ESTUDIO JURÍDICO DE LOS ARTÍCULOS 269A Y 269F LEY 1273 DE 2009 COMO DELITOS QUE ATENTAN CONTRA LAS REDES SOCIALES

SORAYA VALVERDE DELGADO

CÓDIGO: 06396

UNIVERSIDAD LIBRE SECCIONAL CALI

FACULTAD DE DERECHO, CIENCIAS POLÍTICAS Y SOCIALES

SANTIAGO DE CALI

2018

ESTUDIO JURÍDICO DE LOS ARTÍCULOS 269A Y 269F LEY 1273 DE 2009 COMO DELITOS QUE ATENTAN CONTRA LAS REDES SOCIALES

SORAYA VALVERDE DELGADO

CÓDIGO: 06396

Monografía de grado presentada como requisito parcial para optar al título de Abogado

Director de Monografía: Dr. Jesús Fernando Amariles Valverde

UNIVERSIDAD LIBRE SECCIONAL CALI

FACULTAD DE DERECHO, CIENCIAS POLÍTICAS Y SOCIALES

SANTIAGO DE CALI

2018

TABLA DE CONTENIDO

INTRODUCCIÓN

Los avances tecnológicos en los sistemas de comunicación e información han permitido una mayor capacidad en el ser humano de poderse conectar y expresar masivamente con su sociedad, generando transformaciones significativas en las relaciones sociales y jurídicas entre sus asociados y repercutiendo en nuevas formas de conflictos socio-jurídicos, que exigen, de alguna forma, regulación legal que permita controlar y mantener el cuidado, el bienestar, la protección y la satisfacción de estos nuevos comportamientos sociales que se expanden con gran rapidez.

Es así como la presente investigación pretende indagar e identificar el marco técnico jurídico que existe para el tratamiento de los comportamientos ilícitos a través de medios informáticos, herramientas que permiten en cierta forma establecer medidas de prevención y protección a los millones de cibernautas, guardando plena concordancia con lo establecido en nuestra Constitución Política de Colombia y logrando una efectiva persecución y penalización de los Delitos Informáticos. Esta investigación se encaminará, principalmente, a mostrar el desarrollo penal en contra de los delitos que atentan contra las redes sociales, recientemente regulado en Colombia mediante la Ley 1273 de 2009 en los artículos 269A "Acceso Abusivo a un Sistema Informático" y 269F "Violación de Datos Personales", que busca una efectiva persecución penal a sus infractores.

Dentro del plan de trabajo se plantea una estrategia investigativa partiendo de lo general a lo particular o especifico, indagando inicialmente lo relacionado con el desarrollo informático a través de redes sociales y la importancia que ha adquirido por el uso masivo de internet; continuamos con una exploración desde los inicios que tuvo el proyecto de ley creado para contrarrestar los delitos informáticos en nuestra legislación colombiana. También se realiza una breve ilustración del tratamiento jurídico establecido para los delitos informáticos en países hispanoamericanos y anglosajones, con el fin de mostrar dentro del derecho comparado, el significativo avance que ha logrado nuestro país para enfrentar estos delitos. Y, por último, se presentará un caso hipotético, aunque tomado en gran parte de hechos reales, para el desarrollo de una investigación penal que busca la protección de las víctimas y su correspondiente compensación, mediante las facultades que tiene el ente acusador, Fiscalía General de la Nación, para lograr verdad, justicia y reparación.

Cabe mencionar que el esquema penal legislativo, así como el penal investigativo, son muy recientes y su desarrollo se han venido dando sobre la marcha, mostrando algunas dificultades en la campaña liderada en gran parte por influencias internacionales, pero con actores nacionales a quienes con orgullo se exaltan en este trabajo, ya que permitieron acoger los conocimientos desarrollados en la Convención de Budapest para el tratamiento de los delitos informáticos, y darle aplicación efectiva en nuestra sociedad mediante la creación de la Ley 1273 de 2009.

CAPÍTULO I:

1. DESARROLLO DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

En este capítulo se abarcaran temáticas que permitirán introducir al lector paso a paso dentro del contexto de los delitos informáticos sobre redes sociales tipificados en la ley 1273 de 2009 en los artículos 269A y 269F, mostrando, en términos generales, la forma en que se fueron desarrollando los avances tecnológicos, el desarrollo de los medios de comunicación o redes sociales por medio de internet, así como la transformación del ámbito jurídico desarrollados a nivel mundial para proteger las conductas humanas en su continua interacción con estos medios tecnológicos de comunicación, lo cual nos va dar a entender por qué se decidió crear en Colombia la Ley especifica en contra de los Delitos Informáticos, lo que ocasionó una modificación a nuestro Código Penal Colombiano.

1.1. ¿Qué es la tecnológica? Beneficios y consecuencias

Durante la evolución del ser humano hemos ido desarrollando diferentes clases de herramientas que nos permitieran alcanzar nuestros objetivos: alimentación, descanso, protección, salud, bienestar, entre otros. Es así como observamos a través de la historia, cómo nuestra especie humana, dentro de su etapa evolutiva, ha ido perfeccionando las técnicas y las herramientas utilizadas para la cacería, la movilización, la seguridad, las interacciones personales y, en general, para el bienestar propio y de nuestras familias. (Serrano, 2007) expresa que:

> *La evolución se tomó cinco millones de siglos para probar las opciones comunicativas que finalmente han configurado las capacidades comunicativas humanas. Esa evolución ha hecho nuestro cuerpo expresivo y receptivo; nuestro comportamiento simbólico; nuestra mente lógica; nuestro mundo lleno y significativo. Que es como decir, que las transformaciones evolutivas de la comunicación participan de un modo necesario y esencial en lo que tiene de específico la condición humana. (p. 17)*

Esto dio paso a un concepto muy utilizado en estos tiempos: la tecnología, reflejo palpable del evolucionado desarrollo del ser humano en sí mismo y en su interacción con su entorno natural. Más aún se puede observar cómo la tecnología traspasa la naturaleza misma percibida a simple vista por el hombre, llevándolo a un plano transnatural, casi impensable. Así lo manifiesta el doctor (Pérez, 2014) en su artículo:

> *La esencia y el destino de la tecnología"*, expresando que: *"La tecnología sintetiza la evolución de la naturaleza y de la cultura, de la ciencia y de la sociedad. Quiere decir que está constituida por mecanismos complejos donde podemos encontrar lo*

determinado y lo indeterminado, las leyes de la naturaleza y la arbitrariedad del poder, la lógica científica y el azar de los hechos históricos. Las tecnologías avanzadas nos llevan más allá del orden natural y del orden cultural vigente…, los sistemas de información son indicios de que estamos transitando hacia un orden transnatural y transcultural cuyo sentido se nos escapa.

El profesor: (Bijker, 2005, p. 21) establece tres niveles para definir la tecnología, desde su primer nivel que: "*refiere a un conjunto de objetos físicos o artefactos, tales como computadoras, autos o máquinas para votar…*"; su segundo nivel que: *"incluyen actividades humanas, tales como en "la tecnología de voto electrónico", donde también se hace referencia al diseño, la fabricación y el manejo de este tipo de máquinas.";* y su último nivel que refiere que: "*el conocimiento se trata tanto de aquello que la gente conoce como de lo que hace con las máquinas y los procesos de producción relacionados.*" Concluyendo que definir la tecnología desde estos tres niveles permite "*ser más específico que cuando se lo emplea como un concepto contenedor en un nivel macro…*"

Para el doctor (Pérez, 2014) la tecnología: *"pueden ser aquellos elementos tangibles que sirven como herramientas productivas, así como pueden ser los procesos mentales necesarios para alcanzar las habilidades técnicas necesarias para operar, reparar o mejorar de forma intangible cada una de las creaciones materiales."*

Podemos definir entonces la tecnología como ese conjunto de herramientas y de artefactos creados para: *"resolver problemas y satisfacer necesidades individuales y sociales, transformando el entorno y la naturaleza mediante la utilización racional, crítica y creativa de recursos y conocimientos"* como nos indica: (Ministerio de Educación Nacional, 2008)

Ahora, observemos la forma en que el desarrollo tecnológico ha incrementado masivamente la producción de medios de comunicación. Haciendo una simple mirada retrospectiva desde el surgimiento de medios de comunicación de la humanidad, encontramos que posiblemente su génesis se pudo haber dado desde las pinturas rupestres (30.000 A.C.) o mediante las señales de humo, gracias al descubrimiento del fuego, siguiendo con el surgimiento de los pictogramas, luego se pasó a la escritura, entre otros medios menos convencionales, todo esto antes de Cristo, hasta llegar a la imprenta en los siglos medievales; posteriormente se desarrolló el código morse, el telégrafo, el teléfono y la televisión, hasta alcanzar la revolucionaria era digital, logrando un gran avance tecnológico con la llegada de internet, en parte, consecuencia tanto de la globalización del mundo como de la acertada conquista espacial que permitió el ya conocido empoderamiento satelital, (Clarke, 1945).

Sobre este punto, indica el profesor costarricense Harold Hütt Herrera, en su artículo *"Las redes sociales: una nueva herramienta de difusión"*, que ya no nos encontramos

frente a medios de comunicación, sino frente a medios de difusión: *"En la actualidad no se habla de medios de comunicación, sino de medios de difusión, pasando así de un esquema tradicional a un proceso interactivo, cambiante y dinámico. Es decir, ya los medios de difusión involucran tanto los medios tradicionales como los espacios virtuales, dentro de los cuales destacan las redes sociales y los diversos mecanismos de interacción con grupos de personas con el apoyo de la tecnología (blogs, wikis, etc.). La principal regla en este último grupo es que no hay reglas; es decir, no hay censura, línea editorial o restricción que marque la pauta en este tipo de espacios"* (Hütt H., 2012)

Observando todos estos veloces adelantos tecnológicos es lógico pensar en la evolución del ser humano, modificando no solo su forma de interactuar en la sociedad y dentro su entorno natural, sino que ampliando sus fronteras de interacción, logrando tener mayor alcance y capacidad para conectarse con cualquier parte del mundo, repercutiendo en mayores beneficios, sobre todo en el importantísimo factor tiempo así lo indica: (Marín, 2006)

> *La realidad de hoy presenta una imagen en la que los medios de información y comunicación han obtenido un espacio específico en nuestras vidas, determinando el desarrollo de las mismas. La influencia de los mass-media va creciendo en la medida en que los avances tecnológicos se producen. Dentro de ese espacio de influencia los medios nos ayudan a saber y conocer más del resto del mundo, además de permitirnos buscarle un significado y, lo que llama aún más la atención, estructuran y determinan nuestro tiempo libre y de ocio. (p. 193)*

Generando mejor calidad de vida, mejor acceso y comunicabilidad de la información, a la educación, a la recreación, al entretenimiento y a la diversión, incrementando masivamente el ofrecimiento y la negociabilidad de los productos. Pero todos estos beneficios vienen acompañado de ciertas consecuencias, que merecen un adecuado tratamiento para contrarrestar los perjuicios que trae consigo lo que indica:

> (Grisales P., 2009) S*in embargo, ese desarrollo tecnológico, que buscaba mejorar la calidad de vida de los ciudadanos y dinamizar la información de manera veloz e instantánea a través de la red, encontró en los delincuentes informáticos un novedoso y lucrativo nicho para explotar, gracias al desconocimiento casi total de las funciones de los lenguajes de programación y de las diferentes técnicas de intrusión por la mayoría de los usuarios de la red. Esto ha creado nuevas dinámicas delictivas dirigidas a "hurtar" o "apoderarse" de esa información privilegiada –bancaria, personal, privada, secreta, empresarial, política, etc.-, de cada una de las personas y organizaciones para explotarla en beneficio económico propio.*

Vulnerabilidad expuesta a todos los usuarios de la red (personas naturales o jurídicas), encontrándonos propensos a ser sujetos de violaciones de confidencialidad, integridad, dignidad, entre otras, por la falta de protección del manejo de la información

con la cual accedemos y operamos dentro de la red virtual. En este aspecto el profesor costarricense Harold Hütt Herrera, en su artículo mencionado, también se pronuncia al respecto, dando algunas recomendaciones del uso de estos tipos de medios de difusión:

> *"En razón de lo anterior, las empresas, y desde luego las personas, se han visto en la necesidad de establecer pautas y lineamientos propios para interactuar en este ámbito. Por ejemplo, qué tipo de fotografías o información comparto, con quién las comparto, cuáles son mis previsiones en materia de seguridad personal e informática, cuál es la sistematización que voy a establecer para la elaboración de mensajes en términos de frecuencia, tono y forma, así como también, cuáles van a ser mis políticas de respuesta y tratamiento de la información. Sobre estos últimos puntos debemos recordar la primicia de "actos privados, consecuencias públicas". Es decir, su vida privada deja de ser privada cuando usted decide hablar de ella en público o bien ante una serie de receptores que están decodificando de manera permanente sus mensajes y elaborando sus propias conclusiones y conceptos sobre usted y sus acciones. La dinámica en este caso siempre es "personal". Esto implica que usted tendrá la oportunidad de crear una imagen sobre usted mismo, la cual estará ligada de manera indivisoria con la percepción laboral y profesional que proyecte. En consecuencia, sea cauto con lo que escribe y con las personas que admite en su entorno social virtual para evitar consecuencias desagradables."* (Hütt H., 2012). *p.123*

Ante estas vulnerabilidades de los sistemas de intercomunicación y de manejo de la información se ha generado un gran número de delitos informáticos a nivel mundial, aunado a la falta de preparación y de cuidado en el uso de estas herramientas tecnológicas, haciendo necesario de políticas de Estado fuertes, capaces de regular el progresivo y peligroso impacto de la *ciberdelincuencia*. Esto condujo a realizar un integral estudio dogmático en este trabajo investigativo, teniendo como referencia el incremento significativo de las casos de ataques cibernéticos por medio de las redes sociales, situación que día a día se observa en los casos allegados a las Fiscalía General de la Nación Dirección Seccional Cali, con hechos que enmarcan violaciones de derechos fundamentales o de rango constitucional.

1.2. ¿Qué es una red social?

Empecemos definiendo conceptos que vayan encausando esta investigación, comenzando por definir qué es una red social, donde el profesor Javier Celaya expresa al respecto: *"Las redes sociales son lugares en Internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos"* (González, 2010).

Consultando el articulo *"La importancia de las redes sociales en el ámbito educativo"* de María del Mar Muñoz Prieto, María Sandra Fragueiro Barreiro y María Jesús Ayuso Manso, nos indican que el origen de las redes sociales interactivas en internet se

remonta aproximadamente al año 1997 gracias a la masificación que tuvo esta importante herramienta tecnológica, siendo pionero de este servicio social, el inventor Randy Conrads, "*mediante la creación del sitio web que llevaba por nombre "Classmates", y que consistía en una red social que brindaba la posibilidad de que las personas de todo el mundo pudieran recuperar o continuar manteniendo contacto con sus antiguos amigos"* (Muñoz, Fragueiro, & Ayuso, 2013, p.92), ya sean compañeros de colegio, de la universidad, de distintos ámbitos laborales y demás, posiblemente como resultado de esa tendencia a globalización mundial.

> Los abogados (Guevara & Arzuaga, 2012) nos amplían más este concepto expresando que las redes sociales son aquellos sitios *en las cuales cada quien hace una pequeña reseña de su vida con sus gustos e intereses y comparte con otras personas un ideal o simplemente hace una amistad. Las redes sociales son páginas web dedicadas a concentrar la mayor cantidad de individuos en un solo sitio y brindar de forma práctica un permanente contacto con otros usuarios para captar sus intereses y gustos personales. p.129.*

1.3. ¿Por qué proteger la información y los datos?

Obviamente el crecimiento acelerado de la tecnología y su aplicación a sistemas de comunicación, cada vez más avanzados, mostró la necesidad de controlar y poder regular la manipulación de bases de datos de contenido personal, en redes sociales y otras áreas sensibles de la sociedad, como: en el sistema financiero, la salud, en lo judicial, entre otras, dando lugar a la "*protección de datos de carácter personal: que ha venido cobrando gran importancia en el mundo por tratarse de la forma a través de la cual se hace exigible el derecho a la intimidad y se pone freno a los abusos que, desde la perspectiva tecnológica, puede significar el tratamiento de bases de datos personales."* Calle, Sol Beatriz. *"Apuntes Jurídicos sobre la protección de datos personales a la luz de la actual norma de Habeas Data en Colombia"* (Calle, 2009, p.121) , bajo el concepto jurídico del efectivo amparo del derecho a la intimidad, reglamentado desde el artículo 15 de la Constitución Política, lo que dio paso al concepto de intimidad informativa o autodeterminación Informativa (Calle, 2009)**.**

Y en consecuencia del acelerado avance tecnológico de estas nuevas herramientas de difusión y comunicación, los ciberdelincuentes desarrollaron para sus propios fines delictivos, virus informáticos que en un comienzo tan solo podían introducir en los equipos de sus víctimas y que llevaban consigo mismo mediante los primeros medios de almacenamiento de información de la época, "disquete", es así como lo indican en su artículo *"Delitos informáticos y entorno jurídico vigente en Colombia*" los investigadores Jorge Eliecer Ojeda Pérez, Fernando Rincón Rodríguez, Miguel Eugenio Arias Flórez y Libardo Alberto Daza Martínez: *"utilizaron las redes de datos aprovechando la internet"* (Ojeda-Pérez, Rincón-Rodríguez, Arias-Flórez, & Daza-Martínez, 2010,p.45), y aunque en un principio se intentó proteger para evitar todo tipo de ataque ciberdelicuencial, mediante barreras con el uso de contraseñas y otro tipo de restricciones de acceso a estas redes, no fue suficiente para frenar o evitar que los ciberdelincuentes pudieran penetrarlas. Y, paralelamente, continuaron

transportando los virus, mejor conocidos como *malware (Revista Semana, 2010, párr1)* con los masivos bombardeos a través de las redes de internet, usando los correos electrónicos, ahora recientemente los *chat rooms* o salas de conversación virtual, obteniendo mayor cantidad de víctimas. (Ojeda-Pérez, Rincón-Rodríguez, Arias-Flórez, & Daza-Martínez, 2010,p.45).

No obstante, no solamente los ciberdelicuentes actúan por estos medios informáticos, indican los investigadores continuando con el estudio del mismo artículo mencionado que *"otro tipo de delincuentes han encontrando espacios propicios en los distintos medios de comunicación electrónica, para desarrollar crímenes, como los pedófilos, los que buscan generar relaciones de confianza on line con niños inocentes, para luego aprovecharse de ellos y hasta secuestrarlos o asesinarlos. Estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, de drogas, de personas, de pornografía, de información, sicarios y terroristas se agregan a esta tenebrosa lista que utiliza el ciberespacio y la red para multiplicar sus negocios,…"* (Ojeda-Pérez, Rincón-Rodríguez, Arias-Flórez, & Daza-Martínez, 2010,p.45), mostrando de esta forma la importancia que existe en la regulación legal que permite la penalización de los punibles crímenes, que nuestro país están tipificados mediante la Ley 599 de 2000, teniendo en cuenta que las entidades que desarrollaban estos medios informáticos no tenían las debidas herramientas judiciales necesarias para contrarrestar tales vulneraciones de los usuarios de la red, siendo responsable cada unos de los Estados que permitieron el uso de estas tecnologías los que debían implementar instrumentos de control y de sanción a quienes, de manera inescrupulosa, expanden sus actividades delictuales al mundo cibernético, añaden los investigadores que:

"La ley inglesa sirvió para que en otros países, en especial aquellos donde la internet tenía más desarrollo-se sumaran al esfuerzo de discutir y promulgar leyes orientadas a proteger y sancionar la violación de la información. Sin embargo, en el caso colombiano, la reacción fue lenta y tardía, de acuerdo con los estudios realizados por Cisco en el año 2008,…" (Ojeda-Pérez et al., 2010, p.46).

1.4. ¿Qué bienes jurídicos son afectados en los delitos informáticos?

Antes de exponer los bienes jurídicos afectados en los delitos informáticos es necesario entender el concepto de bien jurídico o un bien jurídicamente tutelado. Por ejemplo, para los profesores (Rincón & Naranjo, 2011) el interés social tan solo se convierte en bien jurídico cuando es protegido por el Derecho, haciendo una diferenciación entre valores morales y bienes jurídicos, que si bien se pueden coincidir, advierten que estos dos conceptos no pueden ser confundidos, de tal forma, que cuando un bien se eleva a la categoría de tutelado o protegido por el derecho, mediante su respectiva sanción por conducta(s) que pongan en peligro o lesionen dicho bien, adquiere esta denominación de bien jurídico tutelado:

"Esta concepción del bien jurídico es obviamente fruto de un Estado Social y Democrático de Derecho, y dada su vertiente social requiere una ulterior concreción de la esfera de actuación del Derecho Penal a la hora de tutelar intereses difusos. El origen de la noción de bien jurídico está, por tanto, en la pretensión de elaborar un concepto del delito previo al que forma el legislador, que condicione sus decisiones, de la mano de una concepción liberal del Estado, para la cual es un instrumento que el individuo crea para preservar los bienes que la colectividad en su conjunto quiera proteger". (Rincón *et.al.*, 2011, p.83)

Y concluyen los autores que si llegase a caducar o dejar de existir la norma, el bien no desaparece, pero sí su carácter jurídico y su protección. Es así como se identifican los bienes jurídicos dentro de toda la normatividad existente del Derecho, siendo más evidentes o visibles en la rama del Derecho penal, por tener implícito ese carácter sancionatorio para la protección de los bienes jurídicos tutelados:

"El Derecho Penal, pues, tiene su razón de ser en un Estado Social porque es el sistema que garantiza la protección de la sociedad a través de la tutela de sus bienes jurídicos, en su calidad de intereses muy importantes para el sistema social y, por ello, protegibles por el Derecho Penal. Sin embargo, no debe olvidarse que existen bienes jurídicos que no son amparados por el Derecho Penal, por ser intereses solo morales, por lo cual no todos los bienes jurídicos son bienes jurídico-penales". (Rincón *et.al.*, 2011, p.84)

Dentro de la dogmática general del Derecho Penal, el profesor Velásquez nos define el bien jurídico como: *"... concepto abstracto que en ningún caso puede ser confundido con el objeto sobre el cual recae la acción del agente como se verifica...*", poniendo de ejemplo el delito de hurto, debido a que el objeto sobre el cual recae la acción es la cosa mueble, mientras que al hablar del bien jurídico se debe mencionar que es el patrimonio económico (Velásquez, 2007).

Más adelante observamos que desde el 2009 se vienen exigiendo por jurisconsultos la vinculación de bienes jurídicos dentro de la regulación de los delitos informáticos, así no los hace ver la doctora Leyre Hernández Díaz nos presenta posibles nuevos bienes jurídicos, argumentando que dentro de la dogmática existente para el ámbito de la delincuencia informática, cada vez se tiene más posturas de autores que sostienen la necesidad de crear un nueva postura jurídica penal que abarque todas las conductas vinculadas con el hecho informático, debido a que son usados estos medios para lesionar bienes jurídicos tradicionales, como por ejemplo lo observamos en delitos de Calumnia, de Injuria, de Extorsión, entro otros. De esta manera, nos define un bien jurídico con concepto universal, denominado *"La seguridad informática"* (Hernández, 2009), que en general se trata de un bien cuya protección evita la lesión de una serie de bienes jurídicos de carácter individual puestos en peligro con tales conductas atentatorias **contra la seguridad de las redes** y sistemas informáticos, tanto en el ámbito público como el privado, sirviendo como medio la protección de todos los bienes de carácter individual (patrimonio, intimidad,

libertad sexual, honor, etc.) e, incluso, otros bienes de carácter supraindividual (orden público, paz pública, seguridad del Estado). Enfatizando la gran necesidad de crear este bien por la cuasi dependencia de esta sociedad a las avanzadas herramientas tecnológicas y su constante interacción con estas, que ocasiona que un ataque al sistema informático dañe no solo un bien jurídico individual, sino que también ponga en riesgo a toda la comunidad, razón por la cual se tienen como delitos pluriofensivos, llegándose a considerar como bien jurídico de naturaleza colectiva, indisponible como tal por el individuo concreto que no encuentra suficiente protección mediante la salvaguarda en exclusiva de bienes jurídicos de naturaleza individual. La autora también trae a consideración como bien jurídico la *"intimidad informática –habeas data o autodeterminación informática–"* (Hernández, 2009) contemplado en especial por la doctrina italiana, en la que el bien jurídico individual, "intimidad e inviolabilidad informáticas", se interpreta como una nueva vertiente, como si fuera el domicilio físico de cada persona dentro de la red, de todo ese mundo cibernético, sin perjuicio de lo expuesto anterior, reconociendo que la protección debe ir encaminada a garantizar, también, la seguridad y la integridad de los sistemas informáticos; es decir: *"La seguridad informática"*.

Ahora entremos a considerar los nuevos bienes jurídicos protegidos con la creación de la Ley 1273 de 2009, de la información y de los datos, retomando los conceptos de un colaborador de esta Ley, el doctor (Rincón & Naranjo, 2011) quien explican que el bien jurídico tutelado de la información se constituyó *"por tipos autónomos y no subordinados por circunstancias genéricas o específicas de agravación punitiva de otros tipos, como ha sido la costumbre legislativa en el mundo."*(p.82)

El profesor (Carranza, 2009), con base en lo establecido en el convenio 108 del consejo de Europa, define el concepto de protección de datos personales: *"como el reconocimiento y el establecimiento de prerrogativas, principios y procedimientos para el tratamiento por parte del Estado o de terceros, de la información concerniente a personas físicas."*

En esta investigación se desarrollará, más adelante, la identificación de los bienes jurídicos tutelados en los delitos informáticos de Acceso Abusivo a un Sistema Informático, Art. 269A y Violación de Datos Personales, Art. 269F, no sin antes observar algunas de las más comunes y representativas conductas delictivas que atentan contra las redes sociales informáticas.

1.5. Conceptos de delitos informáticos

Diversos autores han generado conceptos recientes, entendiéndose que la evolución de los sistemas informáticos y el uso de las TIC´S en nuestra sociedad no hace mucho iniciaron.

Comencemos con el concepto esbozado por el Doctor (Acurio, n.d.), para quien se empieza a estructurar el delito informático como consecuencia del avance de la tecnología informática, influenciando casi en todo nuestras vidas sociales, generando paralelamente una serie de comportamientos disvaliosos antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, a tal punto de no poder realizar aplicaciones analógicas prohibidas por el principio de legalidad, razón por la cual, la doctrina ha denominado a este grupo de comportamientos, de manera genérica, como "delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática"

De igual forma los define el profesor Campoli, al realizar distinción entre delito informático y delito electrónico, definiendo a los segundos como una especie de género de los delitos informáticos, en los que el *autor produce un daño o intromisión no autorizada en equipo electrónicos ajenos*, mientras que los delitos informáticos se realiza mediante la utilización de medios informáticos o electrónicos, pero en los que se pone en peligro o se lesiona un bien jurídico tutelado, que se encuentra tipificado en una norma, como una conducta disvaliosa, aun así el bien no se encuentre protegido en la legislación vigente (Rincón *et.al.*, 2011, p.53).

Por otro lado, el profesor (Meek, 2013) expresa que para abordarse el examen del delito informático es necesario comenzar con lo que denomina la *"Triada informática"*, expresión que define la conjunción de tres elementos: el *hardware*, el *software* y el *usuario*, que, vinculados entre sí, dan lugar al nacimiento de una nueva forma al servicio del hombre para expresarse en el mundo existencial, convirtiéndose en el nuevo eje transversal de la criminalidad informática; siendo el *usuario*, la persona que se sitúa frente a un ordenador dispuesta a impartirle órdenes para su funcionamiento; el *software* parte inmaterial del sistema, que comprende y soporta toda la información y los datos informáticos, también los programas necesarios para el funcionamiento del equipo y satisfacción de las necesidades informáticas del *usuario*; y, por último el *hardware*, que viene siendo el puente entre el campo del mundo físico y el de la información y los datos informático. Así las cosas la *"Triada informática"* ayuda a desentrañar la naturaleza de las infracciones mediante el examen de los elementos que intervienen, tales como dispositivos, máquinas y personas puestas en lugares y en sitios distintos.

El Doctor Cossou Ruiz nos ofrece un concepto un poco más simplificado, entendiendo el delito informático como toda aquella conducta ilícita susceptible de ser sancionada por el Derecho Penal por el uso indebido de medio informático.

Expuestas estas definiciones conceptuales se podría concluir que los delitos informáticos son aquellas conductas contrarias a la ley y que se encuentran expresamente prohibida por la legislación Penal. Además, atentan no solamente contra los derechos individuales, sino que también se convierten en delitos que lesionan o ponen en peligro al colectivo, teniendo en cuenta su carácter universal y pluriofensivo, motivo por el cual debe ser regulado efectivamente por el Estado para brindar la debida protección a sus asociados.

1.6. Breve ilustración de delitos informáticos

En el amplio mundo de los delitos informáticos se han generado diferentes denominaciones a las conductas que vulneran o que atentan contra los derechos de las personas y de las organizaciones que interactúan constantemente en estos medios informáticos, clasificación que el abogado (David & Arbeláez, 2011a) definen detalladamente en su artículo: *"Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación"*, a continuación de forma breve algunas de estas definiciones:

1.6.1. Perfiles falsos

Consisten en la creación de perfiles simulados, pero con datos reales de las personas o empresas a suplantar, manipulando toda clase de información como fotos, videos, comentarios, entre otras. En la mayoría de los casos, con el fin de generar una fuerte agresión a las personas suplantadas dentro de su esfera social, vulnerando así la dignidad, la moral, el buen nombre y la integridad, así como menoscabando sus derechos y sus libertades. De la experiencia obtenida en el diario vivir dentro de la Fiscalía se ha observado, en la mayoría de los casos, que la víctima sospecha de un pariente muy cercano o de un ser querido muy allegado, como una pareja sentimental actual o pasada, quienes, a manera de venganza, usan información muy sensible y que solo los seres más allegados puede conocer para realizar este tipo de conductas delictivas.

1.6.2. Fraude informático

Consiste en realizar estafas usando las redes sociales, los lugares más utilizados por los delincuentes que mediante engaños obtienen información personal sensible, permitiéndoles crear cuentas falsas con los datos proporcionados por sus víctimas, evitándoles, incluso, el acceso a sus propias cuentas, ya que han manipulado las claves de acceso. (Grisales P., 2009) nos dice:

> *Pharming**:** es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta… La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios. p.42*

En este tipo de cibercriminalidad, conocido como *phishing*, se simula una aparente comunicación oficial electrónica, por lo común con un correo electrónico que proviene de persona natural (un popular ejemplo puede ser "la carta nigeriana" (Diario el Pais, 2015b) o puede provenir de una empresa persona jurídica (otro muy sonado caso es el correo electrónico que trae adjunto un archivo con una supuesta citación de la Fiscalía General de

la Nación); también se da por medio de algún sistema de mensajería instantánea, incluso utilizando llamadas telefónicas, buscan adquirir información y contraseñas que les permita acceder a los sistemas de identificación para violar la seguridad de los portales electrónicos de las entidades bancarias y, de esta forma, hurtar, transferir o realizar compras electrónicas, logrando defraudar el patrimonio económico de las incautas víctimas. Afecta diversos bienes jurídicos, tales como: la propiedad, la confidencialidad, la dignidad, entre otros.

1.6.3. Daño informático

Las redes sociales son propicias para este tipo de acciones, dado que el intercambio de archivos o de descarga de material puede involucrar casos de virus informáticos. (Diario el Pais, 2015a)

1.6.4. CiberBullying o bullying cibernético

Se realiza mediante “supuestas” bromas, por medios electrónicos muy comunes, tales como: Messenger, Hotmail, Facebook, foros, redes P2P, entre otros, siendo este delito la extensión del acoso escolar, vulnerando derechos de rango constitucional como la moral y la integridad de las personas, cometido no solo por los agresores conocidos por las víctimas, sino que también por personas desconocidas, acrecentando el sentimiento de impotencia y de desamparo de la víctima. (David & Arbeláez, 2011b), p.16.

Estas son algunas de las modalidades delictivas más frecuentes en los delitos informáticos, producto en gran medida de ese progresivo y acelerado avance tecnológico en las redes de comunicación, modificando la interacción social habitual, situación que definitivamente exigió cambios importantes en los comportamientos sociales, económicos y políticos de personas y países, debido al peligroso, paralelo y avanzado desarrollo de las nuevas modalidades delincuenciales, que empezaron a utilizar masivamente estos sistemas de información y comunicación del mundo y lograron posicionarse en uno de los riesgos más inminentes para la seguridad, la vida y la protección de los bienes de las personas y las organizaciones a nivel mundial.

DESARROLLO DEL MARCO LEGAL CREADO PARA LA PROTECCIÓN CONTRA LOS DELITOS ELECTRÓNICOS

A continuación expondremos todo el proceso llevado a cabo para la creación y la tramitación de la ley 1273 de 2009 ante el Congreso de la Republica, con el objetivo de poder llegar a estar en capacidad de distinguir cuales conductas delictivas se enmarcan como delitos informáticos y, por el contrario, cuáles ya se encuentran reguladas o tipificadas en nuestro Código Penal Colombiano, Ley 599 de 2000.

Luego de haber expuesto en forma rápida y generalizada los conceptos indicado en el capítulo anterior, puede resultar más claro entender por qué se tuvo la necesidad de tutelar un nuevo bien jurídico, que tiene como fin brindar protección de manera autónoma, no subordinada por otro tipo penal básico, la integridad de los usuarios en la masiva utilización de medios electrónicos, lo que ha contribuido a una constante comunicación y fluida interacción social, además de reducir notablemente el tiempo en las tareas que se ejecutaban anteriormente de forma manual.

> (Acurio, n.d.) Expresa que nos encontramos en la "Era de la informática" debido a*: "los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y de procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial...".*

Inicialmente se dará a conocer cómo se emprendió el camino para la creación de la Ley 1273 de 2009, objeto de estudio de esta investigación, la cual fue creada para el cumplimiento de la defensa de los derechos que promulga el Estado Social de Derecho proclamado en nuestra Constitución Política y así poder regular y proteger a todos sus asociados, mediante modificaciones positivas dentro del sistema penal con tendencia acusatoria, estableciendo una normatividad que permite perseguir y judicializar los posibles abusos que se presenta en el uso de las nuevas tecnologías que ya son tendencia mundial, gracias a esa notable dependencia de la sociedad hacia las TIC´S.

Desde el proyecto de ley hasta su paso para convertirse en la Ley 1273 de 2009, de acuerdo con la información encontrada, específicamente en el estudio realizado y plasmado por los doctores Rincón Ríos y Naranjo Duque, en su obra titulada *"Delito Informático, electrónico, de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia"*, indicando que no fue un camino fácil de recorrer, teniendo que superar muchas dificultades, en parte porque hubo algunos sectores del poder político que no compartían la necesidad de crear una nueva legislación penal para el tratamiento de los delitos producto o consecuencia de uso de medios electrónicos o de la informática con ánimo doloso o culposo:

"Después de mucho sufrimiento y tras trasegar arduamente en diferentes instancias, se aprueba por el Senado y Cámara el proyecto de ley conciliado, que genéricamente llamamos proyecto de delitos electrónicos en Colombia, que legislativamente se adopta con el nombre de bien jurídico tutelado, denominado DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS" (Rincón *et.al.*, 2015, p.45).

Trabajo que se exalta por la importancia que connota un tratamiento especial para este tipo de delitos, que en su mayoría atentan contra el honor, la protección de datos, en mayor porcentaje contra el patrimonio económico e incluso, hasta puede causar lesiones temporales o permanentes de forma psíquica, razón por la que se pensaba que estos delitos por medios electrónicos en apariencia ya se encontraban protegidos bajo la normatividad penal que regula el hurto, la estafa, la injuria y la calumnia, las lesiones personales, etc., concepto compartido en varias escuelas jurídicas, una de ellas justificada por el profesor argentino Campoli, quien precisa: *"…, si se lesiona el bien jurídico protegido, no importa cuál sea el medio utilizado, corresponde la aplicación de la ley penal vigente y no se requiere una nueva y especifica."* (Campoli, G.A., 2002), es decir, que no se necesita de una tipificación de nuevos delitos por el simple hecho de verse como nuevos, debido a que no son nuevos delitos, ya que su bienes jurídicos tutelados siguen siendo los mismos, tipificados dentro de una normatividad, excepto que su comisión se realiza a través de otros medios, tales como los electrónicos o informáticos. (Rincón *et.al.*, 2011, p.53).

Proyecto de ley para penalizar los delitos informáticos en Colombia

Es menester destacar al autor del proyecto de la ley de los Delitos Informáticos, el doctor (Diaz, 2012), proyecto denominado inicialmente como: "Delitos Electrónicos en Colombia" (atendiendo al termino genérico que encierran estos delitos, concepto también expresado por el doctor Campoli) y que después de afrontar toda una extensa etapa legislativa terminó adoptando el nombre del nuevo bien jurídico tutelado, denominado "De la protección de la información y de los Datos" mencionado anteriormente.

Para poder conocer la creación de esta ley es necesario apoyarse en la memoria histórica que realiza el doctor Rincón Ríos, siendo también un acérrimo participe y gestor de dicho proyecto de Ley, que con sus conocimientos generó un valioso aporte intelectual y académico en el desarrollo de la Ley 1273 de 2009, tarea que comenzó a finales del año 2006, dentro del despacho del viceministro de justicia, doctor Guillermo Reyes, a quien le agradecen enormemente por su interés tenido en esta nueva tendencia de delitos por medios informáticos, teniendo, además, el requerimiento del Presidente de la República, en esa época el doctor Álvaro Uribe Vélez, razón por la cual se planteó la necesidad de legislar en Colombia el creciente fenómeno delictivo electrónico: (Rincón *et.al.*, 2011) y haciendo uso de esa estrecha cercanía con la Dirección de Posgrados de la Universidad Santiago de Cali acordaron trabajar de manera conjunta en dicha tarea, generándose un enlace circunstancial debido a que el doctor Díaz García se encontraba asesorando a la Universidad Santiago de Cali en temas de derecho informático, motivos que llevaron a adoptar el pretensioso

proyecto, contando además con el beneplácito del rector de dicha universidad, para esa época el doctor Hebert Celin Navas. De esta forma procedieron a la publicación del proyecto ante el Ministerio del Interior y de Justicia y luego al Congreso, haciéndoles llegar a sus integrantes un ejemplar, que fue el mismo que se usó para la presentación del 1er Foro de discusión sobre "Fraude en la Contratación Electrónica Internacional", realizado en el mes de marzo de 2007, con expositores nacionales e internacionales, y desarrollando como eje principal la imperante necesidad de establecer una legislación penal en materia de delitos informáticos, por lo que se abrió la posibilidad a todo el público interesado en esta temática para que inscribieran sus respectivas ponencias, publicándolas en la página web www.proyectodelitoelectronico.com, suscitando definitivamente a un debate nacional, lo que condujo a la exposición del proyecto creado y redactado por el Juez de Rovira, Dr. Díaz García, en ese foro (Rincón *et.al.*, 2011, p.46).

Enfatiza el doctor Rincón (2011) que el debate no fue fácil, pues el Ministerio de Relaciones Exteriores de Colombia convocó a debatir el tema y el proyecto del doctor Díaz García en varias sesiones, incluso con la presencia de la Comisión Europea, del cual hasta surgió un proyecto distinto, el del representante German Varón Countrino, quien al parecer, en coparticipación con la Cancillería, mediante un escrito enviado al ente europeo se desconoció la autoría del doctor Díaz García y el patrocinio de los posgrados de los de la Universidad Santiago de Cali, para el nuevo tratamiento judicial planteado en contra de los delitos informáticos, donde el representante German Varón recogió la postura de la Cancillería y la SIJIN (en cabeza del Mayor Freddy Bautista), adoptando la tesis de la agravación punitiva para este tipo de delitos, siendo esta una postura negativa para el proyecto, porque argumentaba que los tipos penales tradicionales, subsumían dichos comportamientos y que era responsabilidad de los fiscales y los jueces para adoptar la calificación de las conductas electrónicas disvaliosas para la sociedad. Esa situación motivo aún más al Juez de Rovira, al doctor Díaz García y a sus gestores a realizar lo que estuviera al alcance de sus posibilidades para la defensa de su proyecto, buscando otras instancias. Gracias a la ayuda obtenida del Senador Humberto Gómez Gallo y del representante Carlos Arturo Piedrahita lograron una positiva intervención del doctor Díaz García, de funcionarios del Ministerio del Interior (en especial el doctor José Gregorio Beltrán) y el doctor Rincón Ríos, exponiendo sus argumentos ante la Comisión Primera de la Cámara y su plenaria, previo al haber sido escuchados por parte de todos los sectores políticos del Congreso en sesión informal, aprobándose en la Comisión Primera de la Cámara y su plenaria el Proyecto de ley, en el que se eliminó la propuesta de SPAM como delito y se generó el nacimiento del tipo legal: "De la protección de la información y de los datos": (Rincón *et.al.*, 2011, p.47)

Continúa relatando el doctor Rincón Ríos que en el desarrollo de todo proyecto siempre van existir puntos de vista contrarios, las *"mal miradas"* oposiciones, naturalmente por las diferentes posturas que se tienen en nuestra sociedad, con ideologías que se construyen por formaciones de corrientes dogmáticas de diversos autores, razón por la que resalta la importancia de la postura negativa que existió por parte del representante, doctor Germán Varón y también del Senador, doctor Parmenio Cuellar, quien fue el que redactó y

presentó la ponencia negativa del proyecto ante la Comisión Primera del Senado el 14 de mayo de 2008, dirigida al doctor Juan Carlos Vélez Uribe (presidente de la Comisión), expresando con argumentos analíticos de tipo jurídico, hermenéuticos o sociales, porque no era necesario el proyecto del doctor Díaz García, para lo cual expondremos algunos puntos que a nuestro parecer son muy relevantes en el desarrollo de esta investigación, captando nuestra atención porque se observa en esa ponencia un lenguaje dogmático coherente que permite concluir, que no fue una oposición caprichosa al proyecto de la ahora Ley 1273 de 2009, sino que en realidad se basaban en una interpretación lógica que buscaba preservar la estructura jurídica y judicial de nuestro Estado: (Díaz, 2014)

"2 Lo primero que debe resaltarse, es la tendencia cada vez más marcada del Estado Colombiano *-por la vía del órgano legislativo-* ***a generar una hiperproducción de leyes. Y lo que es más grave: la tendencia más clara aún de sortear las dificultades que se presentan como manifestaciones de una sociedad con múltiples problemas y pocas oportunidades, a punta de derecho penal****…".*

"3 El ideal del derecho penal *–al menos en el ámbito de un Estado "social y democrático de derecho" –****es que sea mínimo;*** *por tanto, ese ideal no es sitiar al individuo restringiendo cada vez más su libertad –cual si se tratase de un nacionalsocialismo o cualquiera otra forma dictatorial de gobierno…"*

"4 Por regla general, cuanto más derecho penal haya tanto más incapaz será el Estado de dispensar una pronto y cumplida justicia*…"*

"5. A lo anterior se suma otra irreductible tendencia legislativa: hacer casuismo en los códigos y, definitivamente, el casuismo es el mayor enemigo de la cientificidad*, porque ninguna ciencia –o el estado de una ciencia– puede elaborarse con base en* ***todos*** *los casos o variantes que un fenómeno especial presenta,…"*

Se evidencia de este análisis propuesto por el ponente una razonable crítica frente a la técnica en la creación de la normatividad penal, buscando comprobar la existencia de legislación vigente que regula los temas jurídicos propuestos en el proyecto de ley, por ejemplo para los artículos que nos atañe, el 269A y 269F, ambos los aproximó al Art. 192 del C.P.; en lo que concierne al primer artículo expresó que la frase ***"El que ilícitamente…"*** permite tener mayor amplitud al operador jurídico de valoración de la conducta, que la expresión propuesta en el proyecto: ***"sin autorización o fuera de lo acordado…"***; mientras que para el Art. 269F, la expresión **"provecho",** ya sea propio o para un tercero, limita la valoración que el operador jurídico pudiese realizar, resaltando que el Art. 192 va más allá, ya que con la simple "**intromisión"** se establece en delito punible.

Frente a estos argumentos del ponente, específicamente a los dos artículos 269A y 269F, se observa que ciertamente existía una gran proximidad con lo ya tipificado en el Art.

192 de la Ley 599 de 2000, lo que pudo generar que se desarrollara el *"Texto conciliado al Proyecto de Ley No. 281 de 2008 Senado, 042 y 123 de 2007 Cámara Acumulados"*.

Finaliza el autor comentando que *"Triunfó la generosidad"*, ya que el ponente Senador Cuéllar terminó cambiando su posición y presentando propuesta favorable a la Comisión Primera del Senado y su plenaria, la cual fue aprobada con las adiciones y los comentarios de los también senadores Héctor Hely Rojas y Darío Salazar.(Díaz, 2014)

Por su parte, el doctor (Díaz, 2014), autor del libro: "*Apuntes de derecho informático*", también relató un poco los antecedentes de su largo caminar por cerca de 10 años en el desarrollo de tan significativo proyecto de ley, bajo duras y largas labores nocturnas de arduo trabajo investigativo en su despacho judicial, contando que en varias oportunidades vio salir el Sol por las rendijas de su despacho, con el fin de poder sacar adelante ese proyecto de Ley, que terminó alcanzando los objetivos pretendidos, obteniendo una concreta legislación para la penalización de los delitos informáticos, la denominada Ley 1273 de 2009, relatando que fue una difícil tarea de lograr y con su proyecto bajo el brazo, estuvo tocando muchas puertas a legisladores locales y nacionales para que se lo presentaran ante el Congreso, hasta que finalmente por intermedio del ex senador Luis Humberto Gómez Gallo (q.e.p.d), quien aceptó registrarlo en el Parlamento, y con la colaboración del representante a la Cámara Carlos Arturo Piedrahita Cárdenas, quien fue el encargado de deliberarlo brillantemente, pasando por todo un trámite legislativo para nada sencillo (como ya se ilustró anteriormente), debido a que suscitó una gran controversia con el doctor Germán Navas Talero, por quien fue rechazado rotundamente, afirmando que la legislación penal no necesitaba más modificaciones al respecto, encontrándose ya satisfechos los presupuestos en materia informática con las codificaciones costumbristas.

Por otro lado, el doctor (Díaz, 2014) también fue el autor de tramitar completamente en internet la primera acción de tutela amparando el derecho constitucional de hábeas data y la intimidad virtual, por uso impropio del SPAM, igualmente captó nuestra atención la demanda de inconstitucionalidad que presentó el doctor (Diaz, 2012b) en contra del artículo 16, inciso 1º (parcial) de la ley 1142 de 2007 y contra el artículo 245, inciso 2º, de la Ley 906 de 2004 (Código de Procedimiento Penal), acusando protección constitucional al tratamiento de datos personales, debido a los excesos que se dan por parte del Estado en algunos procedimientos contemplados en el Código de Procedimiento Penal dentro del ejercicio del *"ius punendi"*, vulnerando lo previsto en los artículos 15, 21, 29 y 250 de la Constitución Política, así como en el artículo 17, numerales 1º y 2º del Pacto Internacional de Derechos Civiles y Políticos, argumentando el autor una ausencia total de los protocolos internacionales para el manejo del tratamiento de los datos personales en el proceso penal, violando así los derechos fundamentales del procesado y, por ende, sus derechos humanos, resolviendo la Corte Constitucional la inconstitucionalidad parcial de dichos artículos mediante esta sentencia C-334 de 2010 (Corte Constitucional Sentencia C-334/10, 2010).

Naturaleza jurídica y estructural de la (Ley 1273, 2009)

Dentro de la exposición de motivos del proyecto de Ley "De la Protección de la Información y de los Datos", el doctor (Rincón *et.al.*, 2011, p. 82) expresa que para poder hablar de delito informático son necesario dos presupuestos básicos: el primero, es que la conducta constitutiva del mismo esté tipificada por la ley; el segundo es que medie una sentencia condenatoria en la cual el funcionario judicial haya declarado probada la existencia concreta de la conducta típica, antijurídica y culpable del delito informático. En razón a la no existencia de dichos presupuestos se puede colegir que la conducta delictiva por medios informáticos es atípica, por lo que consideró necesario proponer un decálogo de conductas que se encuentran constituidas por tipos autónomos y no subordinados, ni por circunstancias genéricas o específicas de agravación punitiva de otros tipos, con siete (7) conductas aprobadas de un total de diez (10) artículos que originalmente se habían proyectado, dejando por fuera de la legislación la **"Falsedad informática, espionaje informático y el SPAM"**, modificándose el epígrafe **"Espionaje Informático"** por **"Transferencia no consentida de activos".** La Ley integra tres capítulos, encontrando en el primero la tipificación de los delitos: "*acceso abusivo a un sistema informático, obstaculización ilegitima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos y circunstancias de agravación punitiva"*. El segundo capítulo se constituye por: *"hurto por medios informáticos y semejantes, transferencia no consentida de activos"*, terminando el texto con artículos que tipifican circunstancias de mayor punibilidad y la competencia de los Jueces Municipales.

Una de las grandes preocupaciones del autor frente a la realización de su proyecto de ley era la de empezar a generar una correcta cultura en el tratamiento de datos personales, dándole una verdadera relevancia jurídica, convirtiéndonos en unos de los pocos países en el mundo en darle protección penal a los datos personales. Es así como expresa el doctor Díaz (2014), que la existencia del artículo 269 F del C.P. ha generado y seguirá generando una transformación a nivel social e institucional, haciendo correctivos a costumbres mal sanas que violan los datos personales en el diario vivir de nuestra sociedad, frenando o disuadiendo a los delincuentes informáticos a cometer esta clase de infracciones como cuando se publica información sensible en redes sociales o cuando en los ficheros de compañías que compran cartera castigada se actualiza una obligación prescrita sin el consentimiento del titular, a fin de mantener ilegal e indefinidamente los registros negativos en las centrales de riesgo, entre muchos otros casos que se conocen como una violación de datos personales. Es decir, que el autor no estaba solo preocupado por judicializar a los delincuentes que atentaran contra los derechos de personas por medio del uso de medios informáticos, sino que también su mayor interés era la de proteger los bienes jurídicos que pueden ser vulnerados por cualquier persona que acceda ilícitamente a un sistema informático, agrediendo bienes jurídicos, tales como la confidencialidad, la integridad y la disponibilidad de datos veraces o actualizados, almacenados en estos sistemas informáticos (Vgr. Habeas Data).

A continuación se explicará los elementos estructurales de los tipos penales de los artículos 269A y 269F contenidos en el Titulo VII BIS del Código Penal (Ley 599 de 2000) **"De la protección de la información y de los datos"**, modificado por la Ley 1273 de 2909, por el cual se adicionó el capítulo I: **"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos":**

ARTÍCULO 269A DEL C.P. "ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO".

El que sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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 (Ley 1273, 2009).

ELEMENTOS DEL TIPO PENAL (Rincón & Naranjo, 2011)

. **SUJETO ACTIVO:** indeterminado singular → *"El que…"*; debiendo realizar la conducta sin autorización o por fuera de lo acordado previamente con el sujeto pasivo.

. **SUJETO PASIVO:** titular del legítimo derecho → *"quien tenga el legítimo derecho a excluirlo"*

. **VERBOS RECTORES:** acceder: *"acceda en todo o en parte…"*. Mantener: *"mantenga dentro del mismo…"*

. **OBJETO JURÍDICO** (Arzuaga & Guevara, 2013)**:** *"derechos a la intimidad, a la información y a la comunicación"*

. **OBJETOMATERIAL:** el sistema informático sin importar si está protegido o no con medida de seguridad.

. **OBJETO REAL:** la confidencialidad e integridad de la información y los datos.

. **CLASIFICACIÓN DEL TIPO PENAL**:

Tipo penal de peligro: la mera puesta en peligro del objeto real (información).
Tipo penal de mera conducta: no se necesita del resultado para ser lesivo.
Tipo penal de un solo acto: con un solo acto es suficiente para su sanción.

ARTÍCULO 269F DEL C.P. "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.

ELEMENTOS DEL TIPO PENAL (Rincón & Naranjo, 2011)

. **SUJETO ACTIVO:** indeterminado singular → *"El que…"*; debiendo realizar la conducta sin autorización o por fuera de lo acordado previamente con el sujeto pasivo.

. **SUJETO PASIVO:** indeterminado, titular de los datos o de la información.

. **VERBOS RECTORES:** Obtener: "…obtenga…"
Compilar: "…compile …"
Sustraer: "…sustraiga …"
Ofrecer: "…ofrezca …"
Vender: "…venda …"
Intercambiar: "…intercambie …"
Enviar: "…envíe …"
Comprar: "…compre …"
Interceptar: "…intercepte …"
Divulgar: "…divulgue …"
Modificar: "…modifique …"
Emplear: "…emplee …"

. **OBJETO JURÍDICO** (Arzuaga & Guevara, 2013)**:** *"derechos a la intimidad, a la privacidad y a la información personal"*.

OBJETO MATERIAL: "… códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes…".

. **OBJETO REAL:** la confidencialidad, la integridad y la disponibilidad de la información y de los datos.

. **CLASIFICACIÓN DEL TIPO PENAL:**

Tipo penal de lesión: la consumación de la acción configura la lesión.

Tipo penal de resultado: debe existir nexo entre la acción y el resultado.
Tipo penal de varios actos: es preciso participar en más de una etapa lesiva para lograr su sanción.

Concluimos brevemente este capítulo resaltando el gran esfuerzo por parte de todos los realizadores de la Ley 1273 de 2009, logrando por fortuna haber superado las dificultades legislativas con mayoría de los miembros del Congreso, quienes entendieron que les correspondían tipificar estas conductas que lamentablemente se están masificando frente un fenómeno en alza, que a la par del desarrollo tecnológico informático, donde la delincuencia encuentra formas innovadoras para la realización de fraudes y otros delitos que con frecuencia han ido más rápido que los códigos penales, lo cual exige una imperativa necesidad de prevención y de protección de sus ciudadanos, mediante la participación masiva por parte de los Delegados, la Policía Judicial, la Fiscalía General de la Nación y demás cuerpos de seguridad el país, a quienes poco a poco se la ha brindado capacitación de estas nuevas modalidades de delitos y de esta formar buscando evitar tipificaciones erradas, mermando las publicaciones indebidas e ilegales de datos personales en redes sociales, conexión o acceso a redes sin autorización, uso de *software* malicioso, etc., con el fin que esta nueva ley tenga como fin único ayudar a preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones en nuestro país.

CAPÍTULO II:

2. ANÁLISIS JURISPRUDENCIAL

Es apenas comprensible que por la joven normativización de los delitos informáticos no se tenga gran variedad de desarrollo jurisprudencial sobre los delitos que en esta ocasión investigamos (Art. 269A y Art. 269F). Además, se pudo observar anteriormente que, desde su creación, la evolución de la normatividad penal contra el *"Acceso abusivo a un sistema informático"* -Art. 269A - ha tenido grandes dificultades para su promulgación dentro del Código Penal, observación que también la realizó el doctor Ricardo Posada Maya, en su artículo: *"El delito de acceso abusivo a sistema informático: a propósito del Artículo 269A del Código Penal del 2000"*, publicado en la **Revista Derecho Penal No.** 44, al cual nos referiremos como soporte y complemento del estudio de las líneas jurisprudencias de las dos Sentencias representativas de la Corte Constitucional, C-913 de 2010 y C-540 de 2012, que a continuación estudiaremos y que fueron las que permitieron preservar en toda su integridad, no solamente la amenazada normatividad creada contra los delitos de *"acceso abusivo a un sistema informático"*, sino que también los intentos fallidos del poder Ejecutivo y hasta del poder Legislador, al querer modificar forzosamente lo ya establecido en la Ley 1273 de 2009. (Posada, 2013).

Comencemos recordando que anteriormente el Legislador ya había procurado, aunque de forma superficial y sin una significativa penalización, tan solo mediante una multa, sancionar el *"acceso abusivo a un sistema informático"*, normatividad establecida en la Ley 599 de 2000 en su artículo 195 del C.P. dentro del Título III, Capítulo VII "**De la violación a la intimidad, reserva e interceptación de comunicaciones"**, la cual expresa al tenor de letra:

> *"Articulo 195. Acceso abusivo a sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurrirá en multa."* (Ley 599 de 2000, 2000)

Pero luego de la controvertida promulgación de la Ley 1273 de 2009 el legislador demostró su verdadera intención de penalizar *"la violación de intimidad, reserva e interceptación de comunicaciones"*, garantizando la seguridad de los procesos informáticos, con el fin de controlar los ataques cibercriminales mediante el establecimiento de esta figura autónoma frente a los tipos penales tradicionales, incluyendo dentro de la legislación contenida en el Código Penal, el artículo 269A y subsiguientes, del Título VII BIS del Capítulo I dirigido a penalizar *"los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos informáticos"* que se transmiten, contienen o procesan en forma automática.

Según (Posada, 2013) *una de las figuras ampliamente modificadas por esta ley fue el*

delito de acceso abusivo a sistema informático [3]. Tipo penal pionero en nuestro medio jurídico que inicialmente fue regulado por el artículo 195 del C. P. [4] —dentro del capítulo VII, título III, dirigido a castigar "La violación de la intimidad, reserva e interceptación de comunicaciones"—, y que en esta oportunidad fue incluido en el artículo 269A, dentro de las figuras que castigan especialmente "Los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" que los contienen, procesan o transmiten en forma automática. Con ello el legislador penal colombiano confirmó su deseo de garantizar la seguridad de las funciones informáticas propiamente dichas, en contra de ataques cibercriminales [5], como figuras autónomas frente a los tipos penales tradicionales.

Pero, al poco tiempo, ocurre un fallido intento del gobierno en el que se evidencia una posible falta de planeación legislativa, con tan solo los dos meses de haberse promulgado la esforzada modificación en el Código Penal contra la cibercriminalidad, en el mes de marzo de 2009 el gobierno sancionó la Ley 1288 que tenía como objetivo: "*fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir adecuadamente con su misión constitucional y legal, estableciendo los límites y fines de sus actividades, los principios que las rigen, los mecanismos de control y supervisión, **la regulación de sus bases de datos**, la protección de sus miembros, la coordinación y cooperación entre sus organismos y los deberes de colaboración de las entidades públicas y privadas entre otras disposiciones*" (Ley 1288, 2009) observando en varios de sus artículos, regulaciones encaminadas a permitir a las instituciones del gobierno, eso sí, solo mediante labores de inteligencia y de contrainteligencia, infringir la protección y la defensa de algunos derechos fundamentales, principalmente el derecho a la intimidad, razón por la cual por medio de una demanda de inconstitucionalidad en contra de esta ley, la Corte Constitucional desarrolló la línea jurisprudencial contenida en la Sentencia C-913 de 2010 que estudiaremos un poco más en detalle, demanda de inconstitucionalidad específicamente en contra de algunos apartes contenidos en los artículos: 1°, 8°, 10, 15, 16, 17, 18, 19, 20, 21, 23, 25 y 31 de la Ley 1288 de 2009, pero en esta ocasión nos enfocaremos solo en el artículo 31 de la mencionada Ley.

2.1. Sentencia C-913 de 2010

(Corte Constitucional, Sala Plena de la Corte Constitucional, Sentencia C-913/10, 2010): Realizamos una breve introducción, en forma de ficha técnica, para el desarrollo de la línea jurisprudencial y dar una contextualización concreta de la Sentencia. La demanda fue ejercida por los distinguidos juristas: Federico Andreu Guzmán, Fátima Esparza Calderón, Juan Camilo Rivera Rugeles, Jahel Quiroga Carrillo y Gustavo Gallón Giraldo, mediante acción pública prevista en el artículo 241 de la Constitución presentada ante la Corte Constitucional, con demanda de inconstitucionalidad contra varios apartes de los artículos 1°, 3°, 8°, 10, 11, 12, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29 y 31 de la Ley 1288 de 2009.

Con Sala plena de la Corte Constitucional, siendo el presidente de la Corte, el doctor Mauricio González Cuervo (pronunciándose con salvamento de voto*)*, el magistrado ponente, el doctor Nilson Pinilla Pinilla y contando con los votos de los magistrados: Juan Carlos Henao Pérez, Jorge Iván Palacio Palacio, Jorge Ignacio Pretelt Chaljub, Humberto A. Sierra Porto, Luis Ernesto Vargas Silva, y como Secretaria General, la doctora Martha Victoria Sáchica Méndez, en cumplimiento de sus atribuciones constitucionales y de los requisitos y trámites establecidos en el decreto 2067 de 1991 estudian dicha demanda de inconstitucionalidad y emiten sentencia el dieciséis (16) de noviembre de dos mil diez (2010).

Los actores plantean en su escrito siete (7) distintos cargos de inconstitucionalidad, cuestionando uno o más segmentos normativos pertenecientes a diversos artículos de esta ley. Los dos primeros cargos de la demanda aluden a situaciones que los actores consideran vicios de trámite, considerando que el contenido de sus artículos de esta Ley ordinaria 1288 de 2009 hacen parte del derecho fundamental al hábeas data, como se observa en los artículos 1°, 8°, 16, 18 y 19 los cuales deberían estar contenidos en una ley estatutaria, debido a que afecta derechos fundamentales, entre otros, el derecho a la intimidad y la vida privada, el hábeas data, la inviolabilidad de las comunicaciones, el derecho a la honra, la seguridad personal e, incluso, el derecho a la vida. Lo anterior, por cuanto se permite a las autoridades, y a partir de ello potencialmente a otras personas, conocer información de personas que pueden tener interés legítimo de ocultar, con un derecho prevalente de confidencialidad, y que tan en casos específicos y con el compromiso de no revelarlos a terceros, pues su divulgación puede crear molestias o, peor aún, peligros para la integridad o la vida de las personas podrían ser relevados para uso y fines específicos. También solicitaron la inexiquibilidad de esta ley afirmando que los preceptos son contrarios a los artículos 1°, 3°, 15, 114 y 150 del texto superior y que transgreden también el artículo 30 de la *Convención Americana sobre Derechos Humanos* y los artículos 17 y 19 del *Pacto Internacional de Derechos Civiles y Políticos*, debido a que establecieron competencias de regulación en cabeza de entidades o autoridades que hacen parte de la rama ejecutiva, de las materias que por su naturaleza e importancia solo pueden ser válidamente reguladas por el legislador. (Corte Constitucional, Sala Plena de la Corte Constitucional, Sentencia C-913/10, 2010)

En los siguientes cinco cargos restantes cuestionaron directamente el contenido de las normas acusadas, afirmando que existió una omisión legislativa relativa que vicia la constitucionalidad del artículo 20 debido a que no contempló a la Defensoría del Pueblo ni a los Jueces distintos a los penales, dentro del listado de autoridades a quienes no se les podría oponer la reserva legal; observemos a que se refería el artículo 18 de la ley 1288 que establecía que dicha reserva sería inoponible: *"a los requerimientos de las autoridades penales, disciplinarias o fiscales";* dando a entender que la información de inteligencia y de contrainteligencia podría ser utilizada dentro de las actuaciones y de las investigaciones que adelanten solo esas autoridades.

Los actores también observaron otra posible omisión legislativa relativa, dirigido contra el **parágrafo 1° del artículo 31** de la Ley 1288 de 2009, norma que establecía

obligaciones de entrega de información a los organismos de inteligencia y de contrainteligencia a cargo de los operadores de telecomunicaciones, quienes *"estarán obligados a suministrar"* un conjunto de informaciones relativas a suscriptores o usuarios de sus servicios sobre quienes recaigan operaciones de inteligencia, incluso permitiendo la localización de las personas, siendo esta información accesibles con total libertad para los organismos de inteligencia a solicitud de su director, sin que obre de por medio alguna autorización o algún conocimiento de los directamente implicados y sin requerir autorización o control judicial alguno, a continuación:

"CAPITULO VII
Deberes de colaboración de las entidades públicas y privadas

Artículo 31. Colaboración de las entidades públicas y privadas. Las entidades públicas y privadas podrán cooperar con los organismos de inteligencia y contrainteligencia para el cumplimiento de los fines enunciados en esta ley. En caso de que la información solicitada esté amparada por la reserva legal, los organismos de inteligencia y las entidades públicas y privadas podrán suscribir convenios interinstitucionales de mutuo acuerdo. En cualquier caso, la entrega de tal información no constituirá una violación a la reserva legal, toda vez que la misma continuará bajo este principio, al cual se encuentran obligados los servidores públicos de inteligencia y contrainteligencia en virtud de lo dispuesto en la presente ley.

Parágrafo 1°. En cumplimiento de los términos establecidos en la presente ley los operadores de telecomunicaciones estarán obligados a suministrar a los organismos de inteligencia y contrainteligencia, previa solicitud y en desarrollo de una operación autorizada el historial de comunicaciones de los mismos, los datos técnicos de identificación de los suscriptores sobre los que recae la operación, así como la localización de las celdas en que se encuentran las terminales y cualquier otra información que contribuya a la localización. Los organismos de inteligencia y contrainteligencia garantizarán la seguridad de esta información a través de los CPD.

Los directores de los organismos de inteligencia serán los encargados de presentar por escrito a los operadores de telecomunicaciones la solicitud de dicha información.

En todo caso, la interceptación de comunicaciones estará sujeta a los procedimientos legales establecidos por la Constitución y la ley.(…)"

Observemos, como este artículo permitía a los organismos de inteligencia, ponerles a su disposición los datos que necesitaran, tales como:

i) el historial de comunicaciones de estas personas;
ii) los datos técnicos de identificación de los suscriptores;
iii) la localización de las celdas en las que se encuentren los terminales;
iv) cualquier otra información que facilite la ubicación de estas personas.

También el legislador procuró darle un poco de legalidad a dicho trámite investigativo, adicionando dos incisos finales que indicaban la manera como dicha información debía ser solicitada y suministrada, buscando vagamente prevenir posibles violaciones o arbitrariedades en los procedimientos de inteligencia y de contrainteligencia.

El reproche de constitucionalidad se sustentó debido a la ausencia de controles judiciales adecuados dentro de dicha normatividad, en relación con la libre autorización otorgada a la mayoría de las actuaciones de las autoridades que realizan actividades de inteligencia y de contrainteligencia, toda vez que es en contraria a los controles que constitucionalmente han sido provistos por el legislador, con el firme propósito de salvaguardar los derechos fundamentales de las personas, mandato que recae específicamente sobre las personas jurídicas (como operadores de telecomunicaciones) que tienen la información. Los actores reiteradamente señalan que *"la posibilidad de que los organismos de inteligencia accedan a toda esta información sin el conocimiento de los afectados crea serios riesgos para el goce efectivo de varios importantes derechos fundamentales de ellos, entre otros, el derecho a la intimidad y la vida privada, el hábeas data, la inviolabilidad de las comunicaciones, el derecho a la honra, la seguridad personal, e incluso el derecho a la vida",* debido a que la divulgación de dicha información podría infringir en el interés legítimo de confidencialidad o de ocultación que pueda recaer sobre cierta información personal, y que solo se daría a conocer en casos específicos y con el compromiso de no revelarlos a terceros, pues su posible divulgación puede crear futuras molestias no deseadas o, mucho peor, que atente contra la integridad o la vida de las personas. (Corte Constitucional, Sala Plena de la Corte Constitucional, Sentencia C-913/10, 2010)

Los actores continúan realizando el análisis del parágrafo primero de este articulo 31 de la Ley 1288 de 2009, refiriéndose a la omisión legislativa aducida y no encuentran un tratamiento distinto que se deba dar, *"entre el manejo de las interceptaciones y el de las demás situaciones en que se entrega a las autoridades información sensible y relevante que hace parte de la intimidad de las personas, sin el conocimiento de los afectados"*, debido a la relevante afectación de los ya mencionados derechos fundamentales, expresamente consagrados en nuestra Constitución Política, citando el inciso 2° del artículo 15 superior así como el numeral 3° del artículo 250, en los cuales se menciona respectivamente la necesidad de *"orden judicial"* y *"autorización por parte del juez"* para *"la interceptación y registro de la correspondencia y las otras formas de comunicación privada"* y para recolectar pruebas *"que impliquen afectación de derechos fundamentales"*.

Expuestos estos argumentos los actores solicitaron a la Corte se proceda a integrar el ingrediente normativo excluido por el legislador, advirtiendo, entonces, que las actuaciones previstas en este parágrafo del artículo 31 queden sometidas a reserva judicial o como pretensión subsidiaria que la Corte declare la inexequibilidad del referido parágrafo, de tal manera que desaparezca la obligación de los operadores de telecomunicaciones de entregar información sobre sus suscriptores, que no ha de ser objeto del necesario control judicial.

Luego de un detallado análisis y cuatro (4) intervenciones provenientes de instituciones

públicas y privadas que expresaron su particular opinión sobre el planteamiento contenido en la demanda, previamente la Corte advirtió que la decisión que tomaría frente a la demanda de inexiquibilidad, no implicaba juicio alguno sobre la constitucionalidad material de cada uno de los artículos que componen dicha ley, ya que con el solo estudio del primer cargo de la demanda que se refiere al tipo de trámite seguido para la expedición y promulgación de la Ley 1288 se lograría comprobar la inexequibilidad de toda la norma, debido a que encontraba intranscendente entrar en análisis de los restantes cargos de la demanda, indicando que lo desarrollado en dicha ley tiene una cercana relación con el goce efectivo de varios derechos fundamentales, por lo que constituye un trámite especial, siendo ese el propósito constitucional de las leyes estatutarias. A continuación la decisión:

"RESUELVE

Primero.- DECLARAR INEXEQUIBLE *la Ley 1288 de 2009, "Por medio del cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con su misión constitucional y legal, y se dictan otras disposiciones".*

Con este breve estudio de la Sentencia C - 913 podemos evidenciar en la plurimencionada Ley 1288 de 2009 las verdaderas intenciones que se tuvieron de retroceder un poco en el tiempo y en el avance constitucional que ya se venía logrando frente a la violación de importantes derechos fundamentales, tales como el derecho a la intimidad y la vida privada, la inviolabilidad de las comunicaciones, el derecho a la honra, la seguridad personal, mediante la manipulación de los medios informáticos sin las debidas autorizaciones judiciales, queriendo revivir lo anteriormente establecido en el artículo 195 C.P., que con mucho esfuerzo se logró modificar gracias a la creación de la Ley 1273 de 2009, mostrando así el difícil camino evolutivo que desde sus inicios se observa para el artículo 269A.

Pero lo anteriormente mencionado no terminaría allí y, como era de esperarse, las firmes intenciones del gobierno no cesaron, presentando posteriormente un nuevo proyecto de Ley denominado: *"Proyecto de Ley Estatutaria Número 263 de 2011 Senado, 195 de 2011 Cámara, Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contra inteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones"*, la cual fue sancionada y promulgada por el actual Presidente Juan Manuel Santos Calderón como la Ley 1621 de 2013, después de haber superado el minucioso examen de la Corte Constitucional, se observa nuevamente como evita que se modificara nuevamente tan vulnerable artículo 269A, tal y como lo expresó el Dr. (Posada, 2013), en su artículo *"El delito de acceso abusivo a sistema informático: a propósito del Artículo 269A del Código Penal del 2000"*, ley en la que se buscó por parte del gobierno corregir las vicisitudes presentadas en la tramitología empleada en la anteriormente estudiada, Ley 1288 de 2009, cumpliendo ahora así con los fines constitucionales, debido a que se desarrolló un proceso

especial de Ley Estatutaria requerido para el tratamiento de los derechos fundamentales, pero nuevamente esta ley presentó fallas en lo concerniente a la reserva legal que se encuentra inherente en los artículos que regulan el tratamiento de los datos informáticos, en relación con las actividades que desarrollan los organismos de inteligencia y de contrainteligencia, debido a que establecía violación al principio de "unidad de materia", el cual exige que: *"en toda ley deba existir correspondencia lógica entre el título y su contenido normativo, así como una relación de conexidad interna entre las distintas normas que la integran"*. (Matus, 2013)

2.2. Sentencia C-540 de 2012

Fue así como mediante la (Corte Constitucional, Sala Plena de la Corte Suprema de Justicial, 2012) declaró inexequible por vicios de formas los artículos del 40 al 49 *"Sección única reformas penales para la garantía de la reserva legal de la información de inteligencia y contrainteligencia"*, en el que se pretendió modificar nuevamente la regulación desarrollada para hacerle frente a las modalidades criminales que buscan prevenir riesgos masivos y continuos que puedan afectar el funcionamiento confiable y el debido uso de los sistemas informáticos, entre esos, el acceso abusivo a un sistema informático (Art. 269A), debido a que infringió el artículo 158 de la Constitución Política que regula el principio de unidad o relación de materia de las leyes o también conocido como *"conexidad sustancial"*, observando que buscaba la misma finalidad de la anterior Ley 1288 de 2009, resaltando, además, que uno de sus principales objetivos era el fortalecimiento del marco jurídico que regula las actividades de inteligencia y de contrainteligencia, buscando permitir a estos organismos la regulación de las bases de datos, entre otras, poder acceder de manera oportuna y sin ningún control judicial a la información confidencial o íntima que reposa en medios informáticos. (Corte Constitucional, Sala Plena de la Corte Suprema de Justicial, 2012)

Esta sentencia es bastante extensa (aproximadamente de 430 folios), contando el salvamento de voto parcial, en la cual fueron declarados exequibles todos los artículos, salvo los ya mencionados artículos del 40 al 49, (Corte Constitucional, Sala Plena de la Corte Suprema de Justicial, 2012)que fueron declarados inexequibles, de acuerdo al detallado examen de constitucionalidad que realizó la Corte, donde también se tuvo la intervención de la Corte Suprema de Justicia para cada uno de estos 10 artículos (40 al 49), argumentos que a continuación expondremos, pero que para efectos de esta investigación tan solo nos referiremos al artículo 40 de dicho proyecto de ley, donde podremos darnos cuenta de esas pequeñas modificaciones a la norma consagrada en el artículo 269A, para lo cual la Corte Constitucional de manera acertada señaló una vez más la improcedencia de la "Unidad de materia", expresión dogmática ampliamente desarrollada en muchas de sus sentencias anteriores*;* (Ley 599 de 2000, 2000), debido a que si bien el proyecto de ley presentado al Senado y la Cámara de Representantes tuvo como objetivo regular las actividades que desarrollan los organismos de inteligencia y contrainteligencia en cuanto al manejo de la información en las bases de datos, que aunque busca de cierta forma conservar una adecuada reserva legal en sus procedimientos investigativos, no se convirtió en razón

suficiente para realizar modificaciones de disposiciones de tipos penales, dentro de una ley que se desarrolló exclusivamente para regular el manejo de las actividades que realizan los organismos de inteligencia y de contrainteligencia y de los demás servidores públicos que se involucran en el manejo de este tipo de informaciones. Observemos, entonces, cómo fue la modificación que se pretendía realizar a tan vulnerado artículo 269A del Código Penal, seguidamente veremos las explicaciones textuales del examen de Constitucionalidad de la Corte Constitucional, finalizando con el análisis de la Corte Suprema de Justicia:

NORMATIVIDAD MODIFICADA *Código Penal, Código de Procedimiento Penal y Código Penal Militar*	***NORMATIVIDAD INTRODUCIDA*** *Reformas penales para la garantía de la reserva legal de la información de inteligencia y de contrainteligencia*
Artículo 269A del Código Penal: *"Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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".*	*El artículo 269A del Código Penal quedará así:* *"Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión* ***de cinco (5) a ocho (8) años y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.*** ***La pena se aumentará hasta el doble cuando el acceso abusivo beneficie a miembros de grupos armados al margen de la ley u organizaciones de crimen organizado o cuando el acceso abusivo beneficie a gobiernos extranjeros".*** (Ley 599 de 2000, 2000)

Aunque parezca mínima la modificación y aparentemente no afecta la integridad del acceso abusivo a un sistema informático, el Dr. (Posada, 2013) nos explica que se propuso una anti-técnica o una modificación a este artículo por dos razones; primero, nótese que se pretendió aumentar la pena a 10 años de prisión como mínimo, "*la pena se aumentará hasta el doble cuando el acceso abusivo beneficie a miembros de grupos armados al margen..",* y haciendo aplicación del derecho comparado, comenta el doctor Maya que el *"estándar internacional"* para este tipo de delitos son tan solo de cinco años de prisión como máxima pena imponible, aspecto que se estudiará en detalle en el siguiente capítulo

de esta investigación; y como segunda razón, explica el doctor Maya que si bien esta modificación se plantea bajo una esfera político-criminal, su construcción se basa en los resultados de peligro que podría generar la indebida manipulación de la información reservada por parte de los organismos que desarrollan actividades de inteligencia y de contrainteligencia, por lo que afirma que se estaría vulnerando el principio de legalidad que establece la primacía de las leyes, el cual necesariamente debe ser auditado por el organismo judicial, siguiendo lo establecido en nuestra principal norma rectora, la Constitución Política, que, a su vez, integra todo un bloque de constitucionalidad. De igual forma, la Corte Suprema de Justicia expresó al respecto:

> *"…En términos generales y sin que con ello se comprometa su criterio alrededor de temas específicos, llama la atención de que la expresión "el que, sin autorización o por fuera de lo acordado" resulta de extrema vaguedad al no indicar, permitir o precisar a qué clase de autorización o acuerdo se refiere y si deben estar consignados en la ley, el reglamento, una orden o misión de trabajo o en una instrucción verbal."*

Nuevamente se observa que para la Corte resulta más sencillo no estar de acuerdo en modificaciones que pretenden reformar lo ya estrictamente establecido en la norma rectora contra el acceso abusivo a un sistema informático, con simples razonamientos como el de un inadecuado tramite aplicado para dicho fin (es decir, mediante vicios de forma), tal y como se mencionó en la sentencia C-913 de 2010, en la que el gobierno tampoco realizó un adecuado trámite legal para las modificaciones que pretendía en cuanto a las actividades que realizan los organismos de inteligencia y de contrainteligencia y los demás servidores públicos que se involucran en el manejo de este tipo de confidenciales informaciones. Esta oportuna intervención de la Corte permite una vez más exaltar tanto la imperante primacía constitucional, como ese juicioso y complejo proceso de creación que se desarrolló en la Ley 1273 de 2009, creando una regulación adecuada en el manejo de los datos y de la información, y se mantuvo incólume la integridad normativa de toda la Ley, en especial del artículo 269A, evidenciando, además, la rigurosa protección que hemos podido observar a través de estas dos sentencia estudiadas.

2.3. Sentencia T-916 de 2008

Estudiaremos en este capítulo: (Corte Constitucional Sentencia Sentencia T-916/08, 2008) más indicada por el doctor Alexander García en su libro *"Apuntes de derechos informático"*, en el que por medio de una acción de Tutela (expediente T-1817308) la Corte desarrolló la Sentencia T-916 de 2008, pronunciándose frente al acceso ilegal a correos electrónicos, siendo este uno de los medios de comunicación privada con altísima importancia en la actualidad, en consecuencia por el avanzado y acelerado desarrollo tecnológico de la informática.

(Corte Constitucional Sentencia Sentencia T-916/08, 2008) *Uno de los medios de comunicación privada que cobra especial importancia en la actualidad con el surgimiento de la informática es el correo electrónico, sobre el cual, dada la complejidad de la realidad actual exige una aproximación a la intimidad que tenga en cuenta los diversos aspectos que la contempla, entre los cuales se halla el derecho a controlar la información acerca de uno mismo. Por tratarse entonces de un dispositivo que tiene un ámbito privado, es que la regla constitucional prevista en el artículo 15 Superior, referida a la inviolabilidad de la correspondencia y demás formas de comunicación privada, tiene total aplicabilidad cuando se trata de correos electrónicos, pues se trata de una forma de comunicación entre personas determinadas, siendo solamente posible su interceptación o registro, (i) mediante orden de autoridad judicial, (ii) en los eventos permitidos en la ley y (iii) con observancia estricta de las formalidades que la misma establezca..*

Expresa la Corte que es un mandato constitucional reiterado y entendido por dicha corporación, cuando se garantiza imperantemente la inviolabilidad de la libertad del individuo frente a su familia, la sociedad y el Estado, constituyéndose solamente una excepción a la regla, obviamente también regulada constitucionalmente, de la reserva legal y judicial para efectos del registro y de la interceptación de las comunicaciones privadas que ampliamente se ha tratado en varias sentencias del órgano colegiado:

Además, ha sostenido la Corte, las reservas legal y judicial para efectos del registro e interceptación de la correspondencia y las comunicaciones privadas constituyen verdaderas excepciones a la regla general de su absoluta inviolabilidad que, como tales, son de interpretación restrictiva, lo cual indica que no pueden extenderse a ningún otro caso en ellas no previsto, y más cuando la disposición constitucional se vale del adverbio 'solo' para indicar que en ningún evento podrá procederse a interceptar o registrar las formas de comunicación señaladas, sin que medie orden judicial. (Corte Constitucional Sentencia T-696/96, 1996)

La Constitución Política en su artículo 15 dispone:
"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 las demás garantías consagradas en la Constitución.

Para la Corte de ese mandato constitucional se deduce la existencia y la validez de tres derechos fundamentales, que adquirieron especial protección judicial por vía de tutela de manera independiente, además, por las particularidades del régimen jurídico aplicable y

el desarrollo de diferentes reglas para resolver la eventual colisión con el derecho a la información:

1. Derecho a la intimida
2. Derecho al buen nombre
3. Derecho habeas data

En el acceso ilegal a correos electrónicos, principalmente se está violando el derecho a la intimidad, aunque también inciden con los derechos a la honra y al buen nombre, considerando la Corte que se vulnera de tres maneras:

- *"intrusión o intromisión irracional en la órbita que cada persona se ha reservado";*
- *"en la divulgación de los hechos privados";*
- *"en la presentación tergiversada o mentirosa de circunstancias personales, aspectos los dos últimos que rayan con los derechos a la honra y al buen nombre".*

En esta misma sentencia que nos expone el doctor Díaz traen como precedente lo expresado en la sentencia C-1024 de 2002, la cual expresaba lo siguiente respecto a la inviolabilidad de los correos electrónicos:

> (Corte Constitucional Sentencia Sentencia T-916/08, 2008), *Es claro que ese derecho es una extensión de la libertad personal, como ocurre en relación con la inviolabilidad del domicilio y, precisamente por ello, de garantizarlo se ocupa la Constitución Política. No de ahora, sino desde antaño, el derecho a la privacidad de las comunicaciones ha tenido asiento directo en la Constitución por cuanto los seres humanos, a través del lenguaje en sus distintas modalidades, entran en contacto con sus semejantes, hacen conocer de ellos lo que piensan, expresan sus afectos, sus animadversiones, aun sus intenciones más recónditas, sus opiniones políticas, sus convicciones religiosas, reciben informaciones personales, a veces íntimas o que, con razón atendible o sin ella, por su propia determinación no quieren compartir con otros. Por ello, ese derecho a la libertad de comunicación y a la no interceptación ni interferencia de los demás, se extiende incluso a los consanguíneos más próximos y se impone su respeto al Estado como uno de los derechos individuales más caros a los seres humanos, y por ello, no se deja simplemente a que lo establezca la ley, sino que se protege desde la Carta Política.*

Con el estudio de estas tres sentencias de la Corte Constitucional damos por finalizado este capítulo de análisis jurisprudencial, continuando seguidamente con un breve estudio de derecho comparado en relación al desarrollo normativo que han tenido otros países para contrarrestar la vulneración de los derechos fundamentales a la intimidad, confidencialidad además de los datos y de la información, mediante la manipulación de

medios informáticos y de la información, en especial lo concerniente al *Acceso abusivo a los sistemas informáticos*.

Concluyo con este aparte la (Corte Constitucional Sentencia Sentencia T-916/08, 2008) que resume en casi todo lo expuesto en los dos capítulos desarrollados en esta investigación y marca el inicio de los siguientes dos capítulos:

> *"Con todo, el surgimiento de la informática como un nuevo reto que deben asumir los Estados permite avanzar hacia la protección del derecho a la intimidad, no solamente desde una dimensión negativa, entendida como la posibilidad de reaccionar frente a una invasión a esa esfera personalísima, sino también desde una dimensión positiva, de tal suerte que la persona pueda controlar las informaciones que afecten ese ámbito irreductible de su derecho."*

CAPÍTULO III

3. APUNTES SOBRE DERECHO COMPARADO EN LOS DELITOS INFORMÁTICOS

Recordemos que en el capítulo anterior el doctor Maya nos hacía referencia en la sentencia C-540 de 2012 de la Corte Constitucional, artículo 40 correspondiente a la modificación que se pretendió realizar a la norma vigente 269A, respecto al incremento de diez (10) años de prisión (como mínima pena) y máximo dieciséis (16) años que se proponía imponer, indicando el doctor Maya que en el derecho comparado es contrario al estándar internacional que señala como un máximo de pena proporcional y razonable de cinco (5) años, razón por la cual nos explica que esta tendencia es usual en nuestro medio, asociándola "al maximalismo punitivo y al terror penal o neopunitivismo".

Para entender mejor este concepto consultamos el artículo: (Bonavides & Pastor, 2012) "Neopunitivismo o cuarta velocidad del derecho penal delante de los derechos humanos de los ciudadanos de la abogada, Doctora Meire Jany Lopes de Souza, indicándonos que esa tendencia neopunitiva obedece a la ola de política de emergencia inmediata, mediante creación de leyes penales "de impulso" (impulsivas), resultado de acontecimientos concretos, de hechos criminales, con alta intensidad de vulneración de derechos de los ciudadanos, que conmueven fuertemente a la sociedad y afecta la seguridad ciudadana, sin que obre un amplio debate para la creación de leyes que ataquen o contrarreste los delitos. Frente a estos tratamientos políticamente mediáticos, como ya pudimos observar en el capítulo anterior, sale a relucir los controles jurisdiccionales realizados por altas cortes, en especial la Corte Constitucional, que de acuerdo a lo establecido en el artículo 241 de la Constitución Política es la encargada de realizar en algunos casos el respectivo control previo y generalmente control posterior a toda la

creación de leyes, no siendo suficiente porque aun así la tendencia en alzada es la creación de un "derecho penal de expansión" o "inflación penal" o "ley hipertrófica penal", basada en la noción de que el derecho penal es la solución para todos los males es inevitable, es parte de nuestro estandarte humano, "panpenalismo", todas estas definiciones del Doctor (Pastor, 2006), profesor de la Universidad de Buenos Aires.

Para la satisfacción de este trabajo investigativo se ha encontrado suficiente información del tratamiento legislativo que se aplica en los países de Latinoamérica frente a este delito informático, apoyándonos en particular una excelentísima investigación realizada por el abogado Argentino, Doctor (M. Temperini, 2011), especialista profesional e investigador del área de los delitos informáticos, doctor en derecho publicando la tesis *"La regulación de los delitos informáticos en Argentina en relación a los estándares internacionales de la lucha contra el cibercrimen"*. Esta investigación permite conocer a groso modo gran parte de las legislaciones Latinoamericanas vigentes en materia sustantiva, en la que también se observa un detallado análisis estadístico que muestra el porcentaje aproximado de la capacidad jurídica que tienen cada uno de los países estudiados para contrarrestar la vulneración de derechos en el uso de los sistemas informáticos y el manejo de los datos. (M. G. I. Temperini, 2013)

Inicialmente encontraremos la **Tabla No. 1.** "*Cuadro de derecho comparado sobre delitos informáticos en Latinoamérica"* que indica de forma general y sustantiva las legislaciones vigentes en cada uno de los países que poseen sanción penal de los delitos informáticos más comunes internacionalmente (*Accesos abusivos a sistemas informáticos en este caso en particular*) y donde se extracta un breve resumen de lo reglado en algunas de esas leyes.

En la **Tabla No. 2.** *"Estadísticas que expresan el nivel de sanción penal de los delitos analizados, por país"* observaremos dentro del derecho comparado, el porcentaje de sanción penal que existe en los países Latinoamericanos, destacando a Colombia con un gran porcentaje en regulación contra los "delitos informáticos" (75%), posicionándolo como unos de los países Latinoamericanos que más regulación penal tiene para este tipo de delitos, por encima de países como Brasil, Chile, Ecuador, entre otros, información que obtuvo el doctor Temperini utilizando la biblioteca digital del Departamento de Cooperación Jurídica, dependiente de la Secretaría de Asuntos Jurídicos, de la Organización de los Estados Americanos, en la cual existe una sección dedicada exclusivamente al estudio de los delitos cibernéticos y, adicionalmente, consultando en cada uno de los países Latinoamericanos la normatividad específica existente en los códigos penales vigentes, debido que en algunos casos, aunque no encontró legislación especial o reforma legal direccionada al tratamiento de los delitos contra los sistemas de información y el manejo de los datos, el doctor Temperini observó que estos delitos son sancionados utilizando los tipos penales "clásicos".

Cabe anotar que también se consultó otras fuentes de información, encontrando un estudio realizado por dos ingenieros de la Universidad UNAD que optaron para el título de

Especialistas en Seguridad Informática, exponiendo las falencias que ellos observaron desde su campo de estudio de la ingeniería de Sistemas, indicando lo que existe dentro de la legislación colombiana para regular los delitos informáticos, en conformidad con los lineamientos establecidos en el convenio de ciberdelicuencia y realizando un estudio comparativo con seis países de Latinoamérica: Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela, estudio que realizaron con el fin de contribuir con ideas que permitan formular proyectos de ley, con miras a fortalecer la legislación actual y lograr una mejor *"defensa y preservación integral de los sistemas informáticos en contra de los ciberdelincuentes".* (Bolaños & Narvaez, 2014)

Recordemos que apenas a comienzos del siglo XXI fue motivo de discusión en el ámbito internacional el tema de los ataques contra la información y el manejo de los datos, mejor conocido como la ciberdelicuencia, reuniéndose en Budapest los países miembros de la ONU con el fin de poder acordar la manera en que se iba a contrarrestar esa creciente amenaza producto del muy acelerado desarrollo tecnológico que estaba presentándose sin frontera alguna en la mayoría de los países, con resultados hasta ese momento negativos frente a las actividades que realizaban para poder detener dichos ataques, razón por la cual se definió que esos actos se constituirían como delitos informáticos dentro de las distintas legislaciones a nivel mundial. En la monografía denominada: "Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica" pudimos conocer que la fuente utilizada en la convención de Budapest para el tratamiento de los delitos informáticos fue una serie de tratados europeos Nº 185 (Consejo de Europa, 2001a), convenio sobre la ciberdelincuencia, firmado el 23 de julio de 2004, y fue adoptado por 43 países de acuerdo a los datos estadísticos del Concilio de Europa, encontrándose entre los últimos países Panamá y Turquía, comenzando vigencia a finales del año 2014. Es relevante indicar que aunque Colombia ya empezó una responsable tarea por contrarrestar los delitos informáticos, reforzando toda su regulación legal al respecto, hasta la fecha no ha ratificado adhesión al Convenio, pero sí se encuentra dentro del listado de los países que están interesados en pertenecer.

Añade el Doctor Temperini que el objetivo de la Convención al recurrir con la colaboración internacional no fue otra que poder establecer en la mayoría de las legislaciones de todo el mundo, la tipificación y la judicialización de las conductas lesivas que atentan contra los medios informáticos y de comunicación, creando un modelo casi internacional, obviamente respetando las legislaciones locales de cada Estado-Nación, razón por la cual podemos observar en su investigación que el desarrollo legislativo frente a este tema difiere respecto de la cantidad de delitos informáticos tipificados en cada Estado-Nación. Dentro de esta investigación resalta el notable avance de la legislación Colombiana creando la Ley 1273 de 2009, la cual estableció sanciones penales para conductas que no estaban tipificadas anteriormente o al menos que no habían alcanzado el nivel de intensidad en la región para ser considerados como ataques informáticos especiales, encontrando que dentro de esta ley estaban configurados cerca de 10 conductas penales relativas a los delitos informáticos que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y contra los sistemas informáticos, un margen que le pareció bastante alto

comparándolos con los países que gozan de mayor desarrollo legislativo teniendo hasta 15 figuras penales dentro de sus regulaciones.

Resalta el doctor Temperini la importancia de establecer una regulación de los delitos informáticos, necesariamente de forma universal para ser aplicadas en todas las legislaciones del mundo, debido a que los grupos delincuenciales informáticos buscan normalmente organizar sus ataques desde los países en los que existe poca o nula legislación en la materia o si bien ya la tienen, los sistemas de detección y persecución no son muy avanzados o adecuados para lograr contrarrestar a este tipo de avanzado delincuente cibernético.

A continuación se muestra los delitos informáticos contemplados en el Convenio de Budapest, de tal forma que podemos inferir de aquellos cuántos fueron acogidos en la Ley 1273 de 2009, reconociendo que los delitos que atentan contra la integridad de los datos y del acceso ilícito a medios informáticos fueron acogidos en su totalidad, así como el delito contra la pornografía infantil, obviamente por la importancia del bien jurídico protegido:

"El Convenio de Ciberdelincuencia define los Delitos Informáticos distribuidos en cuatro (4) grupos, así:

Artículo 1 no se menciona porque en este hace referencia a un glosario de términos,

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.
Art. 2: Acceso ilícito
Art. 3: Interceptación ilícita
Art. 4: Interferencia en los datos (ataques contra la integridad de los datos)
Art. 5: Interferencia en el sistema (ataques contra la integridad del sistema)
Art. 6: Abuso de los dispositivos (equipos)

Delitos informáticos.
Art. 7: Falsedad informática
Art. 8: Estafa informática

Delitos relacionados con el contenido.
Art. 9: Delitos informáticos relacionados con la pornografía infantil

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.
Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines." (Consejo de Europa, 2001b)

Lo que nos lleva a deducir que tanto los artículos 269A y 269F de la Ley 1273 de 2009, también son producto o consecuencias de regulaciones internacionales integradas dentro de nuestra normatividad penal. Observemos, entonces, los cuadros comparativos ya

mencionados dentro de este estudio del doctor Temperini:

Tabla No. 1. "*Cuadro de derecho comparado sobre delitos informáticos en Latinoamérica".*

País	***Legislación***	***Características generales***
Argentina	*Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)*	*Conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000), pero fue modificado por la Ley 26.388.*
Bolivia	*Código Penal, Ley 1.768 (1997), Ley 3325 (2006)*	*La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.*
Brasil	*Ley 12.737 (2012)*	*La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. (…)*
Chile	*Ley 19.223 (1993)*	*La Ley 19.223 es una ley "Relativa a Delitos Informáticos" de acuerdo a su propio título, donde regula cuatro artículos, desde los cuales se tipifican varios delitos informáticos. (…)*
Colombia	*Ley 1.273 (2009), Ley*	*La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la*

	1366 (2009)	*información y de los datos",…* con *una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles se realicen utilizando medios informáticos, electrónicos o telemáticos".*
Costa Rica	*Ley 9.048 (2012)*	*La Ley 9048 es una modificación importante del Código Penal de este país. Inicialmente reforma los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley No 4573. Por otro lado adiciona el inciso 6) al artículo 229 y un artículo 229 ter. Finalmente modifica la sección VIII del título VII del Código Penal, titulándolo "Delitos informáticos y conexos", donde regula desde el art. 230 hasta el art. 236. En esta modificación bastante integral agrega una importante cantidad de delitos informáticos al Código Penal, desde los más tradicionales hasta algunos más modernos como la Suplantación de Identidad (art. 230) o el espionaje cibernético (art. 231).*
Cuba	*Resolución 204/96, Resolución 6/96, Decreto Ley 199/99, Ley de Soberanía Nacional*	*En este país se ha podido acceder a la Resolución 204/96, la cual dispone el Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos, junto a la Resolución 6/96 que pone en vigor el Reglamento sobre la Seguridad informática, con medidas establecidas para la protección y la seguridad del Secreto Estatal… Si bien no existe legislación específica para delitos informáticos se han encontrado distintas posturas en la doctrina. Por un lado, se opina sobre la necesidad de regulación especial en la materia y, por otro, se considera que por la forma en que están redactados algunos delitos y por la filosofía del Código cubano de sancionar por los valores atacados y por los medios empleados, los tipos penales ya existentes son aplicables.*
Ecuador	*Ley No. 67/2002 (2002)*	*La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "De las infracciones informáticas", el Art. 57 afirma que "se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas*

		al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.
El Salvador	*Decreto 1030 / 1997 (1997)*	*No se ha encontrado legislación específica en la materia. No obstante, posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos, se pueden mencionar los artículos siguientes: 172, 185, 186, 190, 208 No.2, 216, 222 No. 2, 228, 230, 231 y 302 del Código Penal de El Salvador.*
Guatemala	*Código Penal*	*Dentro del Código Penal posee el Capítulo VII, titulado "De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos". Allí incorpora distintos artículos penales para las figuras de los delitos informáticos, en especial desde el artículo 274 inc. A hasta el inciso G.*
Haití	-	*No se ha encontrado legislación sobre la materia.*
Honduras	*Código Penal; Decreto 144/83*	*Si bien no se ha encontrado legislación especial en la materia, sí posee la adaptación de ciertos delitos clásicos a las nuevas modalidades informáticas. Entre ellos podremos encontrar los artículos 214, 215, 223 y 254. Por otro lado, el Decreto 144/83 incorpora algunos delitos para tipificar la pornografía infantil a través del Art. 149 y sus incisos al Código Penal.*
México	*Reforma 75 del Código Penal Federal (1999)*	*Mediante reformas se crearon en el Código Penal Federal, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden, o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.*
Nicaragua	-	*No se ha encontrado legislación sobre la materia.*
Panamá	*Código Penal y sus reformas;*	*No se ha encontrado legislación especial en la materia. No obstante, posee la adaptación de ciertos delitos*

	Ley 51 (2008)	*clásicos a las nuevas modalidades informáticas. Entre ellos pueden citarse los artículos 162 a 165, 180, 184, 185, 220, 237, 260, 283 a 286 y 421. Adicionalmente posee la Ley 51/2008 de Firma Electrónica, en la cual se regula penalmente sobre la falsificación de documentos.*
Paraguay	*Código Penal – Ley 1.160 (1997), Ley 2.861*	*No se ha encontrado legislación especial referida a la materia. Sin embargo, a partir de distintas reformas al Código Penal Paraguayo, se han adaptado algunos delitos para la posibilidad de comisión a través de las nuevas tecnologías y en otros casos se ha incorporado tipos penales específicos (como el caso del Art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.*
Perú	*Ley 27.309 (2000), Ley 28.251 (2004)*	*La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del Art. 183-A. Además, Perú posee la Ley 28.493 (2005) que regula el uso del correo electrónico no solicitado (SPAM), sin embargo en la misma no incluye ningún tipo de sanción penal.*
Puerto Rico	*Ley 146/2012 (Código Penal) + Ley de Espionaje Cibernético 1165 (2008)*	*No se ha encontrado legislación especial al respecto. Sin embargo, Puerto Rico ha optado por la modificación de los tipos penales clásicos, a fin de adaptarlos para su comisión a través de las nuevas tecnologías. Por otro lado, a través de la Ley de Espionaje Cibernético No 1165/2008 si se han incorporado algunos delitos penales especiales para estas figuras relacionados con el espionaje.*
República Dominicana	*Ley No 53-07 (2007)*	*Posee una Ley Especial contra Crímenes y Delitos de Alta Tecnología. Dicha norma regula una parte general, conteniendo algunos principios y conceptos y posteriormente tipifica los delitos informáticos según el bien jurídico afectado. Además, incluye un capítulo dedicado al aspecto procesal penal, así como en la*

		propia normativa genera un órgano encargado de la recepción de denuncias, investigación y persecución de los delitos informáticos.
Uruguay	*Ley 18.600 (2009), Ley 17.520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009)*	*Si bien no se ha encontrado legislación especial en la materia, se han encontrado diferentes normativas parcialmente aplicables a la materia. El Art. 7 de la Ley 17.815 afirma que "constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.", permitiendo así la aplicación de los tipos clásicos del CP. (…)*
Venezuela	*Gaceta Oficial No 37.313 (2001)*	*Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.*

Fuente: Autores

Tabla No. 2. ***"****Estadísticas que expresan el nivel de sanción penal de los delitos analizados, por país".*

País	**%**	**País**	**%**
Puerto Rico	100%	Uruguay	63%
República Dominicana	100%	Brasil	63%
Venezuela	100%	Chile	63%
Argentina	88%	Ecuador	63%
Costa Rica	88%	Perú	63%
Panamá	88%	El Salvador	63%
Paraguay	88%	Bolivia	50%
Colombia	75%	Guatemala	50%
México	75%	Honduras	50%
	Cuba	0%	
	Haití	0%	
	Nicaragua	0%	

Fuente: Autores

CAPÍTULO IV

4. CASOS HIPOTÉTICOS FRENTE A UN ACCESO A SISTEMA INFORMÁTICO Y VIOLACIÓN DE DATOS PERSONALES

Para culminar con esta investigación se propone exponer de forma casuística una de las tantas investigaciones penales que pueden tenerse dentro de la Fiscalía General de la Nación, de tal forma que podamos llegar a entender desde que se instaura una denuncia como es el desarrollo investigativo que se surte para proteger y hacer valer los derechos de las víctimas, que exigen de nuestro Estado–Nación, buscando el eficaz acceso a la justicia, con la posibilidad de encontrar la verdad de lo ocurrido, al igual que obtener su respectiva reparación.

Es menester entonces, explicar de manera breve y concisa todo el marco legal sobre el que se erige y fundamenta todo el procedimiento investigativo penal que realiza la Fiscalía General de la Nación, para llevar a cabo tanto la persecución penal como su posterior ejercicio de la acción penal ante los Jueces Constitucionales. También es importante resaltar que en este capítulo, al igual que en los anteriores, explicaremos varios conceptos que son de uso constante en nuestra cotidianidad, ya sea como profesionales del derecho o como simples espectadores de los acontecimientos rutinarios que vivimos dentro de nuestra sociedad, observados con frecuencia a través de diferentes medios de comunicación, por lo que muy seguramente llegaremos a entender fácilmente los conceptos de: víctima, denuncia, proceso penal, Juez, Fiscal, Defensor, investigador, procedimiento penal, programa metodológico, prueba, entre otros.

Para efectos del debido cumplimiento de la protección de datos establecido en la Ley 1581 de 2012 se han modificado los nombres de los intervinientes, así como los datos que corresponden a fechas y a sitios de ubicación:

4.1. Antecedentes

Del líbelo de la denuncia y la información allegada a la Fiscalía se tiene que:

El pasado 20 de mayo de 2016 se acerca a las instalaciones de la Fiscalía General de la Nación – Sala de denuncias, la señora Paola Arteaga, con el fin de instaurar denuncia penal en contra del señor Marcelo Benítez, manifestando que anteriormente sostuvo una relación sentimental con él por un periodo bastante corto, aproximadamente seis meses, la cual culminó hace un poco más de dos años, pero que mientras que mantuvieron esa relación, el señor Benítez tuvo acceso a su correo electrónico y a su cuenta del Facebook, debido a que un día utilizó su computador portátil, donde siempre mantenía abierta dichas páginas electrónicas, situación que aprovechó el señor Benítez para cambiarle las claves de acceso a dichas páginas electrónicas, impidiéndole poder volver a tener el control de sus

propias cuentas de Facebook y de Hotmail. De igual forma, los comportamientos del señor Benítez se tornaron un tanto violentos, enviándole mensajes ofensivos por WhatsApp, comportamientos por los que ella optó por no prestarle ningún interés.

Continua su relato la señora Arteaga, informando que el domingo diez (10) de abril en horas de la noche llamaron al teléfono de su mamá, una mujer que preguntó por ella y le dijo a su mamá que ella se estaba metiendo con el esposo de ella, pasando la señora Arteaga inmediatamente al teléfono, donde la señora manifestó que era la esposa del señor Carlos De la Torre y pidiéndole que, por favor, dejara de meterse con su esposo y su familia, razón por la cual ella le manifestó que no tenía contacto con el señor Carlos de la Torre, pero que de acuerdo a lo que le manifestaba aquella señora pudo darse cuenta que se trataba de un señor que había visto una vez en un almacén de motos de la marca AKT hacía como un año atrás, cuando fue a comprar una moto, pero que después de ese día nunca más había vuelto a saber de él y, seguidamente, la señora que la llamó le colgó.

Al día siguiente, lunes 11 de abril, fue una señora a la clínica donde ella trabajaba, la señora Angélica Astudillo, acompañando al señor Carlos De la Torre, a quien reconoció inmediatamente, pidiéndole que les regalara unos minutos para dialogar acerca del conflicto que se estaba suscitando entre él y su esposa. Acto seguido, le muestra unos mensajes de Facebook que llevaba impresos, en los que aparecía el nombre de la denunciante y de la víctima, en los que supuestamente sostienen una conversación entre ellos dos, observando la señora Arteaga que dichas conversaciones eran del perfil de Facebook que desde hace dos años había perdido su domino y manejo por culpa de su anterior pareja, perfil que no pudo recuperar, por los ya mencionados actos delictivos del señor Benítez cuando arbitrariamente y sin autorización alguna uso el computador de ella, accedió a sus páginas sociales abiertas en ese momento y decidió cambiar las claves de ambas páginas electrónicas de uso privado, para así quitarle el dominio a la señora Arteaga, obviamente quedando el señor Benítez con el control total de estas.

Indica la denunciante que el problema llegó a una dimensión muy preocupante porque su expareja sentimental estaba suplantando su identidad personal, haciéndose pasar por ella con fines delictivos, como era vulnerar el derecho de otras personas con las cuales no tenía ningún tipo de contacto o relación. De tal forma que inmediatamente se dirigen todos a la última residencia que conocía del señor Benítez, pero no se encontraba en la casa, por lo que decidieron hablar con la mamá y sus dos hermanas, Fernanda y Andrea, y ellas llamaron muy angustiadas al señor Benítez, pidiéndole la mamá que se fuera inmediatamente a la casa para aclarar la situación, aunque él pidió que la pasaran al teléfono, diciéndole que lo demandaran con pruebas porque si no él la iba demandar por falso testimonio.

Por último, manifiesta la denunciante que cuando logró terminar esa traumática relación sentimental con el señor Benítez, de forma abusiva, le reportó su celular como robado, por lo que se lo bloquearon y ella tuvo necesariamente que comprar una *simcard* con otro número celular, pero que los ataques no terminaron allí, ya que él seguía

llamándola a insultarla, no se explica cómo se localizó su nuevo número celular, lo que la obligó nuevamente a cambiar de número celular y eso le tornó más agresivo, ya que continuó sus insultos escribiéndole al número celular de su mamá y de su hermana, con mensajes bastantes ofensivos hacia ella, obviamente, mensajes que provenían desde un número celular que no lo vinculaban directamente, pero que por el contenido de los mensajes era evidente que él los enviaba.

Por lo anterior, la denunciante requiere de la Fiscalía para que intervenga y se logren proteger sus derechos y los de su familia, de tal forma que cesen los constantes ataques de su expareja, que se haga justicia, haciendo pagar al señor Benítez por sus múltiples agresiones.

4.2. Desarrollo de la investigación

Luego de instaurar la respectiva denuncia, procede a un reparto automático asignado por intermedio de un sistema electrónico, que de forma aleatoria carga aun despacho Fiscal destacado para atender el delito tipificado inicialmente por el servidor público que recepcionó la denuncia y a quien el sistema le genera una noticia criminal: (Fiscalia General de la Nación, 2009b) en un formato denominado "Formato único de noticia criminal", la cual se identifica con un numero de 21 dígitos que de forma secuencial y lógico suministra el sistema electrónico, así:

7	6	0	0	1	6	0	0	0	1	9	3	2	0	1	7	0	0	0	0	0
Dpto.		Mpio.			Ent.		U. Receptora					Año				Consecutivo				

Siendo que para el Valle del Cauca encontramos asignado el número 76, número que encabezará todos los radicados que se elaboren en las actuaciones administrativas y judiciales de orden departamental; el siguiente número corresponde al municipio y para la ciudad de Cali observamos que se encuentra asignado el número 001; el siguiente corresponde a la entidad que elabora el documento, en este caso la Fiscalía General de la Nación, en algunos casos estas denuncias las recepciona la Policía Nacional; continúa con el número de la sede que recepciona la denuncia, ya que dentro de las Direcciones de Fiscalía de todo el territorio Nacional, se cuenta con varias sedes para dicho fin. Cali cuenta con aproximadamente seis sedes ubicadas dentro del perímetro urbano; observamos a continuación el año en que se instaura la denuncia y, por último, el número secuencial consecutivo.

En efecto, el servidor público que tiene la función de elaborar la noticia criminal proveída de la denuncia manifestada por la víctima, fuente formal o en ocasiones por fuentes no formales, está investido con las funciones de policía judicial, para lo cual su actuación está regulada por la anteriormente mencionada (Ley 906, 2004), más conocida como Código de Procedimiento Penal, que a partir del artículo 200 y subsiguientes

determina cuáles son las facultades y las obligaciones cuando se le pone en conocimiento de los hechos motivos de investigación.

Bajo este derrotero, el siguiente paso corre por cuenta del Fiscal asignado(a), quien después de la lectura de los hechos junto con los elementos allegados en la carpeta estudiara el caso, proyectando una teoría del caso, "*La teoría del caso es el planteamiento metodológico que cada una de las partes deberá realizar desde el primer momento en que han tomado conocimiento de los hechos, con el fin de proporcionar un significado u orientación a los hechos, normas jurídicas ya sean sustantivas o procesales, así como el material probatorio, que se ha recabado"* (Cesarez & Guillén, 2008), que no es más que una herramienta jurídica de gran importancia para lograr efectivamente el desarrollo tanto de la investigación como del proceso penal que se lleve a cabo, la cual conducirá a elaborar el correspondiente programa metodológico, en reunión con su policía judicial, que buscara construir esa teoría del caso a probar.

Observamos este concepto muy bien explicado en el articulo "La teoría del caso frente al derecho de defensa en sistema acusatorio colombiano" donde los abogados Harold Rodríguez León y Ángelo Giovanny Rondón Garzón, aducen: *"La teoría del caso sirve, por tanto, y debe ser cuidadosamente estudiada, atendiendo a su utilidad para estructurar sistemáticamente el proceso penal y monitorear cada etapa del juicio, con el fin de construir una historia persuasiva y relevante dentro de cada etapa del proceso penal, como son planear y organizar la alegación inicial que contiene la presentación del tema, la narración de los hechos, las pruebas que sustentarán la teoría y se practicaran en el juicio y lo que logrará probarse."* (Rodríguez & Rondon, 2012)

En efecto, el programa metodológico es el instrumento con el cual se proyecta la actividad investigativa a desarrollar por parte de la Policía Judicial bajo la coordinación y la dirección del Fiscal, siendo este la herramienta legal regulada dentro específicamente en el Código de Procedimiento Penal, (Ley 906, 2004) mediante la cual se estudia toda la información inicial y se identifican, clasifican, priorizan, planean y ordenan los actos de indagación tendientes a determinar si existió o no la conducta de la cual se tuvo noticia, indicando si se enmarca o se tipifica más allá de toda duda razonable conforme a nuestra legislación Penal, dentro de las características del delito denunciado frente a la(s) persona(s) indicada(s), o en el caso de ser indeterminada(s) en estado averiguatorio, buscar la forma de poder individualizar o de identificar a su(s) autor(es) y partícipe(s). Igualmente es el medio más expedito e idóneo para establecer las estrategias investigativas, con el fin de obtener información que permita acceder a elementos materiales probatorios requerido, de tal forma que se proceda a la formulación de imputación de cargos dentro del ejercicio de la acción penal que la Fiscalía General de la Nación está facultada y obligada constitucionalmente a realizar, buscando que se sancione más allá de toda duda razonable aquellas conductas reprochables en toda la legislación penal o, por el contrario, si de todas las actividades investigativas no resultan esos elementos materiales probatorios suficientes que permiten a la fiscalía inferir mínimamente que existió la conducta antijurídica de los

hechos denunciados, el Fiscal procederá a ordenar el archivo o la preclusión de dicha investigación.(Fiscalia General de la Nación, 2009a)

En atención a los hechos denunciados por la señora Paola Arteaga, el Fiscal asignado al caso, realiza la correspondiente reunión inicial con la policía judicial adscrita al despacho Fiscal, en la que establecen las estrategias investigativas que permitan obtener un resultado jurídico penal positivo, de acuerdo con los hechos informados por la víctima y el denunciante, dentro del cual se planteó una hipótesis delictiva, que busca precisar la ocurrencia de las conductas punibles denunciadas, Acceso Abusivo a un Sistema Informático y Violación de Datos Personales, artículos 269A y 269F contenidos en el Título VII BIS del Código Penal (Ley 599 de 2000) **"De la protección de la información y de los datos"**, modificado por la Ley 1273 de 2909, Capítulo I: **"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos",** partiendo de las premisas que el indiciado o investigado, señor Benítez, accedió sin ningún consentimiento ni autorización al computador de la señora Arteaga y, además, de forma abusiva y sin previo acuerdo accedió y manipuló un sistema informático protegido con una medida de seguridad, denominado clave, manteniéndose dentro de este en contra de la voluntad de quien tiene el legítimo derecho a excluirlo, pero que aparte de esto de manera ilícita modificó las claves de acceso y uso dicho medio electrónico para enviar ilícitamente mensajes ofensivos a terceros, para provecho propio del agresor. Véase, pues, que frente a esta teoría del caso planteado por el Fiscal se programan una serie de actividades de policía judicial, con el fin de obtener resultados en la investigación que le permita determinar si efectivamente lo fáctico de la denuncia constituye o no delito, si aun así le asiste responsabilidad penal al investigado, logrando reunir los elementos materiales probatorios necesarios para inferir más allá de toda duda razonable el cumplimiento de los verbos rectores que establece la norma infringida, de tal manera que le permita a Fiscalía ejercer la acción penal y lograr la respectiva judicialización y sanción del procesado.

4.3. Actividades judiciales ordenadas por el fiscal

1. Entrevistar a la víctima y denunciante, señora Paola Arteaga, para que se le permita una ampliación de denuncia, se especifique:
    a. Tiene ubicación, dirección de contacto física o electrónica del denunciado
    b. Si tiene fotos donde se pueda individualizar al denunciado
2. Entrevistar a los testigos de los hechos, la señora Angélica Astudillo y el señor Carlos De la Torre.
3. Interrogar al indiciado Marcelo Benítez en compañía de abogado(a) defensor(a).
4. Realizar solicitud de medida de protección para la denunciante y víctima, tanto en su sitio de trabajo como en su residencia, que garanticen las medidas necesarias de atención y protección para la misma y el núcleo familiar que reside con ella.
5. Solicitar a la Registraduría de Estado Civil la tarjeta web decadactilar del denunciado.

6. Realizar arraigo e individualización del investigado, en su dirección de ubicación, residencia o laboral.
7. Solicitar a la empresa Facebook, los datos biográficos y direcciones IP utilizadas en los años 2014, 2015 y 2016, al igual que la ubicación geográfica de dichas direcciones.
8. En caso de llegar a obtener por parte de la denunciante o denunciado la dirección electrónica del investigado, mediante la autorización de Juez de Control de Garantías (Ley 906, 2004), se ordena obtener los datos biográficos de dicha dirección y las IP utilizadas en los año 2014, 2015 y 2016, al igual que la ubicación geográfica de dichas direcciones: (Fiscalia General de la Nación, 2009a) (p.30)
9. Informar pertinente a este despacho Fiscal sobre nuevas solicitudes que se requirieran para el desarrollo de la presente investigación y recaudo efectivo de los elementos materiales probatorios del caso. (Fiscalia General de la Nación, 2009a) (p 30).

4.4. Resultados obtenidos de las actividades realizadas por la Policía Judicial

En efecto, dentro del tiempo ordenado por el Fiscal para el cumplimiento de las órdenes entregadas a la Policía Judicial, la cual contempló un tiempo máximo de 60 días, el grupo de Delitos Informáticos del Cuerpo Técnico de Investigación - C.T.I., en cabeza de su investigador líder dentro del caso investigado, entregó los correspondientes informes de las labores de campo y de laboratorio, en los que se puede observar los siguiente:

1. La denunciante aporta fotos del denunciado y la dirección electrónica de la página de Facebook que logró conseguir del mismo por intermedio de un amigo en común, en la cual el policía judicial logró observar sin ningún restricción el perfil de nombre M Beni Djmix, coincidiendo la foto de perfil a simple vista con las fotos aportadas por la denunciante y donde se pudo observar la siguiente información de dicho perfil, así: (Ley 1581, 2012)

   Empleo:
   - Alcaldía de Tuluá
     Desarrollador de *software*

   Formación académica
   - Universidad Nacional
     Ingeniería de Sistemas de Información, Grado: 2012

   Información de contacto
   - Celular: 310 436 4665
   - Facebook: / M.Beni.Djmix
   - Instagram: MarBenDjmix
   - Correo electrónico: Marcelodjmix@yahoo.es

   Información de contacto
   - Fecha de nacimiento: 5 de abril

Otros nombres:

- Otro: M. Benítez
- Otro: The King

El Fiscal logra ajustar su teoría del caso con esta preliminar información, teniendo como un elemento subjetivo probatorio la calidad del investigado, quien es una persona profesional en el manejo de medios informáticos electrónicos, idoneidad que debe ser verificada mediante solicitud de búsqueda selectiva en bases de datos privadas, solicitando a la Universidad Nacional el respectivo certificado de grado, al igual que se requiere confirmar por parte del operador los datos biográficos de la línea celular que observó en dicho perfil e igualmente elevando solicitud a la Alcaldía de Tuluá para que suministren información laboral del aquí investigado. Por tal motivo, el Fiscal del Caso, solicita nuevamente ante Juez de Control de Garantías orden que permita requerir a estas instituciones la información pertinente dentro del recaudo probatorio que se adelanta por parte del Despacho Fiscal.

Sin embargo, continúan estudiando los otros informes de Policía Judicial, observando que los datos biográficos de la pagina Facebook: / M.Beni.Djmix, aportada por la denunciante en su ampliación de denuncia, corresponden al indiciado Marcelo Benítez, además, se aportó en dicho informe la Consultad en página web de la tarjeta decadactilar de la Registraduría Nacional del Estado Civil, observando a simple vista la similitud de la foto comparada con las que aportó la denunciante y las que se aportan como anexo en el Informe de Policía Judicial, las cuales fueron extraídas del perfil de Facebook del investigado (se recuerda que por políticas de Facebook, esas imágenes son de uso público).

En cuanto a las direcciones IP utilizadas para acceder a la página de Facebook de la denunciante en los años 2015 y 2016, comparadas con las direcciones IP usadas para acceder al perfil de Facebook del investigado dentro de los mismos años, se observa que usaron tres direcciones IP coincidentes en ambos perfiles, razón por la cual el Fiscal infirió que ambas páginas sociales han sido manipuladas desde el mismo computador con la misma red de internet, motivo por el cual dentro de la solicitud de Búsqueda Selectiva en Bases de Datos Privadas, referida en el parágrafo anterior, el Fiscal también solicitó los datos biográficos de las tres direcciones IP observadas de forma coincidentes dentro del informe mencionado, obteniendo como respuesta por parte de los operador de telefonía e internet de Claro, que dicha dirección pertenece al cliente de nombre Marcelo Benítez, indicando número de contrato, dirección de residencia, fecha de apertura del servicio y otros; y por parte del operador de telefonía e internet de Emcali, que pertenece a la Alcaldía de Tuluá.

4.5. Elementos materiales probatorios recaudados dentro del programa metodológico

En efecto, el Fiscal, en una última reunión con su Policía Judicial, organiza toda la información, evidencia física y, en general, todos los elementos de conocimiento que se lograron recaudar en el desarrollo de la investigación, que no solamente han ayudado a soportar la teoría del caso establecida desde los inicios de la investigación, sino que también permitirá a la Fiscalía General de la Nación poder solicitar con vocación de éxito, la correspondiente formulación de imputación de cargos, por los delitos tipificados, recordemos: Acceso Abusivo a un Sistema Informático y Violación de Datos Personales, artículos 269A y 269F, pretendiendo obtener en contra del investigado la respectiva condena sancionatoria, que establece pena de prisión de 48 a 96 meses y, de esta forma, lograr el restablecimiento del derecho de la denunciante y víctima, (Ley 906, 2004) proceso que se adelantará primeramente ante un Juez Penal Municipal con Funciones de Control de Garantías y posteriormente ante el Juez Penal Municipal con Funciones de Conocimiento. (Corte Constitucional Sentencia C-591/05, 2005).

Para finalizar, debemos de tener en cuenta que de acuerdo a acto legislativo 03 de 2002, todas las pruebas deben ser practicadas en Juicio Oral, ante la inminente presencia de las partes, Fiscalía y Defensa con el cien por ciento de la atención del Juez de conocimiento, quien de forma inmediata y concentrada deberá practicar todas las pruebas que alleguen las partes al proceso penal en la etapa de juicio, que buscan demostrar las pretensiones de cada sujeto procesal. (Corte Constitucional Sentencia C-591/05, 2005).

Para culminar es necesario mencionar que en conformidad con el parágrafo 2 del artículo 250 de la Constitución Política de Colombia, el pasado 12 de julio de 2017 entró en vigencia la Ley 1826 de 2017 de enero 12 de 2017, *"Por medio de la cual se establece un procedimiento penal especial abreviado y se regula la figura del acusador privado"*, permitiendo a un abogado o representante de víctimas particular y de confianza, más conocido como acusador privado, en representación de su poderdante, llamase víctima, ejercer todo este proceso investigativo explicado anteriormente y llevar a cabo su respectivo ejercicio de la acción penal, hasta este año facultad exclusiva de la Fiscalía General de la Nación, en conformidad con lo establecido en la Constitución Política de 1991 en su artículo 250 parágrafo 2, con el fin de lograr dentro de dicho proceso penal, la verdad, justicia y reparación de la víctima que represente, debido a que dentro de la referida ley, se incluyó toda la normatividad que regula los Delitos Informáticos contenidos en el Título VII BIS del Código Penal (Ley 599 de 2000, 2000) "De la protección de la información y de los datos", modificado por la (Ley 1273, 2009), por el cual se adicionó el Capítulo I: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos" y el capítulo II: "De los atentados informáticos y otras infracciones". (Ley 1826, 2017).

CONCLUSIONES

El gran interés abarcado en esta investigación radica en conocer, de forma precisa y clara, la importancia que ha tenido el desarrollo de la legislación colombiana para la judicialización e impartición de justicia adecuada, en concordancia con nuestros valores y estándares sociales, así como con los esquemas investigativos de persecución penal, encaminadas a proteger las conductas humanas en la continua interacción con los medios tecnológicos de la comunicación, permitiéndonos entender la gran importancia que tiene haber creado y acogido una legislación específica en contra de los delitos informáticos, contando hoy por hoy con la Ley 1273 de 2009 y observamos a lo largo de esta investigación como esta ley se convirtió en una herramienta eficaz para hacerle frente a los constantes ataques cibernéticos que se presentan en las redes sociales, que en la actualidad ha venido ganando muchos usuarios de todas las edades, principalmente los más jóvenes y vulnerables.

Resaltemos tres aspectos importantes de esta ley creada para proteger la información y los datos: primero que fue propuesta y desarrollada por un grupo interdisciplinario de profesionales destacados por sus amplios conocimientos constitucionales, tal es el caso del doctor Alexander Díaz García, quien en ese momento se desempeñaba como Juez Constitucional con Funciones de Control de Garantías, acompañado del doctor Jarvey Rincón Díaz, quienes con mucho esfuerzo emprendieron tan ardua tarea logrando felizmente cosechar los frutos esperados; como segundo aspecto, observamos la extensa tipificación creada o nominada para la protección de la información y los datos dentro de la Ley 1273 de 2009; y como tercer punto, indudablemente recae sobre la autonomía que se le dio a este campo de los delitos informáticos, obteniendo dentro de la Legislación Penal un Titulo aparte, independiente, dentro de la Parte Especial del Código Penal o Ley 599 de 2000, y en consecuencia creó dentro de los entes investigadores y Acusador, llámese Policía Nacional, C.T.I., Fiscalía General de la Nación, a crear unidades especiales, con Fiscales destacados para contrarrestar estos delitos, en aplicación de la Ley 1273 de 2009.

Ante la evidente falta de cultura informática en nuestra sociedad por múltiples razones, entre ellas el desmesurado y rápido avance tecnológico y de la internet en tan poco tiempo, ha dado lugar en gran parte a la proliferación de estos delitos informáticos, debido a que es un campo donde subyacen muchos incautos e inexpertos en el manejo de estas tecnologías, y si a eso le sumamos la falta de preparación en las organizaciones o instituciones llamadas hacerle frente a dicha problemática, resulta necesario que cada día más se propongan investigaciones jurídicas concernientes a fortalecer la investigación y correcta judicialización de los autores y participes de vulnerar los derechos jurídicos de los múltiples usuarios de estas redes sociales, lo que resulta ser un verdadero reto para la sociedad y el Estado, para los administradores de justicia, Jueces, Fiscales, Defensores, Ministerio Publico, investigadores y demás intervinientes en este proceso, quienes debemos

estar bien preparados tanto en el conocimiento de la Ley y la jurisprudencia, ya que resulta en ocasiones una tarea difícil lograr una correcta tipificación de estos delitos, así como del apropiado conocimiento de los avances tecnológicos informáticos y sus constantes innovaciones delictivas.

BIBLIOGRAFÍA

Acurio, S. (n.d.). Delitos informaticos: generalidades. Jalisco: Universidad de Guadalajara. Retrieved from http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arzuaga, T., & Guevara, L. E. (2013). *La Ley 1273 de 2009 y los delitos informáticos en Santiago de Cali*. Universidad de San Buenaventura. Retrieved from http://bibliotecadigital.usb.edu.co/bitstream/10819/1891/1/la Ley1273_Delitos Informaticos_Santiago de Cali_Arzuaga_2013..pdf

Benavides, L. B., Hernández, M. I., & León, K. K. (2004). *La penalización de los delitos informáticos en el Salvador*. Universidad el Salvador. Retrieved from http://ri.ues.edu.sv/8179/1/LA PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS EN.pdf

Bolaños, A., & Narvaez, T. de J. (2014). *Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica*. Universidad Nacial abierta y a distancia "UNAD." Retrieved from http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2656/1/59830899.pdf

Bonavides, P., & Pastor, D. (2012). Neopunitivismo o cuarta velocidad del derecho penal delante de los derechos humanos de los ciudadanos Meire Jany Lopes de Souza * mn Resumen Abstract ef El presente artículo trata de demostrar lo que se entiende por neo- Surgimiento de la sociedad y la ne. *Nuevos Paradigmas de Las Ciencias Sociales Latinoamericanas*, *III*(5), 53–74. Retrieved from http://www.ilae.edu.co/Publicaciones/files/04. Lopez Neopunitivismo.pdf

Calle, S. B. (2009). Apuntes jurídicos sobre la proteccion de datos personales a la luz de la actual norma de habeas data en Colombia. *Precedente - Anuario Juriíico*, 219–238. https://doi.org/https://doi.org/10.18046/prec.v0.1459

Carranza, E. A. (2009). El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica. *IUS. Revista Del Instituto de Ciencias Jurídicas de Puebla A.C.*, (23), 174–213. Retrieved from http://148.215.2.11/articulo.oa?id=293222963009

Cesarez, O. F., & Guillén, G. (2008). Teoría del caso en el sistema penal acusatorio. México: s.p. Retrieved from http://www.juridicaformativa.uson.mx/memorias/v_coloquio/doc/derechoconstitucional/CAZAREZ_OLGA_Y_GERMAN_GUILLEN.pdf

Clarke, A. C. (1945). Historia de las telecomunicaciones. Retrieved March 16, 2016, from https://www.uv.es/hertz/hertz/Docencia/teoria/Historia.pdf

Consejo de Europa. (2001a). Convenio sobre la ciberdelincuencia. *Serie de Tratados Europeos*, (185), 26. https://doi.org/BOE-A-2012-5403

Consejo de Europa. (2001b). Convenio sobre la ciberdelincuencia. *Serie de Tratados Europeos*, (185), 26. https://doi.org/BOE-A-2012-5403

Corte Constitucional Sentencia C-334/10. Corte Constitucional. Sala Plena de la Corte

Constitucional. (12 de mayo de 2010) Sentencia C-334/10 - Expediente D-7915.[MP Juan Carlos Henao Perez], Corte Constitucional República de Colombia § (2010). Colombia. Retrieved from http://www.corteconstitucional.gov.co/RELATORIA/2010/C-334-10.htm

Corte Constitucional Sentencia C-591/05. Corte Constitucional (9 de junio de 2005) Sentencia C-591 de 2005 - Expediente D-5415.[MP Clara Inés Vargas Hernández] (2005). Colombia. Retrieved from http://www.corteconstitucional.gov.co/relatoria/2005/c-591-05.htm

Corte Constitucional Sentencia Sentencia T-916/08. Corte Constitucional (18 de septiembre de 2008) Sentencia T-916/08 - T-1817308.[MP Clara Inés Vargas Hernández] (2008). Colombia. Retrieved from http://www.corteconstitucional.gov.co/relatoria/2008/T-916-08.htm

Corte Constitucional Sentencia T-696/96. Corte Constitucional (5 de diciembre de 1996) Sentencia T-696/96 - T-105948.[MP Fabio Moron Díaz] (1996). Colombia. Retrieved from http://www.corteconstitucional.gov.co/relatoria/1996/T-696-96.htm

Corte Constitucional, Sala Plena de la Corte Constitucional, Sentencia C-913/10, E. D.-8057. Corte Constitucional, Sala Plena de la Corte Constitucional. (16 de noviembre de 2010) Sentencia C-913 de 2010, Expediente D-8057 [MP Nilson Pinilla Pinilla (2010). Retrieved from http://www.corteconstitucional.gov.co/RELATORIA/2010/C-913-10.htm

Corte Constitucional, Sala Plena de la Corte Suprema de Justicial, S. C.-540/12. Corte Constitucional, Sala Plena de la Corte Suprema de Justicia. (2012) Sentencia C-540 de 2012, [MP María Victoria Calle Correa] (2012). Colombia. Retrieved from http://www.corteconstitucional.gov.co/RELATORIA/2012/C-540-12.htm

David, J., & Arbeláez, R. (2011a). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Retrieved from http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delitos en las Redes Sociales.pdf

David, J., & Arbeláez, R. (2011b). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación.

Diario el Pais. (2015a, June). Delitos informáticos se han incrementado un 100% en Cali. *El Pais*.

Diario el Pais. (2015b, June 18). Delitos informáticos se han incrementado un 100% en Cali. *El Pais*. Retrieved from http://www.elpais.com.co/judicial/delitos-informaticos-se-han-incrementado-un-100-en-cali.html]

Diaz, A. (2012a). Observatorio Iberoamericano de Protección de Datos. Retrieved March 15, 2016, from http://oiprodat.com/alexander-diaz-garcia

Diaz, A. (2012b). Observatorio Iberoamericano de Protección de Datos.

Díaz, A. (2014). *Apuntes de derecho informático*. Bogotá: Casa Editorial Vélez.

Fiscalia General de la Nación. (2009a). Manual de Procedimientos de Fiscalía en el Sistema Penal Acusatorio Colombiano. Bogotá: Fiscalia General de la Nación. Retrieved from https://www.fiscalia.gov.co/colombia/wp-content/uploads/2012/03/spoa.pdf

Fiscalia General de la Nación. (2009b). Manual policia judicial. Bogotá: Fiscalia General de la Nación. Retrieved from

http://agenciabk.net/POLICIA.JUDICIAL.COLOMBIA.pdf
González, R. (2010). Reseña de “Tecnologías de la información y la comunicación, sociedad y educación. Sociedad, e-herramientas, profesorado y alumnado” de Víctor Manuel Amar. *RUSC. Universities and Knowledge Society Journal*, *7*(2), 1–4. Retrieved from http://www.redalyc.org/articulo.oa?id=78016225018
Grisales P., G. S. (2009). *Análisis dogmático de las conductas de Hurto por medios informáticos y semejantes (Art. 269i) y Transferencia no consentida de activos (Art. 269j) Ley 1273 de 2009*. Universidad Eafit, Medellín. Retrieved from https://repository.eafit.edu.co/bitstream/handle/10784/1285/GrisalesPerez_GiovanniSaltin_2013.pdf?sequen
Guevara, L. E., & Arzuaga, T. S. (2012). Los delitos del nuevo siglo: los delitos informáticos *. *Ciencias Humanas*, *9*(1), 129. Retrieved from http://revistas.usb.edu.co/index.php/CienciasHumanas/article/view/1747/1521
Hernández, L. (2009). El delito informático. *Revista Eguzkilore*, (23), 238. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=3343365
Hütt H., H. (2012). Las redes sociales: una nueva herramienta de difusión. *Reflexiones*, *91*(2), 121–128. Retrieved from http://www.redalyc.org/articulo.oa?id=72923962008
Ley 1273. Congreso de Colombia. (5 de enero de 2009) Ley de protección de información de datos. [Ley 1273 de 2009]. DO: 47.223. (2009). Colombia: Diario Oficial. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
Ley 1288. Congreso de la República de Colombia. (5 de marzo de 2009) (2009). Colombia. Retrieved from file:///D:/Usuarios/66817944/Downloads/ley128805032009(1).pdf
Ley 1581. Congreso de Colombia. (17 de octubre de 2012) Ley de protección de información de datos. [Ley 1581 de 2012]. DO: 45.587. (2012). Colombia. Retrieved from http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
Ley 1826. Congreso de Colombia. (12 de enero de 2017). Penal especial abreviado y se regula la figura del acusador privado[Ley 1826 de 2017]. DO: 50.114 (2017). Colombia. Retrieved from http://es.presidencia.gov.co/normativa/normativa/LEY 1826 DEL 12 DE ENERO DE 2017.pdf
Ley 599 de 2000. Congreso de Colombia. Código Penal (24 de julio de 2000). [Ley 599 de 2000]. DO: 44097 (2000). Colombia: Diario Oficial. Retrieved from https://www.procuraduria.gov.co/guiamp/media/file/Macroproceso Disciplinario/Codigo_Penal_L-599-00.htm
Ley 906. Congreso de Colombia. (31 de agosto de 2004) Ley de protección de información de datos. [Ley 906 de 2004]. DO: 45.658. (2004). Colombia. Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=14787
Marín, V. (2006). Medios de comunicación, educación y realidad. *Comunicar*, *26*, 193–197. Retrieved from http://hdl.handle.net/10272/1276
Marquez, C. P. (2002). *El delito informático: la información y la comunicación en la esfera penal*. Bogotá: Editorial Leyer.
Matus, J. P. (2013). El valor de las certificaciones de adopción e implementación de modelos de prevención de delitos frente a la responsabilidad penal de las personas jurídicas. *Revista de Derecho Penal*, (44), 97–142.

Meek, M. (2013). *Delito informático y cadena de custodia*. Bogotá: Universidad Sergio Arboleda.

Ministerio de Educación Nacional. (2008). *Ser competente en tecnología, ¡Una necesidad para el desarrollo!* Bogotá: Ministerio de Educación Nacional. Retrieved from https://www.mineducacion.gov.co/1621/articles-160915_archivo_pdf.pdf

Muñoz, M. del M., Fragueiro, M. S., & Ayuso, M. J. (2013). La Importancia de las Redes Sociales en el Ámbito Educativo. *Escuela Abierta*, *16*, 91–104. https://doi.org/10.5231/psy.writ.2012.1809

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Computer Crime and Current Legislation in Colombia.*, *11*(28), 41–66. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=59522387&lang=es&site=ehost-live

Pastor, D. (2006). La deriva neopunitivista de organismos y activistas como causa del desprestigio actual de los derechos humanos. Retrieved May 8, 2016, from http://www.juragentium.org/topics/latina/es/pastor.htm

Pérez, L. R. P. (2014). Tecnología e informática de la historia. Resistencias e innovaciones en el uso investigativo y pedagógico de las tics. *Orbis*, (29), 67–93. Retrieved from http://www.revistaorbis.org.ve/pdf/29/art3.pdf

Posada, R. (2013). El delito de acceso abusivo a sistema informático. *Revista de Derecho Penal*, (44).

Rincón, J., & Naranjo, V. (2011). *Delito informático electrónico de las telecomunicaciones y de los derechos de autor y normas complementarias en Colombia*. Cali: Universidad Santiago de Cali.

Rincón, J., & Naranjo, V. (2015a). *El delito en la cibersociedad y la justicia penal internacional*. Universidad Complutense de Madrid.

Rincón, J., & Naranjo, V. (2015b). *El delito en la cibersociedad y la justicia penal internacional*. Universidad Complutense de Madrid. Retrieved from http://eprints.ucm.es/33360/1/T36457.pdf

Rodríguez, H., & Rondon, A. G. (n.d.). La teoría del caso frente al derecho de defensa en sistema acusatorio colombiano. Bogotá: s.p. Retrieved from http://repository.unimilitar.edu.co/bitstream/10654/9325/2/RodriguezLeonHarold2012.pdf

Serrano, M. M. (2007). *El lugar de la teoría de la comunicación entre los saberes*. Madrid: McGraw-Hill, Interamericana España. Retrieved from http://eprints.ucm.es/12980/1/Martin_Serrano_(2007)_Lugar_TC_saberes.pdf

Temperini, M. (2011). Derecho informático y seguridad de la información. Retrieved August 5, 2016, from http://mtemperini.blogspot.com.co/

Temperini, M. G. I. (2013). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte. *1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información*, 12. Retrieved from http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

Velásquez, F. (2007). *Manual de derecho penal. Parte general*. Medellín: Temis.