# PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA Y SU POSIBLE AFECTACIÓN POR TERCEROS.

# PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA Y SU POSIBLE AFECTACIÓN POR TERCEROS.

LEONILDE PERDIGON CORREA,
CÉSAR AUGUSTO CIFUENTES ACOSTA

UNIVERSIDAD LA GRAN COLOMBIA
PROGRAMA DE POSGRADO
DERECHO ADMINISTRATIVO
BOGOTÁ
2016.

# PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA Y SU POSIBLE AFECTACIÓN POR TERCEROS.

LEONILDE PERDIGON CORREA,
CÉSAR AUGUSTO CIFUENTES ACOSTA

Presentado a:
DR. JOSE IGNACIO GONZALEZ

UNIVERSIDAD LA GRAN COLOMBIA
PROGRAMA DE POSGRADO
DERECHO ADMINISTRATIVO
BOGOTÁ
2016.

***DEDICATORIA:***

"A todas aquellas personas o entidades que han visto vulnerado su Derecho a la Confidencialidad y han quedado expuestas a la indeterminada utilización de sus Datos Personales"

Leonilde Perdigon Correa y
César Augusto Cifuentes Acosta

## ***AGRADECIMIENTOS.***

Este trabajo fruto de nuestra investigación y nuestro empeño queremos dedicarlo a nuestras familias (por su paciencia), a nuestros maestros (por ser nuestros guías), y compañeros (por sus valiosas criticas) pero antes que todo a nuestro creador fuente de amor y sabiduría.

*Por último, agradecemos a la Universidad La Gran Colombia por permitir espacios y escenarios importantes que motivan al estudiantado a realizar investigaciones, que aportan de alguna manera al desarrollo educativo no solo de un plantel académico, sino también a todo un país*.

RESUMEN.

Decir que la información en general en los últimos tiempos se le ha dado mayor relevancia que antes lo consideramos una falacia. Desde tiempos atrás se ha sabido que la humanidad ha vivido entorno a la información, ejemplo de ello fue en 1944 cuando se dio fin la segunda guerra mundial donde la historia nos enseña que quienes pudieron administrar en debida forma la información, fueron quienes lograron una victoria sin antecedentes al engañar a los Alemanes haciéndolos creer que les atacarían por un territorio distinto al de Normandía, que fue allí donde se desarrolló el hecho determinante el que casi todos conocemos como “EL DÍA D” en la Operación Overlord. Así como dicho acontecimiento, hubieron varios que marcaron a la humanidad como el “9-11” en Estados Unidos, que ocasiona que dicho país cambiara su perspectiva en cuanto a la información privada no solo de sus nacionales, sino también en todo el mundo, incluso líderes mundiales. Pero más allá de todo suceso histórico, notamos un fenómeno acá en Colombia en donde nos ha estado afectando a todos pero que hasta hace poco menos de 10 años el gobierno se ha empezado a interesar para hacer frente a lo que ya nos venía cogiendo ventaja hace muchos años atrás, La Tecnología, La Internet y Las Redes Sociales. Así las cosas, consideramos que se debe estudiar varios mecanismos creados por el Gobierno donde deben garantizar la tranquilidad de cada persona que cuenta con unos derechos fundamentales los cuales no pueden ni deben ser vulnerados por ningún tercero.

PALABRAS CLAVES.

DATOS PERSONALES, ENCARGADO DEL TRATAMIENTO, HABEAS DATA, TRATAMIENTO DE DATOS, TITULAR DEL DATO PERSONAL, USUARIO, ADMINISTRADOR DE INFORAMCIÓN.

SUMMARY.

To say that the information in general in recent times has been given greater importance we consider it a fallacy before. Since time ago it has been known that mankind has lived environment to information, example was in 1944 when it finally gave the Second World War where history teaches us that those who could manage duly information were who achieved a victory no history to fool the Germans into believing that they would attack by a different Normandy territory, which was where the determining fact is that almost all know as "D-Day" in Operation Overlord developed. As this event, there were several that marked humanity as the "9-11" in the United States, which causes the country to change its perspective on private information not only national, but also around the world, even world leaders. But beyond any historical event, we noticed a phenomenon here in Colombia where we have been affecting all but to just under 10 years, the government has become interested to deal with what we had already been taking advantage ago many years ago, technology, Internet and social networks. So, we believe that should be studied several mechanisms created by the government which should guarantee the tranquility of each person who has some fundamental rights which can´t and should not be violated by any third party.

CONTENIDO.

Pág.

## INTRODUCCION.

Vivimos en un mundo de avances significativos en diferentes campos, como lo son entre ellos el auge e imposición de las tecnologías informáticas, haciendo que cada uno de los países no solo se dé a la tarea de su implementación para ser competitivos a nivel mundial, sino a legislar sobre el tema. Ahora bien, si bien es cierto la globalización trae consigo nuevos mercados , generando con ellos eliminación de fronteras tanto comerciales como de comunicación , tampoco debemos desconocer el avance tecnológico que en los últimos años han tenido un auge impresionante, debido a las nuevas formas de comunicación y los medios empleados para el proceso de la información, estos han pasado a ocupar un lugar privilegiado en el campo de la productividad, generando con ello nuevos hábitos y formas para interactuar o relacionarnos. No solamente dentro de nuestro entorno familiar ni mucho menos a nivel País, sino a nivel mundial. Momento que nunca se nos hubiese podido pasar años atrás, pero que hoy en día son una realidad palpable, es así como a partir de estos nuevos medios de comunicación que nos permiten poder estar en contacto con nuestras familias y con el mundo sin importar distancias, de forma simultanea afectan derechos fundamentales a las personas, debido a ello cada Estado ha tenido que implementar normatividades para proteger jurídicamente a sus asociados desprendiéndose así el compromiso y la obligación de todos los gobernantes y gobernados a proteger derechos fundamentales, cuyo fin primordial se enmarca dentro de la protección y garantía de los derechos y libertades de los individuos que conforman la misma. Dentro de estas manifestaciones democráticas, encontramos la protección de Datos. Es así como el Estado tiene a su cargo el velar porque los derechos fundamentales, particularmente, el derecho a la intimidad, al buen nombre, consagrados en la Carta Política sean cumplidos.

En atención a las normas jurídicas vigentes en el Estado colombiano encaminadas a la “protección de datos personales”, como fundamento garantizador de los derechos fundamentales, de allí la importancia de investigar sobre el tema, por lo que nos lleva a reflexionar en el siguiente interrogante: ¿Existe abuso

indiscriminado por parte de quienes realizan tratamiento de la información personal de terceros, y Colombia realmente garantiza la protección de datos personales?

Esta Investigación es importante puesto, que en estos tiempos de apertura de nuevos mercados y formas de comunicación que obligan a traspasar fronteras, el avance tecnológico que el mundo ha evidenciado desde los años 90, donde se hace ineludible brindar información a personas o entidades publica-privadas ,para llevar a cabo cualquier tipo de actividad, lo que hace necesario el inevitable surgimiento de nuevos mecanismos que conlleven a una recopilación y procesamiento de la información ágil y confiable. Así las cosas, la recopilación y el tratamiento de dicha información, están dejando en riesgo la vulneración de los datos personales de los ciudadanos, dado que no se les está brindando un trato adecuado, no obstante existen personas inescrupulosas que de manera fácil acceden a información personal. Debido a ello, se ha tenido que implementar normatividades para proteger a los ciudadanos. Colombia, siendo un estado social de derecho, debe garantizar a sus ciudadanos la protección de los derechos fundamentales, consagrados en la Constitución Política, por ende, nuestra responsabilidad mediante esta investigación, es que el lector tome conciencia sobre el patrimonio intangible que posee cada uno y que debe haber mayor responsabilidad y conciencia social sobre el tema.

Concientizar a las personas, tanto a los titulares de la información como a los que realizan tratamientos de la misma, sobre la importancia de la información personal, la responsabilidad de quienes la suministran y quienes la reciben, al igual, las consecuencias que conlleva el desconocimiento de los derecho y deberes de todos los ciudadanos con respecto a la protección de datos.

Para llevar a cabo la investigación, hemos identificado un gran número de fuentes bibliográficas las cuales nos privilegia la biblioteca de la universidad LA GRAN COLOMBIA, al igual sus bases de datos virtuales.

Por otra parte, el enfoque metodológico que se aplicara para la investigación será por medio de bases bibliográficas, donde se tendrá en cuenta las distintas

argumentaciones de estudiosos del tema mediante tesis doctorales, libros, revistas y artículos científicos, sin dejar a un lado las diferentes sentencias emitidas por los principales tribunales de algunos países al igual que las cortes de Colombia.

De igual forma, de acuerdo a la información recopilada durante la investigación, y siendo consecuentes con nuestra realidad actual, buscaremos el medio más eficaz y eficiente en donde se logre una conciencia colectiva donde cada lector entienda la responsabilidad que se debe tener con la información personal antes de suministrarla.

Pensamos que, con esta investigación se podría generar conciencia sin dejar a un lado los beneficios que trae consigo los avances tecnológicos, pero, que si no se maneja adecuadamente, pueden existir muchos riesgos a los que toda persona se expone, como por ejemplo, el cuidado de los padres con sus hijos, y también desde las mismas instituciones educativas, al igual en las ocasiones en que todos nosotros, sin pensar y sin mirar un poco más allá, queremos estar en todas las redes sociales sin importar como proporcionamos hasta lo más íntimo de nuestros datos y de nuestra vida personal, generando con ello una vida pública.

En sentencia T-260/12 nos brinda a la sociedad una reflexión acerca de las atribuciones y Derechos que tenemos con nuestros hijos o sobrinos o cualquier menor, creemos que por el simple hecho de ser parte de la familia podemos disponer de fotos, videos y comentarios de los niños en la red, realmente lo que estamos, en primer lugar es tomando una decisión por ellos ,porque nos creemos con la autoridad suficiente de decidir por los mismos, y pensamos que lo mejor es lo que nosotros creemos para ellos, en segundo lugar y el peor de todos exponiendo a los niños a cualquier peligro en la red. Nos parece lo máximo subir todo a la red y no nos detenemos un segundo siquiera para pensar las implicaciones que esto puede llegar a traer, sin embargo los amigos con los que compartimos fotos y videos ,realmente cuando el niño crezca no serán los amigos de él ,la Corte en esta sentencia argumenta “Los niños, en virtud de su falta de madurez física y mental -que les hace especialmente vulnerables e indefensos frente a todo tipo de riesgos-, necesitan protección y cuidados especiales, tanto en términos materiales,

psicológicos y afectivos, como en términos jurídicos, para garantizar su desarrollo armónico e integral y proveer las condiciones que necesitan para convertirse en miembros autónomos de la sociedad"

Ese cuidado al que se refiere la Corte al acceso a redes sociales por parte de los menores debe hacerse con el acompañamiento de los padres o personas responsables de su cuidado, a fin de que éstos sean conscientes de que si bien la información y la tecnología trae consigo muchos beneficios para su desarrollo, al mismo tiempo genera una serie de riesgos ,claro está que estos se pueden evitar con un correcto manejo de la información y donde todas las Entidades y Centros educativos se capaciten, para tomar responsabilidad en el mundo de la Tecnología y a su vez orientar a sus estudiantes. Creemos como grupo de este trabajo de grado que la responsabilidad y la cultura que tengamos respecto al auge de la tecnología depende solamente de nosotros.

Realmente Colombia posee gran número de leyes en cuanto a protección de los datos personales. En la LEY 1581 DE 2012. Enfatiza el ámbito de aplicación en los Derechos a la Intimidad, el buen nombre y la autodeterminación informática y las garantías a los gobernados. Vemos al finalizar esta investigación que el estado Colombiano se queda corto en la protección de datos de los menores, debido a la rapidez de las tecnologías. Es realmente necesario materializar dicha protección, porque esa vulneración inicialmente empieza en casa.

**Dentro de las líneas de investigación** que la universidad La Gran Colombia ha dispuesto a sus estudiantes, para el desarrollo de la investigación, se ha identificado la más acorde en cuanto se refiere a la protección de derechos fundamentales como al buen nombre, la intimidad, libre desarrollo de la personalidad, libertad religiosa, entre otros derechos. La línea de "Derecho Constitucional, Administración de Justicia y Bloque de Constitucionalidad", se hace definitiva para abarcar el tema de la protección de la información de personas naturales y jurídicas ante un universo de redes que a diario busca acaparar y trabajar con la información de todos.

Este documento se ha organizado de la siguiente manera: El capítulo I comprende una descripción general del proyecto, en donde se presentan el problema u oportunidad de mejora identificada, la hipótesis, justificación, los objetivos y la metodología utilizada para el proyecto y sus marcos referenciales teórico, conceptual y legal. El capítulo II, nos da una idea de los deberes por parte de las entidades publico privadas en cuanto la protección de datos, y el capítulo III, acerca de los casos reales en que se conoce vulneración de los derechos fundamentales. Por último las conclusiones y biografía.

# CAPITULO I.

## 1. ANTECEDENTES DE LA INVESTIGACIÓN.

### 1.1. PLANTEAMIENTO DEL PROBLEMA.

Si bien es cierto la globalización trae consigo nuevos mercados, donde no existen fronteras, tampoco debemos desconocer el avance tecnológico que en los últimos años han tenido un auge impresionante debido a las nuevas formas de comunicación y los medios empleados para el proceso de la información, estos han pasado a ocupar un lugar privilegiado en el campo de la productividad generando con ello nuevos hábitos y formas para interactuar o relacionarnos, es así como a partir de estos nuevos medios de comunicación que nos permiten poder estar en contacto con nuestras familias y con el mundo sin importar distancias, de forma simultanea afectan derechos fundamentales a las personas, debido a ello cada Estado ha tenido que implementar normatividades para proteger jurídicamente a sus asociados, Desprendiéndose así el compromiso y la obligación de todos los gobernantes y gobernados a proteger los bienes patrimoniales que dentro del territorio nacional se encuentran cuyo fin primordial se enmarca dentro de la protección y garantía de los derechos y libertades de los individuos que conforman la misma. Dentro de estas manifestaciones democráticas, encontramos la protección de Datos. Es así que el Estado como organización jurídica de la nación tiene a su cargo velar por que los derechos fundamentales, particularmente el Derecho a la intimidad, al buen nombre, consagrados en la Carta Política sean cumplidos.

Observando lo anterior, se hace necesario indagar si esta protección De Datos que trata el Art. 15 de la Constitución Nacional," *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 bancos de datos y en archivos de entidades públicas y privadas"* junto con la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Realmente se cumplen y se garantizan en el estado Colombiano. Así mismo la Corte Constitucional, en su jurisprudencia ha establecido que el buen nombre, alude al concepto que del individuo tienen los demás miembros de la sociedad, Sentencia T-228 de 1994; por otra parte el derecho a la intimidad, ha sido delimitado, así: "*El derecho a la intimidad implica la facultad de exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas. Algunos tratadistas han definido este derecho como el "control sobre la información que nos concierne" ("**Estudios sobre el derecho a la intimidad**". Editorial Tecno. Madrid 1982. Pág. 17"); otros, como el "control sobre cuándo y quién puede percibir diferentes aspectos de nuestra persona". La Corte Constitucional, por su parte, ha definido el núcleo esencial del derecho fundamental a la intimidad como "el espacio intangible, inmune a las intromisiones externas, del que se deduce un derecho a no ser forzado a escuchar o a ser lo que no desea escuchar o ver, así como un derecho a no ser escuchado o visto cuando no se desea ser escuchado o visto.*

## 1.2. PREGUNTA DE INVESTIGACIÓN.

En atención a las normas jurídicas vigentes en el Estado colombiano encaminadas a la protección de Datos Personales, como fundamento garantizador de los Derechos Fundamentales, entre ellos, el derecho a la intimidad, al buen nombre, al hábeas data, entre otros; de allí la importancia de investigar sobre el tema, por lo que nos lleva a reflexionar en el siguiente interrogante:

**¿Existe abuso indiscriminado por parte de quienes realizan tratamiento de la información personal de terceros, y Colombia realmente garantiza la protección de datos personales?**

## 1.3. HIPÓTESIS.

El Derecho a la Intimidad Personal, Familiar y Habeas Data está concebida como derecho fundamental, haciendo relación directa con el Derecho al buen nombre, a la honra, y a su vez el Artículo 12 de la Constitución Nacional promulga que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques." Y por lo tanto es deber del Estado garantizar su protección Brindando herramientas que garanticen la protección de datos personales a través de los principios rectores en el tratamiento de datos como lo son autenticidad, confidencialidad, seguridad, transparencia, legalidad, veracidad e integridad de la información, tantos las empresas públicas y privadas como responsables y/o encargadas de protección de datos deberán adoptar procedimientos para garantizar un adecuado cumplimiento de la Ley.

Aun así en la actualidad no se está cumpliendo dicha protección encaminadas a la salvaguarda de estos Derechos Fundamentales debido a que el derecho a la Intimidad, como muchos otros, se ven cada día más amenazado por el auge de la tecnología y porque los diferentes medios tecnológicos colombianos y extranjeros, traspasan constantemente los "límites" de la intimidad personal y familiar dejándolos en riesgo.

## 1.4. JUSTIFICACIÓN.

Esta Investigación es importante ya que en estos tiempos de globalización, con la apertura de nuevos mercados y formas de comunicación que obligan a traspasar fronteras, el avance tecnológico que el mundo ha evidenciado desde los años 90, donde se hace ineludible brindar información a personas o entidades publica-privadas para llevar a cabo cualquier tipo de actividad, lo que hace necesario el inevitable surgimiento de nuevos mecanismos que conlleven a una recopilación y procesamiento de la información ágil y confiable. Así las cosas, la recopilación y el tratamiento de dicha información, están dejando en riesgo la

vulneración de Derechos fundamentales tales como, derecho a la intimidad, derecho al buen nombre, derecho a la información y a la verdad, dado que no se les está brindando un trato adecuado, no obstante existen personas inescrupulosas que de manera fácil acceden a información personal afectando así derechos de las personas, debido a ello se ha tenido que implementar normatividades para proteger a los ciudadanos, Colombia siendo un Estado social de derecho, debe garantizar a sus ciudadanos la protección de los derechos fundamentales consagrados en la Constitución Política, por ende, nuestra responsabilidad mediante esta investigación es que la sociedad, proporcional a nuestras posibilidades, se tome conciencia sobre el patrimonio intangible que posee cada uno y que con éste se pueden hacer grandes cosas que los puede afectar en gran medida.

## 1.5. OBJETIVO DE LA INVESTIGACIÓN.

### 1.5.1. OBJETIVO GENERAL.

Concientizar a las personas, mediante la presente investigación, tanto a los titulares de la información como a los que realizan tratamientos de la misma, sobre la importancia de la información personal, la responsabilidad de quienes la suministran y quienes la reciben, al igual, las consecuencias que conlleva el desconocimiento de los derecho y deberes de todos los ciudadanos con respecto a la protección de datos.

#### 1.5.1.1. OBJETIVOS ESPECIFICOS.

- Investigar la evolución que han tenido los mecanismos de protección de datos personales en Colombia y si el Estado cumple su papel garantista de protección del Habeas Data.
- Establecer los deberes de quienes están en la obligación de garantizar la protección y reserva de datos personales.
- Identificar posibles hechos violatorios con respecto a la protección de datos personales.

## 1.6. ANTECEDENTES:

En Colombia uno de los personajes más reconocidos es el profesor NELSON REMOLINA ANGARITA, el cual ha realizado investigaciones, publicaciones y ha escrito libros, sobre la protección de Datos. La Agencia Española de Protección de Datos (AEPD), El 28 de enero de 2015 le otorgó al Doctor Remolina Angarita el "Premio Protección de Datos Personales de Investigación 2014" sobre trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos. El trabajo ganador se titula "'Tratamiento de información personal. Desde la transferencia transfronteriza hacia la recolección internacional de datos personales: un reto del mundo post-Internet'". Esta investigación es de su tesis doctoral que realizó como estudiante del Doctorado en Ciencias Jurídicas de la Pontificia Universidad Javeriana http://habeasdatacolombia.uniandes.edu.co, algunas de sus publicaciones y libros son: Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012. Los derechos de acceso, rectificación, cancelación y oposición en la ley de datos personales y su reglamento ,Responsabilidad por el tratamiento de los datos personales de clientes, empleados, proveedores y terceros Insuficiencia de la regulación Latinoamerica frente a la recolección internacional de datos personales a través de internet , Aproximación constitucional de la protección de datos personales en Latinoamérica, Revista Internacional de Protección de Datos Personales -RIPDP-. Red Académica Internacional de Protección de Datos Personales ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? , Eliminación de antecedentes penales: un tema para repensar y definir en la Corte Constitucional ,Periódico Ámbito Jurídico. http://www.intercodex.com/libros/recoleccion-internacional-de-datos-personales/9788434021969

Como antecedentes la Ley 1281, que fue un proyecto de Ley del Senador Luis Fernando Velasco, a una necesidad social de protección de datos, así el Senador Velasco, como autor y líder de esta iniciativa logra para Colombia la

materialización de la Ley 1281 de 2012 para la protección de Datos Personales. El Senador sigue trabajando en el tema.

El 26 de agosto en Secretaría General de Cámara de Representantes radico el Proyecto de Ley que modifica y adiciona la Ley de Habeas Data. Este proyecto de Ley pretende disminuir el tiempo de permanencia de los morosos en las centrales de riesgo, que beneficiaría a muchos colombianos para que mejoren su economía, tengan un mayor acceso al sector crediticio y a su vez permite mejorar la ley de Habeas Data generando una mayor protección para los titulares de la información".

### 1.6.1. ANTECEDENTES HISTORICOS LEGALES.

#### 1.6.1.1. LEY 23 DE 1981.

Como primer antecedente en nuestra legislación colombiana encontramos la Ley 23 de 1981: ella refiere al Desarrolló de normas sobre la ética médica, en su artículo 34 desarrollo lineamientos sobre el carácter privado y reservado de la historia clínica "La historia clínica es el registro obligatorio de las condiciones de salud del paciente. Es un documento privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley". Adicional a ello vemos como el medico en su misión de servir al paciente jura Guardar y respetar los secretos a él confiados por parte del paciente, desde este momento se configura una obligación, respeto y diligencia por la información y los datos suministrados al profesional; observamos como grupo el interés del legislador por promulgar normas para la protección de dicha información,

#### 1.6.1.2. LEY 96 DE 1985.

Encontramos en el artículo 51 los datos que tiene la Registradora Nacional del Estado Civil y la clasificación que esta normatividad refiere enunciando cuales son públicos o reservados "Artículo 51. Toda persona tiene derecho a que la Registradora le informe sobre el número, lugar y fecha de expedición de documentos de identidad pertenecientes a terceros. Tienen carácter reservado las

informaciones que reposen en los archivos de la Registradora, referentes a la identidad de las personas, cómo son sus datos biográficos, su filiación y fórmula dactiloscópica. De la información reservada sólo podrá hacerse uso por orden de autoridad competente. Con fines investigativos, los jueces y los funcionarios de policía y de seguridad tendrán acceso a los archivos de la Registradora. Cualquier persona podrá inspeccionar en todo tiempo los censos electorales, pero en ningún caso se podrá expedir copia de los mismos". Posteriormente la Ley 270 de 1996: en el artículo 95 enmarca al Consejo Superior de la Judicatura a implementar la TECNOLOGIA AL SERVICIO DE LA ADMINISTRACION DE JUSTICIA en los siguientes términos "debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información". . Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad, y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley"

#### 1.6.1.3. LEY 527 DE 1999.

También Conocida como ley de Comercio Electrónico define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales; conceptúa el mensaje de datos pero también describe la responsabilidad de las entidades de certificación sobre los datos de los suscriptores del servicio

#### 1.6.1.4. LEY 1273 DE 2009.

Ley de Delitos Informáticos, modifica el código Penal y 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; esta Ley incluyen artículos referentes a violación de datos personales y suplantación de sitios web para capturar datos personales.

## 1.7. MARCOS REFERENCIALES.

### 1.7.1. MARCO TEÓRICO.

Existe una diferencia entre el modelo de regulación con la Protección de Datos entre AMERICA (Estados Unidos) y la Unión Europea. En el caso Americano, su normatividad descansa en una auto regulación vinculante y en el ámbito del derecho de consumo y el de la competencia. Se obliga a las empresas a proteger la privacidad de sus clientes, sin embargo, al no darse dicha situación, se les obliga a responder judicialmente incluso con el pago de indemnizaciones. Por otra parte, el modelo normativo de la UNIÓN EUROPEA, le ha apostado a las herramientas normativas heterónomas, donde a pesar de permitir una autonomía de transferir datos personales internacionalmente, los países Iberoamericanos deberán garantizar la protección de dichos datos. En este último caso, Argentina y Uruguay se han adherido al modelo Europeo estableciendo autoridades de control independiente. (**REIGADA Antonio Troncoso,** Diciembre de 2012, Revista de la red académica internacional de protección de datos personales No. 1, Página 4.) Sin importar las diferencias normativas entre estas dos potencias, se evidencia la necesidad y el compromiso de parte de los gobiernos y autoridades de mitigar lo que podría entenderse como una posición dominante por parte de empresas quienes administran información probada de personas del común. Lo anterior aporta dos enfoques importantes para tener en cuenta en nuestra normatividad Colombiana para llevar a cabo una comparación y concluir lo que lo que con ello se analice. El interés de brindar a las personas una debida protección de datos es de interés global, sin embargo, a nivel internacional se debe trabajar con el fin de unificar criterios para tal finalidad.

Entre los autores que han tratado el tema de protección de datos. Es necesario para nuestra investigación tener referencia de las personas que han trabajado el tema como, lo son el Doctor Nelson Remolina Angarita, Antonio Troncoso Reigada y algunas tesis que pueden aportar a nuestra investigación.

NELSON REMOLINA-ANGARITA, “Tesis Doctoral” articulo resultado parcial de la investigación Doctoral sobre protección de datos personales. El autor realiza en el Doctorado de la Facultad de Ciencias Jurídicas de la Pontificia Universidad Javeriana. Se pretende establecer si Colombia, a la luz de la actual legislación puede considerarse como un país que garantiza un nivel adecuado de protección de los datos personales frente a las exigencias de la Unión Europea que se derivan, especialmente, de la Directiva 95/46/CE. 12 de marzo de 2010 http://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/Tiene-Colombia-nivel-adecuado....Nelson-Remolina1.pdf Concluye su tesis Doctoral indicando que Colombia no cuenta con un marco legal que le permita ser considerado como un país con nivel adecuado de protección de datos personales respecto de las exigencias establecidas en la Directiva 95/46/CE.

ANTONIO TRONCOSO REIGADA, Revista Internacional de Protección de Datos Personales. El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibro en los modelos de protección de datos a nivel internacional, Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia) No. 1 Julio - Diciembre de 2012, Los países iberoamericanos están afrontando en los últimos años un proceso de aprobación de normas de protección de datos personales, que aproxima su legislación al modelo europeo y les aleja del modelo americano.

EMILIO GUICHOT REINA, derecho a la privacidad, transparencia y eficacia administrativa. Un difícil y necesario equilibrio, Revista catalana, núm. 35, 2007, en este trabajo la tensión entre el derecho a la protección de datos y los principios de eficacia y transparencia administrativa.

NELSON REMOLINA ANGARITA, El Habeas Data en Colombia. Señala que el derecho a la intimidad se debe ver por parte del legislador y los jueces en un contexto histórico social, para que así mismo de manera constante estén evaluando esas conductas que desconocen el derecho fundamental a la intimidad. Nelson Remolina Angarita, tratamiento de datos personales aproximación Internacional y comentarios a la Ley 1581 de 2012, primera Edición, LEGIS Editores SA 2013.

También está la Tesis Doctoral Nelson Remolina Angarita Tratamiento de información personal. Desde la transferencia transfronteriza hacia la recolección internacional de datos personales: un reto del mundo post-Interne,' Universidad Javeriana 2015 Argumenta que son insuficientes los mecanismos jurídicos del siglo XX para dar respuesta sensata a los retos del siglo XXI en materia de protección de datos personales., solo el 22% de la población mundial vive en países con normas generales de protección el restante es decir el 78% no tienen ninguna garantía de protección de datos.

La Agencia Española de Protección de Datos (AEPD). El 28 de enero de 2015 el AEPD otorgó al profesor Nelson Remolina Angarita el "Premio Protección de Datos Personales de Investigación 2014" sobre trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos.

Nelson Remolina Angarita Revista Internacional de Protección de Datos Personales Aproximación constitucional de la protección de datos personales en Latinoamérica.

El autor en este texto destaca la importancia que las constituciones latinoamericanas confieren a los datos personales, al habeas data y a la protección de las personas respecto del tratamiento de su información.

### 1.7.2. MARCO CONCEPTUAL.

A la necesidad de entender y comprender los conceptos principales que abarca la Protección de Datos Personales en Colombia, debe haber un entendimiento básico sobre el tema por cada uno de nosotros al considerar que contamos con una titularidad sobre "cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables" (Ley 1581 de 2012)". Lo anterior también conocido como "Datos Personales" los cuales son susceptibles de ser administrados por terceros en el que la norma citada identifica como Personas naturales o jurídicas, pública o privada, que por sí misma o en asocio con otros, tienen la posibilidad de realizar el Tratamiento de dichos datos por cuenta propia. (2012). Sin embargo, como lo mencionábamos antes, siendo

titulares es practico comprender que cualquier información que nos pertenezca podrá ser objeto de tratamiento entendiéndose este último como la posibilidad de ser “manipulada a modo de almacenamiento, recolección, uso, circulación y supresión”. (Ibídem)

Por otra parte, toda información que a menudo suministramos a los encargados o responsables de tratar la misma, debemos saber que dicha información deba ir a un conjunto organizado de datos personales que la misma ley denomina como “base de datos”, para que ésta sea administrada en debida forma. En razón a lo anterior nuestra constitución nacional en su artículo 15 deja claro el derecho de las personas a que cualquier información, cuando haya lugar, pueda ser conocida, rectificada, y actualizada por parte de las entidades, lo anterior implementado en la ley 1266 de 2008. Por tanto se debe considerar que por alguna circunstancia una persona ha autorizado que administren su información personal, pero al dar cuenta que dentro de las bases de la entidad hay información sensible que solo compete al usuario, es deber de la misma entidad permitir el acceso a la misma para que ésta sea “conocida”, así mismo, muchas veces la información puede variar por lo que es indiscutible que se ésta deba “actualizarse”, como por ejemplo el lugar de domicilio, números de contactos, estado civil, entre otros. En el mismo sentido, suele suceder que, bien sea por error de usuario o de la entidad, notamos que la información que reposa en bases de datos no es la que corresponde, y no necesariamente por falta de actualización. Una situación común se presenta cuando quien registra la información de manera errónea podría afectar al usuario titular de la misma, un caso puede ser las bases de datos del SISBEN, muchas veces la calificación no corresponde a la realidad lo que impide que el afectado no pueda beneficiarse los subsidios que el Gobierno ofrezca. Otro ejemplo es cuando los medios de comunicación por caer en el afán de publicar “primicias periodísticas”, sin antes investigar como debe ser, permiten que circule en los diferentes canales de comunicación información que nunca ha correspondido al verdadero contexto (REMOLINA, pág. 196, s.f). En este último caso es frecuente que las autoridades judiciales ordenen rectificar información con la misma relevancia en que se suministró por primera vez. (Sentencia T-03/2011), en

consecuencia a lo anterior, al incurrir las entidades en alguna falla en cuanto al tratamiento de información, se hace evidente que **e**xistiría vulneración a uno o varios derechos fundamentales.

El artículo 5 de la Ley 1581 del 2012 hace referencia entre otras "categorías especiales de datos" a los de tratamiento Sensible que por tener dicho carácter presenta una protección especial salvo en los casos excepcionales que contempla la misma norma, como por ejemplo cuando de ello dependa salvaguardar el interés vital del titular, cuando éste lo haya autorizado de manera expresa, por temas de seguridad nacional o por orden judicial. Nelson Remolina también indica como patrón que en casos de historial clínico la información definitivamente debe ser no solo sensible sino también de plena reserva (pág. 215, año s.f.).

### 1.7.3. MARCO LEGAL.

Las diferentes normas consagradas en nuestra legislación colombiana dan fe del avance legislativo que en los últimos años se ha visto reflejado en nuestro territorio por lo que vale hacer mención de las mismas.

#### *1.7.3.1.* CONSTITUCIÓN POLÍTICA DE COLOMBIA.

Artículo 15º.- Constitución Política de Colombia de 1991 definió el derecho de hábeas data en el artículo 15 como: "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 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 interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá

exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

Artículo 20º.- "Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura".

#### 1.7.3.2. Ley estatutaria 1581 de 2012.

Expedida por el Gobierno el 17 de octubre de 2012, en ella se dictan disposiciones generales para la protección de los Datos personales, al mismo tiempo regula el Derecho Fundamental al Habeas Datas, de igual forma nos señala, el tratamiento de los mismos , .esta Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales que se consagran en el artículo 15 de la Constitución Política; así como el derecho a la información referido en el artículo 20 de la misma. Esta Ley quizás viene a suplir vacíos dejados en la Ley 1266 de 2008 frente a los estándares Internacionales de la Directiva 95/46/CE24 del Parlamento Europeo y del Consejo de Europa, del 24 de octubre de 1995, este compromiso Internacional asumido por Colombia exige a los países expedir regulaciones apropiadas y a su vez implantar cambios Institucionales que proporcionen un nivel adecuado , Vemos que la Ley 1266 de 2008 era una norma sectorial y no general, ya que era solo aplicable a datos personales relacionados con el cumplimiento o incumplimiento de obligaciones financieras ,la norma tuvo falencia tales como no incluir los Datos sensibles donde es obligatorio garantizar un cuidado especial en el almacenamiento y circulación de este tipo de dato, es decir dejo por fuera esta información, por otra parte no consagro el Derecho de Oposición que permite al titular del dato evitar el tratamiento de su información o solicitar el cese de los mismos. Entre otras falencias a las que no haremos referencias, en consecuencia Colombia no cumple con el nivel adecuado de

protección de datos personales respecto a las exigencias de la Directiva, con todo ello la norma busca como fin esencial y primordial salvaguardar los derechos y deberes fundamentales ,los procedimientos y los recursos para su protección, se requiere para su efectiva protección mecanismos que sean idóneos y que garanticen .no solo en el entendido que dependen únicamente de los jueces sino a su vez de una Institución Administrativa que vigile y controle tanto a los sujetos privados como a sujetos públicos, esta Ley también obliga a las Entidades Públicas y empresas privadas a revisar el uso de datos consignados en los sistemas de información y a replantear políticas eficientes que aseguren el manejo ,definiendo fines y medios para el tratamiento de datos de los usuarios.

#### 1.7.3.3. Decreto 1377 de 2013.

No cabe duda que Colombia ha dado un gran avance en la protección de Datos Personales, con la expedición de la ley 1581 de 2012, junto con el decreto reglamentario 1377 de 2013, que enmarca en materia de protección de datos personales: derechos de los ciudadanos, lineamientos del tratamiento de datos, los deberes de los responsables y encargados de los datos personales esta norma busca estar acorde con los lineamientos Internacionales., pero debemos ser claros y consientes todavía falta para estar acorte a los estándares Internacionales. El decreto citado tiene como objetivo facilitar la implementación y el cumplimiento de la ley 1581 reglamentando 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, el ejercicio de los derechos de los titulares de la información, entre otros.

#### 1.7.3.4. Ley 1712 de 2014.

También conocida como LEY DE TRANSPARENCIA Y DE ACCESO A LA INFORMACIÓN PÚBLICA, su objetivo es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

### 1.7.3.5. Sentencia c-748 de 2011.

Con el propósito de proteger el derecho fundamental al habeas data, en sus tres dimensiones: cumplimiento de los principios de la administración de datos (finalidad, utilidad, necesidad y circulación restringida); derecho subjetivo a la supresión relativa de la información personal negativa; y garantía del derecho al trabajo de los peticionarios, la Corte ordenará al Ministerio de Defensa-Policía Nacional, en tanto administrador responsable de la base de datos sobre antecedentes penales que, para los casos de acceso a dicha información por parte de particulares, en especial, mediante el acceso a la base de datos en línea a través de las plataformas respectivas de la Internet, omita emplear cualquier fórmula que permita inferir la existencia de antecedentes penales en cabeza de los peticionarios, si efectivamente estos no son requeridos por, ni tienen cuentas pendientes con, las autoridades judiciales. La Corte de manera acertada se ha pronuncia con referencia a los antecedentes penales. Esta considera que la publicidad indiscriminada de la información sobre antecedentes penales no está cumpliendo con la finalidad legal o constitucional, dado que no es útil ni necesaria. A l contrario, considera l que constituye una barrera para el acceso o la conservación del empleo, facilita prácticas de exclusión social y discriminación prohibidas por la Constitución y vulnera el Derecho al trabajo.

Es indispensable suprimir cierta información en referencia a antecedentes penales, toda vez que no es justa que la persona cumpla su condena y por ello quede reseñado para toda la vida, generando con ello, la vulneración de Derechos Fundamentales, como lo son al buen nombre, al trabajo y peor aun no aportando como estado a que se incorpore nuevamente como sujeto activo de una sociedad a la vida laboral. Por consiguiente, pensamos que existe cierta información que debe ser suprimida, otra de reservada y otra de interés general.

Por lo anterior, la idea es resocializar en la vida civil sin crear inconvenientes al sujeto, por lo que se entiende que no aporta en nada a la sociedad los antecedentes penales, toda vez, que con ellos estamos siendo discriminatorios, y quitándole la posibilidad de reincorporarse de nuevo al mundo laboral.

## 1.8. ENFOQUE METODOLÓGICO.

Para esta investigación se tuvo en cuenta un enfoque bibliográfico en el que se utiliza material que nos permitió realizar un análisis inductivo, deductivo, analógico e histórico que nos permitió mediante las fuentes consultadas, cuyas principales fueron jurisprudencia nacional e internacional, normas no solo colombianas sino también latinoamericanas que hablara acerca de la protección de datos personales, al igual se tuvo en cuenta bibliografía enfocada en el tema; de lo anterior se logró el desarrollo de la investigación que abordamos.

# CAPÍTULO II.

# 2. DEBERES DE LOS ADMINISTRADORES DE LA INFORMACIÓN.

Según la LEY 1581 DE 2012, el Responsable del Tratamiento: es "aquella Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos", cuando se hace alusión al Encargado del Tratamiento: de los Datos, es la Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento y tienen bajo su responsabilidades no solo las enunciadas por esta ley, de igual forma los principios orientadores como:, Principio de Legalidad, finalidad, libertad, veracidad, transparencia, seguridad, acceso y circulación restringida, y por supuesto confidencialidad, pero también deben tener presentes las leyes que regulen su actividad ,

## 2.1. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO.

2.1.1. Artículo 17. *Deberes de los Responsables del Tratamiento.* Los Responsables del Tratamiento deben:

2.1.1.1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

2.1.1.2. Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;

2.1.1.3. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;

2.1.1.4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

2.1.1.5. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;

2.1.1.6. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;

2.1.1.7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;

2.1.1.8. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

2.1.1.9. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

2.1.1.10. Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

2.1.1.11. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;

2.1.1.12. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;

2.1.1.13. Informar a solicitud del Titular sobre el uso dado a sus datos;

2.1.1.14. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

2.1.1.15. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

2.1.2. **Artículo 18.** ***Deberes de los Encargados del Tratamiento****.* Estos deben:

2.1.2.1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

2.1.2.2. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

2.1.2.3. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;

2.1.2.4. Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;

2.1.2.5. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;

2.1.2.6. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;

2.1.2.7. Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;
2.1.2.8. Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
2.1.2.9. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
2.1.2.10. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
2.1.2.11. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
2.1.2.12. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Como podemos observar, si los responsables del tratamiento de los Datos colaboraran para la protección de este Derecho fundamental e importante para la Sociedad, cumpliendo de manera rigurosa y eficiente esta normatividad, se reduciría tantos delitos cometidos en la red, blindando a los ciudadanos con herramientas, recurso humano, orientaciones brindando confianza y garantías de sus servicios.

## 2.2. RESPONSABILIDAD EN LOS MEDIOS DE COMUNICACIÓN.

A veces los medios de comunicaciones por su afán de emitir una chiva y ser los primeros en difundir las noticias, no miden las consecuencias y vulneraciones de Derechos Fundamentales, generando la falta de compromiso y responsabilidad social ante los receptores. La corte Constitucional en su jurisprudencia T-40 de 2013, transcribe “El artículo 20 de la Constitución exige a los medios de comunicación, para ejercer la libertad de información y de prensa, una responsabilidad social, la cual, como ha dicho la Corte Constitucional, “esta

responsabilidad se hace extensiva a los periodistas, comunicadores y particulares que se expresan a través de los medios, en atención a los riesgos que éstos plantean y su potencial de lesionar derechos de terceros, así como por su poder social y su importancia para el sistema democrático. La responsabilidad social de los medios de comunicación tiene distintas manifestaciones. En relación con la transmisión de informaciones sobre hechos, los medios están particularmente sujetos a los parámetros de (i) veracidad e imparcialidad, (ii) distinción entre informaciones y opiniones, y (iii) garantía del derecho de rectificación (…)". En esta sentencia podemos ver como el accionante , solicita la protección de Derechos fundamentales al buen nombre , la honra, toda vez que al ingresar su nombre en la página del buscador google, aparece un artículo como perteneciente a un cartel de la mafia en los Llanos, noticia elaborada y difundida por la casa Editorial El Tiempo, la forma como fue presentada la noticia, relacionándolo sin ninguna explicación clara y suficiente, en el contexto del tráfico de narcóticos en los Llanos, desconoce el principio de veracidad de la libertad de la información y vulnera los derechos fundamentales al buen nombre y a la honra y en cambio tiende a confundir al lector por un hecho no comprobado. Por lo anterior, vale la pena resaltar la evolución de protección de Datos en torno al manejo y divulgación por parte de los diferentes medios de comunicación de la información que estos posean y teniendo siempre como referente la responsabilidad social que tienen frente a la sociedad.

En contexto a lo anterior, se empieza a evidenciar que los medios de comunicación se catalogan como principales fuentes de circulación de información, estos deben ejercer su actividad conforme a la responsabilidad social que les exige la Constitución Política. Lo anterior implica que deben emitir información veraz e imparcial, saber distinguir los hechos de opiniones, y si es el caso realizar las rectificaciones que se soliciten. El afectado por informaciones falsas, erróneas, inexactas o incompletas, que vulneren su honra o buen nombre, tiene el derecho, que hoy es de rango constitucional, a obtener del medio que las haya difundido la correspondiente rectificación en condiciones de equidad. Así las cosas, La Corte señala que los medios masivos de comunicación tienen derecho a

denunciar públicamente los hechos y actuaciones irregulares de los que tengan conocimiento en virtud de su función. Por ello no están obligados a esperar a que se produzca un fallo para informar de la ocurrencia de un hecho delictivo. Sin embargo, deben ser diligentes y cuidadosos en la divulgación de la información que incrimine, pues no pueden inducir al receptor a un error o confusión sobre situaciones que aún no han sido corroboradas integralmente por las autoridades competentes. (Año 2013)

## 2.3. CONTROL, ASEGURAMIENTO Y SUPERVISIÓN DE LA INFORMACIÓN.

En sentencia C-540/12, La CORTE CONSTITUCIONAL al proyecto de ley estatutaria de  estableciendo compromisos de reserva y responsabilidades disciplinarias y penales, instituyendo quienes están obligados a suscribir actas de compromiso de reserva en relación con la información de que tengan conocimiento, ya que al comprender el manejo de información que envuelve caros intereses para el Estado como la seguridad y defensa de la Nación.

En el proyecto de ley Artículo 44. Colaboración con operadores de servicios de telecomunicaciones. “Los operadores de servicios de telecomunicaciones estarán obligados a suministrar a los organismos de inteligencia y contrainteligencia, previa solicitud y en desarrollo de una operación autorizada y siempre que sea técnicamente viable, el historial de comunicaciones de los abonados telefónicos vinculados, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a su localización. Los organismos de inteligencia y contrainteligencia garantizarán la seguridad de esta información y con tal fin, en la solicitud que formulen a los operadores de servicios de telecomunicaciones, limitarán la información solicitada a un período que no exceda de cinco (5) años.” Ahora bien, el artículo 28 nos refiere sobre los  Centros de Protección de Datos de Inteligencia y Contrainteligencia. Donde entabla, “Cada uno de los organismos que desarrolla actividades de inteligencia y contrainteligencia tendrá un Centro de Protección de datos, archivos de Inteligencia y Contrainteligencia (CPD).” Cada uno de los  Centros tendrá un

responsable que garantizará que los procesos de recolección, almacenamiento, producción y difusión de la información de inteligencia y contrainteligencia estén enmarcados en la Constitución y la ley. Para este fin se harán los talleres de capacitación que sean necesarios dentro de cada organismo.

Consideramos que existe un esfuerzo del Gobierno nacional para crear protocolo a seguir con respecto a la protección de Datos por parte de estos organismos, que si se cumple con el fin propuesto pues va a garantizar este Derecho Fundamental. Es de resaltar dentro de este proyecto de Ley la importancia de capacitar a las personas responsables de los procesos de recolección, almacenamiento, producción y difusión de la información de inteligencia y contrainteligencia, esta iniciativa debe ser tanto en el nivel Público como privado para poder garantizar la protección de Datos en Colombia. La connotación de reserva que se le debe dar a sus documentos, información y elementos técnicos estarán amparados por la reserva legal, esto debido a las funciones de inteligencia y contrainteligencia de dichos organismos ,serán por un término máximo de treinta (30) años contados a partir de la recolección de la información y tendrán carácter de información reservada.

## 2.4. GOBIERNO EN LÍNEA.

Uno de los grandes avances que se puede presumir desde el gobierno colombiano es la implementación de mecanismos tecnológicos que buscan facilitar el acceso a la información por parte de sus ciudadanos, brindando herramientas que les ofrezca una serie de trámites y servicios en temas, **como:** Inscripción, corrección y copia del registro civil (nacimiento, matrimonio, defunción), Historia clínica electrónica, Solicitud, corrección, renovación y duplicado de la cédula de ciudadanía. Todo aquello de acuerdo a la necesidad de cada persona, eliminando así desplazamientos innecesarios, por lo que la idea de Gobierno En Línea (GEL) no es únicamente agilizar ciertos trámites, como los que ya mencionamos, sino también, lograr llegar a lugares rurales que no cuentan con acceso tecnológico para tal fin.

Lo anterior, es importante mencionarlo en el presente trabajo debido a que para llegar a una buena articulación entre instituciones se hace necesario entender que la información que repose en ella, refiriendo a la de los ciudadanos, tiene que estar dentro de una base de datos que será administrada por muchas personas desconocidas, por ello, nos empezamos a cuestionar sobre ¿qué información es privada, semiprivada y pública?

En el Manual Y Reglamento De Uso De La Marca "Sello De Excelencia Gobierno En Línea En Colombia", en un aparte hace referencia de unas categorías entre las cuales en una de ellas los requisitos de los datos abiertos, sistemas de información y plataformas colaborativas que propicien un gobierno transparente, abierto y participativo. (MINTIC, s.f.), el Ministerio ha considerado que toda información abierta es aquella que cualquiera puede tener acceso sin que se vulnere los derechos del titular de la información. Ejemplo de lo anterior puede ser el número de cédula de una persona, el estado en que se encuentra las cuentas con tránsito y transporte, o incluso en temas de contratación estatal, lo cual este último debe ser abierto al público con el fin de garantizar la mayor transparencia posible con respecto a la administración de recursos públicos. Ahora bien, hay información que se hace inevitable compartir por tener carácter sensible, pero que aun así, el estado considera de vital importancia tenerla también en su poder por razones de seguridad nacional.

Lo cierto de todo lo anterior es que el gobierno es consciente de la necesidad de seguir blindando al titular de la información con respecto a la protección de datos y prueba de ello son las leyes y decretos aprobados y que hemos hecho mención en el capítulo anterior.

## 2.5. INSCRIPCION EN EL REGISTRO NACIONAL DE BASE DE DATOS RNBD.

Con la Ley 1581 de 2012 las Entidades Públicas como Privadas en su ejercicio recolectar, almacenar, usar, circular y suprimir información de tipo personal se les imponen la obligaciones de cumplir con la ley 1581. Es por ello requieren

expedir políticas de Protección de datos, avisos de privacidad correspondiente y especialmente el desarrollo de protocolo y lineamientos internos que ajusten sus procesos a las exigencias de los principios de la Ley del Habeas Data dentro de los cuales están el principio seguridad, circulación restringida, confidencialidad, finalidad y legalidad así como el cumplimiento de los deberes de protección de datos., esto implica la planeación estratégica de la gestión que minimice los riesgos de vulnerabilidad a que son sometidos los datos personales en consecuencia a su actividad . El concepto de "responsable" de la información tiene su origen en el convenio 108 de 1991 donde lo define como aquel que tiene la facultad de determinad la finalidad para lo cual serán empleado los datos personales que en su poder se encuentran. Al respecto la Corte Constitucional en sentencia 748 de 2011 argumento que los deberes del responsable "buscan garantizar el pleno ejercicio del derecho de habeas data por parte de los titulares y como los principios de administración de datos personales." Entre esto deberes encontramos la autorización previa, expresa y consentida del titular de la información, la cual tiene los siguientes alcances: la característica de "expreso" es la manifestación de la voluntad del titular en confiar su información para unos fines pertinentes, la condición de "previa" implica la anterioridad a la recolección de los datos y la indicación de "consentida" significa saber o conocer la finalidad para lo cual se recolectan los datos

En virtud del decreto 1377 de 2013 y el decreto 886 de 2014 eventualmente se establecerán los plazos para que las entidades públicas realicen el registro nacional de sus bases de datos circunstancia que obliga a las entidades a realizar los inventarios de la información de personales que manejan información.

A través de la circular externa oo2 del 3 de noviembre de 2015 la Superintendencia de Industria y comercio emite a los responsables del tratamiento de base de Datos personales dirigidas a personas jurídicas de naturaleza privada y sociedades de economía mixta inscritas en las Cámaras de Comercio , para que realicen su inscripción de sus bases de Datos en el Registro Nacional de Base de Datos RNBD con fundamento en la Ley 1581 de 2012 en su artículo 19 dado que

es la Superintendencia de Industria y Comercio la autoridad de Protección de Datos, en el cual dispuso que es esta la Entidad que ejercerá la vigilancia para garantizar que en el tratamiento de Datos personales se respeten, derechos, principios, garantías y procedimientos., deberán inscribir la siguiente información: información almacenada en la base de Datos, medidas de seguridad de la información procedencia de los datos personales, transferencia internacional de datos personales, reporte de novedades, reclamos por parte de los titulares , incidentes de seguridad , este registro fue creado mediante el articulo 25 Ley 1581, el cual define como el directorio público de las bases de datos personales sujetas a tratamientos que operan en el país y dispuso que sea administrado por las superintendencia de Industria y comercio.

Creemos como grupo que esta inscripción en el REGISTRO NACIONAL DE BASE DE DATOS es un adelanto en cuanto al manejo y seguridad que las diferentes empresas le están dando a la información personal , ya que esto solo es el principio , puesto que cada entidad deberá crear protocolos y políticas específicas en cuanto a la protección de Datos, donde se hará necesario capacitar al personal en cuanto a la categorización de la información, llámese dato abierto, privado, semi-privado, o datos sensibles, seguidamente que información podemos entregar cuando se nos solicite, sin llegar a poner en riesgo la protección de Datos, por ultimo definir qué personas dentro de cualquier entidad llámese Privada a o Publica va a tener en custodia la información.

## CAPITULO III.

### 3. GARANTAIS A LA PROTECCION DE DATOS PERSONALES EN EL CODIGO DE INFANCIA Y ADOLESCENCIA “LEY 1098 DE 2006”

Es de vital importancia dentro de esta investigación, analizar el cuidado y garantía que trae este código con respecto al menor, en cuanto a la protección de datos personales y su tratamiento, por cuanto son los más expuestos a riesgos y

vulneración de Derechos en las diferentes redes sociales, vemos como en el artículo 33, no se refiere como tal a la protección de datos, pero si nos consagra el Derecho a la Intimidad del menor, en cual nos enuncia, que podrán su derecho, contra toda injerencia arbitraria o ilegal en su vida privada, la de su familia, domicilio, de igual forma serán protegidos contra toda conducta, acción o circunstancia que afecte su dignidad.

El CAPITULO I es muy importante teniendo en cuenta que, nos cita las Obligaciones como familia, como sociedad y como Estado, frente a nuestros menores, vamos a tomar en esta Ley las que más nos interesan dentro de la investigación haciendo referencia a la Protección De Datos Personales, entre ellas:

## 3.1. OBLIGACIONES DE LA FAMILIA ANTE LOS NIÑOS**.**

Este Ítem es la la base de todos los Derechos, si enseñamos a nuestros niños cuáles son sus Derechos, donde terminan, donde empiezan los Derechos de los demás, y que hace parte de la vida privada y que no, y cuáles son los riesgos de publicarla, no habrían violaciones, maltrato, discriminación pero sobre todo muertes en adolescentes por creer que la Internet no tiene límites y que todo lo que aparece allí es verdad.

3.1.1. ARTICULO 39 (**LEY 1098 DE 2006).** “Protegerles contra cualquier acto que amenace o vulnere su vida, su dignidad y su integridad personal” es aquí donde empezamos fallando, omitiendo nuestros deberes como padres, hermanos o como sociedad, con nuestros menores, permitiendo que ingresen a cuanta página de internet les agrade, sin acompañamiento, dejándolos solos a una libertad en la internet, sin límites, con riesgos ”Formarles, orientarles y estimularles en el ejercicio de sus derechos y responsabilidades y en el desarrollo de su autonomía”, debemos hablarles a los menores la importancia del mundo de las tecnologías, todo los beneficios que nos trae pero a su vez los riesgos a los que están expuestos, orientarlos que no todo se puede publicar, enseñarles que una de las cosas más lindas y valiosas del ser humano en su vida privada.

## 3.2. OBLIGACIONES DE LA SOCIEDAD.

Este es un ítem muy importante puesto que se nos olvida que todos las personas somos responsables no solo con nuestros hijos, sino con todos los niños de nuestra sociedad. Esto no es solo decir por decir, sino que es una obligación Constitucional, que tenemos en la protección de los menores,

3.2.1. Artículo 40 (Ibídem), PLANTEA el tipo de obligaciones sociales.

3.2.1.1. Responder con acciones que procuren la protección inmediata ante situaciones que amenacen o menoscaben estos derechos.

3.2.1.2. Participar activamente en la formulación, gestión, evaluación, seguimiento y control de las políticas públicas relacionadas con la infancia y la adolescencia.

3.2.1.3. Dar aviso o denunciar por cualquier medio, los delitos o las acciones que los vulneren o amenacen.

3.2.1.4. Colaborar con las autoridades en la aplicación de las disposiciones de la presente ley.

3.2.1.5. Las demás acciones que sean necesarias para asegurar el ejercicio de los derechos de los niños, las niñas y los adolescentes.

## 3.3. OBLIGACIONES DEL ESTADO**.**

Al Estado le falta más compromiso con los niños y niñas, con respecto a la utilización de las tecnologías, las leyes ya están, se debe materializar en lo que realmente es necesario y es poner en marcha la cultura responsable del uso de la tecnología.

3.3.1. Artículo 41 (**LEY 1098 DE 2006)**

3.3.1.1. Garantizar el ejercicio de todos los derechos de los niños, las niñas y los adolescentes.

3.3.1.2. Asegurar las condiciones para el ejercicio de los derechos y prevenir su amenaza o afectación a través del diseño y la ejecución de políticas públicas sobre infancia y adolescencia.

3.3.1.3. Garantizar la asignación de los recursos necesarios para el cumplimiento de las políticas públicas de niñez y adolescencia, en los niveles nacional, departamental, distrital y municipal para asegurar la prevalencia de sus derechos.

3.3.1.4. Asegurar la protección y el efectivo restablecimiento de los derechos que han sido vulnerados.

3.3.1.5. Investigar y sancionar severamente los delitos en los cuales los niños, las niñas y las adolescentes son víctimas, y garantizar la reparación del daño y el restablecimiento de sus derechos vulnerados.

3.3.1.6. Resolver con carácter prevalente los recursos, peticiones o acciones judiciales que presenten los niños, las niñas y los adolescentes, su familia o la sociedad para la protección de sus derechos.

3.3.1.7. Fomentar la participación en la vida cultural y en las artes, la creatividad y producción artística, científica y tecnológica de niños, niñas y adolescentes y consagrar recursos especiales para esto.

3.3.1.8. Prestar especial atención a los niños, las niñas y los adolescentes que se encuentren en situación de riesgo, vulneración o emergencia.

## 3.4. OBLIGACIONES ESPECIALES DE LAS INSTITUCIONES EDUCATIVAS.

Bajo la perspectiva de la Educación nos falta enseñarles a los jóvenes de manera didáctica la responsabilidad que deben tener en el mundo de las tecnologías.

3.4.1. Artículo 42 (**LEY 1098 DE 2006).**

3.4.1.1. “Garantizar la utilización de los medios tecnológicos de acceso y difusión de la cultura y dotar al establecimiento de una biblioteca adecuada.” Acá

no es solamente el garantizar la utilización de medios tecnológicos, el éxito está en ser responsables y orientarles todas las ventajas y desventajas de la tecnología.

3.4.2. Artículo 43 (**LEY 1098 DE 2006).**

3.4.2.1. Proteger eficazmente a los niños, niñas y adolescentes contra toda forma de maltrato, agresión física o psicológica, humillación, discriminación o burla de parte de los demás compañeros o profesores.

## 3.5. RESPONSABILIDADES ESPECIALES DE LOS MEDIOS DE COMUNICACIÓN.

Uno de los espacios donde más se violan los Derechos de los menores, son los medios de comunicación, en ejercicio de su autonomía y demás derechos, estos deben:

3.5.1. Artículo 47 (**LEY 1098 DE 2006).**

3.5.1.1. Promover, mediante la difusión de información, los derechos y libertades de los niños, las niñas y los adolescentes, así como su bienestar social y su salud física y mental.

3.5.1.2. El respeto por la libertad de expresión y el derecho a la información de los niños, las niñas y los adolescentes.

3.5.1.3. Adoptar políticas para la difusión de información sobre niños, niñas y adolescentes en las cuales se tenga presente el carácter prevalente de sus derechos.

3.5.1.4. Abstenerse de transmitir mensajes discriminatorios contra la infancia y la adolescencia.

3.5.1.5. Abstenerse de realizar transmisiones o publicaciones que atenten contra la integridad moral, psíquica o física de los menores, que inciten a la violencia, que hagan apología de hechos delictivos o contravenciones, o que contengan descripciones morbosas o pornográficas.

3.5.1.6. Abstenerse de entrevistar, dar el nombre, divulgar datos que identifiquen o que puedan conducir a la identificación de niños, niñas y adolescentes que hayan sido víctimas, autores o testigos de hechos delictivos, salvo cuando sea necesario para garantizar el derecho a establecer la identidad del niño o adolescente víctima del delito, o la de su familia si esta fuere desconocida. En cualquier otra circunstancia, será necesaria la autorización de los padres o, en su defecto, del Instituto Colombiano de Bienestar Familiar.

Continuando con la protección de datos de adolescente infractores encontramos el artículo 81, el trae consigo los Deberes del Defensor de Familia: como Guardar reserva sobre las decisiones que deban dictarse en los procesos, so pena de incurrir en mala conducta. Este mismo deber rige para los servidores públicos de la Defensoría de Familia. Otros deberes: a) Adoptar las medidas de restablecimiento establecidas en la ley para detener la violación o amenaza de los derechos de los niños, las niñas o los adolescentes. b) A dictar las medidas de restablecimiento de los derechos para los niños y las niñas menores de catorce (14) años que cometan delitos.

Del mismo modo en el artículo 147 nos dice que las "Audiencias en el sistema de responsabilidad penal para adolescentes. Las audiencias que se surtan en el proceso de responsabilidad penal para adolescentes, ante los jueces de control de garantías y ante los jueces de conocimiento, serán cerradas al público si el juez considera que la publicidad del procedimiento expone a un daño psicológico al niño, niña o adolescente. Cuando así lo disponga, en ellas solamente podrán intervenir los sujetos procesales" .este articulo tiene su base o relación con el artículo 14 del **PACTO INTERNACIONAL DE DERECHOS CIVILES Y POLÍTICOS enunciando** que Todas las personas son iguales, ante los tribunales y cortes de justicia. Toda persona tendrá derecho a ser oída públicamente y con las debidas garantías por un tribunal competente, independiente e imparcial, establecido por la ley, en la substanciación de cualquier acusación de carácter penal formulada contra ella o para la determinación de sus derechos u obligaciones de carácter civil. Esta es la parte más importante La prensa y el público podrán ser excluidos de la

totalidad o parte de los juicios por consideraciones de moral, orden público o seguridad nacional en una sociedad democrática, o cuando lo exija el interés de la vida privada de las partes o, en la medida estrictamente necesaria en opinión del tribunal, cuando por circunstancias especiales del asunto la publicidad pudiera perjudicar a los intereses de la justicia; pero toda sentencia en materia penal o contenciosa será pública, excepto en los casos en que el interés de menores de edad exija lo contrario, o en las actuaciones referentes a pleitos matrimoniales o a la tutela de menores. Cabe resaltar que este pacto fue acogido por Colombia mediante la Ley 74 de 1968.

Como podemos ver esta Ley independientemente que el adolescente haya cometido infracciones, no quiere decir con ello que el Estado, la sociedad y la familia los rechace, discrimine o deje solo, al contrario el Estado a través de esta normatividad busca proteger los Derechos de los menores para no exponerlos en lo público ,cuidando y protegiendo los Datos Personales para no ser discriminado con sus actuaciones y a la vez impone obligaciones que debemos tener como sociedad y administración en nuestro diario vivir con nuestros menores.

## 3.6. MEMORANDUM DE MONTEVIDEO Y SUS RECOMENDACIONES GENERALES.

### 3.6.1. Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes.

Estas recomendaciones juegan un papel muy importante en nuestra sociedad, debido a que ha involucrado al Estado, las Entidades Educativas, los progenitores y otras personas que se encuentren a cargo del cuidado ,los educadores de niños, niñas y adolescentes, brindándoles diferentes recomendaciones, convirtiéndose en un modelo o referente a seguir por los Países, para la protección de Datos, tan importante es este documento, que la La Corte Constitucional Colombiana a través de sentencia T-260/12 trajo a colación las

recomendaciones del Memorandum, toda vez que constituyen criterio de orientación doctrinal para el tema, debido a que esta sociedad de información y de conocimiento, además de traer beneficios y entretenimient , concomitantemente trae infinidad de riesgos para los Derechos Fundamentales ,es por ello que La Corte sabe que cada Día el uso de las tecnologías por parte de niños ,niñas y adolescentes es cada vez mayor, se hace indispensable, la adopción de normas y políticas públicas, con el fin de garantizar un adecuado acceso de todos estos jóvenes a las redes sociales, disfrutando de los beneficios y al tiempo prevenir los riesgos, por ello dentro de esta sentencia cita este escrito, que como grupo para esta investigación se hace valioso dado que en estas recomendaciones, puede estar la solución a este problema gigantesco que las leyes Colombianas no han podido garantizar en su totalidad. Para estas recomendaciones se tuvo en cuenta las particularidades de género , la diversidad cultural que se presenta en América Latina y el Caribe, así mismo la variedad de políticas y de normativas en la manera de enfrentarse al fenómeno de la Sociedad de la Información y el Conocimiento, con especial énfasis en Internet y las redes sociales digitales. Tomaremos algunas recomendaciones a tener en cuenta:

#### 3.6.1.1. RECOMENDACIONES PARA LOS ESTADOS Y ENTIDADES EDUCATIVAS PARA LA PREVENCIÓN Y EDUCACIÓN DE NIÑAS, NIÑOS Y ADOLESCENTES.

**3.6.1.1.1.** Los Estados y las entidades educativas deben tener en cuenta el rol de los progenitores, o cualquier otra persona que tenga bajo su responsabilidad el cuidado de las niñas, niños y adolescentes, en la formación personal de ellos, que incluye el uso responsable y seguro del Internet y las redes sociales digitales. Es tarea del Estado y las entidades educativas proveer información y fortalecer capacidades de los progenitores y personas responsables, sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes en los ambientes digitales.

**3.6.1.1.2.** Toda medida que implique control de las comunicaciones tiene que respetar el principio de proporcionalidad por tanto se debe determinar que la misma

tiene como fin la protección y garantía de derechos que es adecuada al fin perseguido y que no existe otra medida que permite obtener los mismos resultados y sea menos restrictiva de los derechos.

**3.6.1.1.3.** Se debe transmitir claramente a las niñas, niños y adolescentes que Internet no es un espacio sin normas, impune o sin responsabilidades. Deben alertarlos para no dejarse engañar con la aparente sensación de que allí todo vale dado que todas las acciones tienen consecuencias.

**3.6.1.1.4.** Las niñas, niños y adolescentes deben ser advertidos sobre la posibilidad de que cuando creen estar comunicándose o compartiendo información con una persona determinada, en realidad puede tratarse de otra persona. Al mismo tiempo es necesario advertir que la participación anónima o con un pseudónimo hace posible la suplantación de identidad.

**3.6.1.1.5.** En el proceso educativo es necesario enfatizar el respeto a la vida privada, intimidad y buen nombre de terceras personas, entre otros temas. Es importante que las niñas, niños y adolescentes sepan que aquello que puedan divulgar puede vulnerar sus derechos y los de terceros.

**3.6.1.1.6.** El proceso educativo debe proveer de conocimiento acerca del uso responsable y seguro por parte de las niñas, niños y adolescentes de las políticas de privacidad, seguridad y alertas con las que cuentan los instrumentos de acceso y aquellos sitios web en los que las niñas, niños y adolescentes son usuarios frecuentes como las redes sociales digitales.

**3.6.1.1.7.** Se debe promover una política educativa —expresada en términos acordes a la edad de las niñas, niños y adolescentes — que incluya una estrategia informativa y formativa que los ayude a gestionar las potencialidades y los riesgos derivados de la Sociedad de Información y el Conocimiento, en especial del uso de Internet y de las redes sociales digitales.

**3.6.1.1.8.** Asimismo se debe informar sobre los mecanismos de protección y las responsabilidades civiles, penales o administrativas que existen cuando se vulneran derechos propios o de terceros en la red.

**3.6.1.1.9.** Se debe advertir del peligro que supone el llamado robo y/o suplantación de identidad que se puede producir en los entornos digitales que inducen al engaño.

**3.6.1.1.10.** Es necesario explicar a las niñas, niños y adolescentes con un lenguaje de fácil comprensión el espíritu de las leyes sobre protección de datos personales y protección de la vida privada de modo tal que puedan captar la idea de la importancia del respeto a la privacidad de las informaciones personales de cada uno de ellos y de los demás.

**3.6.1.1.11.** La inclusión en los planes de estudios, a todos los niveles educativos, de información básica sobre la importancia de la vida privada y de la protección de los datos personales, y demás aspectos indicados en numeral tres.

**3.6.1.1.12.** La producción de material didáctico, especialmente audiovisuales, páginas web y herramientas interactivas (tales como juegos *online*) en el que se presenten los potencialidades y los riesgos. Estos materiales deberán incluir información acerca de los mecanismos de protección de los derechos.

**3.6.1.1.13.** Los docentes deben ser capacitados para facilitar la discusión y poner en contexto las ventajas y los riesgos de la Sociedad de la Información y el Conocimiento, y en especial de Internet y las redes sociales digitales; pudiendo contar para ello con el apoyo de las autoridades de protección de los datos personales o de todas aquellas organizaciones que trabajen en este tema en los diferentes países.

Encontramos en el Memorándum de Montevideo, recomendaciones para la Industria en cuanto a Protección de Datos, que se hacen valiosos ya que creemos como grupo que es en este mercado donde más se vulnera este Derecho debido a su afán de dar a conocer servicios. Por la presión de ser competitivos, pero sobre todo a obtener mayores utilidades sin importar el riesgo a que exponen a sus clientes y creemos también llámese empresa Pública o Privada que existe gente inescrupulosa que vende esta información a terceros para sacar provecho de estos, es por ello que se hace vital citar algunas recomendaciones para este sector, si este gremio colaborara con la protección de Datos haría que menos gente y más

los niños resultaren perjudicados, vemos que estas recomendaciones también van dirigidas aquellas personas adultas que se encuentren en posición de vulnerabilidad

### 3.6.1.2. RECOMENDACIONES PARA LA INDUSTRIA.

Las empresas que proveen los servicios de acceso a Internet, desarrollan las aplicaciones o las redes sociales digitales deben comprometerse de manera decidida en materia de protección de datos personales y la vida privada —en particular de niñas, niños y adolescentes—, a cooperar con los sistemas de justicia nacionales, desarrollar campañas de prevención y desarrollo de capacidades, entre otros instrumentos mediante compromisos o códigos de conducta, que deben incluir:

3.6.1.2.1. No permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la información recogida con cualquier otra finalidad diferente a la que motivó su tratamiento, y en especial a la creación de perfiles de comportamiento. En el caso de niñas y niños se deberá considerar la prohibición de tratamiento de datos personales. En el caso de adolescentes se deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país, de los que deben darse una información clara.

3.6.1.2.2. Proteger la vida privada debería ser la característica general y por defecto en todas las redes sociales digitales, bases de datos y sistemas de comunicación, entre otros. Los cambios en el grado de privacidad de su perfil de usuario que se quieran realizar deben ser sencillos y sin costo alguno.

3.6.1.2.3. Las reglas sobre privacidad de las páginas web, servicios, aplicaciones, entre otros, deberían ser explícitas, sencillas y claras, explicadas en un lenguaje adecuado para niñas, niños y adolescentes.

3.6.1.2.4. Se deberá proveer información sobre los propósitos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se

realicen a terceros. De igual modo se deberá indicar la persona o personas responsables del tratamiento de la información.

3.6.1.2.5. Toda red social digital debe indicar explícitamente en la parte relativa a la “publicidad” contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a niñas, niños y adolescentes, sobre el hecho de que las informaciones personales de los perfiles de los usuarios se emplean para enviar publicidad según cada perfil. Se deberá evitar publicidad que no sea adecuada para las niñas, niños y adolescentes.

3.6.1.2.6. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de la inscripción y la creación de una cuenta. Se debe por tanto explicar que la fecha de nacimiento exigida tiene por objeto el poder verificar la edad mínima permitida para poder crearse una cuenta en la red social digital. Se debe precisar igualmente cómo se van a utilizar estos datos de carácter personal que hay que facilitar de manera obligatoria.

La industria deberá implementar mecanismos para una verificación fehaciente de la edad de niñas, niños y adolescentes para la creación de una cuenta de usuario y/o acceder a determinado contenido.

3.6.1.2.7. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley. Toda red social digital debe elaborar una política accesible a los usuarios en materia de conservación de la información, en virtud de la cual los datos personales de los usuarios que han desactivado su cuenta sean suprimidos totalmente de los servidores del servicio, tras un periodo de tiempo razonable.

3.6.1.2.8. Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. La indexación de información de niñas y niños debe estar prohibida en todas sus formas, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos.

3.6.1.2.9. Toda red social digital debe establecer las medidas necesarias para limitar el acceso por parte de los terceros que desarrollan las diferentes aplicaciones que el servicio ofrece (juegos, cuestionarios, anuncios, entre otros), a los datos personales de los usuarios cuando éstos no sean necesarios ni pertinentes para el funcionamiento de dichas aplicaciones. La red social tiene que asegurar que los terceros que desarrollan aplicaciones en sus plataformas únicamente podrán acceder a los datos personales de los usuarios con el consentimiento expreso de estos. La red social digital debe asegurarse que los terceros desarrolladores soliciten únicamente la información indispensable, pertinente y no excesiva para el uso de dicha aplicación.

3.6.1.2.10. Las redes sociales digitales deberán establecer un servicio eficiente y eficaz de soporte a los usuarios en estos temas. Este soporte deberá ser en las lenguas oficiales utilizadas en el país del usuario.

3.6.1.2.11. Los desarrolladores de páginas web, servicios, aplicaciones, plataformas, entre otros, deberán establecer filtros de seguridad, como medio complementario a la educación, sensibilización y sanción

3.6.1.2.12. Las industrias deben establecer medidas de índole técnica y operativa para garantizar la seguridad de la información, en particular la integridad, disponibilidad y confidencialidad.

3.6.1.2.13. Para la erradicación de la pornografía infantil en Internet la industria —en un esfuerzo conjunto de todos los actores responsables– deben comprometerse como mínimo a:

a. Notificar a las autoridades competentes todas las ocurrencias de pornografía infantil detectada en perfiles de los usuarios de redes sociales digitales, para que sea posible abrir las investigaciones y acciones que correspondan;
b. Preservar todos los datos necesarios para la investigación por el plazo mínimo de seis meses o entregar esos datos a las autoridades competentes, mediando autorización judicial;
c. Desarrollar herramientas por medio de las cuales las líneas telefónicas de ayuda a niñas, niños y adolescentes puedan encaminar las denuncias para que los funcionarios de la empresa analicen, retiren los contenidos ilegales e

informen a las autoridades competentes cuando contengan indicios de pornografía infantil, racismo u otros crímenes de odio, y preserven todas las pruebas;

d. Desarrollar herramientas de comunicación con las autoridades competentes, para facilitar la tramitación de las denuncias, formulación de pedidos de remoción y preservación de datos;
e. Desarrollar campañas de educación para el uso seguro y respetuoso de las leyes, de Internet y las redes sociales digitales;
f. Financiar la publicación de folletos y su distribución a niñas, niños y adolescentes en escuelas públicas, con información para el uso seguro de Internet y las redes sociales.

## 3.7. CASOS DE VIOLACIÓN DE DERECHOS FUNDAMENTALES Y SUS RESULTADOS.

Existen diferentes derechos fundamentales establecidos en la norma que muestra la vulneración de los mismos ante un tratamiento inadecuado de datos personales por parte de sus administradores. Así las cosas es necesario hacer mención sobre algunas sentencias que han brindado amparo a personas que se han visto afectados por publicaciones, ya sea de fotos e imágenes sin previa autorización, e incluso por la creación de cuentas en internet donde ellos aparecen sin consentimiento. Se tomaran diferentes sentencias y con sus respectivos comentarios.

### 3.7.1. DERECHO A LA PROPIA IMAGEN, INTIMIDAD PERSONAL HONRA Y AL BUEN NOMBRE.

En muchas ocasiones las empresas, publico privadas, abusan al pretender comercializar con la imagen de quienes nunca han autorizado. . En Sentencia T-634/13 la CORTE CONSTITUCIONAL reconoce “El derecho a la propia imagen, a partir de los diversos aspectos desarrollados por la jurisprudencia constitucional, (i) comprende la necesidad de consentimiento para su utilización, (ii) constituye una

garantía para la propia imagen como expresión directa de la individualidad e identidad de las personas, (iii) constituye una garantía de protección de raigambre constitucional para que las características externas que conforman las manifestaciones y expresiones externas de la individualidad corporal no puedan ser objeto de libre e injustificada disposición y manipulación de terceros, (iv) es un derecho autónomo que puede ser lesionado junto con los derechos a la intimidad, a la honra, al buen nombre de su titular, y cuyo ejercicio está estrechamente vinculado a la dignidad y libertad de la persona, (v) implica la garantía del manejo sobre la propia imagen cuyo ejercicio se traduce en una manifestación de la autodeterminación de las personas, y (vi) exige que las autorizaciones otorgadas para el uso de la propia imagen en el marco de la libertad en las relaciones contractuales no sean entendidas como una renuncia al derecho mismo (…) "La Empresa se negó a retirar de la red social Facebook y de otros medios de publicidad, varias fotografías comprometedoras que afectan derecho a la intimidad y al buen nombre de la accionante. , este derecho es de protección constitucional debida a la imagen como expresión directa de la individualidad, identidad y dignidad de las personas. En este sentido, la disponibilidad de la propia imagen esta exige la posibilidad de decidir sobre su cambio o modificación, lo cual constituye a su vez un presupuesto ineludible del ejercicio del libre desarrollo de la personalidad. Es de reconocer la responsabilidad que tenemos al autorizar la comercialización de una imagen sin mirar un poco más hacia el futuro y solo mirar el contexto actual, donde solo interesa salir en las redes sociales publicitando marcas, sin tener conciencia si estas compañías explotadoras serán consecuentes en el momento que no se tenga una relación laboral y acedan al retiro de fotos imágenes por iniciativas de las misma, sin que medie proceso legal alguno. Así las cosas, el panorama se abre para que La responsabilidad que tengamos en la información que subimos en las diferentes redes, sin tener en cuenta los riesgos que esto conlleva, al igual del manejo que terceros puedan dar a nuestra información, desde las redes.

### 3.7.2. EL DERECHO AL OLVIDO.

Colombia ha seguido de manera muy especial los lineamientos en cuanto a protección de Datos por parte de la Unión Europea e implantándolos en nuestro País. Sin embargo se considera que siempre surgirán casos que obliga a las instituciones a replantear los mecanismos que buscan evitar la vulneración de los derechos fundamentales de los ciudadanos. Por ende, vale mencionar una sentencia del TRIBUNAL DE JUSTICIA EUROPEO en la C-131 de 2012, se presenta el caso del Señor Costeja González y los Gobiernos español e italiano el interesado puede oponerse a la indexación de sus datos personales por un motor de búsqueda cuando la difusión de estos datos por la intermediación de éste le perjudica, los derechos fundamentales a la protección de datos y de respeto a la vida privada, que engloban el «derecho al olvido», prevalecen sobre los intereses legítimos del gestor de dicho motor y el interés general en la libertad de información. El Tribunal ha definido que buscadores de Internet como Google deben retirar los enlaces a informaciones publicadas en el pasado si se comprueba que son lesivas para alguna persona y carecen de relevancia y el reconocimiento del derecho de una persona a que sus datos sean eliminados cuando crea que la información que los contiene pueden perjudicarle, o simplemente porque que desee que estos datos e información se “olviden” tras un determinado lapso de tiempo.

### 3.7.3. DERECHO AL HABEAS DATA, INTIMIDAD, AL BUEN NOMBRE Y LIBRE DESARROLLO DE LA PERSONALIDAD.

Existe una sentencia que para nosotros es la más importante, dado que la Corte de una manera muy profunda nos ilustra el deber que tenemos con nuestros niños a disponer de manera responsable cierta información o creación de perfiles en una red social, que nos lleva a lo largo de esta investigación a la misma conclusión y es la responsabilidad y conciencia que debemos tener cuando subimos cierta información a la red, Lo que queremos al terminar esta investigación, es que todos seamos responsables y consientes de la información que brindamos, para no ver nuestros derechos vulnerados ni dejando en riesgo nuestras vidas y aún más angustiante la de nuestros niños. En sentencia T-260 de 2012, la corte hace una apreciación sobre Los derechos fundamentales de los niños, niñas y adolescentes

que gozan de una especial protección tanto en el ámbito internacional como en nuestro Estado Social de Derecho. Ello, dada la situación de indefensión, vulnerabilidad y debilidad de esta población y la necesidad de garantizar un desarrollo armónico e integral de la misma. Los niños, en virtud de su falta de madurez física y mental -que les hace especialmente vulnerables e indefensos frente a todo tipo de riesgos-, necesitan protección y cuidados especiales, tanto en términos materiales, psicológicos y afectivos, como en términos jurídicos, para garantizar su desarrollo armónico e integral y proveer las condiciones que necesitan para convertirse en miembros autónomos de la sociedad.

La Corte también señaló que los derechos de los usuarios de esta red social pueden verse vulnerados "con la publicación de contenidos e información en la plataforma –fotos, videos, mensajes, estados, comentarios a publicaciones de amigos-". La Corte consideró que debido al aumento de posibilidades para compartir, comunicar y entretener, las redes sociales generan también riesgos para los derechos fundamentales a la intimidad, protección de datos, honor, honra, imagen y buen nombre, entre otros. La afectación de los derechos fundamentales en redes sociales como Facebook puede ocurrir no sólo respecto de la información cuando un usuario ingresa a la red social o también cuando permite el ingreso a través de su perfil. La misma corte indica que el acceso a la red social Facebook el desconocimiento de derechos fundamentales, puede "generarse en el momento en el cual el usuario se registra en la red escogida, durante su participación en la plataforma, e incluso en el momento en que decide dejar de utilizar el servicio". Puede ocurrir no sólo respecto de la información que los usuarios de esta red social ingresan a la misma o cuyo ingreso permiten a través de su perfil, sino también con relación a información usada y publicada por terceros en las redes sociales generando riesgos para los derechos fundamentales a la intimidad, protección de datos, honor, honra, imagen y buen nombre, entre otros. Algo también importante que nos deja esta sentencia, es que a los niños no podemos limitarlos de este universo de las tecnologías, este proceso lo debemos llevar de la mano como padres, tíos, profesores, instituciones educativas gobernantes, en un círculo de

acompañamiento responsable para con los menores enseñándoles todos su beneficios pero también sus riesgos.

El derecho de acceso de los menores a la Sociedad de la Información y el Conocimiento, debe ser acorde a la edad y madurez del menor a fin de no afectar su desarrollo armónico e integral. Así también la afectación del derecho fundamental de los menores al habeas data, cuando subimos en la red información o fotos creyendo tener una posición ilimitada frente a ellos, por lo que el llamado es a ser prudentes y responsables de lo que subimos a la red, con nuestros hijos, sobrinos, o cualquier menor, porque con ello ponemos en riesgo varios de sus derechos fundamentales. Es importante no creer que por tener el cuidado de los menores podemos publicar todo de ellos.

## 3.8. DERECHO COMPARADO. PROTECCIÓN DE DATOS EN ALGUNOS PAISES LATINOAMERICANOS.

### 3.8.1. ARGENTINA.

Distintas normas constitucionales y generales de algunos países latinos que buscan la protección de datos personales permite, permite entender que existen diversidad legislativa en Latinoamérica con dos tipos de enfoques donde por un lado una minoría se inclina a la postura de la UNION EUROPEA y los demás, entre ellos Colombia, quienes demuestran su interés constitucional hacia el tema mostrando un enfoque legal AMERICANO (Estados Unidos). Antonio Troncoso en cita a Nelson Remolina que ha estudiado constituciones y normas generales que hablan acerca de la protección de datos en países de Latino América y de dicho análisis ha concluido que no hay constitución que no hable de manera expresa sobre la protección de datos. Sin embargo, en las normas generales, tan solo una minoría de países desarrolla aspectos que regulan la transferencia internacional de datos. “Cfr. N. Remolina Angarita, “Insuficiencia de la regulación latinoamericana frente a la recolección internacional de datos personales a través de internet”, Quaestiones Disputatae Num. 2. Universidad Javeriana, Bogotá, febrero de 2012, págs. 179-226, esp. págs. 208-211.”. Colombia hace parte del 65% de los países, según Remolina,

que incorporan de manera explícita disposiciones para la protección de datos. Entre el 25% de los países que tan solo han implementado como norma general, no constitucional, en Latinoamérica, está Argentina, Uruguay, México, chile y Perú. En el caso de Argentina, ésta cuenta con la Ley 25.326 del año 2000; de allí, el país gaucho cuenta con una DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS, cuyo órgano de control vela por la protección de datos personales de sus conciudadanos. En ese mismo país, en la ciudad autónoma de Buenos Aires, se tiene la Ley 1.845 le brinda competencias de control sobre PROTECCIÓN DE DATOS a la Defensoría del Pueblo de esa ciudad. Por lo anterior, dichas normas le han atribuido reconocimientos por parte de la UNION EUROPEA, quienes en el año 2003 declaran que Argentina es un país garante para la protección de datos. (Revista de la red académica internacional de protección de datos personales No. 1, Página 4. 2012). Ahora bien, Colombia ha ganado terreno en tema legal para la protección de datos personales no solo con la constitución nacional, sino también con leyes aprobadas como la LEY ESTATUTARIA 1266 DE 2008, LEY 1581 DE 2012 con su DECRETO 1377 DE 2013 que la regula. Siendo consecuentes, es evidente la clara inclinación y postura legar que contrasta la UNIÓN EUROPEA al ser Colombia un país con una de las normatividades más completas para la protección de datos dando así una gran empatía con la postura Americana (Estados Unidos).

### 3.8.2. PERÚ.

Aunque no son muchas las normas, fuera de la constitución que Perú ha dado trámite a fin de lograr la protección de datos, es notable la similitud que éstas tienen con la norma Colombiana lo que indica un enfoque legal al AMERICANO (Estados Unidos). Sin embargo, Antonio Troncoso nos recuerda que “Perú establece en el art. 2.5 y 7 de su Constitución que toda persona tiene derecho a solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, exceptuándose las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional (…)”, “(…) los servicios informáticos, computarizados o no, públicos o privados, no

suministren informaciones que afecten la intimidad personal y familiar.” (Revista de la red académica internacional de protección de datos personales No. 1, Página 7, 2012), por ello, reiterando el caso peruano, la constitución de ese país en su artículo 200 establece la acción del habeas data como garantía constitucional, y fue con la Ley 29733 del 2011, hasta ese año surge norma general para la protección de datos personales. (Troncoso, 2012). Perú hace parte de los países que de manera explícita emiten normas mara la protección de datos personales.

### 3.8.3. COSTA RICA.

Costa Rica ha sido de los últimos países en incluir en su constitución la necesidad de la protección del Habeas Data, donde se ve reflejado en el artículo 23 de la misma. También de manera reciente nos ha aportado la lay 8968 que habla sobre la de Protección de la Persona Frente al Tratamiento de sus Datos Personales, de allí, ha entrado a funcionar la Agencia de Protección de Datos de la República de Costa Rica (Troncoso, 2012). El interés de los países latinos para la protección de datos se va dando de manera unánime.

### 3.8.4. MEXICO.

En esta materia, no es el solo el hecho de que se acceda de manera arbitraria a la información personal, hay que tener presente que en ocasiones la información de las personas pueden ser de acceso público, sin restricción alguna, sin embargo, se puede presentar situaciones en la que dicha información no sea la correcta, por ejemplo la hoja de vida de un servidor público cuyo perfil no es el acorde, los antecedentes judiciales que tildan condenas que nunca existieron o que ya fueron cumplidas, o por qué no, los mismos medios de comunicación que informan de manera errada una noticia que involucra la información personal de un individuo. Casos así deben ser respaldados por autoridades judiciales que obliguen a quienes administran información a corregir, aclarar, o eliminar dependiendo el caso. Troncoso nos indica que en el artículo 6 de la constitución de México, se establece que los archivos gubernamentales serán protegidos de acuerdo a leyes secundarias, de igual forma, el artículo 16 de la misma norma, resalta la

obligatoriedad de no afectar la privacidad de toda persona en todo ámbito, salvo orden de autoridad que motive el acto; seguido del mismo artículo, reconoce derecho en cuanto a protección de datos personales, a la cancelación o corrección de la información. (Año 2012, Página 8).

### 3.8.5. CHILE.

Chile apenas cuenta con ley que regula el tema, en materia constitucional, se considera que se queda corto al momento de garantizar la protección de datos en ese país. Chile se limita a regular a través de la Ley 19.628 sobre la Protección de la Vida Privada, dicha ley fue modificada por la Ley 19.812, de 13 de junio de 2002. Ahora bien, como fundamento constitucional en el art. 19.4 de la Constitución, que establece la garantía de respeto a la vida privada, da a entender la necesidad sobre el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares. (Troncoso, Año 2012, Página 10).

### 3.8.6. BLASIL.

Como la mayoría de países latinoamericanos en materia de protección de datos, en Brasil existe una Ley 9.507 del 12 de noviembre de 1997, que regula el derecho de acceso a la información y el habeas data, por lo que su Constitución Federal establece en el art. 5 la acción de habeas data como un mecanismo a través del cual el ciudadano puede hacer efectivo su derecho de acceso y rectificación de datos o someter a confidencialidad cierta información sensible, frente al Estado o un particular. (Troncoso, Año 2012, Página 11). Ahora bien, lo curioso de un país, de los más grandes en territorio y población de Latino América, es que no tengan mayor precedente en cuanto a protección de datos, siendo éste el segundo país con mayoría de usuarios en redes sociales en el mundo.

### 3.8.7. ECUADOR.

En Ecuador existen normas sectoriales que regulan la protección de datos, sin embargo, no hay norma general, únicamente la constitución se reconoce el Habeas Data en su artículo 94. Siguiendo el mismo lineamiento con algunos pises

de América, Ecuador de manera reciente ha considerado la necesidad de regular y proteger a las personas titulares de la información. Troncoso recoge en su escrito en la Revista de la red académica internacional de protección de datos personales que la Legislación sectorial hay que señalar algunas normas como la Ley de Comercio Electrónico, Firmas y Mensajes de Datos el 17 de Abril del 2002 (Artículo 9); la Ley Especial de Telecomunicaciones del 10 de Agosto de 1992 - (Artículos 1, 14 y 39) y la Ley de Buros de Información Crediticia del 18 de Octubre de 2005 (Artículos 5 a 10). Hay algunas normas en proyecto como el Proyecto de Reglamento de Ley de Transparencia del 18 de Agosto 2004, donde se establece lo referente a la “Información Personal o Confidencial”.

La Constitución Política de la República del Ecuador (aprobada el 5 de junio de 1998) señala en el art. 23 que el Estado reconocerá y garantizará a las personas “8. El derecho a la honra, a la buena reputación y a la intimidad personal y familiar. La ley protegerá el nombre, la imagen y la voz de la persona”. (Año 2012, Página 10).

# CONCLUSIONES.

Aunque Colombia ha tenido un importante desarrollo legal y estructural en pro de proteger los datos personales de todo individuo, es evidente que hubo una reacción tardía a este problema por lo que el llamado es a que, mientras se establezcan mecanismos eficaces por parte del Estado, cada uno de nosotros deberá ser el propio garante de sus datos personales., dado que somos todos, incluyendo niños, niñas y adolescente ,adultos, adultos mayores, discapacitados que en cualquier momento vemos vulnerado la protección de datos , debemos ser consecuentes, responsables y tener cultura tecnológica ,que aunque la sociedad de consumo y las nuevas formas de comunicaciones lleguen a nuestras vidas , en ese momento separemos que se puede hacer público .y que no.

Es necesario fortalecer las sanciones civiles y penales a quienes traten de manera indebida la información de otros, dado que la pena de prisión en la actualidad tan solo es de cuarenta y ocho (48) a noventa y seis (96) meses, y en multas oscilan entre 100 a 1000 salarios mínimos legales mensuales vigentes. Esto fue incorporado al Código Penal a través de la ley 1273 de 2009, articulo 269 literal F., la mayoría de las violaciones a este Derecho se quedan en el anonimato, ya sea por miedo infundido, donde no se denuncia dando pie a los abusadores, violadores, explotadores, a continuar sus delitos en las redes generando con ello una cadena de delitos. Para ello debemos hacer que la Sociedad vuelva a creer en la Justicia, para que así puedan tener confianza en la Justicia Colombiana y denuncien para hacer las investigaciones del caso y llegar al culpable para que pague. De la misma manera es necesario que las penas sean mayores dado que a través de estos medios no solo se vulnera el Habeas Data sino ello trae consigo, desapariciones forzadas, violaciones, estafas y muchas veces hasta la muerte

En materia Educativa, es urgente la inclusión de la cátedra de responsabilidad del uso de las tecnologías desde la primaria hasta el bachillerato en los planes de estudio, donde de una manera más clara y de fondo se oriente , se guie al estudiante este fenómeno que parece imparable ,que trae a la sociedad

múltiples beneficios pero también múltiples daños, estas clases deben ser charlas, conferencias amigables, con un lenguaje muy sencillo y con ayudas didácticas que ilustren al menor sobre los beneficios y riesgos que trae el uso del Internet y las distintas redes sociales por medio de las tecnologías, no debemos ser tan pacientes con el tema es otra época que no va a terminar como cualquier moda impuesta por la sociedad, al contrario cada día el uso de las tecnologías va hacer más fuerte que queramos o no va a estar en nuestro diario vivir, dado que cada sociedad .debe cada día ser más competitivo y por ende sus administrados también.

En lo Social debe haber mayor compromiso para con los niños, niñas adolescentes, en el uso de las tecnologías, creemos como grupo que padres, docentes, o garantes de los mismos deben brindar un acompañamiento al menor ,no dejarlos solos cuando ellos ingresen a diferentes redes sociales, saber a qué paginas ingresan mediante controles a las mismas, saber con quién interactúan, quienes son sus amigos en la red y crear reglas de tiempo en la red, porque si bien es cierto no se les puede prohibir el acceso a las tecnologías toda vez que es una necesidad en la sociedad en que estamos y ellos hacen parte de esa sociedad por ende tienen que vivir ese fenómeno, pero con restricciones

Por parte de las empresas exigir más compromiso, crear mayores exigencias y sanciones frente a tratamiento de la información tanto de entidades Públicas como Privadas, exigiéndoles, creación de canales de publicidad por las mismas redes o por medios televisivos, de los derechos que tienen todas las personas a la tecnología, los deberes, con la misma, ante que organismos se puede denunciar, las sanciones a que da lugar, y los riesgos que posiblemente le pueden presentar ., crear incentivos para las empresas que se preocupen y cumplan con el cuidado de los Datos Personales de Su clientes a través de reducción de impuestos o mediante reconocimientos públicos.

En general, las entidades publico privadas están en la tarea de dar cumpliendo a las obligaciones que mediante las normas están establecidas por el estado para la Protección De Datos Personales, sin embargo, hay que seguir

llevando un control exhaustivo a las mismas para así se pueda evitar más casos de usuarios afectados.

BIBLIOGRAFIA.


- ARGOS, NORMA DE PROTECCIÓN DATOS PERSONALES, Versión 001 – (2013)

- CAMARA DE COMERCIO DE BOGOTÁ, CERTICÁMARAS, ABC Para Proteger Los Datos Personales Ley 1581 De 2012 Decreto 1377 De 2013. (2013)

- CONSTITUCIÓN POLITICA DE COLOMBIA.
- DECRETO 1377 DE 2013, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- GOMEZ V. I., Tesis Doctoral, Universidad Autónoma De Barcelona, "El Derecho Fundamental A La Protección De Datos Personales En El Ámbito De La Prevención Y Represión Penal Europea." (2014)

- GOMEZ V. I., Tesis pregrado, Pontificia Universidad Javeriana, Realidad Jurídica Del Comercio Electrónico En Colombia, (2004)

- GUICHOT E. Artículo EL NUEVO DERECHO EUROPEO DE ACCESO A LA INFORMACIÓN PÚBLICA (1). (2007)

- GUICHOT R. E. Ponencia "acceso a la información y protección de datos. Estado de la cuestión". (s.f.)

- GUICHOT R. E., Derecho A La Privacidad, Transparencia Y Eficacia Administrativa: Un Difícil Y Necesario Equilibrio, Revista Catalana De Dret Públic, núm. 35, 2007, p. 43-74. (2007)
- GUICHOT R. E., Universidad De Sevilla, Artículo, "Transparencia Versus Protección De Datos." (s.f)
- LEY 1581 DE 2012.
- LEY ESTATUTARIA 1266 DE 2008.
- REMOLINA A. N. EL HABEAS DATA EN COLOMBIA (2015).

- REMOLINA A. N., Tesis, ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, 16 International Law, Revista Colombiana de Derecho Internacional, 489-524 (2010).
- REMOLINA A. N., Tratamiento De Datos Personales Aproximación Internacional Y Comentarios A La Ley 1581 Del 2012, Primera edición. (2015)
- UNIVERSIDAD LOS ANDES, Revista De Derecho Comunicaciones Y Nuevas Tecnologías, Revista de Derecho, Comunicaciones y Nuevas Tecnologías N.º 6, Diciembre de 2011. ISSN 1909-7786. (2011)
- UNIVERSIDAD DE LOS ANDES. Facultad de Derecho, Revista Internacional de Protección de Datos Personales, (Bogotá, Colombia) No. 1 Julio - Diciembre de 2012. ISSN: 2322-9705 (2012)
- UNIVERSIDAD LOS ANDES, Revista De Derecho Comunicaciones Y Nuevas Tecnologías, Revista No. 5, Enero - Junio de 2011. ISSN 1909-7786. (2011)

ANEXO.

GLOSARIO:

**Base de datos personales**.

Es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

**Base de datos automatizada.**

Es el conjunto organizado de datos de carácter personal que son creados, tratados y/o almacenados a través de programas de ordenador o software.

**Base de datos no automatizada.**

Es el conjunto organizado de datos de carácter personal que son creados, tratados y/o almacenados de forma manual, con ausencia de programas de ordenador o software.

**Cesión de datos**

Tratamiento de datos que supone su revelación a una persona diferente al titular del dato o distinta de quien estaba habilitado como cesionario.

**Custodia de la base de datos.**

Es la persona física que tiene bajo su custodia la base de datos personales al interior de ARGOS.

**Dato personal.**

Es cualquier dato y/o información que identifique a una persona física o la haga identificable. Pueden ser datos numéricos, alfabéticos, gráficos, visuales, biométricos, auditivos, perfiles o de cualquier otro tipo.

**Datos personal sensible.**

Es una categoría especial de datos de carácter personal especialmente protegido, por tratarse de aquellos concernientes a la salud, sexo, filiación política, raza u origen étnico, huellas biométricas, entre otros, que hacen parte del haber íntimo de la persona y pueden ser recolectados únicamente con el consentimiento expreso e informado de su titular y en los casos previstos en la ley.

**Encargado del tratamiento.**

Es la persona física o jurídica, autoridad pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable.

**Fuentes accesibles al público.**

Se refiere a aquellas bases contentivas de datos personales cuya consulta puede ser realizada, por cualquier persona, que puede incluir o no el pago de una contraprestación a cambio del servicio de acceso a tales datos. Tienen esta condición de fuentes accesibles al público las guías telefónicas, los directorios de la industria o sectoriales, entre otras, siempre y cuando la información se limite a datos personales de carácter general o que contenga generalidades de ley. Tendrán esta condición los medios de comunicación impresos, diario oficial y demás medios de comunicación.

**Habeas data.**

Derecho fundamental de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas, conforme lo dispuesto en la ley y demás normatividad aplicable.

**Procedimiento de análisis y creación de información.**

Es la creación de información respecto de una persona, a partir del análisis y tratamiento de los datos personales recolectados y autorizados, para fines de

analizar y extraer perfiles o hábitos de comportamiento, que generan un valor agregado sobre la información obtenida del titular de cada dato personal.

**Procedimiento de disociación.**

Hace referencia a todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

**Principios para el tratamiento de datos.**

Son las reglas fundamentales, de orden legal y/o jurisprudencial, que inspiran y orientan el tratamiento de datos personales, a partir de los cuales se determinan acciones y criterios para dar solución a la posible colisión entre el derecho a la intimidad, habeas data y protección de los datos personales, y el derecho a la información.

**Propietario de la base de datos.**

Dentro de los procesos de negocios de ARGOS, es propietaria de la base de datos el área que tiene bajo su responsabilidad el tratamiento de los mismos y su gestión.

**Responsable del tratamiento.**

Es la persona física o jurídica, de naturaleza pública o privada, que recolecta los datos personales y decide sobre la finalidad, contenido y uso de la base de datos para su tratamiento.

**Titular del dato personal.**

Es la persona física cuyos datos sean objeto de tratamiento. Respecto de las personas jurídicas se predica el nombre como derecho fundamental protegido constitucionalmente.

**Tratamiento de datos**

Cualquier operación o conjunto de operaciones y procedimientos técnicos de carácter automatizado o no que se realizan sobre datos personales, tales como la recolección, grabación, almacenamiento, conservación, uso, circulación, modificación, bloqueo, cancelación, entre otros.

**USUARIO.**

Es la persona natural o jurídica que tiene interés en el uso de la información de carácter personal.

**Violación de datos personales.**

Es el delito creado por la ley 1273 de 2009, contenido en el artículo 269 F del Código Penal Colombiano. La conducta prohibida es la siguiente: "El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en base de datos, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes".

**Violaciones de las medidas de seguridad de los datos personales.**

Será considerado incidente de seguridad aquella situación que implique una violación de las medidas de seguridad adoptadas por ARGOS para proteger los datos personales entregados para su custodia, sea como Responsable y/o Encargado, así como cualquier otra conducta que constituya un tratamiento inadecuado de datos personales en contravía de lo aquí dispuesto o de lo señalado en la Ley. Todo incidente de seguridad que comprometa los datos personales en poder de ARGOS deberá ser informado a la autoridad de control en la materia.

**Cámara de comercio de Bogotá.**

Mediante CERTICAMARAS, en el "*ABC PARA PROTEGER LOS DATOS PERSONALES LEY 1581 DE 2012 DECRETO 1377 DE 2013", nos brinda una*

*claridad sobre inquietudes conceptuales y técnicas las cuales nos permitimos citar a continuación:*

**¿Qué son los datos personales?**

Es cualquier información concerniente a personas físicas, que tenga carácter de privado, que esté ligada a su intimidad y que toque temas susceptibles de discriminación, como orientación sexual, religiosa, étnica, entre otros.

**¿Cuál es la importancia de los datos personales?**

Su importancia radica en que la información personal puede ser utilizada para varios fines, como la comercialización, la vida laboral, e incluso para cometer delitos, ya que su identidad puede ser suplantada si es que se tiene acceso a la información adecuada.

**¿En qué consiste la protección de datos?**

Son todas las medidas que se toman, tanto a nivel técnico como jurídico, para garantizar que la información de los usuarios de una compañía, entidad o de cualquier base de datos, esté segura de cualquier ataque o intento de acceder a esta, por parte de personas no autorizadas.

**¿Quién es el titular de la información?**

Es la persona física cuyos datos son objeto de tratamiento.

**¿Quién es el responsable del tratamiento?**

Es la persona natural o jurídica que decide sobre la base de datos o el tratamiento de datos, ya sea por si sola o en sociedad con otros.