ANÁLISIS DEL DELITO DE VIOLACIÓN DE DATOS PERSONALES (ARTÍCULO 269F DEL CÓDIGO PENAL) DESDE UNA PERSPECTIVA CONSTITUCIONAL

David Felipe Sánchez Cano

Universidad Libre de Colombia

Facultad de Derecho, Ciencias Políticas y Sociales

Santiago de Cali, Colombia

2016

*** Holbein Giraldo Paredes**

ANÁLISIS DEL DELITO DE VIOLACIÓN DE DATOS PERSONALES (ARTÍCULO 269F DEL CÓDIGO PENAL) DESDE UNA PERSPECTIVA CONSTITUCIONAL

David Felipe Sánchez Cano

Código: 124909

Trabajo de Tesis Académica para optar por el título de Abogado

Doctor Holbein Giraldo Paredes

Presidente - Tutor Metodológico

Universidad Libre de Colombia

Facultad de Derecho, Ciencias Políticas y Sociales

Santiago de Cali, Colombia

2016

Página de aceptación

Contiene las firmas de las personas encargadas de aprobar el trabajo de Tesis.

Dedicatoria

A mis abuelos, a mis padres, a mi hermano, a mi mujer y a mi hijo.

Agradecimientos

Para todos aquellos compañeros, maestros, amigos y familiares que hicieron posible que este gran esfuerzo diera sus frutos… ¡Gracias!

Tabla de Contenido

Título

ANÁLISIS DEL DELITO DE VIOLACIÓN DE DATOS PERSONALES (ARTÍCULO 269F DEL CÓDIGO PENAL) DESDE UNA PERSPECTIVA CONSTITUCIONAL

Resumen

El tema de esta tesis académica en el área del Derecho se desarrolla directamente desde la perspectiva constitucional salvaguardando el artículo 15 de la Constitución Política, como lo es el derecho fundamental a la Intimidad y al Buen Nombre; analizando en contraste el diseño del tipo penal del artículo 269F del Código Penal (violación de datos personales), que el legislador implementó mediante la ley 1273 de 2009.

En el siglo XXI, en la era de las tecnologías de la información y las comunicaciones, la sociedad colombiana y mundial se encuentra electrónicamente expuesta en riesgo informático y en la inminente necesidad de proteger todas las bases digitales o virtuales que contengan información personal o datos personales. Debido a esto es necesario proteger el derecho constitucional fundamental consagrado en el artículo 15 de la Carta Política de 1991 (Derecho a la Intimidad, al Buen Nombre, Habeas Data, Inviolabilidad de la correspondencia y documentos privados) pues no solamente se trata de que las bases de información existan, contengan información íntima y personal, sino que se puedan proteger efectivamente de la posibilidad existente y continua de los sabotajes y/o fraudes informáticos. La realidad de hoy en día prueba la existencia de delincuentes muy inteligentes, hábiles, avezados, experimentados y capaces, que se apoderan ilícitamente de esta información contenida en sistemas informáticos y que la utilizan en su provecho o para un tercero. Lo anterior repercute en el deterioro de los derechos fundamentales de la víctima (sujeto pasivo penal) y se transgrede consecuentemente el delito prescrito en el Artículo 269F del Código Penal, el cual estipula una pena de prisión y multa para quien viole Datos Personales. Por eso los instrumentos Jurídico-Penales y Constitucionales surgen para ser utilizados y asegurar el resguardo, la integridad y la debida protección de la información y de los datos de todos los seres humanos que integran la sociedad colombiana.

Abstract

The theme of this academic thesis in the area of Law develops directly from a constitutional perspective safeguarding article 15 of the Colombian Constitution, as it is the fundamental right to privacy and good name; analyzing and contrasting the design of the offense established in article 269F of the Colombian Penal Code (Violation of personal data), which Congress implemented by Law 1273 in 2009.

In the XXI century, the era of information technology and communications, Colombian and global society are exposed electronically to computer risks and the urgent need to protect all digital databases or virtual databases that contain personal information or personal data. Due to this threat, it is necessary to protect the fundamental constitutional right enshrined in Article 15 of the Constitution of 1991 (Right to privacy, Good Name, Habeas Data, Confidentiality of correspondence and private documents) not only because it is the basis of information existence, containing intimate and personal information, but can effectively protect the existing and continuing possibility of sabotage and/or computer fraud. Today´s reality proves the existence of highly intelligent, skilled, seasoned, experienced and capable criminals who illegally seize and rob information contained in information systems, and use it to their advantage or to that of a third party. This results in the deterioration of the fundamental rights of the victim (criminal passive subject); and therefore commits offenses prescribed in Article 269F of the Penal Code, which stipulates a prison sentence and a fine for anyone who violates laws that pertain to illegal retrieval of personal data. Therefore, the criminal legal and constitutional instruments combined should be utilized to ensure the safeguarding, integrity and proper protection of information and data of all human beings that make up Colombian society.

1. Introducción

En este proyecto de investigación, iniciativa de Tesis para optar al grado de Abogado propongo un análisis concienzudo e integral acerca de los delitos informáticos, específicamente el delito de violación de datos personales (artículo 269F del Código Penal colombiano) abordado desde una perspectiva constitucional; por lo cual, enfoco este estudio desde una perspectiva del Derecho constitucional y consecuentemente con la rama penal del ordenamiento jurídico nacional.

En Colombia, el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", en esta nueva disposición, la Ley Penal se encuentra consagrado el TIPO PENAL que analizamos integralmente en esta tesis de grado, el cual se denomina: **VIOLACIÓN DE DATOS PERSONALES (ARTÍCULO 269F DEL CÓDIGO PENAL**.

Los métodos empleados en este proyecto de investigación jurídica han sido discutidos y acordados con el director del mismo y obedecen a una de las múltiples alternativas existentes para el abordaje analítico que facilita el llegar a un resultado en concreto hasta producir un conjunto de conclusiones y recomendaciones idóneas alineadas con el problema bajo estudio.

2. Antecedentes o Estado del Arte

El Estado del Arte y los antecedentes de esta problemática llamada "delitos informáticos" son relativamente nuevos en Colombia; pues los delitos informáticos aparecen conforme avanza la modernidad y la sociedad contemporánea se hace usuaria casi dependiente de las tecnologías de la información y las comunicaciones. Actualmente, en Colombia existe esta problemática en el sentido en que se penalizan algunas conductas que aparecen en nuestro ordenamiento como lesivas de intereses en donde se ve implicado aquel derecho penal moderno, que se puede definir como el conjunto de normas que regula infracciones jurídicas, ya sea como delito o falta, tanto viéndolo de modo objetivo, como parte de todo el ordenamiento jurídico, y desde el punto de vista subjetivo, como la facultad del Estado para imponer esas normas en concreto, y cuyas consecuencias son bien la pena, la multa, o la medida de seguridad.

> *De acuerdo con* (Reyes Cuartas, 2007. p.84.) *en Colombia y el mundo, cada año aumentan las cifras de este tipo de conductas antijurídicas pues al incrementarse la ciber-criminalidad, la sociedad de hoy en día se ve expuesta como sujeto activo de dependencia de estos sistemas automatizados en donde se controla todo tipo de áreas sea marítima, aérea o terrestre en donde solo se pretende llegar a una seguridad autónoma con el fin de establecer un mejor desarrollo global en relación al derecho penal moderno, pues en sí, la informática ha establecido parámetros de desarrollo en la sociedad muy relevantes, y también se han creado vulneraciones hacia este nuevo sistema ya que nos encontramos en la era de la globalización, en la era de la tecnología en donde la sociedad actual depende de ésta ya que se han perdido aquellas costumbres que se establecieron algún día como medios de comunicación, trabajo, diversión, diálogos, entre otros.*

En la actualidad somos La Sociedad de la era de la información y las comunicaciones. Hoy estamos en la revolución de los computadores, los sistemas artificiales de todo tipo y la tecnología informática, que permea prácticamente todos los campos del conocimiento desde las artes (música, escultura, pintura, arquitectura, diseño

gráfico etc.), la medicina, la matemática, la física, el agro, las finanzas, y hasta la manera como nos vivimos y nos comunicamos a diario, por medio del uso de teléfonos celulares inteligentes (Smartphones), tabletas, computadores de escritorio, portátiles, cajeros electrónicos, mini computadores, relojes inteligentes, GPS, electrodomésticos digitales, circuitos cerrados de televisión, cámaras de vigilancia, etc.) de hecho pocas cosas son posibles sin su intermediación, ya que en apariencia nos hace más útil o fácil la vida, sin embargo nos ha hecho dependientes de ellos, viviendo en la era de la información digital o electrónica, en la cual, los datos personales se crean, manipulan y se trasmiten dentro de un nuevo mundo cibernético complejo, por lo tanto, el Derecho ha evolucionado creando un nuevo objeto jurídico de especial protección donde el bien jurídico tutelado se denomina "De la Protección de la información y de los datos" Bien jurídico taxativo en el título séptimo de la Ley 599/2000 (Congreso de la República de Colombia, 2012).

Para el Derecho, las nuevas tecnologías y el avance de la humanidad en cuanto a éstos medios masivos de ciber comunicación es de mucha importancia cuando tiene que ver con factores como lo son la manipulación de información personal y de los datos personales, las estafas a través de medios telemáticos, y los continuos hurtos, dando pie a nuevas conductas ahora típicas, antijurídicas y culpables que cada vez evolucionan más siendo este "DELITO INFORMÁTICO" una amenaza latente que podría perjudicar a cualquier persona que haga parte del sistema de la vida actual (sociedad de la era de la información y las comunicaciones) y que tienen cuentas y hacen uso de correos electrónicos, cuentas bancarias electrónicas, Redes Sociales, y en general de un gran número de portales virtuales que potencialmente podrían estar al alcance de delincuentes que valiéndose de estos sistemas de información cibernéticos, violan datos personales y/o sacan provecho ilícito, convirtiendo en víctimas a los usuarios de estas cuentas virtuales, portales o redes cibernéticas.

La regulación de este tipo de conductas se ha establecido desde los años 80 del siglo pasado a partir del momento que aparece "La Red Global"-"World Wide WEB" o la Internet (International Net) e incluso antes, cuando los primeros delitos informáticos se dieron en los bancos y otro tipo de instituciones financieras a través de micro operaciones o transacciones de sumas poco significativas realizadas por los ingenieros de sistemas

quienes manipulaban la información de los cuenta habientes y trasladaban centavos a cuentas de terceros de cuentas inactivas vulneradas haciendo uso de información privilegiada a la que tenían acceso; luego, se hacían transferencias mayores desde cuentas que manejaban grandes sumas y cientos de transacciones a las cuales era difícil para la época hacerles seguimiento, puesto que se abrían en países denominados paraísos financieros donde poco o ningún control se hacía a los recursos que ingresan los cuenta habientes; y éstas conductas junto a otras de mayor actualidad han sido objeto de estudio para el Derecho penal, el Derecho Constitucional, la ingeniería de sistemas, las finanzas y la sociología ya que aparecen conductas más agresivas con la persona como el sabotaje informático, la pornografía infantil, la alteración de datos, la suplantación de identidad, el hurto de claves de seguridad, la trata de blancas, y el terrorismo informático, así como a la afectación de la seguridad nacional, entre otros. (Sánchez Cano, 2016).

En 1980 A.R.P.A.NET (Advanced Research Projects Agency Network) Del Departamento de Defensa de los Estados Unidos, creó la Internet, herramienta fundamental que actualmente es un instrumento vital en los sistemas informáticos del mundo; la mencionada institución documentó que en su red se emitieron extraños mensajes que aparecían y desaparecían en forma aleatoria, y que algunos códigos ejecutables de los programas usados sufrían una mutación (una especie de virus informático, de poca credibilidad que pudiese existir para la época); en ese momento, los hechos inesperados no pudieron comprenderse pero se les buscó solución. Los técnicos altamente calificados en seguridad informática del Pentágono norteamericano desarrollaron un antivirus para contrarrestar el riesgo y atender la urgencia del caso a los tres días de ocurrido el evento (Trend Micro, 2008). A medida que el uso de la Internet se ha extendido, ha aumentado el riesgo de su uso inadecuado, ilegítimo, dañino e incurso en la intimidad de las personas naturales o jurídicas. Los delincuentes cibernéticos viajan por el mundo virtual y realizan incursiones fraudulentas cada vez más frecuentes y variadas, como el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático y despojo hasta de millas de viajeros frecuentes, entre otros.

Con el pasar del tiempo se necesitó que se coordinaran los países a través de proyectos de cooperación técnica internacional para que se diera un sistema judicial especializado que desarrolle esta conducta como delito que permita procesar a los autores y castigar a quien cometa la conducta, Colombia se unió a estos países en el 2009 (Jarvey, 2012).

Claro está que las herramientas de las personas u organizaciones criminales para irrumpir en este sistema de forma ilegal ha evolucionado y cada día es más rápida su evolución paralelamente con el desarrollo tecnológico como ha venido sucediendo con los virus informáticos, bombas lógicas o malware (programas de computador dañinos), y ese no es solo el problema, puesto que también están los pedófilos y delincuentes sexuales informáticos quienes por medio de perfiles falsos -en las redes sociales- buscan relaciones de confianza online con los menores o con personas poco cautas, para luego aprovecharse de ellos. En una categoría no menos inferior se encuentran los estafadores, los falsificadores, los secuestradores, los ciber proxenetas, traficantes de armas, de drogas, los comerciantes informáticos de pornografía infantil, y demás delitos y determinadores que por medio de esta red o redes virtuales se desarrollan afectando multiplicidad de bienes jurídicos tutelados por el Derecho (Sánchez Cano, 2016).

Con esto las entidades comenzaron a general instrumentos de control y sanción a quienes utilizaban la informática para delinquir y así nació la ley inglesa que sirvió para que otros países donde la Internet estaba en desarrollo se sumaran al esfuerzo de promulgar leyes orientadas a proteger y sancionar la violación a la información electrónica personal, "*Data Protection Act*" que en español refiere "Ley de Protección de Datos" de 1975.

Colombia tenía el nivel más bajo en seguridad para este delito informático en comparación con otros países de Latino América; sin embargo, con el paso del tiempo y con la ganancia en experiencia, habilidad y conocimientos se ha logrado solventar esta falla. De acuerdo con las conclusiones del mencionado estudio realizado por Cisco, líder mundial en redes, las tres principales formas de ataque informático a las organizaciones

son, en su orden: virus informático (45% del total), los abusos por parte de los empleados (42%) y luego la penetración a los sistemas por parte de fuentes externas (13%).

Con la llegada de estas nuevas tecnologías de la información y las comunicaciones (TIC), aparece la protección a la intimidad, ésta nace en Alemania en los años 70, en España en la década del 80 y en Colombia surge en los años 90 con la Constitución Política de 1991, y posteriormente con la regulación de la Ley de Habeas Data.

De acuerdo con la página WEB del Ministerio de Tecnologías de la Información y las Comunicaciones (Gobierno de Colombia, 2016) en la época de la Colonia, se creó el correo mayor de indias, mediante privilegio que concedió la Corona Española, por real cédula del 14 de mayo de 1514 a don Lorenzo Galíndez de Carvajal. Las oficinas del correo colonial se ubicaron en uno de los dos costados de la Plaza mayor de Santafé, luego se trasladaron a la Calle Real hoy carrera séptima. La Casa Real Administración de Correos fue construida desde 1553 en la esquina sur de la catedral de Bogotá. El inmueble de la Administración de Correos estuvo en pie durante siglo y medio y fue demolido en la segunda mitad del siglo XX para construir la residencia del Arzobispo de Bogotá.

El traslado de oficinas de correo de la Plaza Mayor se hizo al antiguo convento de Nuestra Señora del Rosario propiedad de los dominicos. En 1826 el Congreso eligió Presidente de la República al Libertador Simón Bolívar quién tomó posesión el 10 de septiembre de 1827 en las instalaciones del Claustro. El 18 de julio de 1861 se expide el decreto de manos muertas o expropiación de los bienes de los eclesiásticos y de esta manera el convento es ocupado por las tropas del general Mosquera.

Después del sismo de 1917 las oficinas de correos y telégrafos fueron trasladadas al pasaje Cuervo en la carrera 7 con Avenida Jiménez. Posteriormente en la época de la República, en 1847 siendo Presidente el General Tomás Cipriano de Mosquera, se adelantaron las primeras gestiones para la implantación del telégrafo eléctrico con la ayuda de la Gran Bretaña.

En 1851 el Presidente José Hilario López, contrató con la firma Ricardo de la Parra y compañía, la introducción del telégrafo eléctrico, concediéndole la exclusividad de su explotación por 40 años. Sin embargo, este proyecto no se pudo realizar debido a conflictos políticos acaecidos entre 1852-1854. Catorce años más tarde siendo Presidente Manuel Murillo Toro, se cursó el primer mensaje telegráfico entre Cuatro Esquinas (municipio de Mosquera) y Santafé de Bogotá.

Ahora bien, por medio del decreto 160 del 16 de abril de 1876, el Gobierno Nacional reglamentó por primera vez las normas para la construcción y conservación de líneas telegráficas a cargo de particulares, agrupando las líneas existentes en el país en ocho secciones. A su vez, en 1880 el Gobierno concedió permiso a la Compañía Central and South American Cable, para tender un cable submarino entre Panamá y cualquier República de América Central para que enlazara al país con los Estados Unidos vía México.

Posteriormente y después de aproximadamente 29 años, el Gobierno Nacional reasume la administración directa de los teléfonos y telégrafos nacionales, creando para ello la Intendencia de Telégrafos como organismo dependiente del Ministerio de Gobierno. En 1913, la compañía Marconi Wireless inició la prestación del servicio de radiotelegrafía en el país, con una red conformada por 12 ciudades.

En 1919 el Gobierno contrató con la misma empresa, la construcción de la Estación Internacional en Bogotá, obra que fue inaugurada después de cuatro años, es decir, el 12 de abril de 1923.

En 1927 se ordenó la destrucción del Convento de Nuestra Señora del Rosario y mediante las leyes 85 y 198 de 1926 y 195 se ordenó la construcción del Palacio de las Comunicaciones y después de múltiples críticas fue inaugurado en 1944.

En 1953 y por decreto 259 del 6 de febrero, el Gobierno Nacional determinó que a partir del 1 de febrero de ese mismo año el Ministerio de Correos y Telégrafos en adelante se denominaría Ministerio de Comunicaciones, reestructurándolo y estableciendo su funcionamiento con base en los departamentos de Correos, de Telecomunicaciones y Giros.

Para el año de 1976, por decreto 129 de enero 26 el Ministerio de Comunicaciones, es objeto de una nueva reestructuración con el fin de atender las necesidades resultantes de los cambios producidos por las tecnologías aplicadas a las telecomunicaciones y conformar el respectivo sector dentro de la rama ejecutiva del poder público.

Los cambios tecnológicos obligaron al Ministerio no solo a flexibilizar sobre su normatividad sino también este adecuó su la planta física de acuerdo con las exigencias arquitectónicas de la última década.

Desde 2008 se adelanta una remodelación total del edifico que incluye reforzamiento estructural antisísmico, y la recuperación de elementos como la bóveda de cañón que ilumina la primera planta. Así mismo desde el 30 de julio de 2009, fecha en la que el ex Presidente de la República Álvaro Uribe Vélez sancionó la Ley 1341 el entonces Ministerio de Comunicaciones se convirtió en Ministerio de Tecnologías de la Información y las Comunicaciones. La nueva Ley creó un marco normativo para el desarrollo del sector y promover: el acceso y uso de las TIC a través de la masificación, el impulso a la libre competencia, el uso eficiente de la infraestructura y en especial fortalecer la protección de los derechos de los usuarios.

El Edificio Murillo Toro, por su parte, adelanta la construcción del Museo Postal y de las comunicaciones que ya había sido propuesto en 1924 por el ingeniero Karl Ziegler, alto empleado de la administración de correo de Alemania contratado para analizar la defectuosa organización postal y la normatividad vigente.

Por iniciativa de la ex Ministra María del Rosario Guerra se reactivó la idea del Museo Postal recopilando colecciones patrimoniales de sellos emitidos por Colombia y por la UPU, se exhibirán piezas de especies filatélicas como buzones, trajes de carteros, básculas, porteadoras, entre otros. De igual manera se exhibirán elementos de cine, radio y televisión en exposiciones temporales, una manera de adecuarse al futuro a través de la historia.

Con el avance en la infraestructura de tecnologías de la información y las comunicaciones en Colombia, también progresa la regulación penal, que ha implicado la tipificación de delitos llamados informáticos, ya que de no hacerlo, se pondría en riesgo la seguridad nacional, la estabilidad económica, y los derechos o bienes jurídicos de las personas, por ende se introducen al ordenamiento jurídico colombiano tratados internacionales, como el convenio sobre ciber-criminalidad de Budapest del 23 de noviembre del 2001[1]; en este tipo de convenios, vemos que se busca que prime dentro de algún ordenamiento o grupo social la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes y los datos, del mismo modo hace alusión a la protección del uso fraudulento de aquellos sistemas de redes y datos como lo estipulan sus artículos 192 , 194 y 195 de dicho convenio.

Por ejemplo en el artículo 192 del convenio de Budapest, se implementa la sanción a quien destruya el vínculo de comunicaciones privadas, el daño de datos, y el daño en bien ajeno; de igual forma, se puede hablar de la protección de estos bienes a través de la ley penal colombiana.

Podemos resaltar que la vida moderna y contemporánea ha traído consigo un sin número de tecnologías que facilitan la captación de datos y la trasferencia de información personal vía ondas electromagnéticas, ejemplos de ello son el ordenador –como se lo llama en España, el computador personal, la Lap Top o portátil, que son de las herramientas

1 Colombia se ha ratificado en este Tratado internacional que pretende contrarrestar los delitos informáticos y los delitos en Internet mediante la estandarización de normatividad legal en la materia, la mejora de las técnicas de investigación y el aumento de la cooperación internacional en la misma dirección. Fue elaborado por el Consejo de Europa en la ciudad de Estrasburgo, con la participación de Estados observadores entre los cuales se destacan Canadá, Japón y China.

tecnológicas más útiles que el ser humano ha creado en las últimas décadas, pues además de ser artefactos fundamentales de uso cotidiano, éstos almacenan, crean y archivan imágenes, voz, señales y datos, y en las últimas generaciones se ha llegado a considerar que la tecnología mencionada es un ícono del progreso social, de racionalidad y crecimiento intelectual en todo ámbito social, cultural, político, jurídico, laboral; debido principalmente a que por medio de estos aparatos electrónicos se crean verdaderos proyectos intelectuales o se ejecutan millones de transacciones de toda índole, y a través de ellos se estructuran muchas de las cosas y creaciones de fácil uso o dominio para la gente en el mundo entero.

Por otra parte, existen otras tecnologías informáticas complementarias como los teléfonos celulares inteligentes, donde es posible estudiar, organizar datos, enviar mensajes, hacer conferencias, trabajar e incluso emplearlos como medios de entretenimiento y de creación de relaciones sociales, puesto que brindan alternativas masivas de contacto y comunicación entre diferentes partes del mundo, promoviendo entre otras cosas la interculturalidad del Planeta, resaltando que las redes sociales se han convertido en una fuente principal de comunicación masiva.

Hoy en día vemos que el computador a través del tiempo se ha convertido en una herramienta fundamental para la vida del ser humano en sociedad –por la información que en ellos se emite, transmite, comparte o divulga- y a través de este elemento o herramienta se ha incrementado un número considerable de crímenes cibernéticos (delito informático) afectando a las personas en cuanto a sus datos personales, empresas, entidades, comunidades, distintas naciones y gobiernos ya que el fenómeno de la criminalidad cibernética aumenta cada día más en la esfera de la tecnología, los medios informáticos y las tele-comunicaciones.

Se hace oportuno mencionar que la informática y las ciencias de la tecnología en los últimos 50 años han avanzado de manera casi incontrolable, irreversible e incontenible, puesto que es arrollador la manera en que estas ciencias han evolucionado; asunto que refleja grandes beneficios en cuanto a las facilidades de la comunicación y el almacenamiento de la información; y también, se presenta una serie de insatisfacciones de parte de muchos usuarios que creen que se puede estar violentado su privacidad, su honra y su intimidad en la medida que la desconfianza de parte del ser humano hacia otros que

puedan asaltar su información y utilizarla en beneficio propio o en perjuicio de ellos, justificado en que es quien ostenta la información quien ejerce dominio y poder sobre quien la carece. Todo lo anterior, se podría hacer fácilmente solo utilizando una herramienta cibernética como lo es un computador o un teléfono celular inteligente, accediendo a una plataforma tan grande, simple y fácil de acceder como lo es la Internet, el Facebook, el Twitter e incluso el mismo WhatsApp o los correos electrónicos personales o institucionales, o quien pueda acceder a bases de datos privilegiadas, bases de información financiera, o de seguridad pública teniendo a su merced información única, exclusiva de quien real y solamente pertenece (Sánchez Cano, 2016).

Los antecedentes en el tiempo en cuanto al tema, se pueden remitir 27 años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software (Virgilio, 1989).

Al respecto, ha escrito por ejemplo María Yolanda Álvarez y Luz María Restrepo de la Universidad Pontificia Bolivariana, en su libro "EL DERECHO DE AUTOR Y EL SOFTWARE" donde ésta obra contribuye a la formación y protección de una cultura autoral, y de las creaciones del intelecto humano en el marco de la vanguardia cibernética en Colombia, pues argumentan que el Derecho es la herramienta fundamental que protege los datos y los derechos del autor intelectual, resaltando la importancia que tiene para la vida socioeconómica moderna la producción y la gestión de la información (Álvarez María y Restrepo Luz, 1997).

A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas. En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las

violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano: Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones. El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles. (Congreso de la República de Colombia, 2012)

El Código Penal Colombiano expedido con la Ley 599 de 2000, no hacía referencia expresa a los delitos informáticos como tales; no obstante, en varias de sus normas recoge conductas que podrían entenderse incorporadas al concepto que la doctrina ha elaborado a este respecto; pero en la actualidad, está vigente La Ley 1273 de 2009 del 5 de enero de 2009, llamada la Ley de los delitos informáticos, que complementa el Código Penal y crea un nuevo bien jurídico tutelable actualmente llamado "De la protección de la información y de los datos". (Congreso de la República de Colombia, 2012).

En Colombia con la expedición de la Ley 527 de 1999 y su decreto reglamentario 1747 de 2000, se reconoció fuerza probatoria como documentos a los mensajes de datos. El artículo 10º de la Ley 527/99 regla: "Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de procedimiento Civil" (Congreso de la República de Colombia, 1999).

La Corte Constitucional en sentencia C-662 de junio 8 de 2000, con ponencia del Magistrado Fabio Morón Díaz, al pronunciarse sobre la constitucionalidad de la Ley 527 de 1999, hizo las siguientes consideraciones: *"El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento"(Corte Constitucional, 2000).*

El proyecto de ley establece que estos crímenes tendrán penas de prisión de 4 a 8 años para los delincuentes informáticos y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes. Entre las conductas tipificadas como delito están el acceso abusivo a sistemas informáticos, la obstaculización ilegítima de sistemas computacionales o redes de telecomunicaciones, la interceptación de datos informáticos, el uso de software malicioso, la violación de datos personales y la suplantación de portales de Internet para capturar datos personales, entre otras; destacándose:

1. **Violación de datos personales.**

Este delito cobijará a quienes, sin estar facultados para ello, con provecho propio o de un tercero, obtengan, compilen, sustraigan, ofrezcan, vendan, intercambien, envíen, compren, intercepten, divulguen, modifiquen o empleen códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

2. **Acceso abusivo a un sistema informático.**

Será sancionado quien sin autorización acceda a un sistema informático protegido o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

3. **Obstaculización ilegítima de sistema informático o red de telecomunicación.**

Se penalizará a quien impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

4. **Interceptación de datos informáticos.**

Bajo este delito serán castigadas las personas que, sin orden judicial previa, intercepten datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte.

5. **Daño informático.**

Se sancionará a quien, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

6. **Uso de software malicioso. (Malware)**

El proyecto de ley señala que serán castigadas las personas que, sin estar facultadas para ello, produzcan, trafiquen, adquieran, distribuyan, vendan, envíen, introduzcan o extraigan del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

7. **Suplantación de sitios web para capturar datos personales. (Phisihnig)**

Será sancionado quien, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes. También quien modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una dirección IP (Internet Protocol) diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. En este caso, la pena se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Importantes Antecedentes normativos:

- Artículo 15 de la constitución Política de Colombia.
- La norma ISO/IEC 27001 es un estándar para la seguridad de la información.
- Congreso ciberterrorismo de Budapest 2001.
- La Ley 1273 del 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- LEY ESTATUTARIA 1581 DE 2012 (Octubre 17), Reglamentada parcialmente por el Decreto Nacional 1377 de 2013**.** Por la cual se dictan disposiciones generales para la protección de datos personales; conocida como la Ley de Habeas Data.

3. Problema Jurídico

¿El diseño del tipo penal de violación de datos personales ofrece una adecuada protección al Derecho a la intimidad y al buen nombre?

3.1 Descripción del Problema Jurídico

Esta problemática actual de la violación de datos personales a través de los diferentes sistemas cibernéticos o virtuales se ha manifestado como un nuevo campo de investigación, en donde se hace necesario el conocimiento técnico y científico de diversas profesiones relacionadas con la tecnología (ingeniería de sistemas, telemáticas, e informáticas) ya que cada vez los niveles de control y medios de seguridad han quedado doblegados a la audacia de los nuevos autores de esta clase de delitos que infringen la norma y sustraen información personal o datos personales, datos sensibles, claves o códigos de seguridad y por tanto sacan provecho vulnerando los derechos fundamentales de la intimidad, el buen nombre y la honra e incluso el patrimonio económico de las personas.

Considero que es muy importante dar más peso al análisis e investigación universitaria y académica pues este nuevo campo de investigación ha sido poco explorado, por ello se quiere hacer nuevas propuestas que permitan la protección de los datos que se encuentran en medios virtuales de las personas, como también la defensa de estos derechos personales. Es fundamental indagar en el estudio de estos tipos penales (delitos informáticos) ya que muchos de estos hechos quedan impunes ante la justicia y no se puede llegar a una reparación adecuada de las víctimas, pues resultan difícil a nivel probatorio y la tecnología en las investigaciones suele no ser tan eficaz dado que es un tipo de conducta punible relativamente nueva y en constante dinamismo que se puede ejecutar desde cualquier computador conectado a la Internet en un remoto lugar. En este estudio académico se ven implicados sistemas de información, redes de telecomunicación, propiedad intelectual, las redes sociales en conexidad con la integridad de las personas, su moral, su intimidad, su seguridad, patrimonio, su familia y en general con la dignidad del ser humano.

4. Objetivo General

- Determinar si el diseño del tipo penal de "VIOLACIÓN DE DATOS PERSONALES ARTÍCULO 269F DEL CÓDIGO PENAL" garantiza una adecuada protección al derecho a la intimidad y buen nombre.

4.1 Objetivos Específicos

1. Establecer los alcances dogmáticos del tipo penal 269F del Código Penal.

2. Determinar desde el punto de vista Constitucional el contenido y significado del Derecho a la Intimidad y al Buen Nombre.

3. Identificar las formas como puede ser afectado el Derecho a la Intimidad y al Buen Nombre.

5. Justificación

Dado el problema de investigación, y desde el punto de vista sociológico, jurídico, económico, científico, y sobre todo, desde la perspectiva constitucional, se pretende justificar este tema de tesis teniendo en cuenta que se necesita dar respuestas oportunas y eficaces desde los enfoques mencionados frente a esta realidad actual y futurista que representan los llamados delitos informáticos, más específicamente frente al tipo penal expresado en el artículo 269F (delito de violación de datos personales) del Código Penal, puesto que la idea es fortalecer la seguridad jurídica y el cumplimiento de la norma, a la hora de proteger los derechos constitucionales fundamentales de la sociedad colombiana cuando acceden a los diferentes sistemas de redes sociales, comunicaciones y en general a todo tipo de sistemas informáticos de variada complejidad, ya que es una necesidad de la vida moderna el acceder a estos medios para hacer nuestras vidas más fácil, integrada, asertiva y comunicativa en vista de que son necesarios en cuanto a los ámbitos laboral, social, familiar e inclusive necesarios en los escenarios internacionales, y consecuentemente ir a tono con las exigencias de una vida contemporánea del siglo XXI.

Es por esto que, pretendo analizar el tipo penal mencionado y verificar si el diseño de este tipo penal (Art.269F del C. Penal) ofrece una respuesta jurídica oportuna y eficaz que proteja adecuadamente el derecho constitucional a la intimidad y al buen nombre, para después y dado este proyecto de investigación hacer propuestas un poco más completas atemperadas a derecho que permitan un mejor desenvolvimiento, y hacer un frente más adecuado ante este relativamente nuevo tipo de delito, que usa la tecnología como medio delincuencial, pues son muy importantes los bienes jurídicos y derechos fundamentales que se ven afectados o vulnerados cuando somos víctimas de los llamados delitos informáticos, ya que como veremos se argumentará a través de esta propuesta de investigación, que es un tipo de delito pluriofensivo que afecta tanto el patrimonio económico como la dignidad humana a través de la violación a la intimidad y la usurpación de datos personales; es decir va en contra vía del artículo 15 de la Constitución Política Nacional que salvaguarda en su teoría el derecho a la intimidad, buen nombre y la honra.

Para defender esta tesis pongo en evidencia y parto de la base que la legislación colombiana ha hecho un gran avance al proteger de manera especial dentro del Código Penal los derechos de las personas cuando de delitos informáticos se trata, y que desafortunadamente la misma legislación colombiana se queda corta a la hora de desarrollar la protección efectiva de estos derechos procesalmente hablando, puesto que los delincuentes siempre perfeccionan sus métodos para infiltrarse en los diferentes sistemas informáticos y hacer fechorías que atentan contra el patrimonio material o inmaterial de las personas que interactúan a través de redes sociales, bancos, Internet y demás bases de datos que ostentan información privilegiada de hombres y mujeres sin distinción de ninguna clase o condición, por lo cual, todos los ciudadanos somos vulnerables a este tipo de delitos.

Es evidente que necesitamos implementar en nuestra sociedad estrategias tendientes a mejorar la seguridad informática y atacar la problemática penal bajo estudio, para así lograr que no se sigan viendo afectados los bienes tanto materiales como inmateriales involucrados en esta problemática jurídico-penal-social. Es oportuno entonces, mencionar que el Derecho se crea como respuesta a los hechos sociales, y en este caso en concreto el hecho social es la sociedad contemporánea y los medios masivos de información digital, mega bases de datos, cuentas electromagnéticas entre otras y el derecho a la protección de datos personales e inviolabilidad de los mismos es la respuesta a ese hecho social, entonces jurídicamente deseo proponer mejoraras al Derecho que responde a esa problemática señalada y crear mecanismos que aseguren o por lo menos contribuyan al restablecimiento de los derechos cuando hayan sido vulnerados por medio de conductas delictivas tecnológico-cibernéticas, y de esta manera evitar o mitigar el daño antijurídico en este contexto, y especialmente, construir o aportar ideas que contribuyan integralmente a prevenir que las personas sean sujetos pasivos de delitos informáticos en la sociedad colombiana e incluso en otras latitudes, dado que existe la falsa creencia de que lo tecnológico actual es altamente confiable, avanzado, creativo e innovador y el amparo que ofrecen los nombres de las compañías en donde almacenamos nuestra información nos hace sentir relativamente seguros; no obstante, hasta las plataformas aparentemente más seguras han sido vulneradas, infiltradas, accedidas y bloqueadas, demostrándose con esto la latente e inminente debilidad de las transacciones que se hacen en la vida cotidiana personal, laboral o institucional pública, académica, social o privada.

La Universidad Libre seccional Cali, a través del Centro de Investigaciones de la Facultad de Derecho (CIFADER) ha apoyado este tema como proyecto de grado; por ello, ésta investigación jurídica está radicada como propuesta esencial de tesis de grado para optar por el título de ABOGADO, por lo tanto espero seguir construyendo futuro y contribuyendo con herramientas jurídicas a la investigación académica y científica del Alma Mater, y especialmente a brindar elementos a los ciudadanos para que adopten medidas preventivas y conductas más seguras en el manejo de su información personal relevante.

6. Marco Contextual – Histórico

Los delitos informáticos – delito de violación de datos de carácter personal, aparece conforme avanza la modernidad y la sociedad contemporánea se hace usuaria casi dependiente de las tecnologías de la información y las comunicaciones; hoy en día se dice que la humanidad se encuentra en la era de la Globalización, en la era de la tecnología y las redes de comunicaciones, en donde la sociedad actual se desarrolla en todos los ámbitos (social, cultural, laboral, político, familiar y económico) con ayuda de las implementaciones y herramientas tecnológicas que aparecen para mejorar y fortalecer los ámbitos y las condiciones de la vida en las que se desenvuelven las personas. En este mismo sentido, se entiende que el lugar, contexto y desarrollo del problema jurídico específico de esta tesis de Derecho, Ciencias Políticas y Sociales, no es exclusivo de un país del mundo, sino que por el contrario es una problemática transnacional, en la cual para incurrir en la conducta penal no se necesita estar ubicado en la misma esfera geoespacial de la víctima, sino que puede ser cometida desde cualquier lugar del mundo con acceso a la Internet o con acceso al sistema informático contentivo de la información íntima de la gente, datos personales, datos sensibles, documentos, correspondencia, la cual es vulnerada o irrumpida ilícitamente y sin autorización, hasta configurar la conducta penal reprochable y castigable por la Ley penal, por ser violatoria a derechos humanos fundamentales elevados al rango constitucional.

La sociedad de la era de la información y las telecomunicaciones surge gracias a la revolución de los computadores y la informática después de la segunda mitad del siglo XX, con mayor intensidad y expansión después de la apertura económica, la integración de las regiones, el comercio internacional, la Globalización, el acceso y la masificación de la vanguardia tecnológica, donde los artefactos desarrollados por el hombre han hecho que las personas sean dependientes de ellos, facilitándose incluso la vulneración de la dignidad humana a través de las nuevas conductas punibles que utilizan como medio los avances científico-tecnológicos , esto se crea, y se transmite dentro de un nuevo mundo cibernético o virtual complejo, donde el Derecho ha tenido que intervenir por cuanto es el Estado el llamado a regular, sancionar, dirimir y ajusticiar las controversias y fenómenos sociales que se presentan gracias a esta nueva realidad “cibernética”, por lo anterior el Derecho ha

evolucionado creando un nuevo objeto jurídico de especial protección donde el bien jurídico tutelado se denomina “De la Protección de la información y de los datos” Bien jurídico taxativo en el título séptimo de la Ley 599/2000 Código Penal Colombiano (Congreso de la República de Colombia, 2012, p. 125).

7. Marco Conceptual

Para poner en un contexto actualizado al lector neófito o no en el tema de los delitos informáticos, y por supuesto en el tema de la violación de datos personales, se comparte un conjunto sencillo de conceptos que se utiliza como marco conceptual en el contexto de este ejercicio de investigación jurídica con el propósito de facilitar la comprensión del problema, las implicaciones del punible bajo estudio y las alternativas preventivas que se deben tener en la sociedad con los datos que la gente almacena en la multiplicidad de herramientas y dispositivos tecnológicos que cada vez son más numerosos y de diversa índole, costo o complejidad. Las definiciones han sido elaboradas a partir de la investigación y construcción propia de esta tesis jurídica académica, y se presenta en orden alfabético así:

Base de datos: Es un conjunto de información física o en medio magnético relacionada entre sí que se encuentra agrupada o estructurada. La base de datos magnética puede decirse que es un sistema formado por un conjunto de datos almacenados dentro de un software, que contiene información comparable y que se accede directamente a ella por medios electrónicos. Está compuesta por tablas que guardan un conjunto de datos. Cada tabla tiene columnas y filas; que vinculadas entre sí conforman registros individuales accesibles con programas o aplicaciones particulares o comerciales.

Bomba lógica: Tipo de virus informático que se activa al momento de realizar determinada acción, puede bloquear, destruir o copiar información y datos de uno o varios sistemas.

Buen nombre: El buen nombre alude al concepto-valor que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. Representa uno de los más valiosos elementos del patrimonio moral y social de la persona y constituye un factor indispensable de la dignidad que a cada uno debe ser reconocida.

Código: Es una combinación de signos que tiene un determinado valor dentro de un sistema informático establecido.

Confidencialidad: Es la confianza estrecha e íntima entre las personas y su información personal contenida o almacenada en dispositivos o en sistemas electrónicos, tecnológicos o informáticos.

Cracker: Su significado deriva del inglés, "Crack" romper; es una persona u organización con altos conocimientos en informática que tiene saberes, experiencias y técnicas para romper sistemas de seguridad con distintos fines o móviles, estas personas u organizaciones son hábiles en eliminar las funciones preestablecidas de un Sistema de Seguridad en un computador, un sistema o una red informática, teniendo acceso a ella, y, pudiendo obtener información de datos en general de manera ilícita, por ende punible, y castigable por el Derecho Penal colombiano e internacional.

Dato: El concepto de dato en forma amplia, es toda información particular codificada y codificable, que desde el punto de vista de las tecnologías de la información y las comunicaciones (TIC), es una información dispuesta de manera adecuada para su tratamiento o acceso por medio de un ordenador u otra tecnología informática.

Dato personal: Es la información particular o general contenida en variables concernientes a una persona identificada o identificable.

Dato sensible: Son los datos personales de la esfera más íntima de una persona, cuya utilización indebida puede dar origen a perjudicar, discriminar o afectar gravemente a dicha persona sea en su integridad personal, imagen social, o patrimonio económico.

Delito informático: Son los actos o conductas ilícitas realizadas por un ser humano o por una organización criminal dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, que son susceptibles de ser sancionados por el Derecho penal.

Derechos de autor: Son los derechos que se derivan de ostentar la propiedad de una creación artística, obra literaria o invento, comprende por ejemplo libros, canciones, pinturas, esculturas, partituras, películas, diseños, programas informáticos, bases de datos, anuncios publicitarios, mapas, y dibujos técnicos, entre otros.

Fichero / Archivo: El Fichero o Archivo es todo conjunto organizado o no de datos de carácter personal, colectivo o institucional, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Hacker: Es una persona u organización criminal con conocimientos y habilidades en informática que cuenta(n) con un dominio superior al común en lo que respecta a la Programación, y que ingresa ilegalmente a los sistemas informáticos personales o institucionales y redes ajenas como desafío intelectual, y potencialmente como sujeto activo del delito de violación de datos personales, colectivos o institucionales. Este tipo de sujetos u organizaciones criminales son capaces de penetrar en Sistemas Informáticos protegidos, acceder a Bases de Datos y sustraer información confidencial o privilegiada para beneficio personal o por simple gusto o estímulo a su autoestima tecnológica.

Hardware: Es un término en inglés (producto duro o pesado) que hace referencia a los elementos físicos tecnológicos que trabajan o de alguna manera interactúan con el computador o con las herramientas informáticas de manera alámbrica o inalámbrica, incluye elementos internos como el CD-ROM, discos duros interno y externo, disqueteras, lectores y lápices ópticos, cableado inteligente, circuitos electrónicos, gabinetes, mouse, impresoras, escáner, monitores, CPU, pantallas de video, teclado, video beam, detectores de calor, humo, olores, metales, y otros dispositivos.

Honra: Es la estima y respeto de la dignidad propia de cada persona, obedece a la buena opinión, fama o imagen adquirida por la virtud y el mérito de cada quien.

Informática: Conjunto de herramientas tecnológicas disponibles para el procesamiento automático de información, mediante las interacción de dispositivos electrónicos, hardware y sistemas de cómputo o redes conectadas por tecnologías compatibles.

Internet: Es la herramienta cibernética más grande creada en el mundo contemporáneo, es llamada **"**Red informática mundial", descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

Intimidad: Es la zona espiritual íntima o de valor más reservada de una persona. Refiere también a sentimientos, creencias políticas o religiosas, incluye sus datos propios o patrimoniales, códigos claves, información reservada e información clínica o del estado de salud, así como la relativa a la vida sexual de un ser humano, un colectivo, institución o una persona jurídica.

Malware: Es un tipo de "software malo", código maligno, software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar un computador, una red o sistema de información sin el consentimiento de su propietario.

Phishing: Derivación en inglés de "fishing" o "pesca". Se refiere a la captación de datos personales realizada de manera ilícita o fraudulenta a través de Internet. Este método delictivo-informático consiste en una técnica para captar información bancaria o financiera y datos personales de los usuarios del sistema financiero a través de la utilización de la imagen o del sitio web de una la entidad financiera pública o privada.

Privacidad: Es la Información más allá de la intimidad de una persona, que puede definir el perfil de una persona natural o jurídica.

Propiedad intelectual: Es el derecho intangible e inalienable que tiene una persona, cuando fruto de su ingenio o talento, desarrolla una cosa en el ámbito científico, literario, artístico, cultural, industrial o comercial. Este tipo de propiedad goza de especial protección en los Estados modernos.

Red social: Es un conjunto de individuos con equipos electrónicos interconectados que comparten información y que interactúan entre sí para formar una comunidad, siendo la red social una estructura donde tales individuos mantienen vínculos de amistad, de colegas, familiares, sexuales, comunicacionales, laborales o comerciales, entre otros**.** Dichas redes sociales permiten compartir entre personas de todas partes del mundo cualquier tipo de información que se trasmite a través de medios virtuales, tales como sonidos, música, videos, creaciones artísticas, diseños, escritos, dibujos, fotos, mapas, mensaje, noticias, comunicados, esquemas y prototipos entre otros. La red social más popular y utilizada en el mundo es Facebook que tiene más de 1.300 millones de usuarios, y existen otras redes sociales tales como MySpace, Hi5, Linked In, YouTube y Twitter.

Sistema informático: Es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son el hardware, el software y las personas que lo administran y lo usan. De esta manera, y en forma sencilla una persona, su computador personal, los programas y su información o creaciones contenidas en el computador, constituyen un sistema informático.

Software: Es el término en inglés (producto liviano o blando) que hace referencia a los programas o aplicaciones de programación necesarios en lenguaje de máquina (assembler) u otros lenguajes para realizar o ejecutar funciones específicas que se conectan con el hardware o con las redes e incluso con otros programas. El término software incluye diseños escritos en lenguaje de programación, diseño de la arquitectura y su ingeniería, incluye también el sistema operativo de la computadora, controladores, dispositivos, herramientas de diagnóstico, procedimientos, gestión integral de los servidores, navegadores, editores de texto, editores gráficos y de sonido, antivirus y la memoria, entre otros.

Spam: Se define como un tipo de correo electrónico no solicitado o que aparenta serlo que se envía a un gran número de destinatarios con fines publicitarios o comerciales.

Spyware: Es un tipo de software malicioso (software que espía), que accede a los datos de un computador, portátil, tableta, teléfono celular o dispositivos similares y los envía a otros dispositivos sin que la persona "espiada" lo advierta o se dé cuenta de que ha sido irrumpido electrónicamente.

Vida privada: Es un concepto que abarca múltiples aspectos relativos con la integridad física, moral, psicológica y social de una persona. Los límites de la vida privada de la gente, por lo general están en las fronteras que establecen las mismas personas, ya que algunos exponen mayor o menor cantidad de información íntima según el grado de libertad o extroversión de la misma.

8. Marco Teórico

En este marco teórico, se presenta un breve resumen de las teorias que por su naturaleza y esencia se relacionan con el tema objeto de este estudio academico, siendo estas teorias relevantes dado que se presentan como doctrina ajustada a la ciencia, seria, oportuna y pertinente, las cuales tienen un amplio sustento hermeneutico y de pleno reconocimiento a nivel mundial.

Teoría del Derecho:

El Derecho como conjunto de normas sistemáticamente organizadas para regular las relaciones de la sociedad, con carácter coercitivo y de obligatorio cumplimiento se conforma de varios elementos los cuales son descritos y tomados a partir de la obra "Teoría del Derecho" de Máximo Pacheco Gómez, autor de origen Chileno Profesor y ex Decano de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Chile, que aporta en gran medida a la compilación de la teoría del Derecho y que sus estudios configuran una doctrina básica para el estudio de la ciencia del Derecho existente en toda organización social y los fundamentos de carácter científicos y filosóficos que han permito establecer un orden dentro de las sociedades contemporáneas.

El Doctor Máximo Pacheco Gómez en su teoría, determina los elementos básicos que conforman el Derecho mostrando con amplia fundamentación los orígenes, características, funciones, valides, importancia, desarrollo, y en fin una gran cantidad de conceptos que se hace necesario conocer para fundamentar, atemperado a la ciencia jurídica, la construcción de esta investigación jurídica.

Según el mencionado autor: "La regulación externa de la conducta de los hombres, tendiente a establecer un ordenamiento justo de la convivencia humana, es lo que se denomina Derecho. La justicia es el valor absoluto que determina la igualdad que debe existir en las relaciones humanas y ella se expresa a través del Derecho. La justicia, en consecuencia, es el valor supremo del Derecho; y el Derecho, por su parte, aquello que realiza la justicia."(Pacheco Gómez, 1993).

La Teoría Pura del Derecho:

Otra de las teorías más importantes tenidas en cuenta para demostrar la validez de esta investigación jurídica – académica, es la Obra jurídica del célebre filósofo del Derecho de origen austríaco Hans Kelsen, quien hizo importantes contribuciones al estudio de la ciencia del Derecho a toda la tradición jurídica europea, norteamericana, y suramericana, pues a través de su reconocida obra otorgó al Derecho una unidad integradora, y le dio también el carácter científico, además principalmente consagra a la Ciencia Jurídica como una disciplina positivista (Derecho Positivo).

La Teoría pura del Derecho trata de sustentar el Derecho positivo como un orden normativo estricto, jerarquizado y supeditado a una norma de mayor rango de la cual se derivan todas las demás, siendo los objetivos de esta teoría la establecer el carácter científico del estudio del Derecho y aislar ideologías subjetivas del mismo.

(Kelsen, 2009) sustenta un ordenamiento jurídico sobre la base de la jerarquía normativa argumentando que toda norma obtiene su vigencia de una norma superior (Pirámide de Kelsen). Esta jerarquía contempla la Constitución como la norma principal que da valides al ordenamiento jurídico, sin embargo, la Constitución tiene a su vez una norma primaria o fundante denominada por ésta teoría como Norma Fundamental, Norma Fundante Básica o Gran Norma.

El trabajo elaborado por este importante autor se toma como base para la construcción de esta tesis jurídica dada la relación que dicha teoría tiene con el ordenamiento jurídico nuestro, donde en Colombia prima la Constitución como norma fundamental de la sociedad y donde la Constitucionalización del Derecho a permitido que surja el Estado Social de Derecho fundamentando y otorgando validez a todas las normas y leyes en el respeto de principios, valores y Derechos humanos fundamentales.

La perspectiva constitucional de esta tesis jurídica – académica hace que sea necesario revisar los postulados de Kelsen que dan un orden y carácter estructural a la investigación jurídica.

Teoría impura del Derecho:

"Teoría impura del Derecho, La Transformación de la Cultura Jurídica Latinoamericana" de Diego Eduardo López Medina (Abogado y Filósofo)[2]: Esta obra literaria - doctrinal de este autor colombiano se toma como referencia para la elaboración del presente trabajo puesto que referencia muy bien la historia de la integración de la ciencia del Derecho traída de Europa (Sitio de producción original - intelectual) a la cultura jurídica de América Latina (Sitio de recepción) y por supuesto, Colombia. Es una excelente obra que muestra una Teoría aterrizada de la trasformación y mutación que tuvo el Derecho cuando se trasplantó en América Latina y Colombia.

[2] Diego Eduardo López Medina, nacido en Colombia y egresado de la Universidad de Harvard en los Estados Unidos; Realizó estudios de maestría y doctorado en Derecho. Diego E. López ha sido galardonado con la medalla al mérito académico "Andrés Bello" por el Ministerio de Educación Nacional de Colombia. Actualmente vive en Colombia, y ejerce la docencia y la investigación en la Universidad los Andes y la Universidad Nacional de Colombia. Autor de la obra *"El Derecho de los Jueces"* y también de *"La Teoría impura del Derecho, la transformación de la cultura jurídica latinoamericana"*. Profesor reconocido en las Facultades de Derecho de Colombia y Latinoamérica.

La referencia que se toma de la ideología y teoría de este importante jurista colombiano radica en la relevancia que éste hace del precedente judicial para hacer un análisis ajustado a Derecho de cualquier tema o investigación socio – jurídico, pues al investigar la realidad normativa vigente aplicable y cómo las decisiones de las altas cortes van creando reglas aplicables a casos y/o temas análogos posteriores, donde dichas reglas o sub-reglas son de obligatoria observancia y de hecho vincula a la misma Alta Corte (precedente horizontal) y a los demás jueces de inferior jerarquía (precedente vertical) dentro del mismo ordenamiento jurídico. Según la teoría del precedente judicial, la jurisprudencia es fuente de Derecho, y según una interpretación amplia de la Ley, los Jueces siguen sometidos al imperio de la Ley; donde la Ley es en este contexto, La Jurisprudencia.

Desde este enfoque explica en su "Teoría Impura del Derecho", que la implementación del Derecho y su doctrina en América Latina - Colombia ha sido incorporado por importantes autores del Derecho locales, que sin embargo, hicieron una transcripción, copia, transmutación y traducción literal de las doctrinas europeas, las cuales fueron escritas para contextos sociales, políticos, institucionales, culturales etc., diferentes a los existentes en el nuevo continente por cuanto los trasplantes de dichas teorías ha sido transformada, moldeada y ajustada para que pueda alcanzar un buen nivel de aceptación, validez, eficacia, y operatividad, pues no ha sido fácil instaurar un orden social a través del Estado para que las personas convivan con respeto a los derechos inherentes a la condición de seres humanos.

La Transformación de la Cultura jurídica Latinoamericana en los últimos años ha venido dando una prevalencia a la constitucionalización del Derecho, y las Altas cortes Constitucionales ya son una constante en todo el continente; estas cortes en la actualidad tienen una gran importancia dentro de los ordenamientos jurídicos Latinoamericanos, incluyendo Colombia, puesto que son la instancia que salvaguarda la integridad de los postulados y principios más importantes del Estado, incluyendo los Derechos Humanos Fundamentales, las libertades básicas, los Derechos económicos, sociales y culturales, y los derechos al medio ambiente sano y ecológico; todo ello en un marco de prevalencia de los

mencionados principios y derechos buscando satisfacer el bien común y mejorar las condiciones de vida de la sociedad.

Es importante reconocer y tener en cuenta el trabajo de este Filósofo y Abogado Colombiano puesto su obra es un referente nacional e internacional para pensar el nuevo Derecho, para proponer alternativas viables a la solución de los problemas que surgen en la sociedad, y también porque su obra sirve para entender el trasfondo de la verdadera Teoría del Derecho, necesaria para elaborar un excelente análisis del tipo penal propuesto desde la óptica del Derecho Constitucional.

> *El núcleo del derecho legal ordinario en una jurisdicción neorrománica contiene, entonces, soluciones para conflictos que involucran a la persona y sus atributos, la propiedad, las relaciones obligacionales y contractuales y la sucesión. La definición de derechos subjetivos en la esfera civil o privada resulta excluyente, al menos en los países semiperiféricos de Latinoamérica (López Medina, 2005).*

Teoría de los delitos informáticos:

(Rovira del Canto, 2002) , autor de origen español, que en su obra "Delincuencia informática y fraudes informáticos", define tanto los delitos informáticos de manera genérica, como de forma particular el delito de violación de datos informáticos, esta conducta ilícita la asemeja al término "Hacking informático". Según el autor de origen español el término "Hacking" tradicionalmente describe la mera entrada o acceso a sistemas informáticos por el mero gusto de superar las medidas técnicas de seguridad, esto es, sin intención o finalidad alguna de manipulación, defraudación, sabotaje, o espionaje. Pese a lo anterior, su conducta es considerada lesiva, pues traspasa la "formal esfera de la privacidad y del secreto" o "la integridad del sistema informático afectado".

Rovira del Canto es un reconocido jurista español que toda su investigación docente es enfocada al tema de los delitos informáticos, fraudes informáticos, nuevas formas de delincuencia cibernética entre otras, las cuales tienen un amplio reconocimiento mundial por cuanto su obra, trayectoria y estudios lo han convertido en una autoridad sobre el tema objeto de esta tesis jurídico – académica.

Teoría de los Sistemas:

La Teoría General de Sistemas del alemán Ludwig von Bertalanffy (biólogo y filósofo) publicados entre 1950 y 1968 busca solucionar problemas y producir teorías y formulaciones conceptuales que pueden crear condiciones de aplicación en la realidad empírica.

Von Bertalanffy utilizó los principios allí expuestos para explorar y explicar temas científicos, incluyendo una concepción humanista de la naturaleza humana, opuesta a la concepción mecanicista y robótica. La teoría general de sistemas afirma que las propiedades de los sistemas no pueden describirse significativamente en términos de sus elementos separados. La compresión de los sistemas sólo ocurre cuando se estudian globalmente, involucrando todas las interdependencias de sus partes.

Los supuestos básicos de la Teoría General de Sistemas son:

- Existe una nítida tendencia hacia la integración de diversas ciencias naturales y sociales.
- Esa integración parece orientarse rumbo a una teoría de sistemas.
- Dicha teoría de sistemas puede ser una manera más amplia de estudiar los campos no-físicos del conocimiento científico, especialmente en ciencias sociales.
- Con esa teoría de los sistemas, al desarrollar principios unificadores que atraviesan verticalmente los universos particulares de las diversas ciencias involucradas, nos aproximamos al objetivo de la unidad de la ciencia.

- Esto puede generar una integración muy necesaria en la educación científica.

La Teoría General de Sistemas afirma que las propiedades de los sistemas, no pueden ser descritos en términos de sus elementos separados; su comprensión se presenta cuando se estudian globalmente.

La Teoría General de Sistemas se fundamenta en tres premisas básicas:

1. Los sistemas existen dentro de sistemas: cada sistema existe dentro de otro más grande.
2. Los sistemas son abiertos: es consecuencia del anterior.
3. Las funciones de un sistema dependen de su estructura.

La Teoría General de Sistemas busca las materializaciones concretas y particularistas del orden abstracto y de la ley formal que descubre.

(Von Bertalanffy, 1968) aseguró que el "sistema" es un conjunto de unidades recíprocamente relacionadas, de los que se deduce dos conceptos: (El propósito u Objetivo y el Globalismo o Totalidad). La clasificación de un sistema al igual que el análisis de los aspectos del mismo es un proceso subjetivo; depende del individuo que lo hace, del objetivo que se persigue y de las circunstancias particulares en las cuales se desarrolla.

De acuerdo a los datos aportados por Bertalanffy, lo aplicable a esta investigación jurídica – social relacionada con los delitos informáticos, son los sistemas Abstractos (Sistema simbólico o conceptual) y los Sistemas Artificiales (Sistema producto de la actividad humana), los cuales son concebidos y construidos por el hombre, como lo son por ejemplo los sistemas informáticos.

9. Marco Jurídico Legal

En este marco de la investigación, se procede con la revisión de la normatividad legal más importante de carácter nacional e internacional, y la jurisprudencia complementaria respecto al tema bajo estudio, a saber:

- Constitución Política de Colombia de 1991.
- La Declaración Universal de Derechos Humanos de 1948.
- La Convención Americana sobre Derechos Humanos de 1969.
- El Pacto Internacional de Derechos Civiles y Políticos de 1966.
- El Convenio Europeo de Derechos Humanos de 1950.
- La Carta de Derechos Fundamentales de la Unión Europea del año 2000.
- Código Penal - Ley 599 de 2000.
- Ley 1273 de 2009. (05 de Enero) Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "De la Protección de la información y de los datos".
- Ley Estatutaria 1581 de 2012 (17 de Octubre), reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Corte constitucional Colombiana, Sentencia T-696 de 1996 Magistrado Ponente Dr., Fabio Morón Díaz.
- Corte Constitucional Colombiana, Sentencia C-748 de 2011 con Magistrado Ponente el Dr. Jorge Ignacio Pretelt Chaljub.
- Corte Constitucional Colombiana, Sentencia T-229 de 1994 del Magistrado Ponente Dr. José Gregorio Hernández.
- **SENTENCIA SP1245-2015**, **Radicación N. 42.724** (Aprobado Acta No. 44) Bogotá D.C., once (11) de febrero de dos mil quince (2015). SALA DE CASACIÓN PENAL CORTE SUPREMA DE JUSTICIA, **MP: EYDER PATIÑO CABRERA.**

Constitución Política de Colombia:

"Derecho a la intimidad, al buen nombre habeas data, inviolabilidad de correspondencia y documentos privados"

ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en 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.

NOTA: El artículo 15 fue modificado por el Acto Legislativo 02 de 2003, el cual fue declarado **INEXEQUIBLE** por la Corte Constitucional mediante **Sentencia C-816 de 2004,** por el vicio de procedimiento ocurrido en el sexto debate de la segunda vuelta.

CODIGO PENAL COLOMBIANO, Ley 599 de 2000:

TÍTULO VII BIS.

DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS.

CAPITULO I.

DE LOS ATENTADOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y DE LOS SISTEMAS INFORMÁTICOS.

ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO

ARTÍCULO 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.

ARTÍCULO 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.

ARTÍCULO 269D. DAÑO INFORMÁTICO.

ARTÍCULO 269E. USO DE SOFTWARE MALICIOSO.

ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES.[3]

ARTÍCULO 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

ARTÍCULO 269H. CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.

CAPITULO II.

DE LOS ATENTADOS INFORMÁTICOS Y OTRAS INFRACCIONES.

ARTÍCULO 269I. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES.

ARTÍCULO 269J. TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

[3] Tipo penal objeto de estudio específico en esta tesis jurídico – académica.

10. Diseño Metodológico

El diseño metodológico y los métodos empleados en este proyecto de investigación jurídica corresponde a una estudio descriptivo-analítico de orden jurídico que ha sido discutido y acordado con el presidente y tutor metodológico del mismo y obedece a una de las múltiples alternativas existentes para el abordaje analítico dado un problema de investigación relacionado con un tipo penal, que facilita el llegar a un resultado en concreto hasta producir un conjunto de conclusiones y recomendaciones idóneas alineadas con el tema y el problema bajo estudio.

10.1 Metodología

En el desarrollo de esta investigación se utilizó el método de investigación científica cualitativa, en la cual se abordó el tema combinando diferentes estrategias que desde el estudio de documentos implicaron la utilización y el análisis de una gran variedad de materiales tales como libros, códigos, leyes, jurisprudencia, artículos de investigación respecto del tema de delitos informáticos publicados en periódicos de amplio reconocimiento y circulación, programas periodísticos y/o noticiosos de televisión, entrevista en profundidad, experiencia personal, historias de casos acontecidos en el ámbito colombiano, observaciones, textos históricos, imágenes, videos, los cuales sin lugar a dudas tienen registrado y datan de una problemática social-jurídica real que existe en Colombia y en el mundo, la cual ahora es objeto de estudio gracias a esta tesis jurídico-académica.

10.2 Tipo de estudio

El tipo de estudio realizado obedece a un sistema exploratorio descriptivo, en el que el problema de investigación es un tema poco abordado y descriptivo porque muestra desde la perspectiva del Derecho Constitucional la realidad del tipo penal (ARTÍCULO 269F. VIOLACIÓN DE DATOS PERSONALES) en el ordenamiento jurídico de Colombia.

10.3 Población y muestra

Este trabajo de Investigación de Derecho, Ciencias Políticas y Sociales por ser de carácter descriptivo, documental, cualitativo, académico, doctrinario, literario, comparativo legal, y jurisprudencial, no requiere toma de población ni de muestra, puesto que se centra en un tipo penal específico.

10.4 Técnicas de recolección de la información

Las técnicas empleadas para desarrollar la investigación, así como las fuentes de información para la elaboración de la misma fueron:

Análisis y revisión documental de libros, artículos científicos, textos, la Ley, la Jurisprudencia de la Corte Suprema de Justicia y de la Corte Constitucional, artículos de investigación respecto del tema de delitos informáticos publicados en periódicos, programas periodísticos y/o noticiosos de televisión, entrevista en profundidad realizada a un experto en el tema de delitos informáticos -Dr. Gilberto Aránzazu- docente de la Universidad Libre seccional Cali, experiencia y observación epistemológica personal, historias de casos acontecidos en el ámbito colombiano, textos históricos, imágenes y videos entre los más destacados.

Igualmente, se compiló información relacionada con el tipo penal según circunstancias similares tipificadas en otros países, por lo cual, se acudió a técnicas de derecho comparado al confrontar la norma nacional con las de países extranjeros, con el fin de demostrar la trascendencia mundial de este delito.

11. Desarrollo de la Investigación Jurídico Académica - Universitaria

11.1 CAPÍTULO 1

ALCANCES DOGMÁTICOS DEL TIPO PENAL "VIOLACIÓN DE DATOS PERSONALES EN COLOMBIA"

En este primer capítulo de la investigación se tratarán cinco (5) temas que desarrollan de manera lógica como se manifiesta esta nueva problemática jurídico social, señalando sus alcances dogmáticos, definiciones, conceptos, historia, casos específicos en otros países o derecho comparado, y por supuesto su evolución en el contexto político, económico, social y cultural colombiano.

Definición dogmática de Violación de Datos Personales: Frente a este ilícito se ha pronunciado ROVIRA DEL CANTO, en su obra "Delincuencia informática y fraudes informáticos", quien define esta conducta ilícita como "Hacking informático". Según el autor de origen español el término "Hacking" tradicionalmente describe la mera entrada o acceso a sistemas informáticos por el mero gusto de superar las medidas técnicas de seguridad, esto es, sin intención o finalidad alguna de manipulación, defraudación, sabotaje, o espionaje. Pese a lo anterior, su conducta es considerada lesiva, pues traspasa la "formal esfera de la privacidad y del secreto" o "la integridad del sistema informático afectado" (Rovira del Canto, 2002).

11.1.1 Origen de la tipificación del tipo

Para empezar se reitera que en Colombia la regulación de esta problemática jurídica ha implicado la tipificación de estos delitos llamados informáticos, ya que de no hacerlo, se pondría en riesgo los derechos humanos del conglomerado social-humano de Colombia entera, la seguridad nacional, la estabilidad económica, y los derechos o bienes jurídicos de las personas, por ende se introdujo al ordenamiento jurídico colombiano un tratado

internacional específico que se denomina "El convenio sobre ciber-criminalidad de BUDAPEST del 23 de noviembre del 2001"; donde Colombia a través del Congreso de la República se compromete a garantizar que prime dentro del ordenamiento la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes y los datos, y se dice desde ese entonces que la protección de los datos personales es fundamental en la nueva era de las tecnologías de la información y de las comunicaciones, y además quedó claro que el uso fraudulento de aquellos sistemas informáticos, ficheros, bases de datos, redes sociales, redes tipo Intranet, y semejantes serían sancionados por el Derecho Penal y Constitucional por ser violatorios de bienes jurídicos legalmente protegidos y de garantías constitucionales fundamentales.

Concepto de violación de datos:

Al referirnos a este vital concepto en el marco de esta tesis académica es necesario primero establecer cuáles son los características de los datos personales y luego establecer que esta es una violación o trasgresión a los mismos. Para dilucidar este concepto, en las decisiones de la corte constitucional se ha precisado que las características de los datos personales son las siguientes:

1. Estar referido a aspectos de caracteres exclusivos y propios en cuanto a una persona natural.
2. Permitir identificar con certeza a la persona, con ayuda del conjunto que se logre obtener de otros datos que se refieran a la misma persona.
3. La propiedad reside exclusivamente en el titular del mismo, es decir los datos pertenecen (uso, goce y/o disposición) al titular.
4. El tratamiento de estos datos está sometido a reglas especiales (principios) en lo relativo a su recepción, captación, administración, publicación en bases de datos y divulgación.

Acto seguido una violación o transgresión se podría definir como una acción de actuar contra una ley, norma o costumbre, u otra acepción jurídica podría ser el

acto de infringir con intención una ley o un precepto imperativo que se establece válidamente dentro del ordenamiento jurídico.

De este modo, se puede concluir lógicamente que el concepto de violación de datos personales enmarca dentro de lo que se denomina "Delito de Violación de datos personales" artículo 269F del Código penal, pues como dice el código penal en el citado artículo objeto de estudio de esta tesis, *"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes"* (Congreso de la República de Colombia, 2012).

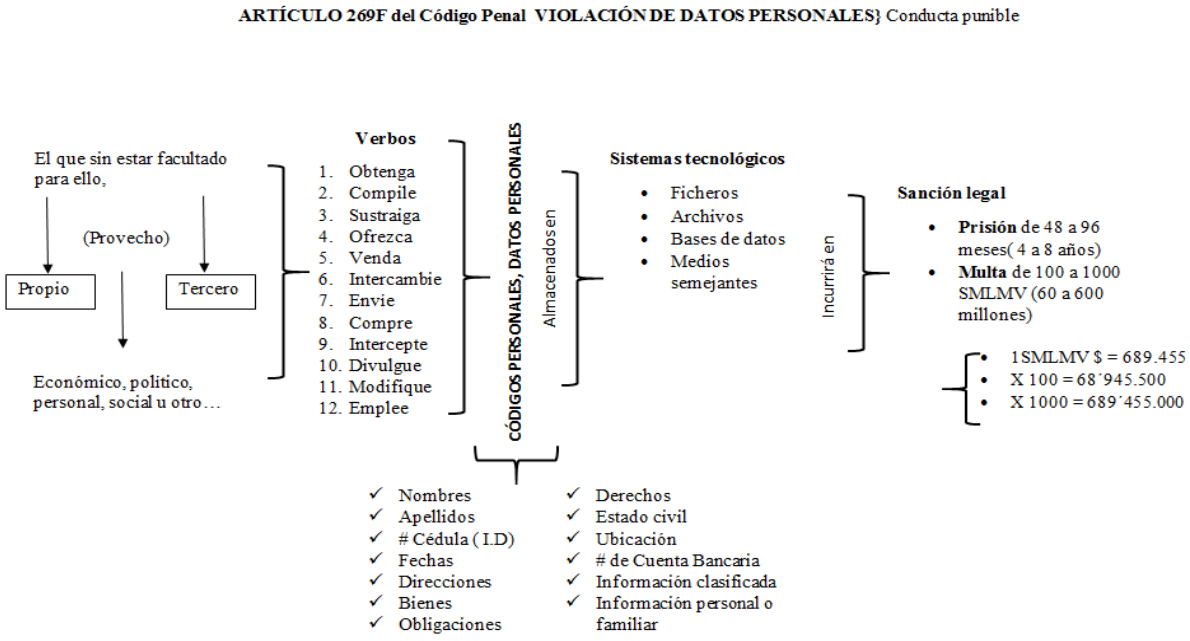
Lo anterior indica como conclusión lógica – argumentativa que el código penal es una ley imperativa de obligatorio cumplimiento por todas las personas dentro del ordenamiento jurídico de Colombia, y su violación o transgresión específica en el contexto investigado configura el delito de "violación de datos personales".

¿Qué es un delito informático en la modalidad de Violación de datos personales?

Un delito informático en la modalidad de violación de datos personales, comprende todas las conductas ilícitas que realiza un ser humano susceptible de sanción por el derecho penal, y que la realice según el tipo penal que describe el artículo 269F del C.P (violación de datos personales).

Textualmente… **Artículo 269F: "*Violación de datos personales*.** El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."

Diseño – Esquema del Tipo Penal:



En efecto el diseño del tipo penal del artículo en estudio, pretende proteger el derecho a la intimidad que se encuentra expresamente reconocido por la Constitución Política, señalando cuáles son las formas o actos que configuran la violación de los datos personales en el contexto de esta era de las tecnologías de la información y las comunicaciones; el diseño que el legislador ha propuesto para integrar el Art. 269F al Código Penal describe los tipos de sistemas tecnológicos que pueden ser objeto de penetración ilícita por parte de los sujetos activos de esta conducta penal, los cuales admiten amplias interpretaciones pues dichos sistemas tecnológicos están en constante crecimiento, expansión, actualización y evolución. En este sentido y haciendo amplio el tipo penal estudiado, se puede decir que el legislador tuvo la intención de proteger y garantizar la efectividad del respeto al derecho a la intimidad, privacidad y al buen nombre pues los verbos que guían el artículo 269F son abstractos y bastos para tratar de abarcar cualquier tipo de infiltración ilícita que vulnere o ponga en peligro el bien jurídico tutelado que es objeto de estudio académico en este proyecto.

Como se puede observar, los datos personales, definidos como la información concerniente a una persona identificada o identificable puede comprender los nombres, apellidos, número de cédula de ciudadanía, fechas, direcciones, bienes, obligaciones, derechos, estado civil, números de cuentas bancarias, además de información clasificada (con códigos cifrados, tokens, passwords, secuencias, respuestas precisas o claves encriptadas) de orden personal, familiar, laboral, social, e institucional; esta información y/o datos exclusivos de cada persona, son por supuesto los datos de la esfera más íntima de una persona (natural o jurídica), cuya utilización indebida o violación puede dar origen a perjudicar, discriminar o afectar gravemente el bien jurídico tutelado bajo la denominación "De la protección de la información y de los datos" y en consecuencia, acarrea las consecuencias jurídico – penales y constitucionales descritas en este importante artículo del Código Penal.

El diseño del tipo penal además describe la sanción legal que se generaría al infractor de la ley penal en este específico delito cuando se decida judicialmente la responsabilidad, la cual podría ser la pena privativa de la libertad de entre cuarenta y ocho (48) a noventa y seis (96) meses y multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

En este punto, se hace necesario definir el Delito informático (Gil Osorio, Juan Fernando y Silva Ossa, 2005) como toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos, obtener ilegalmente información personal contenida en datos, y redes de Internet así como, el empleo de tales herramientas informáticas o de telecomunicaciones para sacar provecho para sí o para terceras personas en detrimento de los bienes de otros. Debido a que la tecnología informática avanza más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como un delito, pues según la "Teoría del delito" y el principio de legalidad (*Nullum crimen sine lege praevia*, *scripta*, *stricta et certa*), la acción penal debe hacerse conforme a procedimientos previamente establecidos y definidos taxativamente (*Nullum iuditio sine praevia lege*), por lo cual se definen apropiadamente como abusos informáticos.

Los delitos informáticos, según los daños, y la lesión del bien jurídico amparado, pueden causar diferentes respuestas jurídico – penales pues la doctrina jurisprudencial argumenta que es o puede ser un delito plural-ofensivo que afecta el patrimonio económico y la privacidad de los datos personales, pasando a ser el objeto de riesgo para cualquier tipo de comunidad que pueda ser vulnerada; entendiendo que en este punto de la existencia humana cualquier comunidad puede tener acceso fácilmente al uso y/o utilización de los medios de comunicación, bases de captación de datos, que almacenan o guardan datos personales de las personas. En este momento, las legislaciones y los ordenamientos jurídicos debaten del cómo establecer parámetros, métodos que ayuden a la protección y descubrimiento de aquellos que comenten delitos informáticos y delitos conexos pues es necesario establecerlos para poder dar garantías a aquellos sujetos que han sido víctimas de este tipo de conductas punibles y así seguir reaccionando a través del Derecho ante esas nuevas realidades de delito que se presentan en la sociedad.

El delito informático llega a violentar tanto el ámbito socio económico como la intimidad de las personas, pues al referirnos a éste, estamos hablando de la privacidad y del derecho a la intimidad consagrado en las constituciones modernas o contemporáneas y en los ordenamientos jurídicos de Occidente, sin duda el derecho a estar tranquilo y en paz en su intimidad es un derecho cierto e indispensable para las personas hombres y mujeres por igual, además que este tipo de delitos pueden llegar a producir daños desde el ámbito familiar, social y laboral, así como en lo colectivo e institucional, incluso en la salva guarda de la seguridad nacional de un país, sin dejar atrás que la intimidad-privacidad aparece como un derecho fundamental en nuestro Estado Social de Derecho artículo 15 de la Constitución Política.

Debe tenerse en cuenta que la interpretación del delito de violación de datos debe ser amplia, ya que al referirnos a los datos también se hace alusión a que estos son datos lógicos, electrónicos pero con un valor económico, y de igual forma constituyen una trascendencia inmaterial ya que este tipo de daños solo es punible en la conducta de dañar o destruir datos o soportes que pretenden paralizar o suspender algún trabajo o acción, además de vender o reproducir aquel documento hurtado u obtenido en forma fraudulenta,

de igual forma la documentación falsa, o aquel que facilite correos en donde haya documentación de pornografía infantil.

Uno de los mayores problemas que encontramos a la hora de investigar esta problemática social y jurídica, es la dificultad probatoria, es decir el cómo demostrar que se ha incurrido en esta clase de delitos, ya que su régimen probatorio es de difícil consecución, obtención y rastreo, por lo que la mayoría de estas pruebas oscilan en la esfera virtual, es pasar de las pruebas en papel (documentales) a las pruebas intangibles, como es considerado el entorno digital. En este momento los jueces fundan sus decisiones con ayuda de Auxiliares de la Justicia, con la guía de peritos expertos que manejan la informática, telemática y la ingeniería de sistemas. Entonces, para que un juez dicte sentencia, ésta tendrá que estar motivada coherentemente de la mano de las ciencias informáticas y la tecnología misma. De esta manera es claro que la dificultad probatoria para este delito es evidente, que la sabiduría de los jueces no basta para impartir justicia en esta clase de delitos, y que cuando se accede a los distintos dispositivos después de varios días o semanas de haberse consumado el delito, hecho la denuncia y la *noticia criminis*, cuando llega la autoridad judicial competente a recolectar "las pruebas", dicha información podrá haber sido modificada, borrada o deteriorada volviendo así casi imposible la recolección de los elementos materiales probatorios. Entre las características más importantes de los escenarios virtuales donde se desarrolla esta conducta penal se destacan la variación de la escena del delito (pues pude ser desde cualquier computador o herramienta tecnológica con acceso a la Internet), la clandestinidad (porque se hace de manera oculta, secreta y desapercibida), la efectividad, los tiempos cortos en la ejecución pues no es un delito que mientras dura su ejecución se prolongue mucho en el tiempo, las ganancias para el delincuente (depende de los motivos personales o económicos que se tengan para la perpetuación del ilícito penal), la falta de testigos (pues solo se necesita de una persona con capacidades y habilidades en la esfera informática, telemática o digital, aunque potencialmente una persona sin conocimientos específicos en cibercriminalidad puede incurrir en el tipo penal analizado), el difícil rastro (pues el régimen probatorio en este tipo de delito es abstracto y materialmente de difícil consecución), la seguridad del delincuente (puesto que este puede hacer sus ¨jugadas tecnológicas ilícitas¨ desde cualquier lugar y no ve como probable que pueda tener consecuencias jurídico-penales), la ingenuidad y

descuido de las personas (en vista de que las personas deben tener claves de seguridad y sistemas de seguridad que generen confianza y que sean de alta complejidad), el perjuicio y daños para la víctima o sujeto pasivo (incluye responsabilidad civil y penal). En este último punto cabe resaltar que "la responsabilidad civil, como la responsabilidad penal son predicables cuando se comete el hecho punible informático, existiendo por consiguiente la obligación de indemnizar los perjuicios causados por la conducta para compensar los daños inferidos a quienes hayan sufrido detrimento con su realización y consumación. La responsabilidad penal, entonces, es la obligación de asumir las consecuencias penales del hecho punible por la concurrencia de los elementos de imputabilidad, culpabilidad y punibilidad"(León Moncaleano, 2013).

Bienes Jurídicos Protegidos:

Según la teoría del Derecho, El objeto jurídico o bien jurídico, es el bien lesionado (dañado, vulnerado o amenazado) o puesto en peligro por la conducta delictual del sujeto activo. En este caso es el nuevo bien jurídico protegido a través de la ley 1273 de 2009 el que se colige del título: ***"De la protección de la información y de los datos".*** Se aprecia como en esta problemática estudiada están involucrados más de un bien jurídico protegido.

Dentro de los delitos informáticos y los delitos de violación de datos personales, podemos adelantarnos a decir que la pretensión mayor es lograr la protección a dichos bienes jurídicos, que se han convertido sin lugar a dudas en bienes o derechos muy apreciados por los titulares de los mismos, entonces, la idea es que se realice desde la perspectiva legal y constitucional de los delitos comunes o tradicionales, con una re-interpretación más amplia que permita dar una mejor respuesta a estos relativamente nuevos tipos penales; esto con el claro objetivo de atender con mejores herramientas jurídico penales las lagunas o vacíos originados por los novedosos comportamientos delictivos que esta problemática acarrea, pues la tecnología crece día a día, y con ella los ciberdelincuentes mejoran sus técnicas de consumación del ilícito penal.

Lo anterior sin duda alguna, da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos comunes o tradicionales, mas siendo re-interpretados, puesto que se les ha agregado algún elemento nuevo, que lo vuelve más amplio para facilitar su persecución y sanción por parte del *ius puniendi* del Estado Social de Derecho.

La sociedad de la era de las tecnologías y las telecomunicaciones, trata la "información" con un valor inmaterial intangible que es susceptible de ser determinado o determinable económicamente, por ello tiene un valor que debe ser protegido adecuadamente por la constitución y las leyes, puesto que hay información catalogable como propiedad intelectual que necesariamente se hace merecedora de la protección del Estado y los convenios internacionales relacionados con la propiedad y los derechos de autor, es por tanto que se enfatiza el hecho de que la información y otros intangibles son objetos de propiedad, la cual está constitucionalmente protegida.

Así las cosas, una conducta punible de este tipo sólo puede asociarse con una pena cuando resulta violatoria con los presupuestos y las metas sociales, culturalmente aceptadas, de una vida en común pacífica, libre, honorífica, feliz y materialmente satisfecha. Es por ello que el bien jurídico protegido en general de la información y de los datos personales está pensado de diferentes formas, ya sea como un valor económico, como uno valor intrínseco e inmaterial de cada persona, pues podrían equipararse con protecciones jurídicas tales como:

- ✓ **EL PATRIMONIO**, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos.

- ✓ **LA RESERVA, LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS**, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los diferentes tipos de infiltraciones ilegales a bancos de datos.

- ✓ **LA SEGURIDAD O FIABILIDAD DEL TRÁFICO JURÍDICO Y PROBATORIO**, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos o mensajes de datos.

- ✓ **EL DERECHO DE PROPIEDAD**, en este caso sobre la información y los datos o sobre los elementos físicos, materiales o inmateriales de un sistema informático, que es afectado por los daños y perturban el derecho real de dominio que pregona el derecho civil y que igualmente es protegido por el derecho penal y constitucional.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde ésta se almacena o transfiere.

Para los autores chilenos Claudio Magliona y Macarena López, reconocidos por su trabajo e investigación en el tema de los fraudes y los delitos informáticos en Chile, los delitos informáticos tienen el carácter de ser pluri-ofensivos o complejos, es decir "*que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes esté independientemente tutelado por otro tipo*" (Magliona, 1999).

En conclusión, no se afecta un solo bien jurídico, sino una diversidad de ellos. Más adelante en este mismo capítulo veremos como el concepto de la Corte Suprema de Justicia en Colombia acoge esta tesis y argumenta de igual modo que el tipo penal estudiado es de carácter pluri-ofensivo.

11.1.2 Algunos casos de países que han avanzado en el tema: Alemania, España, Inglaterra y Estados Unidos

Con la llegada de estas nuevas tecnologías de la información y las telecomunicaciones, aparece la protección a la intimidad y el derecho a la privacidad que nace en Alemania en los años 70, Inglaterra escribe y legisla sobre ella protegiéndola constitucionalmente desde 1975, en España en la década del 80 y en Colombia surge en los años 90 con la Constitución Política de 1991, y posteriormente con la regulación del Habeas Data. Veamos estas muestras de derecho comparado:

Alemania:

En el país Germano Según el Doctor Tiedemann, profesor del Instituto de Criminología y Derecho Penal de Friburgo (Alemania), clasifica a los delitos informáticos así: a) Las Manipulaciones que una persona realice en las actividades de entrada y salida de información o de datos computarizados; b) El Espionaje económico, teniendo en cuenta que la información se almacena en soportes electromagnéticos, la transferencia de datos de un lugar a otro por cualquier medio sistematizado es lo más usual actualmente. Este espionaje económico se utiliza por empresas rivales, así como con finalidades políticas por Estados Extranjeros; c) Sabotaje. Se produje daño, destrucción, inutilización en el procesamiento de datos o información automatizada, en programas o software total o parcialmente; y, d) Hurto de tiempo. Tiene cabida en la indebida utilización, sin autorización de equipos computacionales o salas informáticas. Se penaliza el uso indebido y el tiempo de procesamiento de información o de datos perdidos por el propietario con las inapropiadas actividades. Así, la usurpación o violación de datos personales para el caso Alemán se enmarcan en la clasificación que Tiedemann hace en el primer literal, pues la manipulación de datos a la que se refiere son las que se hacen para sustraer información de otras personas jurídicas o naturales con fines contrarios a la Ley.

Es bastante significativo lo que en este tema ha avanzado el Estado Social de Derecho Alemán, pues el Tribunal Constitucional Alemán ha hecho razonamientos jurídicos en su jurisprudencia en cuanto al Derecho a la intimidad, buen nombre y honra con un concepto creado por el mencionado Tribunal Constitucional, denominado “derecho

a la autodeterminación informativa", concepto que según la teoría jurídica alemana se obtiene del derecho al libre desarrollo de la personalidad, derecho ampliamente reconocido por los países democráticos, incluyendo por supuesto a Colombia, y sin lugar a dudas es muy diferente la óptica alemana de la de Estados Unidos o de España que derivan el derecho a la intimidad y derechos conexos, del concepto de privacidad.

Así pues la teoría alemana y la política garantista de protección a la intimidad y protección de datos personales tiene su fundamento en otro derecho de rango fundamental, el libre desarrollo de la personalidad, derecho que podría decirse que es indispensable para la sociedad alemana y que por tal, la teoría del Derecho en ese país protege tan especialmente, pues por ejemplo según la jurisprudencia del Tribunal Constitucional en este país Europeo se considera al ser humano como una "personalidad capaz de organizar su vida con responsabilidad propia", es decir, que el individuo (Hombre o Mujer) tiene la capacidad para influir y decidir sobre su propio entorno social y, por tanto, decidir dónde, cuándo, cómo, en qué y con quién quiere o no presentarse en ese entorno social.

El Tribunal Constitucional alemán ha fundamentado el derecho a la protección de la intimidad e inviolabilidad de los datos personales de manera injusta o ilícita, desde el concepto de la autodeterminación de la vida íntima de la personalidad humana, rescatando que las personas tienen derecho a decidir cómo llevar su vida en los espacios más íntimos sin limitación alguna, y que la intromisión ilegal o ilícita por parte de un tercero acarrea serias consecuencias jurídico penales. En este sentido, la línea jurisprudencial del Tribunal Alemán considera que tiene preferencia la protección de la personalidad frente a otros derechos, pero igualmente solo a través del método de ponderación de derechos se debe analizar y resolver cada caso.

España:

En España hay también un gran avance en cuanto al derecho a la intimidad y el respeto por los datos personales de las personas contenidos en los distintos medios de almacenamiento, y se ha podido saber que los primeros intentos por legislar sobre esta materia (derecho a la protección de datos personales) en el país ibérico, se encuentran en los trabajos preparatorios, o proyectos de ley del artículo 18 de la Constitución Española de 1980, donde varios teóricos, académicos y juristas establecieron pautas para el tratamiento de la información personal de los ciudadanos españoles y su relación con los derechos humanos; lo que suscitó en ese momento un gran debate iusteórico pues no se advertía en aquel entonces la importancia tan preponderante que en la actualidad tiene este tema de delitos informáticos en general, y en particular, la violación de datos personales, gracias a los avances en las TIC y lo importante que son para el presente siglo para todas las culturas y países en un mundo ya globalizado e interconectado.

La Constitución de España protege íntegramente el derecho a la intimidad y buen nombre, prescrito en la Sección 1 de la Carta Constitucional con el título "De los derechos fundamentales y de las libertades públicas", en el cual taxativamente expresa:

Artículo 18 Constitución Española:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Como se puede observar en el punto #4 del citado artículo de la constitución de España, los derechos alusivos a la intimidad tienen protección cuando están inmersos en la informática, pues el constituyente español pretende garantizar no sólo el Derecho al honor y

la intimidad, sino el ejercicio de todos los derechos. Sin lugar a dudas este artículo inspirado en la protección de la intimidad y de los datos personales, es amplio y abarca otros derechos como la protección del honor personal y familiar.

En España se habla del Derecho al honor, a la intimidad y a la propia imagen, y en este sentido el artículo 18 de la Constitución española se puede equiparar al artículo 15 de la Constitución Colombiana que trata el mismo tema jurídico con la denominación de *"Derecho a la intimidad, al buen nombre, habeas data, inviolabilidad de correspondencia y documentos privados"*. Por lo que es válido decir que la legislación de estos dos países en materia del Delito informático y Protección del derecho fundamental a la intimidad, honor y buen nombre tiene especial protección y garantía constitucional.

En este artículo 18 Constitucional español, se protegen, en primer lugar, el derecho al honor, en segundo lugar, el derecho a la intimidad, tanto personal como familiar, y en tercer lugar el derecho a la propia imagen, derechos con rasgos comunes, y también con aspectos que permiten distinguir tres derechos diferenciados, y en definitiva, como indica la Ley española son tres derechos autónomos, estrechamente relacionados entre sí, pero de igual forma derechos inherentes a la personalidad, derivaos de la dignidad humana y dirigidos a la protección del patrimonio moral, intangible y simbólico de las personas.

En el mismo sentido existe en España la Ley Orgánica 15 de 1999, de Protección de Datos de Carácter Personal, la cual tiene por objeto garantizar y proteger, lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar. Este importante compendio normativo tiene un excelente desarrollo del tema, y es una Ley a la vanguardia de esta problemática jurídico - social que hoy es objeto de estudio en esta investigación.

Inglaterra:

Inglaterra, como país tradicionalmente autónomo y vanguardista en material legal, altamente desarrollado económica, tecnológica, cultural y socialmente aporta en gran medida al avance de la ciencia del Derecho y al progreso de la humanidad en materia de derechos y libertades, es y será siempre un referente en Occidente y otras partes del mundo contemporáneo. Gracias a la influencia del derecho romano, franco y germano, en procura de su independencia normativa pasan por la experiencia de la primera Constitución llamada Carta Magna de 1215, La Teoría del Contrato Social de John Locke (Padre del liberalismo político) que hace al Homo Sapiens salir del estado de Naturaleza y que hace al Hombre vivir en sociedad entregando el derecho a hacer justicia al ente ficticio llamado "Estado" y desde luego Inglaterra ha hecho también una contribución histórica e importante en cuanto a la protección de la intimidad y de los datos personales con todo sus desarrollo jurídico legal.

En la época del desarrollo científico – tecnológico de los comienzos de la década de los 60, Inglaterra se comienza a preocupar por la efectividad de la protección de un nuevo derecho que aparece gracias a la digitalización de la información y de los datos de las personas tanto de entes económicos como personas naturales, y para ello desde el Parlamento se comienzan a esbozar y hacer debates sobre la regulación de la protección de la intimidad de las personas y la protección de los datos, discusiones sobre la privacidad en sentido general, debates sobre la "*privacy*" o "privacidad" en español, de datos almacenados en terminales computarizadas, donde ello deriva años después, con la promulgación de la "*Data Protection Act*" que refiere "Ley de Protección de Datos" de 1975.

Para el derecho inglés la protección de datos personales almacenados informáticamente es de vital respeto, pues la cultura jurídica de ese país así lo ha asimilado durante años, e incluso la regulación en el ámbito Estatal de protección de datos incluye la seguridad nacional, los bancos de datos de las Instituciones Policivas para prevenir y reprimir el delito, los datos médicos que se encuentran en las historias clínicas del sistema

de Salud Inglés, y los datos personales incluidos en las bases de datos de los Bancos, aspectos muy delicados y sensibles para el Estado que tienen una estricta protección legal.

En la doctrina inglesa se pueden encontrar conceptos como el de "*privacy*" que asocia al derecho que tiene cada persona de ser dejado solo, en inglés "*right to be let alone*", ello quiere decir que las personas según su opción de vida o proyecto de vida tienen derecho a estar solos, a disfrutar de una soledad en la que la persona puede desarrollar su personalidad, espíritu o su modo de vida libremente, sin intervenciones ni injerencias ajenas, y que su eventual vulneración, intromisión o peor aún, divulgación de su opción de vida solitaria por parte de alguien podría configurar una actividad jurídico penal con sus respectivas consecuencias.

El concepto de "*privacy*", llevó al Parlamento inglés a debatir y legislar sobre la atención al problema de los bancos de datos personales de todo tipo y su violación ilícita por parte de agentes externos o internos que con el ánimo de sacar algún provecho de esa información clasificada, penetraban en los sistemas informáticos, configurando por ese hecho, una nueva modalidad de delito similar al hurto, por apropiarse de una cosa, pero con claras diferencias porque la información personal tiene características intangibles, y el derecho al respeto de la información también oscila en la esfera inmaterial de los derechos, por lo cual se direcciona desde una nueva perspectiva el debate sobre la "*privacy*" y la protección de los datos personales, llevando a los hacedores de la Ley en Inglaterra a expedir la ya citada "*Data Protection Act*" reguladora del derecho a la intimidad en lo concerniente a la actividad de captación, registro, almacenamiento y difusión de los datos personales.

Según la Ley de Protección de Datos inglesa, los datos personales deben reconocerse frente a los demás, debiendo cumplir las siguientes características:

1. Ser tratados de manera justa y lícita.

2. Haber sido obtenidos para fines determinados y legítimos.

3. Ser adecuados, relevantes y no excesivos.

4. Contener información Precisa y actualizada.

5. No ser conservados más tiempo del necesario.

6. Ser procesados de conformidad con los derechos individuales del titular de los datos.

7. Ser mantenidos razonablemente seguros.

Las anteriores características son el eje fundamental de la ley de protección de datos personales, siendo su fin principal procurar que se apliquen de modo tal que sea eficaz el respeto de las libertades, la dignidad humana y los derechos constitucionales en beneficio de todos los ciudadanos en Inglaterra.

Estados Unidos:

Los acontecimientos terroristas del 11 de setiembre de 2001 en EEUU han llevado a que este país pretenda un estricto control sobre la Internet. El gobierno de los Estados Unidos no sólo se propone controlar la Internet, incluyendo por supuesto los correos electrónicos, sino que también ha solicitado a la Unión Europea de manera formal, para que se reconsidere la legislación existente en materia de protección de datos. Además, se aprobó en el Senado la ley "*Combating Terrorism Act of 2001*, del 13 de setiembre de 2001, que multiplica las posibilidades de monitorización de las comunicaciones; es decir, Estados Unidos de Norte América tiene un sistema donde el Gobierno y las instituciones de inteligencia como el FBI y la CIA, dentro de sus funciones investigativas pueden infiltrarse e interceptar todo tipo de comunicaciones de cualquier ciudadano norteamericano, residente o turista y sin distinción de nacionalidad, posición social, económica, política y en general de ninguna clase, consecuentemente es viable decir que Estados Unidos sacrifica el derecho a la intimidad particular de las personas para salvaguardar la seguridad Nacional sobreponiendo una política antiterrorista y ampliando su radio de influencia legal a prácticamente todo el mundo.

Sin embargo, EE.UU ha sufrido en diversas ocasiones ciber ataques dentro de los cuales se encuentra múltiples robos de identidades y claves para sustraer cuentas bancarias, tarjetas de crédito etc., y por ejemplo en 2013, los *hackers* obtuvieron los datos de las tarjetas de crédito de 40 millones de clientes y la información personal de 70 millones de clientes adicionales con lo cual se ha configurado sin lugar a dudas uno de los más grandes delitos en materia de sustracción, manipulación y violación de datos personales en el mundo; y no es precisamente por fallas en los sistemas de seguridad de las entidades bancarias, sino que los sujetos activos de este tipo de delitos (Piratas cibernéticos, Hackers, Crackers etc.) cada vez hacen más sofisticadas e inteligentes sus formas de intervenir los sistemas informáticos, software o bases de datos contentivas de información y datos sensibles de la gente.

No obstante lo anterior, Estados Unidos de Norte América en la llamada cuarta enmienda de la Constitución hace un acercamiento a la protección de la intimidad y privacidad de las personas, donde no se limita sólo a la protección de elementos de autonomía personal o privada, sino que se aplica a todos los aspectos del derecho criminal. Dice la traducción al castellano de la Cuarta Enmienda Constitucional que: "*El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable*"; y como se sabe el Derecho de Estados Unidos es un Derecho de creación y dinamismo por parte de un papel muy relevante de los Jueces, esta enmienda ha sido interpretada en las sentencias de los casos sobre el tema de protección de datos personales, intimidad, privacidad, honor y buen nombre en el mismo sentido del tema que hoy es objeto de estudio de esta investigación jurídico – académica, por lo que el Juez norteamericano cuando aplica la norma en los casos concretos, sí hace respetar este derecho tan especial y fundamental. Para ello, el Juez Constitucional de Estados Unidos hace uso de la doctrina Norteamericana al respecto como por ejemplo los estudios y opinión jurídica de un caso concreto denominado "*Warren-Brandeis article*", estudios publicados por la Universidad de Harvard el 15 de diciembre de 1890, al que el autor llamó "*The right to privacy*" – en español "Derecho a la Privacidad", que bien puede ser considerado uno de los estudios más importantes de la literatura Jurídica en el tema de Protección del derecho a la intimidad y al buen nombre en profunda conexión

con la creación jurídica ratificada al término de la Segunda Guerra Mundial, Los Derechos Humanos.

Resulta entonces que este tema en Estados Unidos es muy complejo y controvertido, dado las diferentes posiciones que se tienen por parte de los Órganos del poder público dentro del país, donde la aplicación de las normas vigentes es diferente en los distintos distritos federales, y la política que tiene el poder ejecutivo (Gobierno) es sustancialmente diferente a la del poder judicial (Jueces y Corte Suprema de los Estados Unidos).

11.1.3 Historia de la legislación sobre la violación de datos personales en Colombia

Con el pasar de los años, y frente al constante desarrollo tecnológico e interdependencia de las personas con los avances científicos, tecnológicos, de desarrollo y de comunicación digital, se necesitó que se coordinaran armónicamente los países para que se diera un avance que permitiera contrarrestar la nueva clase de criminales que utilizan los diferentes métodos tecnológicos para cometer conductas punibles violatorias de un amplio conjunto de derechos humanos, dicha necesidad quedó evidenciada y teorizada después de arduos debates en la convención de Budapest. Colombia se unió a estos países jurídicamente y taxativamente en el 2009 cuando reguló al respecto.

Aquel 2009 fue muy importante en este mismo sentido en vista de que después de los cuatro (4) debates legislativos reglamentarios y uno adicional conciliado en la Cámara de Representantes y el Senado se logró adoptar un nuevo bien jurídico protegido denominado: "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS", dicho proyecto de ley venía siendo trabajado y elaborado por el Ministerio de Justicia y del Derecho con ayuda de importantes abogados colombianos y europeos que venían haciendo la misma labor en la comunidad Europea, conforme a los lineamientos de la Convención de BUDAPEST sobre ciber-criminalidad. Es de resaltar, que en los primeros debates de

Cámara y Senado el proyecto de ley tuvo gran aceptación y favorabilidad por todos los partidos políticos representados por los diferentes congresistas ya que se hacía claro, evidente y pertinente legislar en esta materia y estar el país entero acorde a las nuevas tecnologías, tendencias y exigencias del siglo XXI.

La regulación colombiana ha implicado la tipificación de estos delitos llamados informáticos, ya que de no hacerlo, se pondría en riesgo la seguridad nacional, la estabilidad económica, y los derechos o bienes jurídicos de las personas naturales y jurídicas, por ende se introducen al ordenamiento jurídico colombiano tratados internacionales, como el convenio mencionado sobre ciber-criminalidad de BUDAPEST del 23 de noviembre del 2001; en este tipo de convenios, vemos que se busca que prime dentro de algún ordenamiento o grupo social la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, las redes y los datos; en igual medida, con la implementación de esta normatividad al bloque de constitucionalidad se dieron más herramientas jurídicas para contrarrestar la infracción a esta nueva modalidad de delito en el país.

Por ejemplo en el artículo 192 del convenio de BUDAPEST se implementa la sanción a quien destruya el vínculo de comunicaciones privadas, el daño de datos, y el daño en bien ajeno; de igual forma, se puede hablar de la protección de estos bienes a través de la ley penal colombiana. Con lo mencionado aquí, vemos como este tratado a través del artículo 92 se compenetra a la perfección con el artículo 15 de la Constitución que tiene por objetivo precisamente entre sus inspiraciones teóricas salvaguardar la correspondencia y demás formas de comunicación privada pues son inviolables, dice además el artículo que hace parte de los llamados Derechos fundamentales, que la correspondencia y demás formas de comunicación privada sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley; esto quiere decir que ello tiene resguardo supra constitucional y es muy importante ser respetado dicho derecho por todas las partes que integran el Ordenamiento Jurídico colombiano.

Una vez creada la norma, enumerada con el 1273 del año 2009, se introduce en el Código Penal (Ley 599 de 2000) el título VII denominado con el nombre y/o bien jurídico

"DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" la corte constitucional hace el correspondiente análisis de control de constitucionalidad, y el Presidente de la República de aquel año sanciona la Ley convirtiéndose esta en una adición al Código Penal vigente en Colombia; y a partir de allí se viene haciendo una reflexión académica, social y jurídica pues al integrarse ésta al ordenamiento jurídico nacional adquiere una importancia para todo aquel que tenga datos personales depositados en los diferentes sistemas electrónicos, bases de datos, y redes cibernético-digitales en general.

11.1.4 Jurisprudencia de Altas Cortes: CORTE CONSTITUCIONAL Y CORTE SUPREMA DE JUSTICIA

En este acápite se resalta la jurisprudencia como fuente principal del Derecho en Colombia, dada la constitucionalización del Derecho y el reconocimiento de derechos humanos, derechos económicos, sociales y culturales además de los de tercera generación que protegen el medio ambiente que han sido reconocidos y elevados gracias al desarrollo dinámico del Derecho que se crea en estas sedes institucionales de la Justicia en el Estado Social de Derecho.

Enseñó la Corte Constitucional en la Sentencia C-748 de 2011 con Magistrado Ponente el Dr. Jorge Ignacio Pretelt Chaljub, que el artículo 15 de la Constitución Política de 1991 era fundamental para el Estado, y reconoció explícitamente en la jurisprudencia constitucional, que el derecho al habeas data fue primero interpretado como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir. También, desde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data como una manifestación del libre desarrollo de la personalidad. Según esta línea, el habeas data tiene su fundamento último en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad. A partir de 1995,

surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al habeas data como un derecho autónomo, en que el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.

En ese mismo sentido la Corte Suprema de Justicia sala de Casación Penal expresa en Sentencia SP1245-2015, Radicación N. 42.724 (Aprobado Acta No. 44) Bogotá D.C., once (11) de febrero de dos mil quince (2015), Magistrado Ponente: Eyder Patiño Cabrera, la corte dice en resumen lo siguiente:

> *"La Ley 1273 de 2009 creó un nuevo bien jurídico y unos delitos para garantizar la determinación informática, entre ellos, el de violación de datos personales; la Corte señaló que ese delito de violación de datos personales, habida cuenta su condición de delito autónomo, NO afecta el patrimonio económico y que además es pluriofensivo" (Corte Suprema de Justicia, 2015).*

Así dentro de la clasificación de los tipos penales el artículo 269F goza de estructura dogmática completa, por plena conjunción de los elementos que deben integrar el tipo penal, al punto que no es necesario que se asocie con otros tipos penales para completar su ordenación o adecuación típica. Entonces, es válido decir que el artículo analizado (269F del C. Penal) corresponde a un tipo penal principal, completo y autónomo, ajeno a toda connotación patrimonial y la Corte no aseveró que a los delitos informáticos no se les puede aplicar la figura de reparación, sino que sólo cabe respecto de atentados contra el patrimonio económico. De igual manera, la reflexión de la Corte Suprema de Justicia – Sala de Casación Penal, se encamina en el sentido que los únicos delitos que admiten la rebaja por reparación integral son los del Título VII del Código Penal, esto es, los lesivos del patrimonio económico.

De otro lado, se puede decir que esta clase de delincuencia no sólo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la componen puede afectar una diversidad de bienes jurídicos tutelados.

Por tanto, es viable sustentar que el desarrollo de las nuevas tecnologías de la información y las comunicaciones en general, está proporcionando nuevos elementos para atentar contra bienes jurídicos ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa. En tal razón se considera al igual la jurisprudencia que este tipo de conductas criminales son de carácter netamente pluriofensivo (afecta varios bienes jurídicos simultáneamente).

Ejemplo de la pluriofensividad del tipo penal estudiado sería el de un Hacker o un Cracker que ingresa a un sistema informático con el fin de vulnerar la seguridad y las claves, para averiguar la información personal que más pueda sobre una cierta y determinada persona natural, empresa, colectivo, organización o Nación. El mencionado ejemplo en primer lugar podríamos decir que el bien jurídico lesionado o puesto en peligro es el derecho a la intimidad (artículo 15 constitucional) que posee esa persona al ver que su información es ultrajada por un tercero extraño, que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. En segundo lugar, el otro bien jurídico lesionado o puesto en peligro sería un bien colectivo, “El orden económico social” que según el autor del libro “DE LA COMUNICACIÓN A LA INFORMATICA JURIDICA PENAL BANCARIA” de William Fernando León Moncaleano este tipo de delitos lesionan y afectan el mencionado bien jurídico, pues en ellos se configura un ataque a la confianza en el funcionamiento de los sistemas informáticos, y ello afecta a la sociedad en general que hace uso de estos medios tecnológicos modernos. Para este autor hay intereses socialmente valiosos que se ven afectados por estas nuevas figuras de criminalidad, y que no sólo afectan de bienes jurídicos particulares.

Analizando el derecho que tienen por igual tanto hombres como mujeres al buen nombre es, necesario estudiar la acepción que el diccionario de la Real Academia de la Lengua Española hace al respecto, en el cual expone que es la "fama, opinión, reputación o crédito del resultado del comportamiento en sociedad". El buen nombre lo tiene quien lo ha adquirido a merced a su buena conducta, pues él no se recibe gratuitamente de los demás. La buena fama es, la buena opinión que las personas tengan de alguien, es el resultado de la buena conducta que la sociedad observa de él. El buen nombre se tiene o no se tiene, según sea la conducta social; éste concepto depende de los hechos o actos de la persona misma. El derecho al buen nombre no es una abstracción, algo que pueda atribuirse indiscriminadamente a todas las personas. En los casos concretos habrá que ver si quien alega que se le ha vulnerado, lo tiene realmente.

Al respecto, La Corte Constitucional Colombiana ha señalado en Sentencia T-229 de 1994 del Magistrado Ponente Dr. José Gregorio Hernández, lo siguiente:

> *"El buen nombre alude al concepto que del individuo tienen los demás miembros de la sociedad en relación con su comportamiento, honestidad, decoro, calidades, condiciones humanas y profesionales, antecedentes y ejecutorias. Representa uno de los más valiosos elementos del patrimonio moral y social de la persona y constituye factor indispensable de la dignidad que a cada uno debe ser reconocida. Se atenta contra este derecho cuando, sin justificación ni causa cierta y real, es decir sin fundamento, se propagan entre el público, bien en forma directa y personal, ya a través de los medios de comunicación de masas-informaciones falsas o erróneas o especies que distorsionan el concepto público que se tiene del individuo y que, por lo tanto, tienden a socavar el prestigio y la confianza de los que disfruta en el entorno social en cuyo medio actúa, o cuando en cualquier forma se manipula la opinión general para desdibujar su imagen. Por su misma naturaleza, el buen nombre exige como presupuesto indispensable el mérito, esto es, la conducta irreprochable de quien aspira a ser su titular y el reconocimiento social del mismo. Entre otros términos, el buen nombre se adquiere gracias al adecuado comportamiento del individuo, debidamente apreciado en sus manifestaciones externas por la colectividad (...) a él es aplicable íntegramente lo*

dicho en esta providencia en el sentido de que no puede alegar desconocimiento o vulneración de su buen nombre quien, por su conducta da lugar a que se ponga en tela de juicio su credibilidad".

Es evidente la gran importancia del derecho al buen nombre como concepto característico de cada persona, y cómo este especial derecho tiene protección y desarrollo jurisprudencial, pues desde la creación de la Constitución Política de 1991 el Estado Social de Derecho, la Corte se preocupa por amparar los derechos fundamentales de los integrantes de la sociedad dentro del marco de una Colombia que respeta estas nuevas garantías y derechos consagrados en una Constitución política pluralista y multicultural.

11.1.5 Casos concretos de violación a derechos por medios informáticos

La historia del 'Hacker' Andrés Sepúlveda:

Este es un caso particular que ocurrió en el primer presidencial de Juan Manuel Santos Calderón, cuando con la intrusión electrónica del delincuente informático Andrés Sepúlveda se logró interceptar las comunicaciones y correos electrónicos sobre los pre acuerdos que se adelantaban entre el Gobierno colombiano de Santos y los Jefes de las Fuerzas Armadas Revolucionarias de Colombia (FARC), en el marco de los diálogos de paz llevados a cabo la Habana Cuba. El "Hacker" como se le conoce en los medios, terminó enredado judicialmente por los presuntos delitos de espionaje, concierto para delinquir, acceso abusivo a un sistema informático, uso de software malicioso y violación de datos personales, por haber, entre otras cosas, intentado infiltrar a los integrantes de la mesa de paz en La Habana, en beneficio del entonces candidato presidencial Oscar Iván Zuluaga y su jefe político el ex Presidente Álvaro Uribe Vélez. Por este caso la Fiscalía ha llamado a interrogatorio al ex candidato presidencial Óscar Iván Zuluaga y a su hijo David Zuluaga, por los nexos y los pagos realizados que rodean los 230 millones de pesos colombianos. Actualmente el 'Hacker' Andrés Sepúlveda se encuentra tras las rejas detenido desde el año 2015 a pena privativa de la libertad de 120 meses y al pago de 120 salarios mínimos mensuales legales vigentes como sanción multa.

La llamada millonaria y otras modalidades delictivas:

Las llamadas millonarias son estafas que se hacen vía teléfono que ponen en contacto directo al delincuente con la víctima, dichas llamadas no son el único mecanismo del que se valen los estafadores para tratar de obtener dinero u otro fin ilícito a través de las nuevos medios tecnológicos, la instalación de un programa malicioso en la computadora y el robo de datos personales, es lo que se conoce en inglés como *phishing* y *hacking*. Los ciber-criminales también utilizan correos electrónicos, enlaces o links y falsos sitios web con el objetivo de convencer a las personas de que descarguen algún programa o hagan "click" en un enlace y obtener así provechos ilícitos.

A través de dichas "llamadas millonarias" utilizan la "ingeniería social", que es la manipulación psicológica que con falsas premisas trata de lograr que la víctima divulgue información personal y actúe de determinada manera incluso con esta modalidad se manipula la autonomía de la voluntad de la persona; dichas técnicas malignas, son herramientas diseñadas específicamente para generar pánico en la víctima, su objetivo es lograr que el receptor del mensaje actúe de inmediato y haga lo que se le pide, asegurando que, si no lo hace, perderá algo, como por ejemplo, el acceso a su cuenta de banco, o por el contrario, asegurándole a la víctima que de realizar o dar lo que se le pide, ganará un gran premio que lo hará millonario.

De otro lado, se ha detectado que muchas de las organizaciones criminales que se dedican al *phishing y al hacking* están en Brasil, y entre los países que encabezan la lista de emisores de correo basura están varios asiáticos, seguidos por Estados Unidos y Rusia. El número de afectados es mayor en los países en los que existe poca educación informática.

El ciberacoso o ciberbullying de Juan Sebastián de 12 años:

Este es el caso de un joven de 12 años que sufrió un hostigamiento a través de redes sociales que afectó directamente la intimidad, honra y entorno social y familiar del menor de edad.

Todo comenzó en el colegio de Juan Sebastián, cuando en un video, el joven de 12 años manifestó sus intereses y orientación sexual homosexual y el video se publicó en redes sociales. Los compañeros de colegio y vecindad al visualizar el video comenzaron a burlarse, hacer bromas y acosar al joven no solo por las redes sociales, sino con llamadas ofensivas, sobrenombres y calificativos abusivos de todo tipo. El "ciberacoso" llegó a tal punto que trascendió el espacio virtual para afectar la vida cotidiana del joven y de su familia. Los hechos causaron molestias a los miembros de su familia y perturbaba la tranquilidad y normalidad de sus vidas, pues luego de hacerse público ese video no podían salir tranquilos a la calle sin que alguien se les acercara para preguntarles por la incómoda situación. Luego de unos meses Juan Sebastián tuvo que cambiarse de colegio y él junto con su familia optó también por mudarse de residencia pues la intromisión a la que habían sido víctimas era insoportable, pues su derecho constitucional a la intimidad personal y familiar había sido irrespetado de tal forma que se tenía que comenzar prácticamente una nueva vida.

De esta manera se da por terminado el primer capítulo de esta investigación jurídica, y queda claro como este fenómeno de la ciberdelincuencia en la modalidad de violación de datos personales se puede manifestar de diferentes maneras, afectando primeramente la intimidad personal y concurrentemente otros derechos, pues al tratarse de un delito pluriofensivo se hace diversa las vías de lesionar el derecho fundamental consagrado en el Art. 15 de la Constitución. En este punto es clara la consciencia de tener aprecio por la protección de la información y de los datos personales pues resulta evidente que es un patrimonio simbólico e inmaterial inherente al ser humano que no solo particulariza la identidad de cada quien sino que es la fotografía ante la sociedad y que hace parte de la libertad individual y opción de vida cada ser humano.

11.2 CAPÍTULO 2

EL DERECHO A LA INTIMIDAD Y AL BUEN NOMBRE, UNA MIRADA CONSTITUCIONAL

El derecho a la intimidad y buen nombre desde la perspectiva constitucional abarca no solo la teoría de este importante derecho fundamental, sino que también la posibilidad que éste tiene de ser garantizado real y efectivamente a través de los métodos que el legislador ha dispuesto para ello, en efecto la tutela judicial se hace efectiva a la hora de que cualquier ciudadano pueda acudir ante el Juez pretendiendo la protección, garantía y cesación de amenaza o vulneración que se pueda presentar cuando se menoscaba dicho derecho constitucional fundamental…

11.2.1 Conceptualización del Derecho a la Intimidad y Buen Nombre

> *"El derecho que tiene cada persona de no ser objeto de una publicidad ilegal; el derecho de vivir sin interferencias ilegales del público en lo concerniente a asuntos en los cuales ese público no tiene un interés legítimo" (Vásquez Ramírez, 2012).*

La Honorable Corte Constitucional desde su creación con la constitución Política de 1991 ha venido desarrollando importantes avances en la teoría del Derecho local, y en la justificación iusfilosófica de los derechos humanos como base fundamental del respeto y de las relaciones sociales dentro del Estado Social de Derecho. En este sentido la honorable Corte Constitucional ha desarrollado doctrina en materia de todos los derechos considerados fundamentales en el Estado Colombiano, y por supuesto el Articulo 15 (Derecho a la intimidad, buen nombre, habeas data, inviolabilidad de correspondencia y documentos privados) de la misma no ha sido la excepción y por el contrario ha tenido un amplio despliegue hermenéutico y doctrinario.

Cuando la Corte se refiere a la garantía del derecho a la intimidad, habla de la protección de los datos que pertenecen a la vida privada y familiar, dicha intimidad es entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir, pues cada ser humano es una cosmovisión diferente, donde cada quien es libre, sujeto de derechos y deberes, pero igualmente libre de decidir con base en sus ideales y consciencia lo que mejor le parezca para hacer de su futuro y su vida.

Sin embargo la línea jurisprudencial que ha prevalecido desde la época de los primeros 9 magistrados de la Corte Constitucional es la que apunta a que el habeas data, la intimidad y buen nombre son como un derecho autónomo, en el cual el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad, incluyendo la libertad económica - financiera. Este derecho como fundamental y autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben depender de los jueces a través de la acción de tutela por ejemplo, sino de una institucionalidad administrativa que además de la inspección, control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos personales y, en razón de su carácter técnico, tenga la capacidad de fijar una política pública en la materia, sin injerencias de ninguna índole e imparcial para el cumplimiento de esas decisiones.

Para delimitar el verdadero contenido de la intimidad, por el contrario al del habas data que tiene un carácter objetivo en su definición, "la libertad reside en la habilidad para controlar el uso que de esos datos personales se haga en un programa de computador" y de contenido “muy amplio”, es el derecho al acceso de los bancos de datos, el derecho a verificar su exactitud, el derecho a actualizarlos y a corregirlos, el derecho a mantener en secreto a los datos sensibles, el derecho a ningún pronunciamiento acerca de los llamados ´datos sensibles´. La teoría tradicional de los derechos humanos solo hace referencia a su exigencia frente al Estado, aunque el derecho a la intimidad generalmente se ha hecho valer por un particular frente a otros particulares, el Habeas Data ha aumentado su alcance. EI Habeas Data ligado a la intimidad y buen nombre es un derecho humano que en su moderna tendencia coloca a los particulares con una responsabilidad muy clara frente al respeto de

estos derechos. Incluso las vías judiciales y administrativas jurídicamente hablando están tomando serias cartas en el tema, y a través de la Superintendencia de Industria y Comercio se puede instar para que se protejan las acciones que vulneran de una u otra forma los datos de las personas. Además a parte de la responsabilidad penal que acarrea el incurrir en el delito descrito en el artículo 269F del código penal (*Violación de datos personales,)* ya en el Ordenamiento jurídico Nacional vigente la protección de datos es tan relevante que se puede defender desde el Derecho Civil, con la ayuda de la figura jurídica de la Responsabilidad civil, pues el mal tratamiento de la información personal puede ocasionar graves perjuicios materiales y morales que, dado el caso, podrían llegarse a estimarse y cuantificarse, y consecuentemente susceptible de ser demandable en un proceso de Responsabilidad Civil Extracontractual por uso ilegal y mal utilización de datos personales.

El concepto de "Derecho a la intimidad" ha evolucionado hacia una nueva interpretación: La Privacidad, la cual se ve seriamente violentada por las nuevas tecnologías de la información y las comunicaciones, al punto que se ha incrementado significativamente las amenazas y vulneraciones a algo que de antaño ara de difícil acceso, además de ser considerado íntimo, personalísimo y sagrado.

De otro lado y según otro alcance dogmático, el iusfilósofo Frosini V. en su obra *"La protección de la intimidad: De la libertad informática, al bien jurídico informático"*, considera el derecho de habeas data como una extensión del derecho a la intimidad o del "right to privacy", pero con un contenido actual más acorde con la realidad; se refiere, a la concepción del "habeas data como aquél derecho que surge fruto de la tecnología informática y que pretende solucionar el conflicto generado por la violación de los derechos a la intimidad y a la información y el conflicto que entre ellos se ha ocasionado. Es un derecho moderno, reciente y en constante evolución".

Es pertinente vislumbrar que cuando se refiere a la protección de datos Personales, en realidad nos estamos refiriendo no a lo protección del dato en sí mismo, sino del sujeto que es titular de dicho dato. Atendiendo su confidencialidad, se puede decir que los datos personales pueden ser: públicos y/o privados, íntimos, secretos o reservados, así:

Públicos: “Aquellos datos personales que son conocidos por un número cuantioso de personas, sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato, ni, por la calidad del datos, pueda impedir que, una vez conocido, sea libremente difundido dentro de unos límites respecto de respeto y convivencia cívicos”.

Privados: estos datos son los que en determinadas circunstancias la persona se ve obligada a proporcionarlos, no realizándose difusión de los mismos y respetando la voluntad de secreto entre su titular y la entidad o base de datos a la cual se entregan.

Íntimos: son los datos que el individuo puede proteger de su difusión frente a cualquiera, pero que, esté obligado por ley a brindarlos cumpliendo sus obligaciones cívicas.

Secretos: los datos que el ciudadano no estará obligado a dar a nadie, salvo casos excepcionales, expresamente regulados en las leyes. La doctrina los ha denominado como “datos sensibles”.

Reservados: aquellos datos que bajo ningún concepto está obligado el titular a darlos a conocer a terceros, si no es su voluntad. Y no admiten excepciones de ningún tipo.

Los datos personales se protegen mediante la invocación del Derecho a la intimidad, articulo 15 de la carta política fundamental.

La privacidad de hombres y mujeres se ha perdido no sólo en el ámbito del manejo de datos sensibles de carácter tradicional como la filiación política, la pertenencia a algún grupo sindical, la comunidad religiosa a la cual se hace parte, tipo de profesión, el grupo humano al que se pertenece, las costumbres sexuales, las apetencias personales y sociales, el historial clínico y jurídico - penal, las cuentas bancarias, la situación económica, los viajes, etc., sino también mediante la digitalización de información intima o privilegiada en distintas “redes” que funcionan como mega bases de datos, que permiten crear un cuadro completo de los aspectos más íntimos de la constitución física, social, moral y hasta psicológica de alguien. Ejemplo de esto son las redes sociales como Facebook que se convierten en canales de distribución de información privilegiada de las personas a

cualquier parte del mundo, pues las barreras de seguridad de dichas plataformas virtuales (Facebook) son de relativo fácil acceso para los sujetos potencialmente victimarios de la clase de delitos materia de estudio de esta investigación.

Con todo ello las distintas personalidades de hombres y mujeres de todas las edades pueden hacerse transparente, quedar expuestas, y hacerse de fácil identificación para fines de mercado y venta de mercancía, pues con la publicación de los ya enunciados datos sensibles, las empresas comercializadoras de productos, en su búsqueda constante de mercado pueden establecer pautas de consumo, y enlazarla con el mercadeo del sistema capitalista a través de la llamada minería de datos; y en consecuencia ”vender” de forma dirigida, pues ya tienen pautas de que es lo que quiere y necesita cada persona. No pretendo decir si ello es bueno o malo, solo hago una reflexión y una descripción de lo que conlleva “abrirse en exceso al mundo”.

11.2.2 Origen e historia del Derecho a la Intimidad y Buen Nombre

El origen y la historia del Derecho a la Intimidad, Buen nombre o Honra es relativamente nuevo en comparación con el origen de otros derechos igual de fundamentales como por ejemplo la libertad, pero sin embargo, se entiende por naturaleza desde hace cientos de años que la intimidad constituye un bien personalísimo al que el ser humano no puede renunciar por cuanto es inherente a la condición de dignidad humana.

El ser humano es social por naturaleza, y son las relaciones de interacción en sociedad las que han llevado y dado origen a la realización del crecimiento en todo aspecto del Hombre como especie superior dentro de la Naturaleza; aunque a pesar de ello, el Hombre y la Mujer siguen teniendo la necesidad de tener y realizar una vida interior ajena a las relaciones sociales que pueda tener con otros individuos y que le permite identificarse o definirse como ser humano, único e irrepetible; siendo el nombre un concepto que, constituye igualmente algo relevante para la construcción de la identidad propia, pues todos necesitamos de un nombre que nos permita dar a entender a la sociedad la existencia y denominación propia de cada individuo dentro de determinada Sociedad. Esta necesidad

que tiene cada persona de conocerse o identificarse a sí mismo, es un tipo de aspecto intangible que vive dentro del cerebro, corazón, alma, espíritu o esencia de cada quien, aspecto el cual todos consideramos importante para desarrollarnos como seres humanos únicos, autónomos, iguales y diferentes al mismo tiempo.

El análisis histórico evolutivo del derecho a la intimidad y Buen nombre, como se puede observar nace de las necesidades humanas, y en el desarrollo histórico se va haciendo cada vez más importante proteger ese derecho que se tiene al respeto de la esfera más íntima e individual de cada quien.

Ahora bien con el advenimiento de la era de las Tecnologías de la Información y las comunicaciones, el derecho en cuestión se empieza a desarrollar en ciertos nuevos espacios que hace que se vinculen los datos personales y la información personal, a plataformas virtuales o cibernéticas que han conducido al surgimiento de modernos mecanismos de tutela judicial efectiva que los distintos ordenamientos jurídicos de diferentes países en el mundo han reconocido constitucionalmente o legalmente debido a la aparición de nuevas problemáticas jurídico - sociales (expresiones de delito) derivadas de la vanguardia de la era tecnológica, como específicamente es el delito de violación de datos personales, problemática social nueva que ha surgido desde que a través de medios tecnológicos se ha digitalizado información personal exclusiva, en bases de datos para su ordenación, clasificación y obviamente sistematización.

Es de esta manera que el Derecho funciona para frenar o contrarrestar las nuevas formas de manifestación delincuencial, creando normas para regular dicha nueva problemática social, y para intentar solucionar las situaciones o actos que vulneren o pongan en peligro los derechos de la población, en este caso el derecho a la intimida y buen nombre ligado a la protección de datos personales; dicha protección de datos se ha ido posicionando como fundamental para el pleno goce y efectividad de los derechos humanos dentro de los territorios de las naciones, y también siendo sujeto de garantías de acuerdo al avance de las realidades jurídicas, políticas, sociales y culturales de cada uno de los países que han reconocido tanto éste especial derecho como los nuevos ámbitos y escenarios de protección del citado derecho que se viene exponiendo en esta investigación jurídico - académica.

La historia del origen del Derecho a la Intimidad personal y Buen nombre en su moderna concepción iusteórica en este siglo XXI, que incluye la "protección de datos personales" y la penalización por el abuso o la trasgresión del derecho al mismo, parte de la experiencia de los Estados Unidos de Norteamérica, y se considera como punto de partida de la construcción Jurídica del concepto de "Derecho a la Intimidad", el que los Estadounidenses denominaron "Privacy" en español "Privacidad", donde el estudio y concepto jurídico de un caso concreto denominado "Warren-Brandeis article", publicado en diciembre de 1890 por la prestigiosa Universidad de Harvard, al que titularon "The right to privacy" "El Derecho a la Privacidad", que bien puede ser considerada la aproximación literaria más importante en Occidente en el tema de protección del derecho a la intimidad desarrollado desde la óptica de las garantías fundamentales constitucionales (Warren Samuel y Brandeis Louis, 1890).

Otro importante antecedente histórico del tema es el que se da en 1859 para un importante pensador de la época, John Stuart Mill, quien afirmó que: "over himself, over his own body and mind the individual is sovereign" en español: "sobre sí mismo, sobre su propio cuerpo y mente el individuo es soberano"; lo que pretendía dar a entender desde ese entonces John Stuart Mill es que el ser humano posee de pleno derecho capacidad de autodeterminación e individualidad. En otras palabras Mill estaba desarrollando desde otro punto de vista su idea de Libertad, que tanto argumentó en sus escritos, especialmente en la Obra "Sobre la Liberad". Y desde la interpretación que se realiza en esta tesis se puede decir que Mill aportó al Derecho a la intimidad porque él pensaba que nadie más que el individuo podía autodeterminarse sin la injerencia directa o indirecta de otra persona, pues el individuo posee características únicas que lo llevan a ser libre en elección de vida y forma de pensar, sin la intromisión a la esfera más íntima del mismo ser humano pues en dicha esfera el individuo es el único soberano. (Mill, 1859)

Los anteriores antecedentes históricos del derecho a la intimidad, buen nombre y a la vida privada hacen parte de los aportes filosóficos propios del liberalismo político elaborados por autores como John Locke, Robert Price y el ya mencionado John Stuart MilI, quienes afirmaban en sus teorías, que la libertad y la autonomía personal serían el sustento de un régimen político que acabaría con el poder absolutista y autoritario del Rey,

conllevando a la transición de un Estado dominado netamente por el Soberano a un Estado donde la base seria la Ley y la Constitución (Estado Constitucionalista), con un parlamento que se encargaría de velar por la democracia y el bien general. En esta concepción liberal, escrita en su momento para Inglaterra, y expuesta por los 3 mencionados autores, el derecho a la intimidad es básicamente una libertad negativa, de no injerencia del Estado o individuos en la subjetividad o esfera individual; es decir es una libertad negativa que forma parte integral del mismo individuo y que comprende los derechos a la vida, la libertad y la propiedad, los cuales como derechos negativos obligan a los demás individuos a No arrebatarlos ni vulnerarlos.

Tiempo después en el mismo país Ingles, un hombre, Lord Mancrotf, introdujo en 1961, junto con otras personas de su partido político, un proyecto de ley que intentaba regular la privacidad de las personas, dándole especial importancia a ese derecho poco ilustrado para la época, siendo este uno de los primeros intentos en Inglaterra que pretendía proteger mediante un procedimiento legal, o una ley, el concepto de "Privacidad" o "Intimidad" para salvaguardar este relativamente nuevo derecho humano.

El Convenio 108 adoptado por La Comunidad Europea a través del Consejo de Europa surtido el 28 de enero de 1981 y ratificado el 27 de enero de 1984, es el primer instrumento internacional de Protección de las Personas con respecto al Tratamiento automatizado de datos de carácter personal, el cual procura regularizar en términos político-jurídico el fenómeno del tratamiento automatizado de datos correspondientes a personas naturales desde una perspectiva que trasciende de la individualidad de los países en Europa, pues el contenido de este instrumento internacional, entraría a formar parte de los países miembros, generando una especie de uniformidad o unidad de materia jurídicamente hablando, en cuanto al tema de protección y garantías legales de este derecho, con el objeto de disponer de una normatividad Europeo-comunitaria la cual permitiera a los Estados miembros contrarrestar la nueva problemática jurídico-penal de violación de datos personales a través de medios informáticos, tecnológicos o semejantes.

Resulta ostensiblemente relevante entender que los orígenes del concepto de Derecho a la Intimidad y Buen nombre no siempre ha sido fácil, pues no siempre se ha asociado este derecho con la protección de datos personales o la libertad informática; este especial derecho es más bien una construcción social, que ha tenido buen desarrollo doctrinal, constitucional y jurisprudencial en los diferentes países del mundo, por cuanto es un fenómeno que se presenta en el marco de una sociedad humana Globalizada, que nació gracias a la creciente era tecnológica y el abuso que resultó a causa de conductas ilícitas cometidas contra los derechos individuales de las personas.

Dada la génesis del derecho en cuestión, resulta igualmente interesante comprender que la evolución histórica del mismo se da gracias a la necesidad creada por factores inherentes a la misma dinámica evolutiva de los derechos, y es necesario comprender el pasado de los conceptos y/o derecho a la intimidad y buen nombre como herramienta fundamental para proponer nuevas tesis en el presente, hacer críticas constructivas y aportar hacia el futuro para la creación de nuevas formas de proteger este importante derecho; pues como es bien sabido por los métodos científicos de investigación, las experiencias históricas de la vida humana sirven para conocer una historia específica, más su contexto, y por consiguiente, al conocerla, se tiene la ventaja de no repetir los errores pasados, teniendo la posibilidad de tomar mejores decisiones, basadas en fundamentos históricos, hechos y estadísticas, para así lograr óptimos resultados, que permitan una mayor eficacia, eficiencia y efectividad en este tipo de investigaciones de Derecho.

11.2.3 Derecho a la Intimidad y Buen Nombre en las Constituciones Internacionales

A la hora de hacer un análisis de Derecho comparado en cuanto al tema objeto de esta tesis, se puede dar como referencia las siguientes normatividades afines de carácter internacional, llamados también instrumentos jurídicos internacionales, los cuales protegen teórica, jurídica y políticamente El derecho a la intimidad y sus diferentes formas de manifestación y expresión:

- La Declaración Universal de Derechos Humanos de 1948.
- la Convención Americana sobre Derechos Humanos de 1969.
- El Pacto Internacional de Derechos Civiles y Políticos de 1966.
- El Convenio Europeo de Derechos Humanos de 1950.
- La Carta de Derechos Fundamentales de la Unión Europea del año 2000.
- La Organización para la Cooperación Económica y el Desarrollo (OCDE) ha esbozado una definición del delito de "violación de datos personales", la cual define dicha conducta punible como "cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos".

Desde la época de los años 70´s las Constituciones de Europa, previendo situaciones de vulneración del derecho a la intimidad por medio o a través de los avanzados medios científicos, tecnológicos, virtuales y/o digitales, comenzaron dichos Congresos, Parlamentos y/o Gobiernos a presentar proyectos orgánicos de Ley, para establecer dentro de sus ordenamientos jurídicos la protección a la venidera problemática del ciber crimen.

Estas iniciativas legislativas, comprenden por ejemplo las siguientes constituciones Internacionales:

- En Nueva Zelanda, que en 1976 aprobó el Wanganui Computer Centre Act, Ley para la protección de la Intimidad y datos computarizados.
- En Inglaterra con La "Data Protection Act" que traduce "Ley de Protección de Datos" de 1975.
- En Canadá, donde el 2 de junio de 1977 entró en vigor el Human Rights Act.

- En Francia, la ley relativa a la informática, a los archivos y a la libertad; el 8 de junio de 1978.
- En Dinamarca, la ley sobre los registros privados, seguida por la de los registros públicos; el 9 de junio de 1980.
- En Noruega, la ley sobre los registros de datos personales, vigente desde el 1 de enero de 1980.
- En Austria, la ley sobre la protección de los datos personales, precedida y preparada por un proyecto de ley gubernativo presentado en el Parlamento en diciembre de 1975.
- En Luxemburgo el 31 de marzo de 1979 realizó la ley para reglamentar la utilización de los datos nominativos en los procesamientos informáticos.
- En Bélgica en 1976, Ley de Protección de datos Personales.
- En Holanda en 1976, se presenta proyecto de Ley para la Protección de la Información y de los datos.
- En España con el artículo 18 de la Constitución de 1980, relativo a la protección del Derecho a la intimidad, el honor y la intimidad personal y familiar de los ciudadanos en territorio Español.

Estados Unidos, como país altamente desarrollado, Industrializado, y de avanzada tecnología, es importante destacar que ha contribuido bastante desde la academia en la promoción del derecho a la intimidad y buen nombre como derecho humano fundamental para el pleno ejercicio de la libertad, igualmente y aún más importante, La Cuarta Enmienda de la Constitución Norte Americana, no se limita solo a la protección de elementos de autonomía personal o privada, sino que abarca la inviolabilidad arbitraria e injusta de las aprehensiones y registros arbitrarios de personas en sus lugares de habitación y sus documentos privados.

Otro ejemplo de Regulación en las constituciones internacionales es el del continente oceánico, donde Australia en el año de 1994 promulgó la "Ley De La Intimidad Y La Protección De Los Datos" en inglés, "The Privacy and Data Protection Bill 1994", siendo esta normatividad uno de los más recientes estatutos legales que regulan la protección de los derechos fundamentales en el mundo, especialmente el derecho a la intimidad, cuando

los datos personales han sido sometidos a un proceso de almacenamiento y registro informatizado, por medios informáticos, electrónicos o telemáticos.

11.2.4 Derecho a la Intimidad y Buen Nombre en la Constitución Política de Colombia

El tema de esta tesis académica se desarrolla directamente desde la perspectiva constitucional salvaguardando el artículo 15 de la constitución política, derecho fundamental a la intimidad y buen nombre que taxativamente expresa:

ARTICULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en 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.

NOTA: *El artículo 15 fue modificado por el Acto Legislativo 02 de 2003, el cual fue declarado* ***INEXEQUIBLE*** *por la Corte Constitucional mediante* ***Sentencia C-816 de 2004,*** *por el vicio de procedimiento ocurrido en el sexto debate de la segunda vuelta.*

Hasta aquí se ha visto el recorrido histórico que ha tenido la evolución del derecho a la intimidad y buen nombre, además de los diferentes tratamientos que éste ha tenido en otros países del mundo y se ha podido comparar con la legislación vigente respecto del tema en Colombia, concluyendo que Colombia como Estado Social de Derecho, soberano y alineado con la política supraconstitucional de Los Derechos Humanos, es protector de este principal derecho, y además, otorga herramientas jurídicas tanto penales como constitucionales para defender con validez y eficacia el Derecho fundamental plasmado en el art. 15 de la Constitución Política.

11.3 CAPÍTULO 3

FORMAS COMO SE HAN AFECTADO EL DERECHO A LA INTIMIDAD Y EL BUEN NOMBRE

Dentro de esta investigación se he establecido la importancia de identificar las formas como puede ser afectado el derecho a la intimidad y buen nombre, pues resulta vital esclarecer las modalidades bajo las cuales se violentan los datos personales, las bases de datos, los programas cibernéticos, y cómo dichos actos atentan el derecho a la intimidad, buen nombre y honra de las personas en particular, que dada la Globalización e internacionalización de la era tecnológica utilizan todo tipo de medios computacionales y de telecomunicaciones para estar conectados con el mundo, y así realizar todo tipo de actividades incluyendo las laborales, sociales, recreativas, financieras, políticas, culturales etc.

En este capítulo se expondrá las formas como se han afectado el derecho a la intimidad y buen nombre en países que han realizado un aporte valioso desde la academia y el Derecho constitucional a la construcción del concepto, e igualmente han realizado una regularización del tema que aporta desde distintos ángulos, y sin lugar a dudas, políticas públicas para afrontar esta nueva problemática jurídico – social.

11.3.1 Formas como se ha afectado el Derecho a la Intimidad y el Buen Nombre a nivel Mundial (una visión panorámica del fenómeno)

Se puede decir que las formas como se ha afectado el derecho a la intimidad y buen nombre abarca distintos modos de cometer la conducta, pues son variadas las formas en que se ha visto que se puede afectar la esfera de la privacidad e intimidad de las personas. Al indagar sobre este especifico aspecto, es válido decir que en términos generales las formas de transgredir este derecho son muy parecidas en todos los países del mundo, pues la Globalización y la era de las TIC´S han creado un lenguaje y mundo virtual (hablando en

términos de ingeniería de sistemas o telemática) en el que es casi estándar la captación, recepción, registro y almacenamiento de información en bases de datos computacionales, digitales o en red de Internet, con lo cual las formas de violar datos personales contenidos en estas herramientas de sistematización son muy similares en todas partes del Globo terráqueo, dado que en Estados Unidos, Europa, Suramérica, África e incluso el continente Asiático los medios cibernéticos, digitales y tecnológicos son de similares características y funcionan muy parecido, a pesar que existen diferencias en los niveles de tecnología entre los países, dichos medios están interconectados y hacen uso de la Red Global (Internet) haciendo que la Globalización sea más evidente en este contexto; por lo cual si los medios son semejantes entre sí, las formas de trasgredir y afectar el derecho a la Intimidad, Buen Nombre, y Honra serán semejantes en los distintos países. Lo que puede variar como veremos más adelante será la forma como los Ordenamientos Jurídicos, a través de sus normas y políticas públicas asumen los conflictos que se presentan en cuanto al tema.

El derecho a la Intimidad y Buen nombre contiene en toda jurisdicción Occidental la protección a la vida privada, y plantea la necesidad y mantenimiento de una identidad personal, asociada a un nombre y un apellido, sin más limitaciones que las que sanamente exprese la Ley. Así, por ejemplo, en el viejo continente Europeo, los países tienen desarrollada la concepción de que la protección de la intimidad, privacidad y Buen nombre hace parte de la dignidad humana, y consecuentemente, estos países entienden tal derecho como algo inherente a la personalidad individual de cada ser humano.

Sin embargo las políticas públicas y las formas como se protege este derecho en cada país son diferentes, pues el tratamiento y protección de datos personales, ligado a la intimidad o privacidad personal, ha cambiado, e incluso ha sido sometido con el argumento de prevalencia del interés general sobre el interés particular; dicha situación ha ocurrido desde principios de siglo cuando se presentaron graves perturbaciones a la seguridad tras los atentados terroristas del 11 de septiembre en Estados Unidos y el 11 de marzo en Europa, los cuales dejaron cuantiosos daños materiales, muertos, heridos y miedo generalizado en las ciudadanos.

Es por estas nefastas situaciones que los Gobiernos de las distintas naciones han tomado serias decisiones en materia de seguridad Nacional y políticas antiterroristas, con lo cual muchas veces el tratamiento de información personal resulta determinante para afrontar los lamentables ataques terroristas que se presentan ocasionalmente debido a concepciones político-religiosas o cosmovisiones diferentes de ver y entender la vida en este mundo. Todo ello está conduciendo a una política europea integrada que contrarreste con pautas claras, directivas y sobre todo políticas públicas que se antepongan cuando se presente dicha problemática que incluye entre otras cosas retención de datos personales en las comunicaciones de todo tipo; pues según esta óptica, es mejor sacrificar el derecho privado y particular, y no exponer al colectivo social a una amenaza o atentado de carácter terrorista.

La política antiterrorista que incluye hacer interceptaciones a los datos privados de la gente es más evidente y legitima en los Estados Unidos, pues este país tiene una política exterior e interior más agresiva en cuanto tal. Y comparándola con Europa, claramente dicha política estadounidense es menos garante del derecho a la intimidad.

11.3.2 Formas como se han afectado el Derecho a la Intimidad y el Buen Nombre Caso Estado Unidos

El tema del respeto a la intimidad y buen nombre, así como su vulneración a través de medios tecnológicos y semejantes es muy complejo y controvertido en los Estados Unidos, puesto que las diferentes posiciones que se tienen por parte de los distintos distritos federales hacen que su aplicación varíe dependiendo de cada estado, pero la última razón la tiene el poder judicial (Jueces y Corte Suprema de los Estados Unidos) ya que como se ha dicho el derecho norteamericano es dinámico, los jueces son fuente de Derecho y el precedente judicial es doctrina establecida que se debe acatar para solucionar los casos con situaciones fácticas y jurídicas análogas o semejantes.

Estados Unidos como país ideológicamente capitalista, garante de la libertad y de la multiculturalidad ha creado por ejemplo leyes que regulan el derecho a rechazar atención médica por concepción o creencias religiosas, también tiene regulado constitucionalmente el registro ilegítimo de una vivienda (derecho a la privacidad físico-espacial), leyes sobre el derecho a monitorizar las computadoras en los lugares de trabajo (privacidad informática), leyes en varios estados en cuanto a elegir el tipo de matrimonio o unión marital (privacidad de elección), así como también leyes para incluir o excluir a terceras personas de instituciones societarias (privacidad en la asociación); las mencionadas leyes han tenido desarrollo y aplicación por parte de los jueces que cumplen la función pública de administrar justicia mediante un proceso, aterrizando o materializando la doctrina sentada por la Corte Suprema de Justicia en cuanto al tema de "Privacy" – Privacidad, a través del precedente judicial.

Según se ha podido investigar, existen formas definidas de los tipos de problemáticas que afectan el derecho a la privacidad, buen nombre y honra en los Estados Unidos, las cuales conllevan a acciones legales definidas para llevar a juicio las posibles violaciones a este fundamental derecho que trata esta investigación.

Se ha podido constatar que la invasión a la privacidad por intromisión y difusión pública de hechos privados es una forma de menoscabar el derecho a la intimidad, la cual podría conllevar a un caso por Responsabilidad Civil y Penal por violación a la privacidad, en el que como cualquier otro caso civil, requiere daños causados, perjuicios, nexo de causalidad y pruebas que sean suficientes y legítimas para que ameriten la instauración de la Demanda. Dichos perjuicios deben repercutir en lesiones a la dignidad humana de la persona (perjuicios morales) que ameriten un resarcimiento, el cual viene acompañado de una compensación económica cuantificable, la cual es difícil tanto de probar como de estimar por ser de carácter subjetiva; este argumento es la razón por la cual se hace complejo o difícil que las acciones legales por violaciones de la privacidad sean dirimidas en los estrados judiciales, y muchas veces este tipo de reclamaciones legales son rechazadas por los jueces, con la consecuencia de que las Cortes Federales de los EE.UU no conozcan de estos casos. Sin embargo se puede decir que cuando las vulneraciones son cometidas contra personas reconocidas públicamente

por ser actores, políticos o deportistas, las acciones tienden a repercutir social - política y judicialmente, pues a ellos se les afecta de una manera más visible, y los medios de comunicación como periódicos y noticieros publican los hechos y el proceso judicial en esas circunstancias sí toma la relevancia que debe tener toda intromisión arbitraria perjudicial para la intimidad, buen nombre y privacidad.

En el Derecho Estadounidense existen 4 acciones constitucionales - civiles que se pueden distinguir para hacer defensa jurídica ante posibles violaciones a la privacidad, las que se pueden resumir como:

1. La intromisión en el ámbito más íntimo y privado – Right to be alone.
2. La apropiación del Nombre.
3. La distorsión de la imagen - The false light privacy.
4. La difusión pública de hechos privados.

Las mencionadas acciones legales se presentan cuando se ocasionan daños relacionados con la privacidad e intimidad de los ciudadanos Norteamericanos.

En la primera, La Intromisión en el ámbito más íntimo y privado – Right to be alone, acarrea Responsabilidad civil por violación de datos personales y captación ilegal de información personal; Es decir, se aplica a situaciones donde la información es obtenida o sustraída de una manera ilegal de un lugar privado, puede configurarse por inmiscuirse física o virtualmente a una computadora, puede ser también por la intromisión en la reclusión o soledad de otra persona en sus asuntos íntimos, familiares, o problemas privados, lo que ocasiona una seria ofensa a la dignidad de la persona.

La configuración de esta forma de violar la intimidad y privacidad le brinda a la víctima el derecho a recobrar daños patrimoniales y extra-patrimoniales por invasiones arbitrarias que puede ser físicas, cibernética, digital, interceptación telefónica, correo, correo electrónico, incluso el espiar visual con cámaras video fotográficas.

En la segunda, La apropiación del nombre o la figura, comprende principalmente una violación al derecho de propiedad, y como se sabe la Propiedad es uno de los principales fundamentos del Ordenamiento Jurídico de los Estados Unidos. Esta segunda acción legal es para protegerse de una forma de violar el nombre de uso comercial o la identidad de una persona, pues si un individuo tiene un interés legal de cualquier tipo, o derecho de propiedad sobre su nombre o figura para los fines legales y libres que el disponga, nadie puede sacar provecho y apropiarse de dicho nombre y/o figura.

Esta acción que se está mencionando, se aplica cuando la información del nombre o figura es usada por un tercero, que de manera aprovechada e ilícita usa la imagen, nombre o signo distintivo para propósitos comerciales, y sacar provecho de una imagen o nombre que en cierta medida ya está posicionada en el mercado, que tiene dueño, y que no puede ser usada por cuanto ha sido patentada, reconocida como marca individual, y además no ha dado autorización para ser usada por otra persona que no ostenta el derecho de uso, el disfrute, goce o la disposición.

En lo atinente a la tercera, La distorsión de la imagen - The false light privacy, es una acción derivada de la violación a la privacidad. Esta acción se enfoca en reparar el daño causado a la paz mental del individuo (daño moral). En esta forma de violación a la privacidad, buen nombre e imagen del individuo, se engaña al público con información falsa sobre un individuo particular, que perjudica gravemente la honorabilidad de la persona, hiriendo también la dignidad y los valores que la persona reconoce de sí misma. La distorsión de la imagen tiene que involucrar asuntos inherentemente privados, o sea que los actos realizados en lugares públicos, o divulgados en sitios abiertos al público, que se divulguen o publiquen por terceros a otras personas, no es protegible sin importar cuán ofensivas sean sus repercusiones, puesto que el hecho a pesar de que puede contener contenido privado, no se hizo dentro de la intimidad privada, por el contrario se hizo en un contexto abierto a todos.

La cuarta acción, Difusión pública de hechos privados, conlleva a una compensación económica por la publicación injustificada de hechos verdaderos pero sin valor informativo, además de privados y ofensivos para el sujeto pasivo de esta conducta (Victima). Esta forma de violar el derecho a la intimidad y la información personal, requiere que se de publicidad al hecho real, que se enmarque en el contexto de la esfera privada, que la información no sea del interés legal o legitimo del público, y que la difusión sea altamente ofensiva.

De todas maneras, existen leyes que promueven la garantía constitucional a la libre expresión, libertad de conciencia y difusión de pensamiento, las cuales podrían entrar en colisión con el derecho que tienen las personas de disfrutar de su vida privada, y aun así los asuntos con significado público o de valor informativo en los cuales hay un interés legítimo del colectivo social, no están cubiertos por esta acción, y no podría haber lugar a iniciar una demanda por acciones derivadas de la violación a la privacidad.

Hasta aquí se mostró las formas como la justicia norteamericana dirime los conflictos que se presenten en materia de privacidad e intervención arbitraria a la intimidad, y los mecanismos jurídicos para acudir ante los jueces norteamericanos en aras a restablecer y resarcir los daños causados por la injusta intromisión a la esfera más próxima de los ciudadanos.

11.3.3 Formas como se han afectado el Derecho a la Intimidad y el Buen Nombre Caso Alemania

En el ordenamiento jurídico de Alemania se puede distinguir y hacer respetar las formas de violación a la intimidad, buen nombre y privacidad primeramente desde la constitución, y segundo mediante la Ley Penal (Código Penal) que engloba una serie de circunstancias que configuran agresiones a bienes jurídicos protegidos por el Derecho alemán; en este apartado se describen las formas como se puede llegar a afectar el derecho objeto de este estudio jurídico – académico, en el país Germano.

Según la ley de (Legislador, 1871), El Código Penal Alemán del 15 de mayo de 1871, reformado el 31 de enero de 1998, proscribe en su parte especial, específicamente en la Sección decimoquinta, La Violación al ámbito de la intimidad personal y al ámbito del secreto personal, una norma que comparativamente se puede equiparar al título séptimo del Código Penal Colombiano puesto que el bien jurídico protegido y la inspiración de defensa jurídica es la Protección de la Información y de los Datos, de este modo se puede decir que en términos de Derecho comparado Alemania y Colombia tienen leyes especiales de protección a una garantía constitucional fundamental, la cual es el derecho a la intimidad y buen nombre ligado al libre desarrollo de la personalidad, libertad, condición de dignidad humana y respeto por los Derechos Humanos; más aún por cuanto los dos países se hacen llamar así mismos Estados Constitucionales y Estados Sociales de Derecho.

El mencionado instrumento Jurídico-Penal Alemán, en la Sección decimoquinta, titula "La Violación al ámbito de la intimidad personal y al ámbito del secreto personal", y a continuación describe en los artículos subsiguientes, los tipos penales que son las formas como se puede ver vulnerado o afectado el derecho a la intimidad y las respuestas o consecuencias jurídicas que conlleva el cometer dichos ilícitos penales, que en su mayoría como también lo hace el código penal colombiano establecen penas privativas de la libertad y multa para este tipo de delitos con contenido informático.

Los artículos del mencionado Código Penal Alemán que describen dichas formas son los numerales 201, 202, 203, 204 y 205, los cuales se exponen así en síntesis:

Artículo 201. Violación al secreto de la palabra:

Señala este artículo que… "con pena privativa de la liberta hasta por tres años o con multa, será castigado quien sin autorización grabe mediante dispositivo de sonido la palabra no pública hablada de otro o utilice una grabación producida de tal manera que la haga accesible a una tercera persona".

Igualmente dice la norma que: De la misma manera será castigado quien sin autorización oiga con un dispositivo interceptor la palabra no pública de otro y no destinada para su conocimiento, o también quien comunique públicamente en su sentido literal o en su contenido esencial, la palabra hablada de otra grabada.

La norma en el citado artículo hace las siguientes aclaraciones y/o precisiones:

a. El hecho será punible cuando la comunicación pública sea apropiada para perjudicar los intereses legítimos de otro.

b. El hecho no es antijurídico cuando la comunicación pública se haga para defender intereses públicos relevantes.

c. El hecho será castigado con pena privativa de la libertad hasta de cinco años o con multa, cuando quien como titular del cargo, o como especialmente obligado, por ser servidor público lesione la confidencialidad de la palabra.

d. El hecho será punible en el grado de tentativa.

e. Los aparatos de grabación de sonido y de interceptación que el autor o partícipe empleen pueden ser confiscados.

Es necesario mencionar que en este artículo cuando se refiere a “otro” se hace alusión a una persona. Importante también es decir que no se especifica el precio o monto cuando se hace referencia a la consecuencia de multa.

Artículo 202. Violación del secreto de correspondencia:

Dispone la norma que “Quien sin autorización abra una carta cerrada u otro escrito cerrado que no estén destinados para su conocimiento o se procure conocimiento del contenido de tal escrito sin abrir el cierre bajo utilización de medios técnicos será castigado con pena privativa de la libertad hasta un año o con multa”.

Este artículo guarda especial relación con el artículo 15 de la constitución política de Colombia porque trata de la misma forma la inviolabilidad de la correspondencia y documentos privados.

Artículo 202 A. Piratería informática:

Dispone este que "Quien sin autorización se procure para sí o para otro datos que no estén destinados para él y que estén especialmente asegurados contra su acceso no autorizado, será castigado con pena privativa de la libertad hasta por tres años o con multa. Los Datos son solo aquellos que se almacenan o trasmiten en forma electrónica, magnética, o de otra manera en forma no inmediatamente perceptible".

Este artículo es el análogo del articulo 269 F del código penal Colombiano pues guarda una especial relación al garantizar las violaciones ilícitas a los datos personales contenidos en medios cibernéticos, virtuales, computacionales o semejantes; con la diferencia de que el delito en Colombia es castigado, en teoría, con una pena muchísimo más alta en comparación a Alemania, pues el máximo en la Justicia colombiana es 8 años de cárcel, mientras que en Alemania son 3 años.

Artículo 203. Violación de secretos privados:

Este artículo expone que "Quien sin autorización revele un secreto ajeno, es decir, un secreto perteneciente al ámbito de la vida personal, o un secreto de empresa o negocio, que le haya sido encomendado a él, o que de otra manera lo haya conocido como médico, odontólogo, médico veterinario, farmacéutico, o miembro de otra profesión de salud que requiera para su ejercicio profesional o para la denominación profesional una formación regulada por el Estado, sicólogos profesionales con examen final científico reconocido por el Estado, Abogado, abogado de patente, notario, defensor en un proceso ordenado por ley, auditor, contador juramentado, asesor fiscal, apoderado fiscal u órgano o miembro de un órgano de una sociedad económica o contable, o de asesoría de fiscal, Asesor matrimonial, de familia, de educación, de juventud, así como asesor para asuntos de adicción en una dependencia de asesoría que sea reconocida por una autoridad o corporación, establecimiento o fundación del derecho público, Miembro o encargado de una reconocida dependencia de asesoría, Trabajador social reconocido por el Estado, o pedagogo reconocido por el Estado, Personal de una empresa del sector privado de seguro contra

enfermedades, accidentes o de vida o de una Caja de Compensación será castigado con pena privativa de la libertad hasta por un año o con multa.

Este artículo exclusivo de la Ley Penal alemana, se equipara a la obligación legal de guardar el secreto profesional en el ordenamiento jurídico de Colombia, y su exposición injustificada a otros es sancionable disciplinaria y penalmente. Sin embargo la pena para este delito es pequeña (1 año) y no se específica la cuantía de la multa.

Artículo 204. Aprovechamiento de secreto ajeno:

"Quien sin autorización aproveche un secreto ajeno sobre todo un secreto de empresa o de negocios para lo cual esté especialmente obligado a guardar el secreto según, será castigado con pena privativa de la libertad de hasta dos años o con multa".

Artículo 205. Querella:

"En los casos de los artículos 201 a 204 el hecho se perseguirá solo por petición. Si el lesionado muere, entonces el derecho de petición pasa a los parientes."

De esta manera es como la Ley Penal Alemana penaliza y persigue los delitos que atentan el derecho de las personas a la confidencialidad de la información personal y de los datos, subrayando que hay sin duda alguna una estrecha relación doctrinal y legal entre Colombia y Alemania, porque el tratamiento que se le da a este tipo de delito es similar en cuanto al diseño, inspiración, redacción, además de tipicidad y antijuridicidad. Por ello se puede concluir a priori que Colombia está en un muy buen nivel de protección constitucional y legal del derecho a la intimidad, buen nombre y honra a la par de otros Estados con un mayor grado de desarrollo.

11.3.4 Formas como se han afectado el Derecho a la Intimidad y el Buen Nombre Caso España

España, es de los países en Europa con una clara política pública de protección del derecho a la intimidad, buen nombre, habeas data, protección de datos sensibles, y en general como Estado Social de Derecho, bien sabe de la fundamental importancia que tiene este derecho para el desarrollo de la persona en condiciones libres y dignas. El derecho fundamental a la intimidad, privacidad, y protección de datos ha prosperado en un entorno normativo y jurisprudencial muy favorable que la sociedad española en gran medida respeta por cuanto asume que este particular derecho es básico en esta era de la tecnología y la moderna sociedad digital.

Es así como la Constitución española en el artículo 18 (Congreso de España, 1978) y la Ley Orgánica de Protección de datos personales de 1999, con sus 49 artículos y disposiciones, firmada por el Rey de España de ese entonces Juan Carlos I y el Presidente del Gobierno José María Aznar López (España Juan Carlos I, 1999), ofrecen una normatividad jurídica altamente avanzada para que se tutele efectivamente las intromisiones arbitrarias e injustificadas a la intimidad de las personas, generando una cultura de protección de datos a las instituciones públicas y privadas que utilicen bases de datos y ficheros para organizar, digitar y sistematizar la información concerniente de los usuarios, clientes, pacientes y en general de todas las personas miembros del país.

La Ley Orgánica de Protección de datos personales de 1999 española surgió precisamente para ordenar y estandarizar la captación y seguridad de los datos de las personas, puesto que con el devenir de la Globalización y dado la masificación de los avances tecnológicos, se identificaron formas de trasgredir la información personal a través de medios virtuales que repercutían en la lesión de una variedad de derechos (Pluriofensividad), y por supuesto se configuraba un delito; por ejemplo se configuraba el delito de hurto si la información que se capturaba a través de los medios virtuales le servía al delincuente para apropiarse de dinero consignado en bancos, o también se configuraba violación a los derechos de autor si la información sustraída ilícitamente era para sacar provecho del intelecto escrito o redactado de un poeta, escritor, artista, periodista, político etc., Dicho lo anterior es oportuno decir que estas formas de trasgredir la intimida y

privacidad de la información personal, no es un problemática social exclusiva del país ibérico, sino que por el contrario es un problema ya generalizado en todo el mundo que utiliza los sistemas tecnológicos computacionales, por cuanto como se ha dicho es una consecuencia de la interconexión Global de las distintas naciones.

Otra problemática española, pero no exclusiva de este país, es el tratamiento de los datos personales y la información personal que actualmente se hace visible por voluntad propia de la gente a través de las redes sociales (Facebook, Twitter, Instagram, WhatsApp, Linked In, y semejantes) las cuales ofrecen a los usuarios la posibilidad de hacer público información personal como nombre, teléfono, dirección , profesión u ocio, estado civil, gustos, y en fin dan la facilidad de definir el perfil físico, social, racial, político, religioso y cuanto ámbito sea posible, dejando a la persona transparente ante toda la ciber-comunidad. Esta cantidad casi ilimitada de visibilizar los datos personales en las redes sociales impide que los usuarios tengan en gran medida salvaguardado su derecho a la intimidad, privacidad y buen nombre por cuanto quedan expuestos al océano gigante que es el internet como red global de información.

Siguiendo con esta forma trascendental de vulneración de intimidad y privacidad que es la divulgación de los propios datos en las redes sociales, el usuario puede en cualquier momento cambiar la visibilidad de su perfil, actualizar la información e incluso actualizar imágenes que tenga de sí mismo, lo cual no significa que ello sea bueno o malo, pero que sin embargo y en el contexto estudiado en esta tesis es un potencial peligro para los violadores de los datos personales y de la información personal, pues tener perfiles personales colgados en las redes sociales es una actividad generalizada en los países en que la sociedad tiene acceso a las TIC´S.

Este problema de las redes sociales de mostrar gran parte de la información del usuario sin contar con el consentimiento del mismo es lo que genera inseguridad para un derecho principal y necesario que a pesar de ser intangible es fundamental para la condición de dignidad humana inherente a los hombres y las mujeres. Entonces regular y/o graduar la visibilidad de los datos personales o sensibles dentro de las redes sociales con el pleno consentimiento y autonomía de la voluntad de los usuarios podría funcionar como una sana barrera para no ser víctima de los que cometen este tipo de delito.

Ahora bien recordando que el Ámbito de aplicación de la Ley Orgánica de Protección de datos española, la cual dice que la aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados, dicha norma legal no abarca en su totalidad la protección que se debe tener del derecho a la intimidad y privacidad de la información en los programas, software, plataformas o redes sociales que se encuentran a disposición de cualquier persona en internet, sin embargo el Tribunal Constitucional Español en una interpretación amplia proyecta el derecho fundamental a la protección de datos sobre los elementos del artículo 18 de la constitución española, de modo que en presencia de un dato personal la Corte advierte que, con independencia de su naturaleza pública o privada, éste puede servir para la confección de perfiles, ideológicos, raciales, sexuales, económicos o de cualquier otra índole, subrayando que tal actividad podría constituir una potencial amenaza para el individuo, para el derecho consagrado en la norma fundamental de España.

11.3.5 Formas como se han afectado el Derecho a la Intimidad y el Buen Nombre Caso Colombia

Colombia ha tenido un importante crecimiento en términos de desarrollo económico, industrial, de infraestructura, académico, de Tecnologías de la información y las telecomunicaciones entre otros, en los últimos años, ello gracias a la apertura económica y al modelo de Estado que se tiene desde la proclamación de la Constitución Política de 1991. Este desarrollo se puede percibir en la posibilidad que tiene cada persona de acceder a distintos bienes y servicios necesarios para favorecer las condiciones de vida y el progreso en este nuevo siglo XXI. Gracias a la vida contemporánea y a la Globalización, los grandes problemas de la humanidad se han hecho ya parte de casi todas las naciones del mundo, incluyendo Colombia, así como también las cosas favorables como los Derechos Humanos, las garantías constitucionales, los derechos y las libertades inherentes a la

condición de ser humano que también se han expandido a lo largo y ancho del Globo terráqueo, y cada vez más culturas y naciones reconocen derechos que por naturaleza nos corresponde íntegramente como raza humana.

Uno de los problemas que se ha generalizado en las distintas naciones es la violación de datos personales a través de los medios virtuales, tecnológicos y semejantes. Colombia no es ajena a esta problemática y como ya se ha dicho el país tiene una clara preocupación por salvaguardar el derecho a la intimidad, buen nombre, habeas data, inviolabilidad de la correspondencia privada, y en general un ideal de proteger por las vías jurídico-legales una serie de derechos que se pueden ver afectados o vulnerados de distintas formas gracias a que es necesario y casi que obligatorio para hacer parte de las relaciones sociales dentro del Estado social de Derecho, en esta vida contemporánea, hacer parte de los sistemas de las bases de datos, ficheros, y programas de ordenación de información.

En Colombia al igual que en el resto de países del mundo se han identificado formas de afectación del Derecho a la Intimidad y el buen nombre, sin embargo dichas formas guardan una estrecha similitud fáctica por cuanto los modos de operar son de idénticas características, es decir la vulneración de tal derecho se constituye por hechos similares en todas partes del mundo; donde el sujeto pasivo (victima) puede ser cualquier persona que tenga datos personales o información clasificada y sensible en su computador personal o en bases de datos de entidades públicas o privadas, y por otra parte el sujeto activo de la conducta punible es todo aquel que con el ánimo de sacar provecho para sí o para un tercero mediante maniobras fraudulentas, capta datos o trasfiere información personal de otro vía ondas electromagnéticas con la ayuda de aparatos tecnológicos de relativo fácil acceso como un computador, PC Portátil o Smartphone, donde el bien jurídico tutelable vulnerado es la información personal y los datos personales, cuyo derecho sustancial inmerso es el derecho a la intimidad, buen nombre y honra.

La más grande herramienta de la era de la Globalizada es el Internet; y con ella los programas de comunicación y registro de información más utilizados como Facebook – Twitter – WhatsApp - Correos electrónicos tipo Hotmail, Gmail, Yahoo etc. son los más propicios para acceder a esas bases de datos privilegiadas, y cometer el ilícito penal. Sin embargo otras bases de datos muy utilizadas son las que guardan información financiera,

pues los Bancos se han consolidado como las instituciones idóneas para que las personas guarden el patrimonio activo que consiguen. Dicho lo anterior son las bases de datos financieras las más buscadas por los delincuentes informáticos para apropiarse de información personal que consecuentemente les permita obtener provecho económico de las cuentas bancarias de los usuarios. Se hace pertinente comentar que cometer este ilícito es muy rentable para los delincuentes cibernéticos tanto en Colombia como en el resto del mundo.

En Colombia está vigente La Ley 1273 de 2009 del 5 de enero de 2009, llamada la Ley de los delitos informáticos, que complementó el Código Penal (Ley 599 de 2000), la cual creó un nuevo bien jurídico tutelable llamado "De la protección de la información y de los datos", con un capitulo que se denomina “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”, en este se describen las formas como puede ser afectado este bien jurídico, y adecúa en una serie de delitos, las conductas típicas y antijurídicas que afectan el derecho a la intimidad personal, buen nombre, habeas data y otros derechos conexos como los derechos de autor, dignidad, patrimonio entre otros dependiendo del caso, porque como ha reconocido la doctrina y la jurisprudencia, este tipo de delitos son de carácter pluriofensivo, que afectan simultáneamente varios derechos protegidos por la constitución y las leyes.

Sin embargo la legislación colombiana y ésta Ley penal 1273 de 2009 que opera en el territorio nacional no es suficiente para la protección efectiva de estos derechos, pues los delincuentes tienden a perfeccionan sus métodos y medios digitales y/o tecnológicos para infiltrarse en los diferentes sistemas de ordenación y guarda de datos personales con el objetivo de cometer las conductas punibles establecidas en los artículos 269A a 269J del Código Penal. Se dice que no es suficiente la norma ya que ésta requiere de unas instituciones fuertes con personal suficientemente capacitado en ingeniería de sistemas, telemática e informática forense para hacer seguimiento y atender de manera oportuna esta problemática real que hoy afecta a muchas personas, y que como se ha expuesto anteriormente, esta problemática se desenvuelve en un contexto intangible o virtual de difícil rastreo y dificultad probatoria.

En este orden de ideas, hay que tener en cuenta las formas especiales que existen de configurar los delitos descritos en la Ley 1273 de 2009, donde hay circunstancias de agravación punitiva, dispositivos amplificadores del tipo penal que configuran formas graves de atentar contra los tipos penales analizados. Así el Artículo 269H del código penal contempla taxativamente circunstancias de agravación punitiva para los delitos de:

a. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.
b. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
c. INTERCEPTACIÓN DE DATOS INFORMÁTICOS.
d. DAÑO INFORMÁTICO.
e. USO DE SOFTWARE MALICIOSO.
f. VIOLACIÓN DE DATOS PERSONALES. [4]
g. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

Los anteriores tipos penales, representan cada uno de manera autónoma verdaderas formas de atentar contra la intimidad, privacidad, buen nombre y honra, pues como dice el nombre del capítulo, dichas transgresiones son consideradas atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, donde el titular de esos datos son personas de carne y hueso con derechos.

Expresa el artículo 269H las circunstancias de agravación punitiva así:

"Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

[4] Delito objeto de estudio en esta tesis jurídico – académica, *"Análisis del Delito de Violación de Datos Personales desde una perspectiva constitucional*".

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales."

Estas 8 formas especiales de limitar el derecho humano a la intimidad, buen nombre y privacidad son castigadas un tanto más severo por la Ley dado los medios sobre los que se vale el autor para cometer el delito, también por la calidad del sujeto que realiza el ilícito penal (servidor público) o por estar en posición de garante por vínculo contractual o por disposición de la Ley; también es más drástica esta Ley, cuando la conducta se comete con fines perjudiciales para la nación como terrorismo o riesgos para la seguridad de Colombia.

Con este resumen de las formas como se puede ver afectado el derecho a la intimidad y buen nombre en la legislación Colombiana, se da por terminado el último capítulo de esta investigación académica, no sin antes hacer referencia a lo verdaderamente avanzado que está Colombia en la tipificación de este tipo de conductas punibles, pues es un ejemplo para Latinoamérica y el mundo de cómo se debe abarcar esta problemática desde el punto de vista jurídico penal y constitucional.

12. Conclusiones

El hombre en su constante interés por la tecnología, la informática y su desarrollo, ha logrado una gran influencia en la misma, alcanzando muchos logros y avanzando en cuanto a hacer más fácil y productivas las actividades diarias que las personas jurídicas y naturales realizan. Podemos decir que la informática está en todo el mundo permitiendo la comunicación y creando cada vez más, nuevas formas de contacto entre los diferentes países y culturas del planeta, demás que su avance trae para cada espacio geográfico del mundo conocimiento, acercamiento con las verdades universales, educación sin censura e intercambio multicultural a distancia; pero por esta misma razón se hace necesario reforzar las leyes que protegen los derechos humanos que están inmersos en los escenarios virtuales.

Como conclusión se podría destacar la importancia social y jurídica que tiene este tema en la actualidad ya que el desarrollo del mundo entero está ligado directamente a las tecnologías de la información y las comunicaciones, siendo el problema de los delitos informáticos, y la violación de datos personales un aspecto que se debe tener en cuenta a la hora de proteger judicialmente y jurídicamente los valores y derechos fundamentales inherentes a las personas que interactúan con las herramientas, programas y en general con cualquier tipo de escenarios virtuales.

Colombia es un fiel exponente de la vanguardia en el tratamiento de datos personales, y está muy a la par de la protección que ofrece la mayoría de las naciones del mundo en este tema, especialmente los países pertenecientes a la Comunidad Europea. Por ello la descripción amplia que hizo el legislador colombiano del articulo 269F del Código Penal, es un gran avance legislativo, y está acorde a las exigencias que se hacen en otros países que han avanzado en el tema de tratamiento de datos personales, pues el modo amplio como fue diseñado el tipo penal (Violación de datos personales), junto con sus verbos rectores permite que las conductas típicas, antijurídicas y culpables se adecuen con alguno de ellos, castigando con una pena privativa de la libertad drástica, al igual que una sanción consistente en multa, que afectará económicamente a los delincuentes que incurren en este delito en concreto.

Una conclusión que aporta al avance de la protección de los derechos a la inviolabilidad de la intimidad, buen nombre y habeas data, sería que los diferentes países del mundo entero afronten esta problemática jurídico-social tutelando penalmente cualquier intento de agresión que se cometa contra la información contenida en las distintas modalidades de bases de datos de las personas tanto jurídicas como naturales. La era de la información, está marcada por el desarrollo constante de la industria científica de las tecnologías de la información digital y de las telecomunicaciones, la globalización del uso de computadores para toda clase de servicios debe estar regularizada jurídicamente tendiendo siempre a proteger materialmente los derechos fundamentales consagrados en la Constitución Política Nacional.

Las aplicaciones de la informática en general y el constante desarrollo que ésta tiene son cruciales para el funcionamiento y la seguridad de los sistemas informáticos en el mundo de los negocios, la administración y la sociedad en general, pues una necesidad primaria para el ser humano sigue siendo la comunicación, y los avances científicos – tecnológicos ayudan cada vez más a que dicha necesidad del Hombre sea cada vez más efectiva, segura y rápida, sin mayores limitaciones, alzándose para el Derecho la obligación de hacer cumplir y respetar los derechos de las personas que están inmersos en la problemática de los delitos informáticos; la mencionada obligación para el Derecho debe seguir siendo primordial , pues es la Ley la que está llamada a perseguir el delito informático, proteger que no se cometan atentados de tipo criminalidad informática, ya que cada día crece exponencialmente en Colombia y en el mundo dichas infracciones que, bien se ha dicho, afectan el bien jurídico protegible de la información y de los datos.

Consecuentemente es imprescindible hacer implementaciones en el Ordenamiento Jurídico Nacional que permitan a las instituciones competentes como la fiscalía por ejemplo, contar con las herramientas científico - tecnológicas adecuadas, y con profesionales y técnicos preparados para que los delitos descritos en esta tesis no queden en la sola letra del Código Penal y que por falta de medios idóneos no se pueda detectarlos a tiempo. La función de investigar este tipo de punibles debe seguir siendo a cargo del Estado Social de Derecho, y para ello se necesita una institucionalidad fuerte, con políticas y

protocolos claros que sirvan de apoyo para contrarrestar en el menor tiempo posible el delito descrito en esta tesis jurídico-académica

Este proyecto de investigación hecho para optar por el título de Abogado, pretendió hacer un intento jurídico académico crítico sobre la evolución del derecho a la Intimidad y Buen Nombre en su dimensión teórica constitucional, estudiando el tipo penal de violación de datos personales descrito en el artículo 269F del Código Penal, y esclareciendo la creciente demanda que tiene la sociedad de protección de sus datos personales contenidos en los distintos medios tecnológicos – cibernéticos – virtuales - de captación, registro y almacenamiento para salvaguardar lo que no ha sido fácil conseguir y que tanto ha costado conseguir, lo cual es, el respeto por los Derechos Humanos consagrados en la Constitución Política, bajo el título de Derechos Fundamentales.

13. Recomendaciones

Como recomendaciones finales es pertinente sugerir:

1. No dar a conocer información personal o datos personales a páginas electrónicas desconocidas.
2. No confiarse de promesas y ofertas para adquirir bienes y servicios a precios muy bajos por Internet.
3. Siempre utilizar claves seguras, combinando números y letras con mayúsculas y minúsculas.
4. Verificar las cuentas bancarias y estados financieros personales solo en computadores personales de confianza.
5. No publicar datos personales como dirección de residencia, teléfonos, ocupación y edad en las redes sociales.
6. No abrir links o enlaces en la red sospechosos o desconocidos.
7. Acompañar y supervisar a los menores de edad cuando naveguen en la red de internet.
8. Conocer los derechos a la Intimidad, Buen Nombre y Honra que poseemos los seres humanos y darles el verdadero valor que tienen.
9. Promover prácticas sanas de comunicación virtual.
10. Promover una política pública de promoción y prevención en defensa de los derechos a la Intimidad, Buen Nombre y Honra y prevención del delito de violación de datos desde la óptica de sujeto activo y sujeto pasivo de la conducta punible.
11. Usar la lógica y el sentido común a la hora de entrar y utilizar las herramientas que trae consigo la era de las tecnologías de la información y las comunicaciones.
12. Nunca entregar el control del computador personal a una persona desconocida, a menos de que se esté completamente seguro de que se está pagando por un servicio de mantenimiento, ajuste o reparación a una persona que está dedicada a ello profesional o técnicamente, y que tenga un nivel de experiencia, experticia y honestidad definido, con pleno conocimiento de su existencia, fiabilidad y buen servicio.

13. Las empresas prestadoras de servicios electrónicos - computacionales no hacen llamadas que no se han solicitado para arreglar o hacer mantenimiento a un computador. Si se reciben este tipo de llamadas, se deben considerar sospechosas y no se debe suministrar ninguna información. Por el contrario se debe anotar los datos que más se pueda y hacer la respectiva denuncia ante las autoridades competentes Fiscalía o la Policía Nacional.
14. Es pertinente y necesario afrontar el estudio de las medidas jurídicas que la sociedad, a través del Estado, puede y debe utilizar para intentar que los delitos informáticos en particular el de Violación de datos personales, no implique un menoscabo de los derechos y libertades fundamentales de los ciudadanos en Colombia.

14. Referencias

14.1 Bibliografía

Álvarez María y Restrepo Luz. (1997). *EL DERECHO DE AUTOR Y EL SOFTWARE* (Universidad Nacional de Colombia). Bogotá.

Colombia (1991), Constitución política de Colombia (1991) 2da Editorial Leyer.

Colombia (2013), Código civil, Ley 57 de 1887, Bogotá, Editorial Leyer.

Colombia (2014), Código General del Proceso, Ley 1564 de 2012, Bogotá, Editorial Leyer.

Colombia, Congreso Nacional de la Republica (2012, 17 octubre) "Ley estatutaria 1581 de 2012 Reglamentada parcialmente por el Decreto Nacional 1377 de 2013. Por la cual se dictan disposiciones generales para la protección de datos personales." Bogotá.

Colombia, Congreso Nacional de la Republica (2009) Ley 1273 del 5 de enero de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Colombia, Congreso Nacional de la Republica (1999, 18 agosto) Ley 527 de 1999 de Agosto 18, "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.", publicada en el Diario Oficial No. 43.673, de 21 de agosto de 1999.

Colombia, Congreso de la República de Colombia. LEY 527 DE 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones., Pub. L. No. 527 (1999). Colombia. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

Congreso de la República de Colombia. Código penal, Ley 599 de 2000, Pub. L. No. 599 de 2000 (2012). Colombia.

España, Congreso de España. Constitución Española (1978).

España, Rey de España, Juan Carlos I, . Ley Orgánica de Protección de datos personales, Pub. L. No 15. Ley Orgánica 15/1999 (1999).

Fronsini, V. (1998) Informática y Derecho. Colombia, editorial Temis. Bogotá

Gil Osorio, Juan Fernando y Silva Ossa, S. (2005). *REFLEXIONES ENTORNO A LA EVOLUCIÓN DEL DELITO INFORMÁTICO EN LA LEGISLACIÓN PENAL COLOMBIANA* (Universidad de Antioquia). Medellin, Colombia.

Herrán Ortiz, A. (1999) La violación de la intimidad en la Protección de Datos Personales.

Dykinson S.L

Jarvey, R. R. (2012). *DELITO INFORMÁTICO ELECTRÓNICO DE LAS TELECOMUNICACIONES Y DE LOS DERECHOS DE AUTOR* (EDITORIAL IBAÑEZ). Bogotá.

Kelsen, H. (2009). *Teoría pura del Derecho* (Editorial EUDEBA). Argentina. Buenos Aires.

Legislador, ALE. Codigo Penal Alemán, Pub. L. No. RGBl. S. 127 (1871). Alemania.

León Moncaleano, W. F. (2013). *DE LA COMUNICACIÓN A LA INFORMATICA JURÍDICA PENAL BANCARIA* (Doctrina y ley). Bogotá, Colombia.

López Blanco, H. F. (2007). EL Procedimiento Civil. Bogotá: Temis.

López Medina, D. E. (2005). *Teoría impura del derecho* (LEGIS). Bogotá.

Magliona, C. y L. M. (1999). *DELINCUENCIA Y FRAUDE INFORMÁTICO* (Editorial jurídica de Chile). Santiago de Chile.

Mill, J. S. (1859). *On Liberty* (Batoche Bo). Kitchener - Ontario, Canada.

Pacheco Gómez, M. (1993). *TEORÍA DEL DERECHO* (Editorial TEMIS S.A). Santiago de Chile.

Peces Barba, G (1983) Derechos Fundamentales. España. Madrid: Facultad de Derecho de la Universidad Complutense de Madrid.

Reyes Cuartas, J. F. (2007). El delito informático en Colombia: insuficiencias regulativas. *Revista Universidad Externado*, (28), 84.

Rovira del Canto, E. (2002). *Delincuencia informática y fraudes informáticos* (Comares). Barcelona.

Sánchez Cano, D. F. (2016). *Análisis del Delito de Violación de Datos Personales (Articulo 269F del Código Penal) desde una perspectiva constitucional*. Universidad Libre de Cali.

Vásquez Ramírez, J. (2012). *Algunas nociones sobre el derecho a la intimidad* (Universidad Lima). Lima, Perú.

Virgilio, B. DECRETO 1360 DE 1989 "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor"., Pub. L. No. 1360 (1989). Colombia. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10575

Von Bertalanffy, L. (1968). *General Systems Theory* (GEORGE BRA). Edmonton, Canada.

Warren Samuel y Brandeis Louis. (1890, December). The Right to Privacy. *Harvard Law Review, Vol. 4, No. 5*, 193 – 220.

14.2 Net grafía

http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html. Ministerio de las Tecnologías de la información y las comunicaciones MINTIC (2016), Tomado el 14 de febrero de 2016.

Gobierno de Colombia, M. (2016). Historia, acerca del MINTIC. Retrieved from http://www.mintic.gov.co/portal/604/w3-propertyvalue-6077.html

14.3 Jurisprudencia

Referencia de Sentencias de Constitucionalidad, Tutela, de instancia y Unificadoras de Jurisprudencia, las cuales contienen decisiones e interpretaciones de Derecho que se relacionan y desarrollan el tema objeto de este estudio Jurídico – académico pues en el contexto de esta tesis la jurisprudencia es una de las principales fuentes, y se presenta en orden cronológico así:

1. Colombia, Corte constitucional (1992), “Sentencia T-414”, M. P. Angarita Barón, C., Bogotá.

2. Colombia, Corte constitucional (1992), “Sentencia T-480”, M. P. Angarita Barón, C., Bogotá.

3. Colombia, Corte constitucional (1992), “Sentencia T-530”, M. P. Cifuentes Muñoz, E, Bogotá.

4. Colombia, Corte constitucional (1993), “Sentencia T-413”, M. P. Gaviria Díaz, Carlos, Bogotá.

5. Colombia, Corte Constitucional (1994), “Sentencia T-229 – 1994, M.P. Hernández Galindo, J., Bogotá.

6. Colombia, Corte constitucional (1996), “Sentencia T-696”, M. P. Morón Díaz, F., Bogotá.

7. Colombia, Corte constitucional (1997), “Sentencia T-552”, M. P. Naranjo Mesa, V., Bogotá.

8. Colombia, Corte constitucional (2000), “Sentencia T-169”, M. P. Beltrán Sierra, A., Bogotá.

9. Colombia, Corte constitucional (2000), “Sentencia T-1000”, M. Pc Escobar Gil, R., Bogotá.

10. Colombia, Corte constitucional (2001), “Sentencia T-1233”, M. P. Araújo Rentería, J., Bogotá.

11. Colombia, Corte constitucional (2002), “Sentencia T-729”, M. P. Montealegre Lynett, E., Bogotá.

12. Colombia, Corte constitucional (2004), “Sentencia T-787”, M. P. Escobar Gil, R., Bogotá.

13. Colombia, Corte constitucional (1993) “Sentencia SU-528”, M. P. Cifuentes Muñoz, E, Bogotá.

14. Colombia, Corte constitucional (1995) “Sentencia SU-056”, M. P. Arango Mejía, J., Bogotá.

15. Colombia, Corte constitucional (1996) “Sentencia SU-256”, M. P. . Naranjo Mesa, V., Bogotá.

16. Colombia, Corte constitucional (2000) “Sentencia SU-1723”, M. P. . Morón Díaz, F., Bogotá.

17. Colombia Corte Constitucional (2000) “sentencia C-662”, M.P. Morón Díaz, F., Bogotá.

18. Colombia, Corte constitucional (2003) “Sentencia C-692”, M. P. . Monroy Cabra, M. G., Bogotá.

19. Colombia, Corte constitucional (2004) “Sentencia C-816”, M. P. . Monroy Cabra, M. G., Bogotá.

20. Colombia, Corte constitucional (2004) “Sentencia C-816”, M. P. . Córdoba Triviño. J., Uprimny Yepes, R., Bogotá.

21. Colombia, Corte constitucional (2008) “Sentencia C-186”, M. P. . Pinilla Pinilla, N., Bogotá.

22. Colombia, Corte Constitucional (2011) “Sentencia C-748”, M.P. Pretelt Chaljub, J., Bogotá.

23. Colombia, Corte Suprema de Justicia sala de Casación Penal (2015, Febrero), “Sentencia SP1245-2015”, M. P. Patiño Cabrera, Eyder., Bogotá.