 de 2008.” [27]

El acceso a este tipo de datos requiere una limitante ya que solo se podrá obtener y ofrecer por medio de una autoridad administrativa en el cumplimiento de sus funciones o en el marco de los principios de la administración de datos personales.

2.8 DATO PRIVADO

El concepto de dato privado no fue definido en la Ley Estatutaria 1581 de 2012, su concepto fue definido en la ley 1266 de 2008, la cual define que el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información. En este grupo se encuentran por ejemplo los libros de los comerciantes, las historias clínicas, los archivos de las personas acogidas al programa de protección de víctimas en un proceso penal, los datos suministrados por el DANE, en desarrollo de los censos y encuestas, esta información solo podrá ser obtenida por orden de autoridad judicial y el cumplimiento de sus funciones.

2.9 DATO SENSIBLE

Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación. Es así como los datos sensibles fueron definidos en la Ley 1581 de 2012 y en el Decreto 1377 de 2013 como: *“Aquellos que afecten la intimidad del titular o cuyo uso indebido pueda generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos organizaciones sociales, de derechos humanos o que promueva interés de cualquier partido político o que se garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométrico”* [28]

A continuación en la tabla 2, se presentan algunas definiciones dadas por documentos internacionales de dato sensible.

DOCUMENTO	DEFINICIÓN DE DATO SENSIBLE
Convenio 108 de 1991	“No utiliza la expresión de dato sensible pero se refiere a los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o la vida sexual. (artículo 6°)” [29]
Resolución 45/95 de la ONU (1990)	No se refiere explícitamente a los datos sensibles pero menciona la información sobre el origen racial o étnico, color vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación en un sindicato. (núm. 5°, principio de no discriminación)”
Principios de Puerto Seguro, USA (2000)	No los define, pero cuando menciona el principio de opción (choice) da algunos ejemplos como: “datos sobre el estado de salud, el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la afiliación sindical o la vida sexual de la persona”
Directrices de la Red Iberoamericana de Protección de Datos (2007)	No se emplea la expresión dato sensible pero se refiere a los datos que revelen la ideología, afiliación sindical, religión o creencias del afecto y los relacionados con la salud, el origen racial y la vida sexual.(núm. 3.3 y 3.4)
Resolución de Madrid (2009)	Serán considerados sensibles aquellos datos de carácter personal: a. Que afecten a la esfera más íntima del interesado; o b. Cuya utilización indebida pueda: i. Dar origen a una discriminación ilegal o arbitraria, o ii. Conllevar

	un riesgo grave para el interesado. En particular, serán considerados sensibles aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas; así como los datos relativos a la salud o a la sexualidad (núm. 13)
Propuesta de reglamento general de protección de datos del Parlamento Europeo y del Consejo (2012)	No lo define pero en el artículo 9° sobre tratamiento de categorías especiales de datos personales da los siguientes ejemplos de datos sensibles: datos personales que revelen el origen étnico o racial, las opiniones políticas, la religión o las creencias, la afiliación sindical, así como el tratamiento de los datos genéticos o los datos relativos a la salud, la vida sexual, las condenas penales o medidas de seguridad afines (núm. 1°)” [30]

Tabla 2. Definición de dato sensible en diversos documentos internacionales, Fuente, Angarita Nelson Remolina, Tratamiento de datos personales, 2013, Pág. 150 y 151

“Los datos sensibles son una categoría especial de datos personales que requieren una protección exclusiva, por lo cual por regla general su tratamiento está prohibido, salvo las excepciones que se encuentran descritas en el artículo 6° de la ley 2581 de 2012” [31]

Otros conceptos relevantes son los siguientes:

Autorización: Es el aprobación previa, del titular para llevar a cabo el tratamiento de los datos personales.

Base de Datos: Es un conjunto de datos que pertenecen a un mismo contexto que para la investigación serán datos personales objeto de tratamiento.

Encargado del tratamiento: Es una persona natural, jurídica, pública o privada, que sola o con otros realice el tratamiento de los datos personales.

Responsable del tratamiento: Es una persona natural, jurídica, pública o privada, que sola o con otros decida o tome decisiones sobre la base de datos.

Titular: Es la persona natural que sus datos serán objeto de tratamiento.

Tratamiento: Es aquella acción o conjunto de acciones que se realicen sobre los datos tales como el almacenamiento, uso, circulación, recolección o supresión

A Qué Datos Personales no se Aplica La Ley

- ✓ “A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- ✓ Las que tengan por finalidad la seguridad y defensa nacional la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- ✓ Las que tengan como fin y contengan información de inteligencia y contrainteligencia.
- ✓ Las que contengan información periodística y otros contenidos editoriales
- ✓ Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda”.

El dato sensible hace referencia a aquellos datos que por su naturaleza se encuentren relacionados con aspectos muy íntimos de la persona como, su origen racial, étnico, convicciones religiosas, información referente a la vida sexual o cualquier otro dato que por su naturaleza, o contexto pueda generar discriminación o comprometer los derechos y libertades de las personas. Jurisprudencialmente se ha catalogado como información secreta. Lo cual hace que tengan una protección especial y que las personas no se encuentren obligadas a proporcionarlos. Los diferentes documentos hacen referencia en la forma que deben proteger los datos sensibles y hacen referencia a un mismo concepto o definición de dato sensible.

2.10 CÓMO SE RECOLECTAN LOS DATOS PERSONALES

Los datos personales se pueden recolectar de diferentes formas ya sea de manera verbal, por escrito, por internet, por cámaras sin embargo siempre que se recolecte cualquier tipo de dato se debe cumplir con lo que dicta la norma como lo es informar y solicitar el consentimiento. “Los datos personales conforman la información necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios. Así, por ejemplo, cuando hacemos una solicitud de crédito ante una entidad financiera, se requiere diligenciar formularios con nuestra información personal, o cuando realizamos una compra y para realizar la factura de venta solicitan datos como el número de documento de identidad, correo electrónico, dirección y teléfono de contacto, entre otros.” [32]

2.11 DELEGATURA DE LA PROTECCIÓN DE DATOS DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

A finales del año 2011, la Superintendencia de Industria y Comercio fue reestructurada mediante el Decreto 4886 de 2011 (que derogó los Decretos 3523 de 2009 y 1687 de 2010 con excepción de algunas normas). De esta reestructuración vale resaltar la creación de dos nuevas Delegaturas: una para el Control y Verificación de Reglamentos Técnicos y Metrología Legal y otra para la Protección de Datos Personales.

La Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, es la Autoridad de Protección de Datos encargada de vigilar y garantizar que las entidades públicas y privadas, respeten los principios, derechos y garantías en el tratamiento de los datos personales regulados en la Ley 1266 de 2008 y la Ley 1581 de 2012” [33].

3 ANÁLISIS DE LA REGULACIÓN COLOMBIANA

En el presente capítulo se realizará una retrospectiva de las diferentes leyes que existen en Colombia junto con la exposición de motivos lo que lleva a la generación de estas leyes. La protección de datos que para el caso de Colombia ha tenido un tratamiento diferencial, desde la perspectiva jurídica, en dos (2) aspectos: La protección de los datos financieros, Ley 1266 de 2008, *“por el cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en la base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”* [34] y la protección de los datos personales, Ley 1581 de 2012, *“Por la cual se dictan disposiciones generales para la protección de datos personales”*. [35]. Además, otra disposición normatividad que tiene relación con el manejo de información es la ley 1712 de 2014 *“Por medio de la cual se decreta la ley de Transparencia y de derecho de acceso a la información Pública Nacional y se dictan otras disposiciones”*. [36]

El desarrollo de las normas antes citadas, muestra el interés del Estado colombiano por proteger la información y los datos, sin embargo, la implementación de medidas y sistemas que contribuyan a permitir realizar operaciones, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante Tratamiento) por parte de entidades de naturaleza pública y privada lleva a encontrar un vacío regulatorio en cuanto a la transferencia internacional de datos personales. Autores como Nelson Remolina Angarita en su revista Colombiana de Derecho Internacional a lo largo del estudio realizado en diferentes países sobre la Protección de Datos Personales llegan a concluir que *“Colombia al igual que otros países latinoamericanos aún no cuenta con la aprobación de “la Comisión Europea ya que considera no garantiza un nivel adecuado para la protección de datos debido a que no cumple con la regulación jurídica suficiente para la protección de los ciudadanos”*. Este concepto emitido por

el abogado según lo que dice la Unión Europea, no quiere decir que Colombia no sea un país autónomo de emitir sus leyes, [37]

3.1 ANTECEDENTES DE LA REGULACIÓN COLOMBIANA

La información es el activo más importante en el mundo actual, es por ello que el 17 de octubre de 2012 el Congreso de la Republica expidió la Ley Estatutaria 1581 de 2012 mediante la cual se dictan disposiciones generales para la protección de datos personales, en ella se regula el derecho fundamental de hábeas data y se señala la importancia en el tratamiento del mismo tal como lo corrobora la “Sentencia de la Corte Constitucional C – 748 de 2011” [38] donde se estableció el control de constitucionalidad de la Ley en mención.

Esta nueva ley busca que se protejan los datos personales que estén registrados en bases de datos y que se utilicen para realizar operaciones como recolección, almacenamiento, circulación, uso para el tratamiento por parte de entidades de naturaleza pública y privada. Al ser esta una ley estatutaria (Ley de especial jerarquía), tiene como fin proteger los derechos y deberes fundamentales, como también los procedimientos y recursos para su protección. La Jurisprudencia Constitucional presentó desde los inicios el derecho del hábeas data como garante del derecho a la intimidad, es así que desde el hábeas data se hablaba de la protección de datos que hacen parte de la vida privada y familiar, la cual es entendida como el bien individual en la que cada persona puede realizar su proyecto de vida y que ni el Estado ni otros entes particulares pueden inferir.

Actualmente el Hábeas Data se conoce como un derecho autónomo, que a su vez se encuentra con dos características relevantes como la autodeterminación informática y la libertad (incluida la libertad económica). Este derecho que es fundamental y autónomo, necesita para su efectividad y protección mecanismos que lo garanticen, los cuales requieren no solo de los jueces sino de la

institucionalidad administrativa de los entes asignados de control para la vigilancia y control para personas de derecho público como privado, que certifiquen la efectiva protección de los datos y, en razón de su carácter técnico, se encuentren en la capacidad de establecer políticas públicas en la materia, sin intrusiones de carácter político para el acatamiento de estas decisiones.

Dentro de los establecimientos mínimos que se encuentran en el derecho del “hábeas data está consignada que las personas tienen derecho a conocer y tener acceso a la información sobre ellos que se encuentren recogidas en bases de datos, lo que permite tener acceso a las mismas en donde se encuentre esta información; adicionalmente el titular de la información tiene derecho a incluir nuevos datos con el fin que se suministre una imagen completa del titular: otro derecho que tiene es a actualizar la información con el fin de estar al día con estas bases de datos; a su vez tiene derecho a que la información que se encuentre en las bases de datos sea rectificada o corregida, de acuerdo que sea la información real; otro derecho es excluir información de la base de datos, ya sea porque se está realizando el uso indebido de la información que se encuentra en la base de datos o porque el titular así lo requiere, salvo las excepciones que dicte la normatividad.

La ley exige a las entidades públicas y privadas a revisar el uso de los datos personales que se encuentren en sus sistemas de información para así revisar y replantear sus políticas de manejo de información y el fortalecimiento de sus herramientas, como responsable del tratamiento de los datos (sea persona natural o jurídica, pública o privada que por sí misma o por medio de otros decida sobre la base de datos y sobre el tratamiento de los mismos) como también se debe definir los medio para el tratamiento de los datos de los usuarios incluidos quienes sean en medio de recolección y los deberes que corresponden a los principios de la administración de datos y al derecho de la intimidad, hábeas data y dato del titular.

Una vez presentados los antecedentes jurídicos, es fundamental entender que la información en la actualidad se toma como un activo importante y que es utilizado para actividades cotidianas, como se puede evidenciar en el flujo de la información que se ha incrementado en los últimos años, lo que implica que en el mundo globalizado que nos encontramos se deba proteger presurosamente los datos personales.” [39]

3.1.1 Exposición de motivos

La exposición de motivos en todo proyecto de ley puede concebirse desde dos perspectivas: una de forma y otra de fundamentación. Respecto a la primera se puede decir que la exposición de motivos es un elemento requerido de todo proyecto de ley sin el cual no habrá lugar al trámite del mismo según se puede concluir de lo establecido en el artículo 145 de la Ley 9 de 1992 que es el reglamento que rige el órgano legislativo. Establece esta norma: **“ARTICULO 145.** *Orden en la redacción del proyecto. En la presentación de todo proyecto debe incluirse: título, encabezamiento, parte dispositiva y exposición de motivos. Sin este orden el Presidente devolverá el proyecto para su corrección.*”

De esta norma se puede concluir que todo proyecto de ley tiene cuatro requisitos: título, encabezamiento, parte dispositiva y exposición de motivos y la ausencia de cualquiera de ellos dará lugar a la devolución.

Por otra parte, la exposición de motivos corresponde a la justificación del proyecto de ley; y en tal sentido, la importancia de esta parte radica en el hecho que la sustentación incompleta o inadecuada del proyecto podría dar lugar a argumentos para la negación y posterior no aprobación de la ley y por el contrario, un proyecto de ley con una exposición de motivos amplia y bien fundamentada contribuye a la obtención de una respuesta positiva en el proceso de creación de una ley. No son pocos los casos que para cualquier investigador en cualquier tema que haya sido objeto de un proyecto de ley, la exposición de motivos se constituye en una fuente

de información para sustentar argumentativamente el tema que se esté estudiando.

En la investigación se realiza un recorrido por la exposición de motivos para tener una visión más acertada de la forma como los proponentes de estas leyes afrontaron la realización de las mismas, encontrando que parámetros no obedecen al planteamiento de la Ley.

3.2 LEY 527 DE 1999 "POR MEDIO DE LA CUAL SE DEFINE Y REGLAMENTA EL ACCESO Y USO DE LOS MENSAJES DE DATOS, DEL COMERCIO ELECTRÓNICO Y DE LAS FIRMAS DIGITALES"

La ley 527 de 2009 se expidió bajo la necesidad de establecer controles para definir y reglamentar el uso de mensajes electrónicos y firmas digitales en todas las actividades de los sectores privados y públicos, bajo el marco jurídico integral. La ley define que podrá ser aplicada a todo tipo de información en forma de mensajes teniendo en cuenta que se presenta dos excepciones, una de ellas es las obligaciones contraídas por el Estado Colombiano en virtud de convenios o tratados internacionales y la segunda excepción hace referencia a que las advertencias escritas por disposición legal deben ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Es así que la normatividad *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales"* [40] establece la base para la implementación del proceso administrativo electrónico, en razón a que esta contempla los conceptos y principios que desarrollan la seguridad, eficacia y validez de los actos administrativos a través de medios electrónicos.

Es así que las nuevas tecnologías de la información su incorporación en la vida cotidiana de las personas ha motivado a un cambio que muchos han llamado la “sociedad de la información” en la que esta desarrolla un rol importante y estratégico. Toda esta transformación ha trascendido en una serie de aspectos, relacionados con el manejo de la información y que tienen una incidencia jurídica.

Algunos de los aspectos son incremento exponencial de la producción documental, evolución incesante de las tecnologías empleadas para la creación y gestión de estos documentos, con mayor potencia, rapidez y soportes de almacenamiento.

Los nuevos soportes tecnológicos conviven con los documentos en papel, lo cual hace que existan o se presenten casos de duplicidad de soportes por lo cual hace que se enmarque un nuevo derecho en la libertad y confianza que va acorde a un hecho factico imposible de negar como es la interdependencia a través de los avances tecnológicos.

La administración tecnológica es una vía para avanzar hacia el desarrollo del “mejor gobierno” de las administraciones públicas en donde la tecnología es fundamentalmente un medio y no un fin en sí mismo.

El valor de la administración tecnológica no se encuentra en el traslado de servicios, sino que debe responder a la optimización y reorganización de los esquemas del servicio público, de tal manera que permitan una mayor eficiencia y eficacia en las relaciones con los ciudadanos y las empresas.

3.3 LEY 1266 DE 2008 “POR LA CUAL SE DICTAN LAS DISPOSICIONES GENERALES DEL HÁBEAS DATA Y SE REGULA EL MANEJO DE LA INFORMACIÓN CONTENIDA EN BASES DE DATOS PERSONALES, EN ESPECIAL LA FINANCIERA, CREDITICIA, COMERCIAL, DE SERVICIOS Y LA PROVENIENTE DE TERCEROS PAÍSES Y SE DICTAN OTRAS DISPOSICIONES” [41]

La ley 1266 conocida como el habeas data en Colombia se expide con el fin de regular el manejo de información que se encuentra en bases de datos personales en especial información financiera, comercial y crediticia y la que proviene de terceros países a su vez permite a los ciudadanos conocer, actualizar y rectificar la información contenida en dichas bases de datos.

En los artículos 15 y 20 de la Constitución Política se establecen los derechos a la intimidad y la información distinguen el derecho que tienen las personas a conocer, actualizar y rectificar la información que hayan recogido en bancos de datos, en archivos de entidades públicas y privadas. El contenido y el alcance de este derecho ha sido desarrollado por la jurisprudencia de la Corte Constitucional, a partir de análisis de fallos de tutela sobre la administración de datos personales de carácter financiero, almacenados en centrales de información y destinados al cómputo del nivel de riesgo crediticio.

Las herramientas concretas de protección del derecho fundamental contenidas en el proyecto de ley demuestran que la intención del legislador estatutario fue establecer un régimen jurídico de protección de datos personales de naturaleza comercial, financiera, crediticia.

En esta ley se denoto la necesidad de proteger a los usuarios de abusos realizados por parte de las entidades financieras no solo con información crediticia sino también en cuanto a la protección de datos personales ya que era

utilizada con fines indebidos generando traumas a los ciudadanos, lo que llevo a la necesidad de expedir una nueva normatividad que fuese más completa para la protección de datos y no solo financieros.

3.4 LEY 1273 DE 2009 “POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO DENOMINADO “DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS” Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES”

El 05 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273.

La ley impuesta en el 2009 fue el comienzo de la penalización de los delitos informáticos en el país, a su vez se caracteriza y se clasifican los delitos informáticos.

La ley 1273 fue expedida con la finalidad de neutralizar una nueva conducta delictiva que se estaba presentando en Colombia, porque jurídicamente había un vacío normativo de cómo se debía regular esta conducta, es cuando nace la necesidad objetiva de brindar las herramientas necesarias a jueces y fiscales además de establecer una manera más adecuada de tipificación del delito ya que estas conductas tienen incidencia fuera de medios convencionales o conocidos. Además todo esto tiene una relación colectiva porque desde la aparición de la tecnología ha tenido un gran auge en las personas.

Esto condujo a que personas inescrupulosas se aprovecharan de personas inexpertas que utilizan la tecnología, llegando al punto de vulnerar los bienes titulados como consta en la Constitución Política de 1991.

Es así que con la evolución de la tecnología como herramienta para el desarrollo de diferentes ámbitos, también aparecen y van evolucionando las amenazas y los riesgos que ponen en tela de juicio la protección de la intimidad de las personas, sus transacciones y en general la información digital que se manobra a diario, provocando que se presenten problemas que van más allá de la pérdida de un documento o una clave de alguna red social. Colombia no ha sido un país ajeno a que se presenten este tipo de actos, por tal motivo se modifica el código penal y se adiciona en uno de sus títulos la ley estatutaria donde se incluye la penalización económica y de privación para aquellas personas que se valgan de medios informáticos para atentar contra la integridad, disponibilidad y confidencialidad de la información

3.5 LEY 1581 DE 2012 “POR LA CUAL SE DICTAN DISPOSICIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES”

La Ley 1581 reglamenta aspectos relacionados con la autorización del titular de la información para el tratamiento de los datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información.

3.5.1 Análisis de la Ley 1581 de 2012

Esta ley fue promulgada en octubre y busca ampliar y complementar la protección de datos personales en Colombia, no solo para el sector financiero acogiendo los datos de personas que se encuentren registrados en bases de datos que sean susceptibles de tratamiento sin que importe si es de naturaleza pública o privada. Es por esta razón que la ley asigna a la Superintendencia de Industria y Comercio la función de autoridad de la Protección de los Datos.

“La ley 1581 de 2012 de Protección de Datos personales, es una ley que complementa la normatividad vigente que hace referencia a la protección del derecho fundamental a la cual tienen derecho las personas naturales, a autorizar, actualizar y rectificar la información personal que se encuentre recolectada en bases de datos o archivos, junto con los derechos, libertades y garantías constitucionales como se encuentra estipulado en el artículo 15 de la Constitución Política.” [42].

Sin embargo en la normatividad vigente es necesario que se expidan otras disposiciones reglamentarias para la transferencia internacional de datos, debido a que en la presente Ley es uno de los temas que presenta falencias, si bien es cierto que se encuentra estipulado un responsable o encargado no garantiza que los datos que salen de un país y llegan a otro se les brinde la protección adecuada.

Hoy por hoy vemos como aumenta diariamente el porcentaje de personas que tienen acceso a internet en el mundo, es decir una persona ubicada en cualquier lugar del mundo pueda recolectar los datos personales convirtiéndose en una actividad incontrolable.

Finalmente se realiza una explicación de la estructura de la Ley de protección de datos, constituida por IX títulos los cuales se mencionan a continuación,

“TITULO I: Objeto, ámbito de aplicación y definiciones

En este título se definen el objeto de la ley junto con otras temáticas como son la autorización que hace referencia al consentimiento del titular para que se manejen sus datos personales; Bases de datos, que son un conjunto de datos que serán utilizados para algún tratamiento; Dato personal entendido como información que pueda asociarse a una o varias personas; Encargado del tratamiento, es una

persona natural o jurídica que realice algún tratamiento de los datos personales por si misma o en conjunto con otros: Responsable de la información, es una persona natural o jurídica que sola o en conjunto decidan sobre la base de datos y el tratamiento de los datos; Titular, son aquellas personas cuyos datos serán objeto de tratamiento; Tratamiento, es un conjunto de acciones que se realicen sobre los datos personales como la recolección, almacenamiento, uso, circulación o supresión.

TITULO II: Principios rectores

En este título se definen los principios para el tratamiento de los datos personales junto con la interpretación y la aplicación de la ley. Los principios rectores de la protección de datos son: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad

TITULO III: Categorías especiales de datos

En la categoría de datos especiales se encuentra los datos sensibles que hace referencia a aquellas que afecten la intimidad del titular como también sus creencias religiosas, origen racial, orientación política, filosóficas entre otros.

En esta categoría de datos especiales se encuentran los derechos de los niños, niñas y adolescentes en el cual se debe asegurar el respeto de sus derechos y el tratamiento responsable de la información.

TITULO IV: Derechos y condiciones de legalidad para el tratamiento de datos

En este título se define el derecho que tienen los titulares a que los datos personales sean revocados, suprimidos, acceder de manera gratuita en los cuales siempre será necesaria la autorización del titular. Los casos en que tendrá una

excepción serán, cuando se requiera esta información por parte de una entidad pública en ejercicio de sus funciones legales o por orden judicial, las otras excepciones son cuando los datos sean de naturaleza pública, casos de urgencia médica, datos relacionados con el registro civil de las personas. Siempre haciendo la salvedad que se deberá solicitar autorización del titular.

TITULO V: Procedimientos

En este título se define la manera en que los titulares realizaran la consulta, como también se define los reclamos que se tengan en cuanto al tratamiento de los datos y el requisito de procedibilidad lo cual hace referencia a que el titular después de agotar todos los medios podrá dirigirse ante la Superintendencia de Industria y Comercio para realizar el reclamo del tratamiento que ha dado el responsable o encargado de la información.

TITULO VI: Deberes de los responsables del tratamiento y encargados del tratamiento

Los responsables del tratamiento de los datos deberán cumplir con lo estipulado en la normatividad, para garantizarle al titular el derecho que tiene establecido en el Hábeas Data, como a su vez informar sobre el propósito de la recolección de la información, y conservar las condiciones de seguridad para que no se presente pérdida, adulteración, fraudulento, acceso no autorizado.

Otro de los deberes del responsable de la información es garantizar que la información que va a suministrar sea veraz, exacta, completa, actualizada, comprensible y comprobable; se deberá actualizar la información, rectificar, tener un manual interno de políticas y procedimientos que garanticen el cumplimiento de la ley. Deberá permitir el acceso a la información solo a quienes se encuentren autorizados.

TITULO VII: De los mecanismos de vigencia y sanción

Este título se encuentra subdividido en tres capítulos, los cuales son:

Capítulo I De la autoridad de protección de datos

La Superintendencia de Industria y Comercio será el ente encargado de ejercer vigilancia y control para garantizar que el tratamiento de datos personales se respete los principios, derechos, garantías y procedimientos establecidos por la ley. A su vez en las funciones que desempeñara este ente se encuentran, velar por el cumplimiento de la legislación en protección de datos; realizar investigaciones de ser necesarias y ordenar medidas efectivas para el cumplimiento del derecho del hábeas data; solicitar que sean bloqueados los datos del titular siempre y cuando las pruebas realizadas arrojen un riesgo de los derechos fundamentales mientras toman las medidas correspondientes; promover campañas de divulgación para que los ciudadanos conozcan y se capaciten acerca del derecho fundamental a la protección de datos; difundir procedimientos y medidas para los responsables del tratamiento y los encargados como se encuentra en la ley; manifestar las declaraciones sobre la transferencia internacional de datos; Administrar el Registro Nacional Público de Bases de Datos emitiendo las ordenes necesarias para que se cumpla su funcionamiento; proponer mejoras a la normatividad actual conformes a la evolución tecnológica, informática y comunicacional; Solicitar cooperación a la entidades internacionales cuando los derechos de los titulares se vean afectados en la recolección internacional de datos personales.

Capitulo II: Procedimientos y sanciones

La Superintendencia de Industria y Comercio una vez haya identificado los incumplimientos por parte de los encargados y responsables del tratamiento de los

datos impondrá las sanciones adecuadas. Las multas que se impongan varían desde dos mil salarios mínimos mensuales vigentes que serán de carácter personal o institucional; suspensión de las actividades relacionadas con el tratamiento de los datos personales hasta por seis meses; cierre temporal por el incumplimiento de las sanciones impuestas por la Superintendencia de Industria y Comercio; cierre definitivo de la operación del tratamiento de datos sensibles; renuncia por el incumplimiento de lo impuesto por la Superintendencia de Industria y Comercio.

Capítulo III: Del Registro Nacional de Bases de Datos

El Registro nacional de Bases de Datos se definió en el artículo 25 como el directorio público de las bases de datos que se encuentran sujetas a tratamiento que operan en el país. El RNBD (Registro Nacional de Bases de Datos) será administrado por la Superintendencia de Industria y Comercio y también será de consulta libre para los ciudadanos. Las entidades deberán cumplir con lo establecido por la Superintendencia de Industria y Comercio junto con las políticas del tratamiento de la información obligando a los responsables y encargados al cumplimiento de lo establecido y en caso de su incumplimiento se verá sometido a las sanciones.

TÍTULO VIII: Transferencia de datos a terceros países

En este título se realiza la prohibición de transferencia de datos personales a otros países que no brinden el nivel de protección adecuado. Para ser un país que brinde los estándares requeridos deberá cumplir con el estándar que define la Superintendencia de Industria y Comercio. Esta prohibición no será efectiva excepto cuando la información tenga autorización del titular para realizar su transferencia; transferencia de datos para tratamientos médicos exigido por salud o higiene pública; transferencias bancarias, acorde a la legislación que le aplique;

transferencias pactadas en el marco de tratado internacional en donde la Republica de Colombia sea parte, como principio de reciprocidad; transferencias que impliquen salvaguardar interés público, proceso judicial, defensa de un derecho o por reconocimiento.

TÍTULO IX OTRAS DISPOSICIONES

En el artículo 27 se define Normas Corporativas Vinculantes, en donde el Gobierno Nacional expide la reglamentación referente a las Normas Corporativas Vinculantes para la certificación de buenas prácticas de protección de datos personales y la transferencia a terceros países.” [43]

La información se ha convertido en un símbolo representativo de la cultura actual y la revolución a los métodos tradicionales en las organizaciones.

Sin embargo la recolección, el almacenamiento y tratamiento de datos personales, datos que antes solo formaban parte de la vida privada de cada ser humano y era conocido por un mínimo sector, en la actualidad se ha convertido en una práctica habitual de control y almacenamiento de los sectores privados y públicos, lo que representa un riesgo si no se resguarda esta información de manera idónea.

4. IDENTIFICACIÓN DE PAÍSES QUE CUENTAN CON NORMATIVIDAD SOBRE PROTECCIÓN DE DATOS PERSONALES

En esta fase se realiza una investigación de la normatividad de los países que serán referentes y los conceptos significativos de lo que se encuentra estipulado en la Ley de cada país. Los países que se tuvieron en cuenta son España y Chile debido a la trayectoria que tiene la normatividad, y por su modelo jurídico es semejante al de Colombia.

4.1 ESPAÑA: LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

En España la ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), es de carácter orgánico, cuyo objetivo es garantizar y proteger lo referente al tratamiento de datos personales, las libertades públicas, como también los derechos fundamentales de las personas bien sea físicas y en especial el honor, la intimidad personal y familiar.

La cual fue aprobada por las cortes generales el 13 de diciembre de 1999. Esta ley se basa fundamentalmente en el artículo 18 de la constitución española de 1978, sobre el derecho a la intimidad familiar, personal y el secreto de las comunicaciones.

El objetivo principal de regular tratamiento de los datos y ficheros, de carácter personal independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos las obligaciones de aquellos que los crean o tratan.

Dicha ley afecta a todos los datos que hacen referencia a personas registradas en cualquier soporte informático o no. Quedan excluidos de esta ley aquellos datos que fueron recolectados para uso doméstico, las materias clasificadas del estado y

aquellos ficheros que recogen datos sobre terrorismo y otras formas de delincuencia organizada. A partir de esta ley se creó la Agencia Española de Protección de Datos, de ámbito estatal que vela por el cumplimiento de esta Ley.” [44]

4.1.2. Obligaciones Legales Básicas de La Normatividad

Calidad de los datos: “Los datos de carácter personal sólo se podrán recoger para su 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, no podrán usarse para otras finalidades incompatibles con aquellas, serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado y serán cancelados cuando hayan dejado de ser necesarios o pertinentes (Art. 4 LOPD).

Deber de secreto: El Responsable del Fichero 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 del fichero (Art. 10 LOPD).

Información en la recogida de datos: Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información, del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación, y de la identidad y dirección del responsable del tratamiento. Cuando se utilicen cuestionarios u otros impresos para la recogida,

figurarán en los mismos estas advertencias en forma claramente legible (Art. 5 LOPD). Consentimiento del afectado: El tratamiento de los datos de carácter personal

Consentimiento del afectado: El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa. No será necesario dicho consentimiento cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas (Art. 6 LOPD), sean necesarios para un contrato o figuren en fuentes accesibles al público.

Comunicación o cesión de datos: 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. Sin embargo este consentimiento no será preciso cuando la cesión esté autorizada en una Ley, o cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica (cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros), o cuando los datos
Página 3 de 6 procedan de fuentes accesibles al público, o cuando la cesión sea de datos relativos a la salud y sea necesaria para solucionar una urgencia (que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica), o cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos (Art. 11 LOPD).

Tratamiento por cuenta de terceros: Deberá estar regulado en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el Encargado del

Tratamiento únicamente tratará los datos conforme a las instrucciones del Responsable del Fichero, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad del RD 1720/2007 que el Encargado del Tratamiento está obligado a implementar.” [45].

La normatividad española en el título II desarrolla los principios de la protección de datos. Este título presenta gran importancia, en cuanto a la naturaleza de estos principios que constituyen la base en la cual se sustenta la protección de datos de carácter personal. Siendo de gran utilidad para el lector conocer estos conceptos de la normatividad de uno de los países pioneros en protección de datos personales.

La ley de protección de datos proporciona un cambio en el uso habitual de los datos personales y la obligación de todas las personas jurídicas, públicas y privadas que tienen acceso a las base de datos de las personas.

La normatividad protege toda la información personal de un individuo permitiéndole disponer de su información y decidir quién puede tratarla, acceder a ella, como también determinar la finalidad con la que se utiliza.

4.2 DEFINICIONES SEGÚN LA NORMATIVIDAD ESPAÑOLA

Dato de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

Fichero: Conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.

Afectado o Interesado: Persona física titular de los datos que sean objeto del tratamiento.

Tratamiento de Datos: Cualquier operación o procedimiento técnico, automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo, supresión o cesión de datos.

Responsable del Fichero o Tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Usuario: Persona o proceso autorizado para acceder a datos o recursos

Derecho ARCO: Todo ciudadano tiene el derecho fundamental de proteger sus datos y para ello podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición (ARCO).

Calidad de Los Datos

“Los datos de carácter personal sólo se podrán recoger para su 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, no podrán usarse para otras finalidades incompatibles con aquellas, serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado y serán cancelados cuando hayan dejado de ser necesarios o pertinentes (Art. 4 LOPD)”.

- FINALIDAD: Solamente podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas.
- LEGITIMIDAD: Prohibida la recogida de datos de forma fraudulenta, desleal o ilícita.
- COMPATIBILIDAD: No podrán usarse con una finalidad incompatible con aquella para la que se recogieron.
- PROPORCIONALIDAD. Sólo se tratarán los que sean adecuados, pertinentes y no excesivos en relación con la finalidad.
- VERACIDAD: Exactos y puestos al día.
- ACTUALIZACIÓN: Los datos inexactos o incompletos deben ser cancelados o sustituidos en un plazo de 10 días.
- LIMITACIÓN TEMPORAL: Serán cancelados cuando no sea necesario conservarlos para la finalidad por la que fueron recogidos.
- DERECHOS DEL INTERESADO. Serán almacenados de forma que el interesado pueda ejercer sus derechos ARCO.
- A-E-I-O-U de la Protección de Datos.

A) Inscripción de Ficheros. Toda persona o entidad que posea ficheros con datos personales está obligada a inscribir en el Registro General de protección de Datos la estructura de los ficheros de que disponga (art 26 LOPD).

E) Información previa al interesado. Este deber es correlativo al derecho que tiene el sujeto, cuyos datos van a ser utilizados, de ser informado “de modo expreso, preciso e inequívoco” de conformidad con los artículos 5 y ss LOPD.

I) Acceso a datos por cuenta de terceros. Regulado mediante un contrato de conformidad con el artículo 12 LOPD, y artículo 83 en caso de prestaciones de servicios sin acceso a datos.

O) Medidas de seguridad. El RDLOPD obliga a cumplir unos niveles de seguridad con el fin de que se protejan los datos personales contenidos en los ficheros. Distingue tres niveles de seguridad (básico, medio y alto) en función de la naturaleza de la información tratada.

U) Formación a usuarios y responsables de seguridad. Es obligación del Responsable del Fichero informar a los usuarios acerca de las funciones y obligaciones en materia de protección de datos en cumplimiento con el RDLOPD” [46]

Las definiciones que se encuentran trata de una norma dictada en el desarrollo del artículo 18 de la constitución política de la constitución española, la cual recogía un concepto de privacidad que pretendió ir más allá de la protección de la persona. Por lo tanto la norma normatividad de España con sus definiciones pretende delimitar una nueva frontera de la intimidad, el honor, la, calidad de los datos, usuario, entre otros, siendo un ámbito de aplicación delimitado a los ficheros

Toda persona tiene derecho a decidir sobre su información lo que conlleva, necesariamente a conocer si la información personal está siendo tratada adecuadamente para los fines a los cuales se le informo, como también se encuentra en la obligación de rectificar la información en caso de encontrarse incompleta o inexacta, solicitando al responsable la cancelación de sus datos

personales cuando considere que los mismos no se están tratando conforme a lo definido en la normatividad.

4.3 CHILE - LEY N° 19.628 “SOBRE PROTECCIÓN DE LA VIDA PRIVADA Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL” [47]

Por su parte en Chile “La protección de datos personales se encuentra regulada en diversos instrumentos jurídicos, clasificables en normas generales y sectoriales. Las normas generales son la Constitución Política de 1980, en adelante la Constitución, la Ley N° 19.628 “*Sobre protección de la vida privada y Protección de Datos de Carácter Personal*”, en adelante Ley N° 19.628 y el Reglamento del Registro de Bancos de Datos Personales a cargo de Organismos Públicos, en adelante el Reglamento.”

En el año 2008 se publicó la Ley N° 20.285 “Ley de Transparencia y Acceso a la Información Pública” en adelante “Ley de Transparencia”. [48] Con esta ley se creó un organismo autónomo denominado, el Consejo para la Transparencia, encargado entre otras funciones de promover la transparencia de la función pública, garantizar el derecho a la información, y además establece los procedimientos para el ejercicio del derecho, amparo y la protección de los datos personales, que se verifique únicamente en el sector público.

A nivel legal: “Boletín N° 6.994-07” [49]restringe el uso de datos personales de carácter sensibles disponibles en redes sociales en Internet. Los cuales no podrán ser utilizados por terceras personas, para otros fines, más que para aquellos, que, dentro del contexto doméstico o socializador de la red social, sean utilizados o estén disponibles, a menos que cuente con el consentimiento expreso del titular.

El 7 de mayo del 2010 Chile firmó el Convenio de Adhesión a la Organización para la Cooperación y el Desarrollo Económico (OCDE) y compromete plena

dedicación a la consecución de los objetivos fundamentales de la Organización. Dicha organización ha puesto una serie de recomendaciones, entre ellas destaca la Recomendación sobre Protección de la Privacidad y Flujo Transfronterizo de Datos Personales, materia, entre otras, ausente en la Ley N° 19.628.” [50]

La ley 19.628 dispuso que se debiera ajustar a sus regulaciones el tratamiento de los datos de carácter personal en registros, bancos de datos, organismos públicos o particulares. Definiendo dato personal como los relativos a cualquier información sobre personas naturales que se puedan identificar o no, adicionalmente define el dato sensible como aquellos datos personales que tienen características físicas, morales, o circunstancias de su vida o intimidad tales como hábitos personales, ideologías, origen racial, opiniones políticas, creencias religiosas, los estados de salud físico y la vida sexual. El titular del dato lo define como la persona natural a la que se refiere los datos de carácter personal. El banco de datos lo define como el conjunto organizado de datos de carácter personal, sea automatizado o no, y sin importar la forma de su creación que permita relacionar los datos entre sí.

Los derechos de los titulares de los datos en la normativa son cuatro, los cuales son: I. El derecho de acceso de información, II. El derecho de modificación o rectificación. III. El derecho de cancelación. IV. El derecho de bloqueo.

El derecho de acceso de información se define como la posibilidad de efectuar una serie de preguntas o cuestionamientos al responsable del registro o bancos de datos; las preguntas que se generan son a los datos de su persona. ¿Qué datos tiene sobre mi persona?, ¿Qué tipos de datos son?, ¿Qué datos son? En cuanto a su procedencia se pregunta ¿De dónde vienen los datos?, ¿Cuáles son sus fuentes?, para el destinatario se realizan preguntas como ¿Quién o quienes utilizaran mis datos?

El derecho de modificación hace referencia a la facultad de todo titular de los datos para solicitar la rectificación de aquellos datos que se consideren erróneos, inexactos, equívocos o incompletos. Se define dato erróneo como el falso o equivocado, el dato inexacto como falto de identidad, el dato equivoco como que produce confusión o diferentes interpretaciones y por último el dato incompleto como aquel que le falta información.

El derecho de cancelación es la facultad de todo titular de los datos para exigir la destrucción de datos que hayan sido almacenados, sin importar cual allá sido el procedimiento empleado para su almacenamiento, cuando este carezca de fundamento legal o se encuentre caducado. El dato estará caducado cuando la ley así lo disponga, por el incumplimiento de la condición señalada para su vigencia, cuando se presenta un cambio en los hechos o circunstancias que se pactan inicialmente o porque la norma establece lo contrario.

El derecho de bloqueo es aquel que corresponde a todo titular de datos para exigir la suspensión temporal de cualquiera de las operaciones del tratamiento de datos, este bloqueo se realizara en los casos que no se pueda certificar la exactitud o la vigencia de los datos pueda ser dudosa.

La normatividad Chilena impone la autorización previa y escrita del titular para cualquier tratamiento de sus datos personales, le otorga a los titulares una serie de derechos y garantías como son la modificación, bloqueo y eliminación de los datos haciendo responsable a la persona natural o jurídica que administra los datos de los daños materiales y morales que puede generar en caso de incumplimiento.

Los datos personales juegan un papel importante en la era de la información por el desarrollo tecnológico, iniciativas como información en la nube, bases de datos automatizadas, internet de las cosas, redes sociales, forman un escenario que

alimenta las bases de datos cuyo tratamiento y protección han sido los actores de los involucrados en la normatividad.

La normatividad busca la protección de los datos de carácter personal que han sido entregados, con una finalidad establecida y acotada. En esta ley se destacan puntos como la obligatoriedad del consentimiento previo y expreso del titular para recolectar sus datos, informando por correo electrónico una vez al año la existencia de los datos personales en sus bases de datos.

4.4 DEFINICIÓN DE CATEGORÍA DE DATOS SEGÚN LA NORMATIVIDAD CHILENA

Dato: “puede ser entendido como una unidad básica de información cuando la información que porta el dato es relativa a una persona determinada o susceptible de serlo, se denomina dato personal o dato nominativo, esto es, una unidad de información que se predica de persona determinada o determinable”. [51]

Dato de Carácter Personal o Datos Personales: “son aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables”. [52]

Datos Sensibles: “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual”. [53]

Dato Caduco: “aquel que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia

o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna”. [54]

Dato Estadístico: “el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable. Este último queda, por tanto, fuera del ámbito de aplicación de la ley”. [55]

Chile al igual que otros países que regulan el tratamiento de datos personales comparte una estructura y contenido en su normatividad en general, es así como estas señalan, en primer lugar, su ámbito de aplicación, los principios generales en el tratamiento de datos personales, los derechos y las obligaciones de los involucrados en este tratamiento, los medios por los cuales puede hacer efectivo el derecho de los titulares de los datos y el cumplimiento de las obligaciones por parte de los responsables para que se cumpla lo establecido en la normatividad.

CONCLUSIONES PROTECCIÓN DE DATOS PERSONALES EN CHILE

Chile fue el primer país iberoamericano que aprobó la ley de protección a la privacidad y contiene principios fundamentales sobre la protección de datos personales. En la ley 19628 en su artículo 4° también hace referencia a la legalidad del “spam” o correo comercial no solicitado al cual hace referencia en lo siguiente: “No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión, actividad, títulos educativos, dirección o fecha de nacimiento, o sean necesarias para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.” [56].

La ley 19.628 no solo busca proteger a los individuos del tratamiento de datos que se realiza por terceros, sino regular el mercado de tratamiento de datos personales. Lo que lleva a concluir la falta de sanciones ante la vulneración de la normatividad, falta de registro de bases de datos privadas, excepciones al consentimiento para el tratamiento de datos y mecanismos procedimentales de resguardo efectivo.

Aunque la normatividad tiene diecisiete años de vigencia, existe una necesidad de realizar actualizaciones debido al acceso de las tecnologías y redes por el flujo fronterizo de los datos ya que estos pueden realizarse sin limitaciones.

5. ESTUDIO DE DERECHO COMPARADO

La normatividad de Protección de Datos Personales contiene una serie de límites para la utilización de los datos personales. Es así que la legislación de cada país debe conjugar, los derechos que poseen los ciudadanos sobre el uso, el tratamiento y el destino que se le brinden a los datos para garantizar la seguridad de la información. El cumplimiento de las obligaciones legales en cuanto a la protección de datos es imprescindible y no puede posponerse su aplicación.

Esto con lleva a precisar que el derecho a la protección de datos personales y el derecho a la intimidad han sido analizados por diversos sectores normativos. Es por esta razón que los datos de las personas deben ser objeto de protección para que los mismos puedan ser tratados, convertidos y como resultado, solo puedan ser utilizados para fines pertinentes y personas autorizadas.

Entendiendo como dato personal toda información sobre una persona física o identificable. Siendo la protección de datos más que una idea individualista de protección. Es así que en la tabla número 8 se resaltan aspectos relevantes de la normatividad de los países (Chile, España y Colombia), que se tomaron para el estudio de la investigación. Se realiza una comparación de artículos de las normatividad que se refieren a un mismo tema.

La aparición de medios que permiten la gestión automatizada de la información, el tratamiento y el análisis discriminado de grandes volúmenes de datos y la accesibilidad y capacidad de procesamiento de estos medios se ha incrementado en las últimas décadas, lo que afecta la protección de datos de carácter personal y también puede afectar en el ámbito de la intimidad de las personas. Es por esto que proteger adecuadamente los datos personales exige delimitar el contenido que establece cada país en su normatividad.

Aspectos tales como Objeto de la Ley, que es aquel que regula las condiciones básicas que garantizan la igualdad en el ejercicio del derecho de los ciudadanos y se enmarca en un régimen de comportamientos aceptables. Otros aspectos que se validan son ámbito de la ley, definiciones, calidad de los datos, derecho del titular a ser informado entre otros, que se evidencian a continuación.

ESTUDIO BIBLIOGRÁFICO			
CARACTERÍSTICAS	CHILE	ESPAÑA	COLOMBIA
Comunicación a la ANPD		X	X
Autorización de la ANPD	X	X	X
Consentimiento y/o conocimiento del titular	X	X	X
Información previa al titular	X	X	X
Preservación del interés público		X	X
Cumplimiento de tratados Internacionales	X	X	

Tabla 3. Estudio Bibliográfico Chile, España, Colombia, Fuente propia

Los países seleccionados para realizar el estudio bibliográfico muestra características en común de los tres países, uno de los puntos a que hace referencia la tabla 3 es al consentimiento y/o consentimiento del titular e información del titular, haciendo referencia a una persona natural la cual será informada sobre el propósito del tratamiento de sus datos para resguardar el derecho de la persona a controlar la información. Otro aspecto que se tiene en cuenta es a la preservación del interés público, en Colombia es conocido en la normatividad como dato público, datos que para cuya recolección y tratamiento no

es necesaria la autorización del titular de la información. El tratamiento de tratados internacionales cada país lo ha definido en diferentes formas, siendo España uno de los países pioneros en resguardar la información que se transfiere a otros países.

Como se ha dicho los aspectos anteriormente citados y haciendo referencia en la sociedad que vivimos la cual se puede decir que es de riesgos en diferentes ámbitos, pero aquí tendremos presente el de la sociedad de la información, las conocidas tecnologías de la información, siendo internet uno de los más comunes, medio por el cual tiene la capacidad de difundir y almacenar información, entre ella datos personales de toda la sociedad, sin que los titulares de dicha información muchas veces tengan injerencia o decisión sobre los registros o bases de datos en los cuales se almaceno. Para limitar estos riesgos la normatividad de cada país ha establecido controles para que se haga efectivo y no se vulnere la información, no se puede afirmar que hasta el momento sea suficiente los controles generados ya que siempre se encuentra una brecha o un vacío ante estos lineamientos.

Así mismo otro aspecto a mencionar y de gran importancia para el desarrollo de la investigación se presenta los principios sobre la protección de datos personales basado en el estándar europeo; si bien no todos los países tienen una protección uniforme se presenta una serie de principios comunes contenidos en la directiva 95/46, el convenio 108 de 1981, las directrices de la organización para la cooperación y desarrollo económico de lo anterior concluyo que las normas deberían contar con un mínimo de elementos los cuales se presentan en la siguiente tabla.

Principios mínimos que debe contener la regulación sobre Protección de Datos Personales según el estándar Europeo

Principios Básicos	Aspectos aplicables a tipos esenciales de tratamiento
Limitación de la finalidad	Dato sensible
calidad de los datos y proporcionalidad	Mercadeo directo
Transferencia	Decisión individual automatizada
Seguridad	
Acceso, rectificación y oposición	
Restricciones a las transferencias sucesivas a otros terceros países	

Tabla 4. Principios mínimos en protección de datos según estándar europeo. Fuente, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, Nelson Remolina-Angarita, 2010

Lo anterior es una serie de principios mínimos que se recomienda para la regulación de protección de datos según el estándar Europeo haciendo énfasis en la transferencia internacional de datos.

Estos principios se han expuesto para que se considere como un país con el nivel de protección adecuado, dado que no es una tarea fácil debido a que se debe iniciar la tramitología con la Comisión Europea que muchas veces exige que la normatividad de cada país cuente con cambios institucionales, cambios que pueden llegar a tardar años y no garantiza que se apliquen debido a los procedimientos o lineamientos internos que se manejen en cada país frente a su normatividad.

En Colombia la Ley 1266 de 2008 en su encabezado comprende disposiciones generales sobre el habeas data en el cual se regula la información financiera,

crediticia y comercial, junto con una serie de definiciones como principio de veracidad o calidad de servicios, principio de finalidad, principio de circulación restringida, principio de temporalidad de la información, principio de interpretación integral de derechos constitucionales, principio de seguridad, principio de confidencialidad, estos principios son consistentes con lo que enuncia el modelo europeo, pero después de realizar un estudio por la Corte Constitucional concluye que la ley solamente es aplicable a los datos personales relacionados con el cumplimiento o incumplimiento de obligaciones financieras. Es así que la ley 1266 de 2008 es una regulación parcial que solo se puede aplicar a la información financiera, crediticia. Debido a esto la corte constitucional ratifica que Colombia carece de una ley sobre protección de datos. Como se cita en la ley 1266 de 2008 en su numeral f) del artículo 5 sobre la transferencia internacional de datos queda no bajo el ente de control si no queda en cabeza del operador lo cual no garantiza que Colombia cuente con el nivel adecuado para la protección de datos ya que no avala que un banco de datos extranjero pueda brindar o certifique el nivel adecuado que se requiere para la protección de datos.

Si bien Colombia en sus normativas ha intentado establecer la debida protección de datos en la transferencia internacional teniendo presente las recomendaciones que realiza el estándar Europeo no han sido lo suficientemente efectivas para que se brinde la protección adecuada, lo que genera que se deba realizar un replanteamiento de la normatividad vigente.

A continuación se presentan características de la normatividad de los países que sirvieron para estudio de la investigación en la cual se denotara las diferencias y/o similitudes.

PAÍS	CONSTITUCIÓN POLÍTICA	NORMA	REGLAMENTO	ORGANISMOS DE CONTROL
CHILE	Artículo 19: La constitución asegura a todas las personas: 4. ° El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.	Ley 19.628 sobre protección de datos de carácter personal	Decreto 779/2000, por el que se reglamenta la Ley 19.629, que regula el registro de bancos de datos personales a cargo de los organismos públicos.	Consejo para la Transparencia
ESPAÑA	Artículo 18.4: 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.	Ley Orgánica 15/1999 del 13 de diciembre de protección de datos de carácter personal.	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal	Agencia Española de Protección de Datos.
COLOMBIA	Artículo 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los 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.	Ley Estatutaria 1581, de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.	Decreto 1377, de 27 de junio de 2013, por el cual se reglamenta parcialmente la Ley N. ° 1581.	La Superintendencia de Industria y Comercio- Delegatura de Protección de Datos.

Tabla 5. Estudio Bibliográfico- Características Chile, España, Colombia, Fuente propia

Para dar inicio se realizara una breve explicación de cada uno de las característica que se tuvieron en cuenta para realizar el estudio bibliográfico y las diferencias encontradas en cada aspecto, es por esto que se inicia con la explicación de a que hace referencia la constitución política y la jerarquía de en qué se encuentra cada aspecto seleccionado.

La constitución se define como la ley fundamental de un estado que es aceptada como guía para su gobernación, también es conocida como Carta Magna. Es así que la constitución contiene leyes o doctrinas que establece la forma de organización política y fija los límites y relaciones entre los poderes legislativo, ejecutivo y judicial. Asimismo establecen los derechos y los deberes de los ciudadanos y gobernantes, como también la organización del territorio en municipios, provincias, para el caso de España se hace referencia a las comunidades autónomas.

La constitución puede ser modificada con el fin de mejorarla o ponerla al día, el encargado de esto será el Tribunal Constitucional verificando si las leyes son conformes con la constitución y cuáles no, y en caso de presentarse un cambio importante se deberá realizar la consulta a los ciudadanos mediante un referéndum o reforma constitucional, en donde por medio del voto se expresa el acuerdo o el desacuerdo al cambio.

En la primera columna se encuentra la definición que cada país tiene en su constitución en cuanto a la vida privada de cada persona, todas haciendo énfasis en el respeto, la protección a la intimidad personal y familiar, vida privada, buen nombre todo enfocado en la normatividad de protección de datos personales.

Las leyes pueden clasificarse de diferentes maneras en atención a su alcance, su naturaleza, su importancia, sus fines o consecuencias, es así que se pueden clasificar en leyes orgánicas y leyes ordinarias

Dando inicio con la ley orgánica y poniéndola en una escala de jerarquía con respecto a la constitución se encuentra en mayor rango la constitución política, seguida de la ley orgánica y continua la ley ordinaria.

Pero la ley orgánica tiene como característica principal que es dictada con un carácter complementario de la constitución de un estado, es decir, la ley orgánica se necesita desde el punto de vista constitucional, con el fin de regular ciertas normas específicas. Es por esto que este tipo de leyes tratan sobre derechos fundamentales, imponiendo límites para su aplicación y garantizar el cumplimiento.

Para que la ley pueda ser emitida requiere una serie de requisitos constitucionales, como la reunión de condiciones extraordinarias, contar con una mayoría de votos para que pueda ser aprobada, entre otros. Esta ley orgánica por su nivel de jerarquía no se puede modificar con facilidad, ni por voluntad de un gobernante.

Mientras que la ley ordinaria es aquella que se dirige a los ciudadanos para regular casos concretos sobre alguna materia. La ley ordinaria tiene la función de regular aquellas situaciones que dejan de regular las leyes orgánicas, asimismo no sirven de marco para realizar otras leyes, por lo que no proceden en reglamentos y decretos, además no pueden aplicarse a derechos fundamentales señalados en la Constitución.

Con lo anteriormente citado se puede denotar la referencia que cada país quiso implementar en sus normatividades para la protección de datos, sin embargo Colombia cuenta con una ley estatutaria la cual no es una ley ordinaria, sino que tiene un rango superior en todas las demás leyes y su estudio es de carácter prioritario. Esa jerarquía se lo da el hecho que la naturaleza de los temas que trata es la espina dorsal de la Constitución Política.

Cada país selecciono entes de control que velaran por el cumplimiento, el buen uso de la normatividad en protección de datos, mediante acciones de mejoramiento continuo.

Después de realizar la explicación de cada aspecto que se tuvo en cuenta para plasmar las características en la tabla 5 se puede denotar las diferencias y/o similitudes encontradas en cada país seleccionado, encontrando más similitudes que diferencias debido a que todas hacen énfasis en la protección como un derecho fundamental establecido en cada Constitución, el título de la normatividad se encuentra dirigido a la protección de datos y así mismo designan entes que velen por el cumplimiento de lo establecido en cada ley.

ESTUDIO BIBLIOGRÁFICO DE LA NORMATIVA DE COLOMBIA, ESPAÑA Y CHILE		
PAÍS	REQUISITOS	BIEN JURÍDICO PROTEGIDO
CHILE	La normativa chilena define que la comunicación de datos consiste en “dar a conocer de cualquier forma los datos de carácter personal a personas de distintas del titular, sean determinadas o indeterminadas”. 1. Consentimiento del titular: Se aplican las reglas prevista en la normativa chilena para la recogida y tratamiento de los datos personales. 2. Nivel de protección equivalente/adecuado en el destino: No se exige en la normativa chilena vigente que el país de destino cuente con un nivel de protección equiparable al previsto en ella. 3. Comunicación a la Autoridad: No se exige actualmente por la legislación chilena que se deba comunicar las TID a la autoridad competente. 4. Autorización previa de la Autoridad: Tampoco es necesaria para las TID ningún tipo de autorización previa por autoridad judicial o administrativa alguna.	“En la normativa chilena el bien jurídico sobre protección de datos ha sido difícil de determinar por los autores chilenos debido a como se encuentra definido el sistema jurídico en la Constitución política de 1980. En las diferentes reuniones del poder legislativo incluyeron como bien jurídico protegido a la vida privada, la intimidad, el honor y el derecho a la identidad, para postular directamente que se estaría frente a un derecho implícito, el denominado derecho a la autodeterminación informativa”. “En la legislación chilena no se encuentra presente la autodeterminación informativa”

Tabla 6. Estudio Bibliográfico- Características Chile, España, Colombia, Fuente propia.

ESPAÑA	La normativa española define a la TID como el «tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.» referencia 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, art. 5.1.s). 1. Consentimiento del titular: Se aplican las reglas previstas en la legislación española para la recogida y tratamiento de los datos personales, sin que exista una particularidad en cuanto a este requisito referido a las TID, salvo por el hecho de que no será necesario que el país de destino prevea un nivel de protección equiparable al de la legislación española, si el titular ha dado su consentimiento inequívoco a la transferencia prevista. 2. Nivel de protección equivalente/adecuado en el destino: Es requisito general exigido que el país de destino tenga un nivel de protección equiparable al de la ley española, en caso contrario deberá obtenerse la autorización previa del Director de la Agencia Española de Protección de Datos (AEPD),” [52] Salvo que se trate de algunos de los supuestos excepcionados en la ley.	“La ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), lo que define en su artículo 3, a) Cualquier información concerniente a personas físicas identificadas o identificables” Según la definición que se encuentra definida por la Directiva 95/46/CE, “Se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación, características de su identidad física, fisiológica, psíquica, económica, cultural o social”
---------------	--	--

	3. Comunicación a la Autoridad: Para las TID la normativa española requiere en todo caso la notificación previa a la AEPD ” 4. Autorización previa de la Autoridad: Asimismo es necesario obtener la autorización previa del Director de la AEPD para los casos en que el país de destino de una TID no garantice un nivel de protección equivalente.	
--	---	--

COLOMBIA	Legalmente, se constituye que «la transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.» [55].	El derecho a la protección de datos es la facultad de una persona de controlar y administrar a su voluntad, la información personal que otros tienen de él o de los menores a su cargo. La Ley atribuye a los ciudadanos la titularidad, el control, el poder de disposición y autodeterminación sobre sus datos personales, supeditando el tratamiento de los mismos al consentimiento e información previa. En la normativa Colombiana en el artículo 3 se define datos como privado, semiprivado, público y definiciones que son de gran relevancia como autorización, Base de datos, Dato personal, Encargado de Tratamiento, Responsable del Tratamiento, Titular y Tratamiento.
	1. Consentimiento del titular: Se aplican las reglas previstas en la legislación colombiana para la recogida y tratamiento de los datos personales. Se permiten las TID a un destino que no ofrece nivel de protección adecuado si el titular de los datos ha dado su autorización expresa e inequívoca al efecto”. [56]	
	2. Nivel de protección equivalente/adecuado en el destino: Sí se exige que el país de destino cuente con un nivel de protección adecuado, que no podrá ser inferior al que exige la Ley colombiana.	
	3. Comunicación a la Autoridad: La legislación colombiana no exige actualmente la previa comunicación a la Superintendencia de Industria y Comercio (SIC). 4. Autorización previa de la Autoridad: No se prevé de forma expresa en la normativa colombiana vigente el requisito de la autorización previa por parte de la Autoridad competente. No obstante, para aquellos Casos en que el país de destino no garantiza un nivel adecuado de protección, corresponde a la SIC emitir la declaración de conformidad relativa a la TID.	

El cuadro trata aspectos tales como el consentimiento del titular, en donde la normatividad de cada país aplica las reglas previstas para la recolección y el tratamiento de los datos personales, en este punto Colombia y España permiten que los datos sean transferidos a países que no cuenten con el nivel adecuado de protección de datos si el titular ha dado su consentimiento, mientras que Chile es un aspecto que no tiene definido.

El siguiente aspecto es el nivel de protección equivalente /adecuado en el destino, Chile no exige que el país cuente con el mismo nivel de protección, para el caso de España si exige que el país cuente con el mismo nivel o sea similar en cuanto a la protección de datos y en caso de no cumplir con este requisito se requiere la autorización previa del Director de la Agencia Española de Protección de Datos, salvo que se encuentre alguna excepción en la ley, Colombia por su parte también exige que el país de destino cuente con el mismo nivel de protección sin presentar alguna autorización especial, como lo presenta España.

Otro aspecto es la comunicación con la autoridad, actualmente en la normatividad de Colombia y Chile no exige que se tenga una notificación a la autoridad competente, para el caso de España si solicita la notificación para la Agencia Española de Protección de Datos.

Así pues continuando con la revisión es el autorización previa de la autoridad, Chile en su normatividad no presenta ningún tipo de autorización previa por autoridad judicial o administrativa, Colombia de forma expresa no lo tiene plantado en la normatividad, sin embargo en caso de que el país no garantice el nivel adecuado de protección, la Superintendencia de Industria y Comercio como ente encargado será quien revise, España solicita tener la autorización previa del Director de la Agencia Española de Protección de Datos para los casos en que no se garantice el nivel de protección adecuado.

ESTUDIO BIBLIOGRÁFICO DE LA NORMATIVA DE COLOMBIA, ESPAÑA Y CHILE			
PAÍS	INFORMACIÓN Y CONSENTIMIENTO	DATOS ESPECIALMENTE PROTEGIDOS	CALIDAD DE LOS DATOS
CHILE	“En la normativa chilena hace referencia al consentimiento del titular de los datos personales para que sea legítimo en el tratamiento. Sin embargo existen excepciones legales lo que permite cierto grado de formalidad pero carente de contenido y sentido. La normativa específica que la identificación de del tratamiento de datos personales solo se podrá realizar por la autorización de la ley o por autorización del titular, donde por escrito deja de manera explícita lo que no será conocido por otras personas. Otros medios utilizados para la recolección de información exige un mínimo deber por parte de quien realiza la recolección de datos de estos titulares”	Los datos personales como especialmente protegidos hacen referencia a los datos sensibles, los que, por regla no pueden ser objeto de tratamiento. Aunque es motivo de discusión debido a que la normativa no es eficaz para la protección de este tipo de datos ya que en empresas, prensa y otros medios circulan libremente. Esto se debe a que aunque se solicite autorización por escrita a los titulares se vulneran los derechos lo cual hace que termine en denuncias, reclamos hasta que se les brinde una compensación	En la normativa chilena no se encuentra tan específico la calidad de los datos lo que se realiza en la Ley 19.628 es una clasificación en cuanto a la eliminación, bloqueo, cancelación, publicación de datos financieros y económicos y la responsabilidad de los organismos públicos con el tratamiento que le den a los datos personales, las infracciones, faltas disciplinarias y la definición en el principio de calidad como dato caduco.

Tabla 7. Estudio Bibliográfico- Características Chile, España, Colombia, Fuente propia.

ESPAÑA	"La normativa española, en su artículo 5 de LOPD establece que los interesados a quienes le soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos y de los destinatarios de la información, del carácter obligatorio de la respuesta a las preguntas que le sean planteadas, de las consecuencias de la obtención de los datos suministrados y de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante "	En España de acuerdo en el artículo 16 de la CE, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando hace referencia a este tipo de datos se requiere el consentimiento del titular y se advertirá acerca de su derecho a no prestarlo sin que se deje por escrito por parte del afectado a que serán objeto los datos que revelen la ideología, afiliación sindical, religión.	En España la Ley Orgánica 15/1999 entre sus principios ya se encuentra el principio de calidad de datos, que junto con el principio de proporcionalidad de los datos exige que los datos que sean recogidos cumplan con la finalidad. La recolección y el tratamiento de los datos de carácter personal deben efectuarse como lo estipula la ley. En las sentencias 290/2000 y 292/2000 de 30 de noviembre se definió el derecho a la autodeterminación informativa de carácter personal y cita "«persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»"
----------------------	---	---	---

COLOMBIA	La legislación colombiana en su artículo 9 y 10 de la Ley 1581 de 2012 especifica la autorización previa e informada que debe dar y/o otorgar el titular del dato personal, la cual debe dejarse por cualquier medio que pueda ser objeto de consulta y posterior verificación. La recolección, almacenamiento, uso y circulación o supresión de los datos personales por parte de cualquier tercero, requiere del consentimiento libre, previo, expreso e informado del titular de los mismos.	En la normativa colombiana en los artículos 5 y 6 de la Ley 1581 de 2012, se encuentra la definición para el tratamiento de datos sensibles, realizando una descripción y se alude por primera vez al dato biométrico. Es así que la definición de dato sensible hace referencia a lo que afecte la intimidad del titular o cuyo uso indebido pueda generar su discriminación, como lo puede ser el origen étnico, la orientación sexual, convicciones religiosas o políticas, como también salud, huellas digitales, etc.	Colombia en su normativa no tiene definido el principio de calidad de los datos
------------------------	--	---	--

A continuacion se presenta un cuadro con la comparacion de leyes para Colombia, Chile y España, para el efecto se ha definido en cada casilla una descripcion general del tema y de forma muy breve, debido a que citar todo el texto resultaria excesivamente extenso.

Pero bien los aspectos aquí citados son la informacion y consentimiento, para Chile este concepto hace referencia al consentimiento del titular de los datos personales para que el tratamiento sea legitimo, donde se dejara constancia escrita y de manera explicita lo que no sera conocido por otras personas, con la excepcion legal lo que permite cierto grado de formalidad pero que llega a ser carente dde contenido.

España en este concepto es un poco mas especifico ya que en su normatividad establecio que los interesados de la recoleccion de datos personaels debiera previamente informar de modo expreso, preciso e inequívoco la finalidad de los datos y los destinatarios de la información, teniendo como carácter obligatorio responder las preguntas que surgan en este proceso.

Colombia por su parte lo define con la autorización previa e informada al titular del dato personal, teniendo similitud al planteamiento que realiza españa en esta definición.

El siguiente aspecto es los datos especialmente protegidos, para los tres paises cuando se hace referencia a este concepto se define como aquellos datos que no pueden ser objeto de tratamiento, datos que afecten la intimidad del titular o cuyo uso indebido pueda generar discriminación como lo puede ser su ideología, convicciones religiosas o políticas, entre otros.

Para concluir el ultimo aspecto que se tuvo en cuenta fue la calidad de los datos, para el caso de Colombia en la normatividad vigente no se tiene definido el

principio de calidad de datos, Chile por su parte en la normatividad vigente no lo tiene tan definido como calidad de los datos, lo que presenta es una clasificación de eliminación, bloqueo, cancelación de datos financieros y económicos, recayendo la responsabilidad sobre los organismos públicos con el tratamiento que le den a los datos y las infracciones que deban asignar por el incumplimiento.

España si tiene definido en la normatividad vigente el principio de calidad de los dato, en la cual exige que la recolección de los datos cumplan con la finalidad y se cumpla lo establecido en la ley.

Considero finalmente que la vigencia y la actualidad en la normatividad de los países escogidos para el estudio poseen un fundamento sólido para fueran referentes en la investigación

PAÍS	PRECEPTO CONSTITUCIONAL	NORMA GENERAL	NORMA SECTORIAL
CHILE	No existe norma expresa, pero la construcción jurídica de la protección de datos personales se basa en el artículo 19 n° 4, inciso primero, de la Constitución Política de la República, que reza: “CAPITULO III. De los Derechos y Deberes Constitucionales Artículo 19.- La Constitución asegura a todas las personas: (...) 4°.- El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia.”	Ley 19.628 “SOBRE PROTECCIÓN DE LA VIDA PRIVADA”, publicada el 28 de agosto de 1999, modificada por la Ley N° 19.812, de 13 de junio de 2002. Esta ley excluye de su aplicación los tratamientos de datos que se realicen en virtud del ejercicio de la libertad de información. El Reglamento de la Ley 19.628 es el Decreto 779 de 2000 del Ministerio de Justicia que regula el registro de Bancos de Datos Personales a cargo de los Organismos públicos.	No existe

Tabla 8. Derecho comparado entre Chile, España y Colombia. Fuente Propia.

COLOMBIA	El artículo 15 de la Constitución, modificado por el acto legislativo N° 02 del 18 de diciembre de 2003 dice lo siguiente: “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los 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. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley.	Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013,22 se regulan aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados y el ejercicio de los derechos de los titulares de la información.	El artículo 95 de la Ley 270 de 1996 (estatutaria de la administración de justicia) ordena que los procesos que se tramiten con soporte informático garanticen (...) “la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley”. Comercio Electrónico y firmas digitales: Las “Entidades de Certificación”, por su parte, están obligadas a: “garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor” (Literal c del artículo 32 de la ley 527 de 1999) “respetar las condiciones de confidencialidad y seguridad de acuerdo con las normas vigentes respectivas” (Art. 25 del decreto 1747 de 2002), y “Garantizar la confidencialidad de la información que no figure en el certificado” (Literal 11 del artículo 13 del decreto 1742 de 2002)
----------	--	--	--

ESPAÑA	Artículo 18.4: 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.	Ley Orgánica 15/1999 del 13 de diciembre de protección de datos de carácter personal.	Junto a la Ley Orgánica 15/1999 tenemos varias normas sectoriales posteriores entre las que podemos destacar: - En materia de telecomunicaciones: la Ley 32/2003, de 3 de noviembre, General de Tele-comunicaciones y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, modificada por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica;
---------------	--	--	---

Antes de dar inicio, con las similitudes o diferencias de los conceptos seleccionados se dará una aclaración del significado de los mismos. El precepto constitucional se conoce como un artículo que forma parte de la constitución y que establece una orden o mandato, encontrando dos tipos de preceptos, los que hacen referencia a los derechos fundamentales y los que giran en torno a los poderes del estado.

Para el caso de Chile no existe una norma expresa pero en la constitución jurídica de protección de datos se basó en lo plasmado en el artículo 19 de la constitución política que hace referencia al derecho a la vida y a la integridad física y psíquica de la persona, la igual protección de la ley en sus derechos.

España en el artículo 15 de la constitución política se refiere a que toda las personas tienen derecho a su intimidad personal y familiar, buen nombre, haciendo que el estado los respete y los hace respetar, a su vez tienen derecho a actualizar, conocer, actualizar y rectificar los datos que se encuentren en bancos de datos y archivos de entidades públicas y privadas. Solo podrán ser registrados mediante orden judicial y en casos que la ley lo establezca.

Colombia por su parte lo define el artículo 18 en donde la ley limitara el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos.

En el precepto constitucional los tres países presentan similitudes en la definición de lo establecido en la constitución refiriéndose a la protección de las personas en lo personal, familiar y la igualdad en la protección de sus derechos.

En cuanto a la norma sectorial los tres países tienen definido la ley de protección de datos personales con lineamientos similares, España y Chile con mayor antigüedad en su normatividad, con respecto a Colombia, normativas que los

países se encuentran evaluando para realizar ajustes en los aspectos que consideran mejorar o que no se estipularon en su momento.

ANÁLISIS DE LEYES EN PROTECCION DE DATOS			
TEMA	CHILE	ESPAÑA	COLOMBIA
Objeto de la Ley		Art.1. Proteger los datos personales. Libertades públicas y derechos fundamentales, en especial el honor e intimidad	Art.1. Desarrollar el derecho constitucional de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y derechos relacionados con la recolección, tratamiento y circulación de datos
Ámbito de la Ley	Art.2. El tratamiento de datos de carácter personal, registros o bancos de datos públicos o privados. Excepción al derecho de opinión e información	Art.2 Datos de carácter personal, registrados en soporte físico y susceptible de tratamiento. Carácter de ley orgánica territorialidad, régimen, excepciones, ficheros	Art.2 Todos los datos de información personal, registrados en un banco de datos, sean administrados por entidades públicas o privadas. Se exceptúa la información del DAS y fuerza pública.
Definiciones	Art.2. Almacenamiento de datos, bloqueo de datos, comunicación de datos, dato caduco, dato estadístico, dato de carácter personal, dato sensible	Art.2. Dato de carácter personal, fichero, tratamiento de datos, responsable del fichero, afectado o interesado. Procedimiento de disociación. Encargado del tratamiento	Art.2. Titular de la información, fuente de información, operador de información, usuario, dato personal, dato público, dato privado, información financiera, crediticia y la proveniente de países terceros
Calidad de los Datos		Art.4, Adecuados, pertinentes y no excesivos a las finalidades compatibles, datos inexactos. Deben ser almacenados de manera que permitan el ejercicio de libre acceso	Art.4. Principios de la administración de datos, veracidad y calidad de los datos, finalidad legítima. Circulación restringida, temporalidad de la información. Interpretación de los derechos constitucionales. Principio de seguridad, confidencialidad

Tabla 9. Análisis de Leyes de Protección de Datos en países como España, Chile y Colombia. Fuente Propia.

ANALISIS DE LEYES EN PROTECCION DE DATOS			
TEMA	CHILE	ESPAÑA	COLOMBIA
Derecho del titular a ser informado. Consentimiento del afectado	Art.3. En toda recolección de datos, se debe informar a las personas sus derechos	Art. 5. Derecho de Información en la recogida de datos, informados previamente y de forma expresa e inequívoca. Art6. Consentimiento del afectado, salvo que la ley disponga otra cosa, salvo el ejercicio de las administraciones públicas.	Art.6. Derechos de los titulares frente a los operadores de datos, frente a las fuentes de información, frente a los usuarios
Datos expresamente protegidos - Datos sensibles	Art. 10. Prohibición de tratamiento de datos, sensibles salvo autorización de ley.	Art. 7. Nadie puede ser obligado a declarar respecto a su religión, ideología, creencias, salvo consentimiento expreso y escrito del afectado. También se encuentran los artículos 13 y 22	
Seguridad de los datos - Mandato expreso de la ley para el tratamiento de datos	Art.4. El tratamiento de los datos personales solo se puede efectuarse conforme la ley. Art. 7. Los responsables deben guardar secreto cuando los datos provengan de fuentes no accesibles.	Art.9. Responsables de ficheros, medidas técnicas y organizativas necesarias para la seguridad. Art. 10. Los responsables y quienes intervienen en cualquier fase del tratamiento de datos,	Art.5. Circulación de la información, puede ser entregada bajo condiciones a los titulares, usuarios, entidades públicas, órganos de control. Operadores de datos y personas autorizados por la ley.

Conclusiones Estudio de Derecho Comparado

- La protección de datos personales promueve la integridad y el respeto a la privacidad de las personas, como también controla el uso inadecuado de la información.
- Resguardar la información de la vida privada de personas se ha vuelto difícil ya que por su profesión o condición social pueden estar más al alcance de la vida pública, aunque se conserve el derecho a la intimidad.
- El avance tecnológico acentúa el peligro sobre la intimidad de las personas debido a que facilita la el acceso de terceros en la información que desea reguardar, tal como conversaciones telefónicas, domicilio, registros privados, ideología, datos financieros, aunque se encuentre establecido en la normatividad la protección de los mismos.
- La normatividad de los países como Chile, España y Colombia son muy similares y han sido tratamiento y evolución por lo que constituyen un elemento esencial para el desarrollo de la presente investigación
- La normatividad de los datos personales se ha convertido en un hecho importante que se ha ido acogiendo en las constituciones latinoamericanas
- El derecho comparado aporta la experiencia de cada país en protección de datos, cada uno de estos enfocándose a la protección de la información de las personas, algunas normativas más completas que otras ya que han tenido más aspectos a proteger que otras, como se denota en España con respecto a Chile o Colombia.

- Una de las diferencias en cuanto al consentimiento del titular Colombia y España permiten que los datos sean transferidos a un país que no cuente con el nivel adecuado de protección si el titular ha dado su consentimiento, mientras que Chile no tiene definido esto en su normatividad
- Para la comunicación con la autoridad, actualmente en la normatividad de Colombia y Chile no exige que se tenga una notificación a la autoridad competente, para el caso de España si solicita la notificación para la Agencia Española de Protección de Datos.
- Cada país tiene definida su normatividad en una ley orgánica, ley estatutaria, ley ordinaria, con características únicas que le dan un orden jerárquico y especial.
- Se puede concluir que todos los lineamientos sobre protección de datos personales de cada país contienen en general los derechos de acceso, rectificación, cancelación y oposición para los titulares, con sanciones a cargo de los organismos de cada país.

5.1. ESTUDIO COMPARADO LEY ORGÁNICA 15/1999 - LEY ESTATUTARIA 1581 DE 2012

A continuación se presenta en la tabla número 9 artículos y principios de la normatividad Española y Colombiana para realizar un estudio de derecho comparado, como por ejemplo cuando se hace referencia al encargado del tratamiento es una persona natural o jurídica, pública o privada que por sí misma en asocio con otros realice el tratamiento de los datos personales, otro de las obligaciones a las cuales se hace mención es el principio de seguridad la cual es un proceso dinámico que constantemente se encuentra en evolución, pretendiendo que exista el nivel adecuado en las diferentes etapas del tratamiento de los datos personales, los otros principios no menos importantes se toman también como referentes ya que la normatividad Colombiana y la Española tienen semejanzas.

PRINCIPALES OBLIGACIONES	ESPAÑA	COLOMBIA
INSCRIPCIÓN DE FICHEROS	ART. 26 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal	ART. 19 Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales
Diferencia Normatividad	Notificación e inscripción registral	Autoridad de protección de datos
CONSENTIMIENTO Y DEBER DE OBLIGACIÓN	ART. 5 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.	ART. 12 Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales
Diferencia Normatividad	Derecho de información en la recogida de datos.	Deber de informar al titular

	ART.6 Consentimiento del afectado	
ENCARGADOS DEL TRATAMIENTO	Art. 12 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.	Art. 17 y Art.18 Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales
Diferencia Normatividad	Acceso A Los Datos Por Cuenta De Terceros	Deberes De Los Responsables de Tratamiento y de Los Encargados De Tratamiento
PRINCIPIO DE SEGURIDAD	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	Art. 4. g) Ley Estatutaria 1581 de 2012 , por la cual se dictan disposiciones generales para la protección de datos personales
Diferencia Normatividad	Principio De Seguridad De Los Datos	Principio de seguridad
FORMACIÓN	Art. 89 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.	Art. 17.k) Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales
Diferencia Normatividad	Funciones y obligaciones del personal	Adoptar un manual interno de políticas y procedimientos para garantizar el cumplimiento de la ley

Tabla. 10. Derecho comparado Ley Orgánica 15/199- Ley Estatutaria 1581/2012.
Fuente propia

Realizando una revisión de la tabla anterior y de las principales obligaciones de la normatividad de España y Colombia podemos evidenciar las similitudes que presentan en la definición con el fin común de la protección de datos. La normatividad de España fue un referente para Colombia en la creación de la ley de protección de datos.

Sanciones impuestas por Colombia vs España en cuanto a protección de datos de carácter personal.

Con la entrada en vigencia de la ley estatutaria 1581 de 2012 asigno a la Superintendencia de Industria y Comercio ente descentralizado del orden nacional, la vigilancia y control del tratamiento de datos personales en Colombia asignando con autoridad sancionatoria para que se minimice el indebido uso de información por parte de los responsables de su tratamiento.

Esta asignación a la Superintendencia de Industria y Comercio introduce tres actividades especiales las cuales son: control a la eficiencia de la gestión empresarial, protección de usuarios y control de las conductas.

Es así que la superintendencia presenta el siguiente reporte.

- “La Superintendencia de Industria y Comercio, en ejercicio de sus funciones de inspección, vigilancia y control del régimen de protección de datos personales, ha impuesto multas que superan los \$21 mil millones de pesos.
- En total, la Superindustria ha impuesto más de 610 sanciones desde el 2010, cuando empezó a regir el régimen legal de protección de datos personales en Colombia.

- Cerca del 80% de las sanciones impuestas por la Superindustria se relacionan con violaciones del habeas data financiero por: (i) reportes a centrales de riesgo que no corresponden con la realidad; (ii) no actualización oportuna de información; (iii) por no avisar al deudor antes de hacer el reporte a las centrales de riesgo”. [57]

Por su parte España en el título vii de la ley orgánica 15/1999 protección de datos de carácter personal establece las sanciones que serán aplicadas por parte de la agencia española de protección de datos, clasificándolas como infracciones leves, graves y muy graves las cuales oscilan en multas de 600 euros por la infracción más leve y 600.000 euros por la infracción más grave.

La agencia española de protección de datos pública que para 2015 se presentó un incremento del 15,70% en las denuncias y en las reclamaciones que ya se dieron por resueltas. Los sectores más sancionados para ese año fueron las telecomunicaciones, entidades financieras y comercialización de servicios de agua y energía.

En el análisis anual que realiza la entidad se encontró que atendieron promedio 220.000 consultas a través de diferentes medios es decir que incrementó un 23.6% con respecto al año anterior, en los primeros lugares se encuentran la cancelación de procedimientos, seguidos por oposición y rectificación.

Para el 2016 destacan que se presentó un descenso del 6,53% en las denuncias presentadas y un aumento en las reclamaciones de un 24,30%. Las denuncias presentadas fueron por la inclusión indebida en ficheros de morosidad y contratación irregular. Las reclamaciones se presentaron debido al derecho de

cancelación de datos personales lo que evidencia la preocupación de los ciudadanos sobre el tratamiento de sus datos personales.

Se destaca una reducción en un 21% las sanciones impuestas por parte de la agencia española de protección de datos.

A continuación se presentan dos graficas de las denuncias y reclamos en España por la normatividad de Protección de Datos personales.

DENUNCIAS Y RECLAMACIONES REGISTRADAS					
TIPO	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Escritos de reclamación de tutela	1.997	2.099	2.082	19,70	-0,81
Escritos de denuncia	8.607	10.074	8.489	80,30	-15,73
TOTAL	10.604	12.173	10.571	100	-13,16

DENUNCIAS Y RECLAMACIONES RESUELTAS					
TIPO	2013	2014	2015	% RELATIVO	Δ% 2014/2015
Reclamaciones de tutela de derechos	2.108	1.818	2.113	16,27	16,23
Denuncias	8.633	9.404	10.871	83,73	15,60
TOTAL	10.741	11.222	12.984	100	15,70

Grafica 1. “Denuncias y reclamaciones en España por protección de Datos Personales, Fuente: Agencia Española de Protección de Datos” [58]

SANCIONES ECONÓMICAS IMPUESTAS						
	2012	2013	2014	2015	Δ% 2014/2015	
TOTAL SANCIONES	21.054.656,02	22.339.440	17.002.622	13.712.621	-19,35	
ÁREAS CON MAYOR IMPORTE GLOBAL DE SANCIONES						
ACTIVIDAD	2012	2013	2014	2015	% RELATIVO DEL TOTAL 2015	Δ% 2014/2015
Telecomunicaciones	15.368.938	15.035.008	10.750.502	7.090.004	51,70	-34,05
Entidades financieras	2.853.004	1.811.501	2.018.501	2.395.902	17,47	18,70
Suministro y comercialización de energía/agua	1.270.001	2.084.901	1.862.900	1.205.002	8,79	-35,32
Comunicaciones electrónicas comerciales – spam (LSSI)	541.507	526.010	645.506	897.403	6,54	39,02
Organizaciones asociativas incluyendo partidos políticos y sindicatos	147.202	40.400	19.800	525.500	3,83	2.554,04*
Publicidad (excepto spam)	137.000	481.004	751.411	502.108	3,66	-33,18
TOTAL DE LAS 6 PRIMERAS ACTIVIDADES	20.317.652	19.978.824	16.048.620	12.615.919	92	-21,39

Grafica 2. Denuncias y reclamaciones en España por protección de Datos Personales, Fuente: Agencia Española de Protección de Datos [59]

Después de validar las sanciones que ha impuesto Colombia en comparación con España por la protección de Datos se puede denotar que la normatividad española impone sanciones que se encuentran tipificadas en tres grupos que son infracciones muy graves, las cuales hacen referencia a la cesión de datos de carácter personal sin contar con la legitimación cuando los datos hacen referencia a ideología, afiliación sindical, religión o creencias, al origen racial, salud, vida sexual y datos referentes a la comisión de infracciones penales o administrativas, graves se refieren a la cesión de los datos de carácter personal sin contar con la legitimación para ello y leves que son el incumplimiento del deber de información al afectado acerca del tratamiento de sus datos de carácter personal cuando los datos sean obtenidos por el propio interesado. Las multas que impone España son superiores en cuantía en referencia con Colombia lo que lleva a que la

normatividad Española pueda hacer que las empresas que incumplan con lo establecido en la Ley de Protección de Datos den cierre de las mismas, mientras que en Colombia solo se impone la sanción monetaria y los datos de las personas siguen siendo utilizados.

CONCLUSIONES DEL DERECHO COMPARADO DERECHO LEY ORGÁNICA 15/1999 - LEY ESTATUTARIA 1581 DE 2012

- En Colombia con la expedición de la Ley 1581 de 2012 forma parte de los países que cuentan con una regulación adecuada y adicionalmente cuenta con ente que vigila y ejerce control sobre la protección de los datos.
- La protección de datos se concibió como un derecho fundamental, autónomo e independiente que se deriva de la vida privada, familiar, dignidad humana, confiriendo al titular de la información a reservar todo lo relacionado con su información.
- La Ley de protección de Datos personales es un instrumento jurídico que potencializa el adecuado manejo y uso de la información.
- En las terminologías de intimidad y privacidad se puede concluir que la intimidad forma parte de la privacidad aunque las dos terminologías son reservadas.

PAÍS	LEY	AÑO DE PUBLICACIÓN	REFORMAS DE LA NORMA
ESPAÑA	Ley Orgánica 15/99 Protección de Datos de Carácter Personal	13 de mayo de 1999	Entrará en vigor el 25 de mayo de 2018, según como lo plantea la Unión Europea
CHILE	la Ley 19.628 de Protección de Datos de carácter personal	28 de agosto de 1999	Se encuentra en discusión la reforma de la normatividad según como lo plantea la Unión Europea
COLOMBIA	la Ley 1581 de 2012 Protección de Datos	17 de Octubre del 2012.	Colombia no ha planteado un cambio en la normatividad

Tabla 11. Año de creación de las leyes y las nuevas reformas. Fuente propia

CONDICIONES PARA EFECTUAR TRANSFERENCIAS INTERNACIONALES DE DATOS								
PAÍS	CARACTERÍSTICAS DE LA NORMATIVA							
ESPAÑA	Nivel de protección adecuado o equivalente	Comunicación a la ANPD	Autorización de la ANPD	Consentimiento y/o conocimiento del titular	Cumplimiento de tratados internacionales	Prevención, diagnóstico, asistencia o tratamientos médicos (interés vital del titular)	Cumplimiento de relaciones jurídicas, contractuales o pre-contractuales	Prevista legalmente/ Requerida por autoridad judicial
COLOMBIA	No cuenta con el nivel adecuado según la normativa Europea		Autorización de la ANPD	Consentimiento y/o conocimiento del titular		Prevención, diagnóstico, asistencia o tratamientos médicos (interés vital del titular)	Cumplimiento de relaciones jurídicas, contractuales o pre-contractuales	Prevista legalmente/ Requerida por autoridad judicial
CHILE	No cuenta con el nivel adecuado según la normativa Europea			Consentimiento y/o conocimiento del titular	Cumplimiento de tratados internacionales			

Tabla 12. Condiciones para efectuar transferencia Internacional de Datos. Fuente propia

Teniendo en cuenta las recomendaciones que realiza la Unión Europea para la transferencia de datos internacionales en la tabla se encuentran definidas algunas características y se evalúa si en los países que se tomaron como referentes han establecido algunas de estas recomendaciones, una definición es establecer si la normatividad cuenta con el nivel adecuado de protección de datos.

Para realizar la circulación fronteriza de datos es necesario que se brinde la apropiada protección, el respeto y la garantía de los derechos de los titulares aspectos mínimos que se procuran al realizar la transferencia internacional. No se trata solo de proteger la información si no salvaguardar los derechos de los titulares cuando su información es enviada a otro país.

Continuando con el análisis de las características los tres países han definido el consentimiento del titular en sus normativas.

España y Chile han tenido en cuenta el cumplimiento de tratados internacionales mientras que Colombia no lo tiene definido en la normatividad actual.

Es así que debido a la integración económica, social y cultural entre otras cosas exportar e importar los datos personales entre Estados ha aumentado significativamente y seguirá acrecentándose debido al crecimiento de usuarios en internet y la inmersión masiva de las TIC en el mundo.

6. RETOS REGULATORIOS

En el estudio realizado a lo largo de la investigación se encuentra como reto regulatorio para la normatividad la transferencia de datos internacionalmente debido a que la ausencia en la normatividad general de protección de datos personales añade principios básicos y adicionales que contienen el tratamiento de esta información.

Si bien la ley 1266 de 2008 incorporó reglas para la transferencia internacional de datos como se estipula en el artículo 5 del numeral lo cual cita *“la información personal suministrada de conformidad con lo dispuesto con la ley a los operadores que hagan parte del Banco de datos que administra, podrá ser entregada de manera verbal, escrita o puesta a disposición de las siguientes personas y en los siguientes términos;”* [60] f) (..) queda expuesta a disposición del titular de la base de datos, lo cual no garantiza que se le brinde la debida protección en los datos personales a los usuarios. Pero determinar si el banco de datos de un tercer país garantiza el tratamiento adecuado para la información de los Colombianos no quedo bajo la responsabilidad de la autoridad Colombiana si no en cabeza de los operadores.

Esta disposición permite la transferencia internacional de datos sin garantías ni control a las personas, lo que con lleva desconocimiento y graves implicaciones para el país y los ciudadanos por la transferencia indebida internacionalmente.

Los datos personales han tomado relevancia gradualmente en lo social y la economía, haciendo que se tilde como “la nueva moneda del mundo digital o el nuevo petróleo de la internet” [61] La información se ha convertido en un bien que comercializan a nivel nacional e internacional permitiendo que con la información recolectada puedan nutrir sus bases de datos. La recolección de información se

hace de manera imperceptible, como también la circulación de la misma permitiendo que se transfieran y traspasen las fronteras.

Es así que diariamente, se puede denotar como se recolectan datos desde el exterior, convirtiéndose en un fenómeno que crece a medida que aumenta la participación de personas que tienen acceso a internet en el mundo. Cualquier persona que se encuentre en otro país puede denotarse como un recolector internacional de información. Esta situación se convierte en una actividad incontrolable que genera retos a las autoridades designadas para velar por los derechos de aquellos que sean vulnerados por la recolección de datos en otros países y por el cumplimiento de la normatividad.

Europa es pionera en diseñar formas jurídicas para la circulación de los datos en terceros países, una de las exigencias que ha creado hace referencia a que el país con el cual se desee realizar la transferencia cuente con el nivel adecuado como se encuentra plasmado en el estándar Europeo.

“Colombia al igual que otros países latinoamericanos aún no ha sido considerada como un país garante en la protección de datos” [62] según la Comisión Europea para que pueda ser considerado con el nivel adecuado debe cumplir con tres puntos básicos como lo son, que la protección jurídica de la información ciudadana aumente ya que el modelo europeo se caracteriza por ser riguroso en este aspecto, otra de las características es garantizar que el país sea lo suficientemente competitivo para que se puedan realizar negocios que involucren transferencia de información personal, la tercera característica se basa en la efectiva protección de los datos.

Las empresas y el gobierno constantemente realizan transferencia de datos personales bien sea por seguridad nacional, investigaciones de terrorismo, seguridad pública, inteligencia militar o policial, call centers, entre muchos otros,

esto es conocido como “movimiento internacional de datos o flujo transfronterizo de datos” [63]

En diferentes documentos publicados por organizaciones internacionales han determinado que para realizar la transferencia de datos personales de un país a otro se debe garantizar que el país importador tenga el nivel adecuado de protección de los datos personales. La palabra “adecuado” se refiere a que tanto el país que exporta como el que importa tengan un grado de protección superior o equivalente al país exportador. Pablo Palazzi cita, “evitar la creación de paraísos informáticos, es decir, jurisdicciones donde la carencia de leyes de protección de datos, las transforme en sitios atractivos para realizar tratamientos de datos personales que puedan ser violatorios de otras leyes de privacidad” [64]

Debido a que no todos los países cuentan con una normatividad de protección de datos uniforme, la directiva 95/46/CE, el convenio 108 de 1981 y las directrices de la Organización para la Cooperación y el Desarrollo Económico, dictaminan que los elementos mínimos que debe tener la ley de protección de datos.

Una vez realizado este análisis se denota que Colombia presenta retos regulatorios la transferencia de datos a nivel internacional ya que en la normatividad expedida en el año 2012 no queda estipulado la debida protección que se debe tener para ser garante de la transferencia de información con terceros países; en la ley del Habeas Data se hace mención a un posible acercamiento de lo que se debería regular pero debido a que esta ley se enfocó en la parte financiera no cumple con lo que actualmente se requiere.

Otro retro que se encuentra en la normatividad de protección de datos personales son las sanciones que impone el ente regulador cuando las entidades incumplen lo establecido, es decir si una empresa incumple lo que dicta la ley el ente regulador impone la sanción monetaria máxima pero los datos siguen quedando

disponibles por la entidad que los recolecto, no se garantiza que los datos se les brinde el debido tratamiento, adicional a esto las políticas de protección, las notificaciones a los usuarios, publicación de manuales y la claridad sobre las formas en que las entidades pueden bloquear, suspender servicios no son claras para los usuarios resulta confuso.

Adicional a este estudio que se realiza de la normatividad para identificar los retos regulatorios se realiza la retrospectiva de estrella de mar que es un análisis en el que se presenta en cinco partes que son:

Empezar a hacer: Que nos gustaría que se desarrolle para realizar una mejora teniendo en cuenta el riesgo que de la novedad.

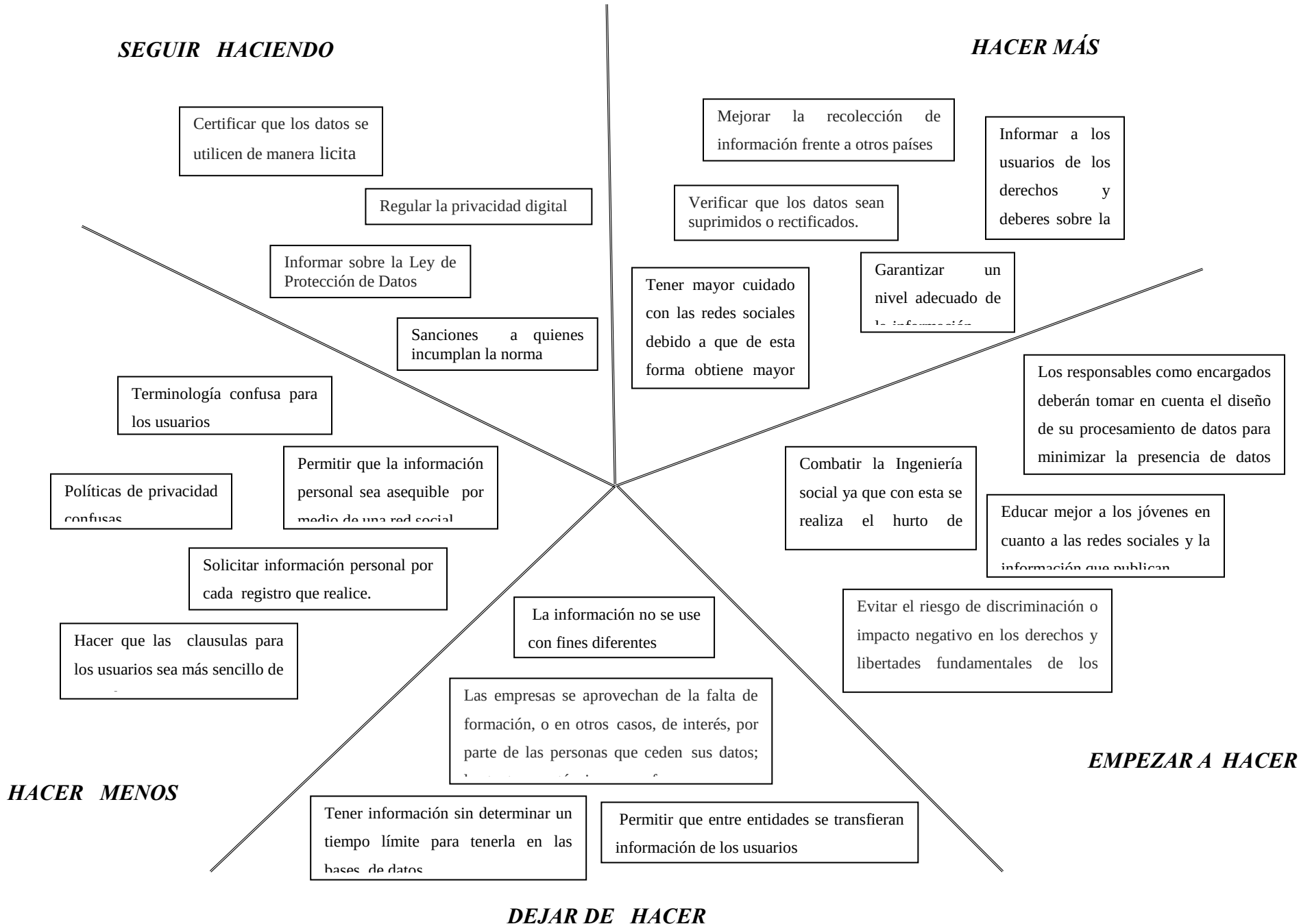
Hacer más: Son aquellas que aportan valor para que son la parte positiva del desarrollo que se está realizando.

Seguir haciendo: Son las que aportan valor y se deben seguir fortaleciendo como se están realizando.

Hacer menos: Son aquellas que no ayudan al objetivo que se tenía planteado lo cual lleva a realizar cambios.

Dejar de hacer: Son aquellas de no agregan valor y por lo cual es mejor eliminarlas

STARFISH RETROSPECTIVA ESTRELLA DE MAR



RECOMENDACIONES BASADAS EN LOS RETOS REGULATORIOS IDENTIFICADOS

Como se analizó anteriormente, la normatividad Colombiana presenta como retos regulatorios la transferencia de datos a terceros países, políticas de protección y las sanciones que impone el ente regulador a las entidades

La libre circulación de los datos transfronteriza, la apropiada protección de datos, el respeto, la garantía de los derechos de los titulares de la información son aspectos que se deben tener en cuenta cuando se realiza la transferencia internacional de datos. Es así que no solo se trata de proteger la información del titular, si no que proteger los derechos de las personas cuando su información es transmitida a otro país.

Algunos documentos internacionales realizan recomendaciones como la Unión Europea como lo cita en el “El Convenio 108 del Consejo de Europa, del 28 de enero de 1981, establece las pautas para proteger las personas respecto al tratamiento automatizado de datos de carácter personal. En primer lugar, un Estado parte del Convenio no puede, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte. En segundo lugar, un Estado parte puede prohibir o someter a autorización especial el flujo internacional de datos cuando se desee enviar información personal a un Estado no contratante, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la parte contratante,” [65] recomendaciones que ayudan a que el país importador garantice un nivel adecuado de protección de datos.

La palabra “adecuado” hace referencia a que el país importador tenga establecido en su normatividad un grado de protección superior, igual o similar al país exportador” [66]

Es debido a esto que se realiza la recomendación para la normatividad Colombiana fortalecer y contar con un control efectivo ya que las personas se encuentran vulnerables al realizar esta acción, se propone en un capítulo especificar la forma adecuada de realizar la transferencia de datos a terceros países.

También es importante resaltar que las políticas que plantean para la protección de los datos sean más claras para los usuarios, sencillas de entender ya que esto va dirigido a toda la población.

Por parte de la Superintendencia de Industria y Comercio ente que ha sido encargado de velar por la protección de datos e impone las sanciones requeridas cuando se incumple lo que establezca la ley, se sugiere que no solo sea el ente que impone correctivos si no que los datos que han sido recolectados por estas empresas que no siguen los lineamientos que establece la normatividad le garanticen al usuario que los datos que reposan en sus bases de datos se les dará el tratamiento adecuado y la protección.

Concluyendo y con respecto a la recopilación de la normatividad en Protección de Datos, Colombia goza de un marco regulatorio que ha crecido que ha estado acompañada por decretos y resoluciones que reglamentan el sector, lo cual es un buen indicio que nuestro país busca un cambio para estar a la vanguardia. Sin embargo, por la constante evolución tecnológica se hace necesario realizar actualizaciones y modificaciones a la normatividad de Protección de Datos Personales debido a que carece de temáticas que son de gran importancia como lo es la transferencia internacional de datos, políticas más claras y revisión de las sanciones a las empresas, tener presente las recomendaciones que realiza la Unión Europea y catalogar a Colombia como un país garante.

CONCLUSIONES

Dando un vistazo general respecto a la protección de datos se podría decir que aparentemente a nivel mundial se encuentra bien establecida y encaminada hacia el objetivo principal por el cual se dictaron las normas que inicialmente se establecieron, que fue proteger a los ciudadanos del abuso que se venía presentando por el almacenamiento y mal uso de los datos.

Pero a pesar que los gobiernos promotores y creadores de la normatividad intenten aplicar correctamente lo establecido y sancionar a entes privados y públicos los ciudadanos no se siente seguros en la transferencia internacional de datos ya que no garantiza que el respeto y el derecho de los titulares. Si bien es cierto llegar a garantizar la protección de los datos a un 100% es muy difícil debido al avance tecnológico que se presenta día a día en el mundo de las TIC.

Es así que la protección de datos es un derecho que se deriva de la vida privada y la intimidad de las personas, datos que se encuentran en riesgo debido a la manera en que se modifica, almacena y distribuye la información. En esta búsqueda de protección se crea la normatividad, estableciendo límites y también principios básicos para la sociedad. Es por eso que al realizar la investigación se concluye:

1. La terminología que se utiliza para Protección de Datos debería ser global debido a que cuando se realiza la transferencia siempre se envían o reciben datos.
2. La protección de datos personales promueve el respeto a la privacidad y la integridad de los mismos, siendo una forma de controlar el uso que las entidades le dan a los datos de los usuarios y vela porque estos datos se

administren conforme lo dicta la ley, con lo cual no se asegura el correcto uso debido a que la tecnología tiene muchas variables que hacen casi imposible que los ciudadanos perciban cuando alguien esté haciendo un uso indebido de sus datos.

3. La Ley fue diseñada para garantizar la protección de datos personales y la efectividad frente a actos indebidos en cada territorio nacional, pero no tiene el nivel adecuado para el intercambio de información con otros países
4. Actualmente la sociedad se encuentra en la era de la “sociedad de la información” en donde continuamente se intercambian datos, siendo información valiosa y utilizada para diferentes fines.
5. La ley 1266 de 2008 “Hábeas Data” es insuficiente para aseverar que Colombia tiene un marco legal apropiado para la protección de datos y la transferencia de los mismos.
6. Se considera que para mejorar la protección de datos personales de los ciudadanos se deberá realizar modificaciones a la normatividad vigente para que quede estipulado la debida protección en la transferencia internacional de los mismos.
7. La normatividad vigente presenta una necesidad de establecer reglas generales e integrales para el tratamiento de datos personales cuando se realiza su transferencia
8. La normatividad de protección de datos requiere una revisión ya que no todos los aspectos cumplen con la finalidad deseada y para mejorar y tener un riguroso control sobre la protección que se desea brindar a los ciudadanos

9. Las políticas que plantean las entidades debe tener un lenguaje más claro y menos técnico para que los usuarios comprendan los riesgos a que se acogen cuando brindan su información personal y el tratamiento que se le dará.
10. Se sugiere una revisión de la normatividad actual para actualizar aspectos que presentan falencias como la transferencia internacional, políticas, sanciones y tener en cuenta las recomendaciones que realiza la Unión Europea para mitigar este tipo de inexactitudes que se han presentado.
11. Era importante tomar a España para la investigación porque es un país promotor de la Protección de Datos Personales, ya que con las reformas que ha rerealizado ha logrado resultados con impacto a nivel Internacional y sirve de referente para otros países.
12. Continuar en la participación de foros Internacionales y Nacionales abiertos a los ciudadanos para formentar la cultura de la protección
13. Realizar auditorias externas a la entidad reguladora de protección de datos, para así fortalecer aspectos que se estén pasando
14. Adopción de medidas de seguridad para la recolección y ciclo de vida del dato personal

ANEXO A.

PORQUÉ UNA INFOGRAFÍA

La infografía es un medio de comunicación visual en el cual se puede describir un proceso o un relato que permite captar, entender o asociar con mayor claridad la información o informaciones que se deseen dar a conocer. En Colombia la población lectora año tras año disminuye, estudios recientes realizados por Colciencias informan que desde el año 2010 se ha reducido en un 11,2% de los lectores, es por esto que la infografía aporta por medio de las ilustraciones una manera más fácil de entender la normatividad de protección de datos y la seguridad de la información. Pero si bien es cierta la frase que dice que el desconocimiento de la norma no nos excluye de cumplirla también es válido que para el cumplimiento de la ley se debe primero identificarla y entenderla. Siendo indiscutible que la capacidad de comprensión de nuestros derechos y de los medios que disponemos para defendernos depende de la facilidad para entender la norma jurídica que aplique a la necesidad de cada persona.

Como se ha dicho la infografía es un estilo o una tendencia la cual permite captar la atención del lector obteniendo su mayor atención por medio de estímulos visuales de manera cómoda y sencilla por los colores, simplicidad y claridad del texto logrando así captar al lector rápidamente.

La infografía es un material que fácilmente se puede difundir en las redes sociales como Facebook, twitter, periódicos, páginas web, etc., lo que hace que sea atractivo para el lector.

Algunas características de la infografía son: permite crear un mensaje claro y visual que resume las ideas en pocas líneas, capta la atención del lector a través de la vista, ayuda a recordar más fácilmente un concepto, se puede compartir por las redes sociales y está comprobado por un estudio que realizó 3M corporation que el 90% de la información transmitida al cerebro es visual y las imágenes se procesan más rápido en el cerebro que el texto.

REFERENCIAS

- [1] P. Óscar, El habeas data en Indoiberoamérica, Sobre el habeas data,, Bogotá: Temis, 1999.
- [2] *Sentencia C-355/06*, 2012.
- [3] *Diario Oficial N.47219.*, 2008.
- [4] C. d. I. R. d. Colombia, «Qué es una Ley,» Enero 09 2015. [En línea]. Available: <http://www.senado.gov.co/legales/item/11164-que-es-una-ley>. [Último acceso: 10 Octubre 2017].
- [5] R. A. Española, «Diccionario Real Academia Española,» 10 Octubre 2014. [En línea]. Available: [http://dle.rae.es/?id=Bskzsq5\[BsnXzV1](http://dle.rae.es/?id=Bskzsq5[BsnXzV1). [Último acceso: 01 Mayo 2017].
- [6] C. Definición, «Definición de Datos,» 18 Abril 2015. [En línea]. Available: <http://conceptodefinicion.de/datos/>. [Último acceso: 25 Noviembre 2016].
- [7] *Proyecto de Ley Estatutaria No.27/06*, 2008.
- [8] *Sentencia 1011-08*, 2008.
- [9] *Sentencia T- 414 de 1992*, 2011.
- [10] *Ley 1581 de 2012*, 2012.
- [11] *Decreto 1377*, 2013.
- [12] S. d. I. y. Comercio, «Manejo de Información personal "Habeas Data",» [En línea]. Available: <http://www.sic.gov.co/manejo-de-informacion-personal>. [Último acceso: 20 Noviembre 2016].
- [13] P. André, «OECD Guidelines on the Protection of Privacy,» 2002. [En línea].

Available: <http://www.oecd.org/sti/ieconomy/15590267.pdf>. [Último acceso: 20 Febrero 2016].

[14] «Convenio 108 de 1981,» 28 Enero 1981. [En línea]. Available: <http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DCONVENIO%2520108.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1202800216772&ssbinary=true>. [Último acceso: 20 Febrero 2016].

[15] *Diario Oficial No.281*, 1995.

[16] L. A. Rallo, «Estandares Internacionales sobre protección de Datos Personales y Privacidad,» 05 Noviembre 2005. [En línea]. Available: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf. [Último acceso: 20 Febrero 2016].

[17] M. Schulz, «Access to European Union Law,» 27 Abril 2016. [En línea]. Available: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>. [Último acceso: 20 Febrero 2016].

[18] R. Nelson, Definición de Dato Personal en Documentos Internacionales, Bogotá: Legis, 2013, p. 135.

[19] *Diario Oficial 44097*, 2000.

[20] *Corte Constitucional*, 1995.

[21] *Cfr. Corte Constitucional, Sentencia T-261*, 1995.

[22] *sentencia T-729*, 2002.

[23] *Diario Oficial 48834*, 2013.

- [24] *Cfr. Corte Constitucional, Sentencia T-729, 2002.*
- [25] *ley 1581 de 2012. Cfr. Literal b) del artículo 10, 2012.*
- [26] *Decreto 1377 de 2013, artículo 5, 2013.*
- [27] *Ley 1266 de 2008- Cfr. Literal g) del artículo 3°, 2008.*
- [28] *Artículo 5° de la Ley 1581 de 2012,, 2012.*
- [29] C. d. Europa, «Convenio 108,» 28 Enero 1991. [En línea]. Available: <http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DCONVENIO%2520108.pdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1202800216772&ssbinary=true>. [Último acceso: 20 Febrero 2016].
- [30] O. d. I. N. Unidas, «Resoluciones Aprobadas por la Asamblea General durante el 45° período de sesiones,» 14 Diciembre 1990. [En línea]. Available: <http://www.un.org/es/documents/ag/res/45/list45.htm>. [Último acceso: 01 Marzo 2016].
- [31] S. d. I. y. Comercio, «Superintendencia de Industria y Comercio,» Bogotá, 2013.
- [32] S. d. I. y. Comercio, «Sobre la Protección de Datos Personales,» 10 Febrero 2016. [En línea]. Available: <http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales>. [Último acceso: 20 Enero 2017].
- [33] S. d. I. y. Comercio, «Qué es la Delegatura de Protección de Datos,» [En línea]. Available: <http://www.sic.gov.co/que-es-la-delegatura-datos-personales>. [Último acceso: 02 Febrero 2017].
- [34] *Diario Oficial N. 47219, 2008.*

- [35] *Diario Oficial* 48587, 2012.
- [36] *Diario Oficial* 49084, 2014.
- [37] R. A. Nelson, «¿Tiene Colombia un nivel adecuado de Protección de Datos Personales,» *Revista Colombiana de Derecho Intenacional*, pp. 489- 524, 2010.
- [38] *Sentencia C-748*, 2011.
- [39] Certicamara, «ABC para proteger los Datos Personales, Ley 1581 de 2012, Decreto 1377 de 2013,» 29 Agosto 2013. [En línea]. Available: <https://colombiadigital.net/actualidad/articulos-informativos/item/5543-abc-para-proteger-los-datos-personales-ley-1581-de-2012-decreto-1377-de-2013.html>. [Último acceso: 04 Febrero 2017].
- [40] *Diario Oficial* 43.673, 1999.
- [41] *Diario Oficiial* 47.219, 2008.
- [42] *Sentencia C-1011*, 2008.
- [43] *Sentencia T- 414*, 1992.
- [44] «Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal,» 13 Diciembre 1999. [En línea]. Available: <https://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>. [Último acceso: 15 Febrero 2017].
- [45] *Ley Orgánica 15/1999, De Protección De Datos De Carácter Personal*, 1999.
- [46] *Ley Orgánica 15/1999, De Protección De Datos De Carácter Personal. Art. 4*, 1999.
- [47] C. L. Rafael, «Biblioteca del Congreso Nacional de Chile,» 06 Agosto 1999. [En línea]. Available: <https://www.leychile.cl/Navegar?idNorma=141599>. [Último acceso: 15 Marzo 2016].

- [48] B. d. C. N. d. Chile, «Sobre acceso a la Infomación Pública,» 20 Agosto 2008. [En línea]. Available: http://www.oas.org/juridico/spanish/mesicic3_chl_sc_anex10.pdf. [Último acceso: 15 Marzo 2016].
- [49] Z. Andrés, «Senado de la República de Chile,» 15 Abril 2015. [En línea]. Available: <http://www.senado.cl/appsenado/index.php?mo=sesionessala&ac=getCuenta&iddocto=55807>. [Último acceso: 10 Marzo 2016].
- [50] P. E. Sebastian, «Modificaciones a la Ley 19.628,» 25 Noviembre 2011. [En línea]. Available: <http://www.oas.org/es/sla/ddi/docs/CH4%20Proyecto%20de%20Ley%20que%20Modifica%20la%20ley%20N%2019628.pdf>. [Último acceso: 12 Marzo 2016].
- [51] C. Alberto, Legislación sobre Protección de las personas frente al tratamiento de Datos Personales, Chile: Centro de Estudios en Derecho Informático, 2012.
- [52] *Ley 19.628 - Artículo 2º f)*, 1999.
- [53] *Ley 19.628 - Artículo 2º g)*, 1999.
- [54] *Ley 19.628 - Artículo 2º d)*, 1999.
- [55] *Ley 19.628, Artículo 2º e)*, 1999.
- [56] *Ley 19628 Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal*, 1999.
- [57] S. I. y. Comercio, «Sanciones por violación de Datos Personales,» 08 Junio 2017. [En línea]. Available: <http://www.sic.gov.co/noticias/por-violaciones-de-datos-personales-superindustria-ha-impuesto-sanciones-por-mas-de-21-mil-millones-de-pesos>. [Último acceso: 23 Agosto 2017].
- [58] A. E. d. P. d. Datos, 20 Enero 2017. [En línea]. Available: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/index-ides->

idphp.php. [Último acceso: 23 Agosto 2017].

[59] A. E. d. P. d. Datos, «Denuncias y Sanciones por Protección de Datos,» 20 Enero 2017. [En línea]. Available: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/index-ides-idphp.php>. [Último acceso: 23 Agosto 2017].

[60] *Ley 1266*, 2008.

[61] M. Kuneva, «La Protección de los Datos Menores,» Bogotá, 2009.

[62] N. R. Anagrita, «Tiene Colombia un nivel Adecuado de Protección de Datos,» 12 Marzo 2010. [En línea]. Available: <http://www.scielo.org.co/pdf/ilrdi/n16/n16a15.pdf>. [Último acceso: 23 Noviembre 2016].

[63] D. G. Ana, Tratamiento de datos personales y derechos fundamentales, Madrid: Dykinson, 2004.

[64] P. Pablo, Comercio electrónico, transferencia internacional de datos personales y armonización de leyes en un mundo globalizado, Bogotá: Legis, 2013.

[65] R. N. Angarita, ¿TIENE COLOMBIA UN NIVEL ADECUADO DE PROTECCIÓN DE DATOS PERSONALES LA LUZ DEL ESTÁNDAR EUROPEO, Bogotá: Legis, 2010.

[66] R. N. Angarita, Tratamiento de Datos Personales, Bogotá: Legis, 2013.

[67] M. W. a. S. Thilakawardana, «Initial Analysis of TV White Space,» BBC, UK, 2012.

[68] S. d. I. y. Comercio, «Delegatura de la Protección de Datos,» 23 Febrero 2016. [En línea]. Available: <http://www.sic.gov.co/historia..> [Último acceso: 29 Enero 2017].

[69] *Diario Oficial* 43.673, 1999.

[70] *Diario Oficial* 43.673, 1999.

[71] *Diario Oficial* 47.223, 2009.

[72] «Consagra el Derecho a Protección de los Datos Personales,» 11 Junio 2014. [En línea]. Available: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9384-07. [Último acceso: 23 Marzo 2016].

[73] «Modificaciones a la Ley 19.628,» 25 Noviembre 2011. [En línea]. Available: <http://www.oas.org/es/sla/ddi/docs/CH4%20Proyecto%20de%20Ley%20que%20Modifica%20la%20ley%20N%2019628.pdf>. [Último acceso: 23 Marzo 2016].

[74] «Protección de Datos Personales vinculado con el derecho a la vida privada,» 01 Junio 2001. [En línea]. Available: <http://www.derecho-chile.cl/rol-2-299-2001-proteccion-de-datos-personales-vinculado-con-el-derecho-a-la-vida-privada/>. [Último acceso: 23 Marzo 2016].

[75] P. Pablo, «Protección de Datos Personales,» 26 Junio 2014. [En línea]. Available: <http://www.derecho-chile.cl/proteccion-de-datos-personales-ii-parte/>. [Último acceso: 23 Marzo 2016].

[76] S. R. Chile, «Boletín N° 6.987-07,» 16 Junio 2010. [En línea]. Available: <http://www.senado.cl/appsenado/templates/tramitacion/index.php>. [Último acceso: 23 Marzo 2016].

[77] B. L. Palma Pablo, «Protección de Datos Personales,» 26 06 2014. [En línea]. Available: <http://www.derecho-chile.cl/proteccion-de-datos-personales-parte/>. [Último acceso: 10 Mayo 2017].

[78] C. P. d. Chile, «Biblioteca del Congreso Nacional de Chile,» 28 Agosto 2005. [En línea]. Available: http://www.bcn.cl/pags/legislacion/leyes/constitucion_politica.htm. [Último acceso: 05 Julio 2017].

[79] *Constitución Política De Colombia*, 1999.

[80] *Ley 19628 Sobre Protección de la Vida Privada*, 1999.

LISTA DE GRAFICAS

GRAFICA 1. DENUNCIAS Y RECLAMACIONES EN ESPAÑA POR
PROTECCIÓN DE DATOS PERSONALES, FUENTE: AGENCIA ESPAÑOLA DE
PROTECCIÓN DE DATOS 99

GRAFICA 2. DENUNCIAS Y RECLAMACIONES EN ESPAÑA POR
PROTECCIÓN DE DATOS PERSONALES.....100

LISTA DE TABLAS

TABLA 1. DEFINICIÓN DE DATO PERSONAL EN DOCUMENTOS INTERNACIONALES.....	28
TABLA 2. DEFINICIÓN DE DATO SENSIBLE EN DIVERSOS DOCUMENTOS NTERNACIONALES.....	35
TABLA 3. ESTUDIO BIBLIOGRÁFICO CHILE, ESPAÑA, COLOMBIA.....	68
TABLA 4. ESTUDIO BIBLIOGRÁFICO- CARACTERÍSTICAS CHILE, ESPAÑA, COLOMBIA.....	70
TABLA 5. ESTUDIO BIBLIOGRÁFICO- CARACTERÍSTICAS EN PAÍSES CHILE, ESPAÑA, COLOMBIA.....	72
TABLA 6. ESTUDIO BIBLIOGRÁFICO- CARACTERÍSTICAS CHILE, ESPAÑA, COLOMBIA.....	76
TABLA.7 DERECHO COMPARADO ENTRE CHILE Y COLOMBIA.....	81
TABLA. 8 ANÁLISIS DE LEYES DE PROTECCIÓN DE DATOS EN PAÍSES COMO ESPAÑA, CHILE Y COLOMBIA.....	86
TABLA 9.DERECHO COMPARADO LEY ORGÁNICA 15/199- LEY ESTATUTARIA 1581/2012.....	91

TABLA 10. AÑO DE CREACIÓN DE LAS LEYES Y LAS NUEVAS REFORMAS.....	96
TABLA 11. CONDICIONES PARA EFECTUAR TRANSFERENCIA INTERNACIONAL DE DATOS.....	102
TABLA 12. PRINCIPIOS MÍNIMOS EN PROTECCIÓN DE DATOS SEGÚN ESTÁNDAR EUROPEO.....	103