

**MODALIDADES, PARTICIPACION Y SANCIÓN EN LA COMISION DE DELITOS  
INFORMATICOS EN COLOMBIA A PARTIR DE LA LEY 1273 DE 2009**

**EBERZON MANUEL ORTIZ MUÑOZ  
ABOGADO**

**UNIVERSIDAD LIBRE DE COLOMBIA  
FACULTAD DE DERECHO  
CENTRO DE INVESTIGACIONES SOCIO JURIDICAS  
ESPECIALIZACIÓN EN DERECHO PENAL Y CRIMINOLOGÍA  
PEREIRA - RISARALDA  
2012**

**MODALIDADES, PARTICIPACION Y SANCIÓN EN LA COMISION DE DELITOS  
INFORMATICOS EN COLOMBIA A PARTIR DE LA LEY 1273 DE 2009**

**EBERZON MANUEL ORTIZ MUÑOZ  
ABOGADO**

**Trabajo de grado, para Optar Título de Especialista  
VI Cohorte Especialización en Derecho Penal y Criminología**

**ASESORAMIENTO  
Dr. WALTER GARCIA MORALES  
Dr. JHONIER CARDONA SALAZAR  
Dr. EDGAR AUGUSTO ARANA MONTOYA**

**UNIVERSIDAD LIBRE DE COLOMBIA  
FACULTAD DE DERECHO  
CENTRO DE INVESTIGACIONES SOCIO JURIDICAS  
ESPECIALIZACIÓN EN DERECHO PENAL Y CRIMINOLOGÍA  
PEREIRA - RISARALDA  
2012**

## **DEDICATORIA**

*Una meta que he cumplido en mi vida, la he conseguido, en medio de alegría y esfuerzo por ese motivo tengo la oportunidad de dedicar con mi corazón, éste trabajo a todos y cada uno de los que hicieron parte de ésta gran experiencia:*

*A Dios por darme la oportunidad de existir, y por llenarme cada día con el motor de la sabiduría, por brindarme en cada devenir de la vida, una esperanza nueva, una palabra más, un segundo lleno de experiencias, y por protegerme en los momentos más difíciles, por la inspiración en éste trabajo; a él y solo a él, dedico éste paso por un mundo lleno de ideas, pensamientos, críticas, argumentos razonables; a él, y solo a él, que es mi padre celestial, a quien le doy la gloria infinita.*

*A mi madre Doris Margoth Muñoz, mi reina eterna, la luz de mi inspiración, que con su apoyo incondicional, sus dificultades, su paciencia y sabiduría, es el ser humano más incondicional, sin el cual no hubiera sido posible realizar mis sueños, a ella, que es la persona más importante de mi vida.*

*A mi padre Manuel Ortiz Orozco (Q.E.P.D), quien donde esté, estoy seguro está orgulloso de mí, a quien le aprendí la madurez, la templanza, la fuerza, quien murió queriendo lo mejor para mí.*

*A mis abuelitos Luis Muñoz y Cecilia Bravo, los mejores que Dios les de vida eterna.*

*A mis queridos hermanos Albeiro, Daniel, Viviana, Alejandra, Jhon Fredy, Danilo, y Tatiana; quienes forman una estructura esencial en mi vida, pues la distancia y separación me ayuda a sacrificarme más y más.*

*A todos y cada uno de los que hicieron posible éste sueño.*

**Eberzon Manuel Ortiz Muñoz**

## *AGRADECIMIENTOS*

*A mi padre celestial, poderoso y grande, a DIOS, creador de mi vida, dueño y rey de toda la humanidad, por darme la oportunidad de ser un profesional.*

*A mi madre Doris Margoth Muñoz, por patrocinar esta experiencia y por su apoyo sincero e incondicional.*

*A los profesores, y respetadísimos Doctores, Dr. Walter García Morales, Dr. Jhonier Cardona Salazar, Dr. Edgar Augusto Arana Montoya, por su contundente orientación y asesoría en éste trabajo.*

*A los profesores, directivos, y estudiantes de la Universidad Libre de Colombia que llenaron mi vida de sabiduría, entendimiento y fortaleza, a ellos que fueron parte importante en mi formación académica.*

*Y a todos los que directa e indirectamente rodean mi existencia, gracias y mil gracias.*

*Eberzon Manuel Ortiz Muñoz*

*ACEPTACION:*

**MONOGRAFIA DE GRADO: MODALIDADES, PARTICIPACION Y SANCIÓN EN  
LA COMISION DE DELITOS INFORMATICOS EN COLOMBIA A PARTIR DE LA LEY  
1273 DE 2009.**

*OBSERVACIONES:*

.....  
.....  
.....  
.....  
.....  
.....

*SUSTENTACION: DIA..... MES..... AÑO.....*

*CALIFICACION: .....*



#### DIRECTIVOS NACIONALES:

Dr. Luis Francisco Sierra Reyes..... Presidente Nacional  
Dr. Nicolás Enrique Zuleta Hincapié.....Rector Nacional  
Dra. María Inés Ortiz Barbosa.....Vicepresidenta Nacional  
Dr. Benjamín Ochoa M.....Censor Nacional  
Dr. Pablo Emilio Cruz Samboni.....Secretario Nacional

#### DIRECTIVOS SECCIONALES:

Dr. Jaime Cortés D.....Presidente Seccional  
Dra. Gloria María Atehortua R.....Rectora Seccional  
Dr. Giovanni Arias..... Secretario General  
Dr. William Dávila Arbeláez.....Delegado del Censor  
Dra. Diana Gonzales J.....Decana Faculta de Derecho  
Dr. Fernando Cadavid.....Director Seccional de Invest.  
Dra. Luisa Fernanda Hurtado Castrillon..... Directora Centro de Investigaciones de Derecho

#### INVESTIGADORES ASESORES:

Dr. Walter García Morales  
Dr. Jhonier Cardona Salazar  
Dr. Edgar Augusto Arana Montoya  
CENTRO DE INVESTIGACIONES SOCIO JURÍDICAS

**PEREIRA-2012**

<p><b>¿POR QUÉ EL TEMA ES NOVEDOSO PARA LOS ÁMBITOS ACADÉMICO, JURÍDICO Y DE REGIÓN?</b></p>	<p>Por su aparente ocurrencia en el Derecho Penal.</p>
<p><b>¿CUÁL ES LA PREGUNTA CENTRAL QUE SE PRETENDE DESARROLLAR Y CUÁL SERÍA EL APORTE DE ESTUDIO A LA DISCIPLINA JURÍDICA?</b></p>	<p>¿Cuáles son las modalidades, participación y la sanción en los Delitos Informáticos?</p>
<p><b>ACTUALIDAD DEL TEMA CON RESPECTO A LOS NUEVOS DESARROLLOS DEL CONOCIMIENTO EN EL ÁREA</b></p>	<p>Mostrar una realidad oculta o maquillada en materia de Delitos Informáticos.</p>
<p><b>UTILIDAD PRÁCTICA DEL TEMA</b></p>	<p>Verificar la existencia de situaciones de participación, comisión y sanción en materia de Delitos Informáticos.</p>
<p><b>¿CUÁLES SON LAS FUENTES DE INFORMACIÓN PRIMARIA (EXPERTOS) Y SECUNDARIA (TEÓRICAS Y LEGISLATIVA) QUE SE HAN UTILIZADO EN LA CONSTRUCCIÓN DEL PROYECTO?</b></p>	<p>Los utilizados por los profesionales; tales como normatividad, doctrina, y jurisprudencia.</p>

## CONTENIDO

Pág.

INTRODUCCION .....	10
1. PROPUESTA DE INVESTIGACION .....	12
2. PLANTEAMIENTO DEL PROBLEMA .....	13
2.1. ARTICULACION DE LAS CAUSAS Y SÍNTOMAS DEL PROBLEMA .....	13
2.1.1. Causas.....	13
2.1.2. Síntomas.....	13
2.2. FORMULACION DE LA PREGUNTA .....	13
2.3. SISTEMATIZACION.....	13
3. OBJETIVOS DE LA INVESTIGACION.....	15
3.1. OBJETIVO GENERAL .....	15
3.2. OBJETIVOS ESPECÍFICOS .....	15
4. JUSTIFICACIÓN .....	16
5. ESTRATEGIA METODOLÓGICA .....	18
5.1. TIPO DE INVESTIGACIÓN.....	18
6. MARCO TEORICO.....	20
7. MARCO JURIDICO .....	31
8. CRONOGRAMA.....	32
9. MODALIDADES PARA LA COMISIÓN DE DELITOS INFORMÁTICOS.....	33
9.1. DATOS MALICIOSOS .....	33
9.2. INFILTRACIÓN DE INFORMACIÓN.....	36
10. FORMA DE PARTICIPACIÓN EN LA COMISIÓN DE DELITOS INFORMÁTICOS .....	43
10.1. AUTORÍA EN LA COMISIÓN DE DELITOS INFORMÁTICOS.....	43
10.1.1. Coautoría en la comisión de delitos informáticos. ....	50
10.2. PARTICIPACIÓN EN LA COMISIÓN DE DELITOS INFORMÁTICOS.....	52



10.2.1.	El cómplice en los delitos informáticos. ....	54
10.2.2.	El interviniente en los delitos informáticos. ....	56
11.	SANCIÓN EN LOS DELITOS INFORMÁTICOS .....	58
11.1.	ANTECEDENTES LEGISLATIVOS. ....	58
11.1.1.	Marco Constitucional .....	58
11.1.2.	Marco legal .....	59
11.1.3.	Marco Internacional .....	61
11.1.4.	Ley 1273 de 2009.....	62
12.	CONCLUSIONES .....	68
	BIBLIOGRAFIA.....	70
	GLOSARIO .....	71

## INTRODUCCION

Modalidades, participación y sanción en la comisión de delitos informáticos en Colombia a partir de la ley 1273 de 2009, es un estudio académico de interés actual, basado en planteamientos básicos de informática, técnicas para la materialización de conductas que atentan contra el sistema penal, estudio dirigido con un enfoque autodidáctico, con aplicación en la práctica judicial, respecto de las consecuencias novedosas de la informática y los sistemas en la vida social.

Este es un acercamiento a las modalidades, participación y sanción de los delitos informáticos, en Colombia, tema de gran importancia en la actualidad y de poco conocimiento de los abogados, que afectan la vida social y los derechos fundamentales de las personas.

Se plantea un análisis detenido sobre la materialización en materia de delitos informáticos, la estructuración de las diferentes técnicas para afectar los bienes jurídicos tutelados, la forma de participación en la realización de los tipos penales y termina con un desarrollo de las sanciones penales que consagra la ley 1273 de 2009, en Colombia.

Este trabajo puede resultar una fuente de referencia y actualización, para los juristas y legisladores, quienes en últimas regulan las posibles conductas hipotéticas criminales en que se pueden incurrir los delincuentes con la utilización de los medios tecnológicos, en aras de garantizar los bienes jurídicos paralelos y crear otros más contundentes y así lograr su represión.

Este análisis sobre los delitos informáticos es de gran apoyo intelectual y práctico para quienes están en contacto directo con estas situaciones criminales, además toda la sociedad se ve afectada por el avance tecnológico, toda vez que el aumento de los ciberdelincuentes está en auge, por eso el desarrollo de estos temas académicos.

Finalmente toca temas como la violación de derechos fundamentales, de quienes utilizan estos medios de comunicación, pues existe una amenaza directa de la información y las bases de datos, lo que raya de manera efectiva con una serie de derechos, como lo es la libertad de expresión, el libre desarrollo de la personalidad, la intimidad y los derechos de autoría intelectual, temas que se

encuentran en vilo, por el desarrollo de la informática en nuestra sociedad y de gran acogida a nivel mundial.

## 1. PROPUESTA DE INVESTIGACION

**TEMA:** Delitos Informáticos

### **DEFINICION DEL TEMA:**

**QUE:** Modalidades, participación y sanción en los delitos informáticos

**DONDE:** En Colombia

**CUANDO:** A partir de la ley 1273 de 2009

## **2. PLANTEAMIENTO DEL PROBLEMA**

### **2.1. ARTICULACION DE LAS CAUSAS Y SÍNTOMAS DEL PROBLEMA**

#### **2.1.1. Causas**

- Sin una regulación especial y acorde con los avances tecnológicos, donde los individuos cometen conductas que afectan el normal funcionamiento de la sociedad y su evolución.
- Violación de la información y los datos personales, utilizados con los medio de comunicación.
- Acceso indebido a la información ciberespacial.
- Aumento de delincuencia a través del internet.

#### **2.1.2. Síntomas**

- Regulación de conductas relevantes para el derecho penal.
- Necesidad de proteger los datos personales.
- Limitar el acceso a la información y por contera garantizar derechos fundamentales.
- Contrarrestar la delincuencia a través del internet.

### **2.2. FORMULACION DE LA PREGUNTA**

¿Cuáles son las modalidades, participación y la sanción en los delitos informáticos a partir de la ley 1273 de 2009?

### **2.3. SISTEMATIZACION**

¿Cuáles son las modalidades para la comisión de delitos informáticos a partir de la ley 1273 de 2009?

¿Cuáles son las formas de participación en la comisión de delitos informáticos a partir de la ley 1273 de 2009?

¿Cómo se dieron las sanciones de los delitos a partir de la ley 1273 de 2009?

### **3. OBJETIVOS DE LA INVESTIGACION**

#### **3.1. OBJETIVO GENERAL**

Determinar las modalidades, participación y la sanción en los Delitos Informáticos en Colombia a partir de la ley 1273 de 2009.

#### **3.2. OBJETIVOS ESPECÍFICOS**

- Determinar las modalidades para la comisión de Delitos Informáticos, a partir de la ley 1273 de 2009.
- Establecer la forma de participación en la comisión de Delitos Informáticos, a partir de la ley 1273 de 2009.
- Analizar la sanción en los Delitos Informáticos, a partir de la ley 1273 de 2009.

#### 4. JUSTIFICACIÓN

Este tema es de gran ilustración académica, en tanto que su manejo en la actualidad es enorme, hemos visto como ha evolucionado la criminalidad a través de la tecnología y como los delincuentes las utilizan a diario para cometer delitos, es decir estamos frente a un tema de gran importancia para la academia y sobre todo para la sociedad, que va sin frenos, rumbo al conocimiento tecnológico; entonces de ahí parte la evolución continua de este tipo de escritos que pretenden ampliar el conocimiento para contrarrestar la criminalidad cibernauta, dentro de un mundo académico que ilustre las conductas jurídico penales que afectan los bienes jurídicos tutelados.

Dentro de la sociedad este tipo de avances tecnológicos trae consigo, el desarrollo de la tecnología y la implementación al que hacer de los humanos, tanto en su vida personal como profesional; además utilizada para facilitar las relaciones comerciales y espaciales de una sociedad, por ende adelantar un pequeño rastreo de estos aspectos tan importantes que nos están atropellando a diario; serviría de mayor relevancia para las nuevas generaciones y la regulación de la política criminal que debe manejar un estado, la mayoría le huye a este tipo de temas por la falta de conocimiento y por el poco materia formal que existe, pero no podemos ser indiferentes con estos temas que avanzan a pasos de gigante.

La necesidad de adelanta un estudio académico de tanta trascendencia en el país y en el mundo entero, como lo son en la actualidad los delitos informáticos, crea un gran avance en política criminal del estado y por ende el control social que se debe estudiar.

Si bien es cierto, hay pocos escritos, sobre estos temas, uno más, sería de gran ayuda para los lectores y la justicia Colombiana, En cuanto a nuestras debilidades y fortalezas es conveniente trasegar éste tipo de situaciones jurídicas, ya que trae consigo múltiples beneficios académicos, teóricos y prácticos; es por ello, que el estudio es necesario e importante, pues sus implicaciones trascienden las esferas de la epistemología.

Este estudio puede ser utilizado como fuente o referencia para nuestros legisladores, quienes en últimas regulan las posibles conductas hipotéticas criminales en que se pueden incurrir los delincuentes con la utilización de los medios tecnológicos, en aras de garantizar los bienes jurídicos paralelos y crear otros más contundentes y así lograr la represión.



Finalmente, este análisis sobre los delitos informáticos es de gran apoyo intelectual y práctico para quienes están en contacto directo con estas situaciones criminales, además toda la sociedad se ve afectada por el avance tecnológico, toda vez que el aumento de los ciberdelincuentes está en auge.

## **5. ESTRATEGIA METODOLÓGICA**

### **5.1. TIPO DE INVESTIGACIÓN**

De acuerdo a su naturaleza, el estudio que se desarrollara está enmarcado dentro de la modalidad de un proyecto de carácter descriptivo, debido a que está eminentemente orientado a narrar las modalidades, formas de participación y sanciones en materia de delitos informáticos a partir de la entrada de en vigencia de la Ley 1273 de 2009, por lo tanto, se realizará un trabajo de rastreo bibliográfico y jurisprudencial, respecto a estos temas, encaminado a resolver los problemas planteados y dar a conocer diferentes percepciones del alcance de estas conductas Jurídico Penal Relevantes.

En relación a este tipo de conductas se analiza las nuevas percepciones tanto doctrinales como jurisprudenciales referente a la forma de perpetrarlas o consumir sus conductas que por contera deben trascender la esfera del derecho penal, toda vez que el alcance es muy amplio; habida cuenta que estamos frente a la globalización y sistematización de los delitos, ya sea por vías tecnológicas o simplemente de informática, que es utilizada para dañar los bienes jurídicos tutelados de una forma muy particular.

La legislación Colombiana a tratado de compilar y proteger los bienes jurídicos de las personas, a través de leyes que sancionen este tipo de conductas, pero como sabemos, es obvio que por tratarse de situaciones que alteran la sociedad de una forma muy especial, es mucho más complicada su protección, toda vez que las conductas delincuenciales son desplegadas con la utilización de medios externos a éste, que necesariamente obstruyen una verdadera judicialización en metería de delitos informáticos.

Lo anterior, conduce al análisis de varios temas, la forma de cometer este tipo de delitos, la participación en la realización de ellos y como consecuencia la sanción que se les está dando en la actualidad; siendo este un estudio que converge y aflora muchas más situaciones jurídicas en la sociedad, importantes para la política criminal de un estado; entonces lo que se pretende es enfocar los delitos informáticos en la actualidad y el trato que se les está dando; además de encontrar en la jurisprudencia, posibles dicotomías y vacíos respecto de los delitos informáticos.

Este trabajo pretende dirigir sus expectativas a la luz de los derechos humanos y la vulneración de las prerrogativas individuales, tales como: La libertad, la intimidad, la dignidad entre otros derechos fundamentales como base fundamental en su estructura como seres humanos.

El análisis que se realizó con el rastreo normativo y jurisprudencial, está enfocado desde el objeto de estudio y parte de la problemática que nos hemos trazado, de tal manera, las conclusiones que se pretende alcanzar se deriven principalmente de los objetivos generales y específicos.

Por último y para llegar a las conclusiones, hemos reiterado que asumimos un enfoque teórico y de rastreo jurisprudencial y doctrinario, el cual a lo largo del desarrollo del estudio nos permitirá la búsqueda de los datos necesarios que nos conducirán a resolver los objetivos inicialmente planteados.

## 6. MARCO TEORICO

En Colombia se ha venido tratando estudios académicos sobre el tema de delitos informáticos, tema este de gran importancia en la actualidad mundial, en vista y como consecuencia de los problemas sociales que afrontan las redes, la web y por contera la vulneración de los derechos de los usuarios, donde existe una amenaza directa de la información y las bases de datos, lo que raya de manera efectiva con una serie de derechos fundamentales, como lo es la libertad de expresión, el libre desarrollo de la personalidad, la intimidad y los derechos de autoría intelectual, temas que se encuentran en vilo, por el desarrollo de la informática en nuestra sociedad y de gran acogida a nivel mundial. En nuestro país los estudios adelantados respecto de los delitos informáticos es muy reciente y de actualidad, habida cuenta que es uno de los aspectos más importantes por la cual atraviesa la comunidad ciberespacial, máxime cuando la tecnología avanza con pasos de gigante, desbordando por contera los límites de su propio control.

En la actualidad se ha escrito mucho a nivel extranjero en materia de delitos relacionados con la utilización de los medios tecnológicos y su comisión delictiva, utilizado como herramienta u objetivos en el punible; pero en nuestro país, cualquier escrito respecto de estos temas es un avance, pues en la actualidad tenemos vigente la ley 1273 de 2009, que regula los delitos electrónicos en nuestro país, en realidad la utilización de las herramientas tecnológicas como el internet a aumentado la cibercriminalidad, los delincuentes informáticos ha aumentado considerablemente, las plataformas de internet y la bases de datos, son la escena virtual perfecta para desplegar sus conductas criminales.

Lo que tienen preocupado a los países y a sus gobiernos, radica en la constitución de tipos penales que regulen estas conductas criminales, novedosas en la actualidad; claro que la tipificación de estas conductas es un proceso muy arduo, que genera por cierto un estudio sistematizado de la política criminal de un estado y de plantear hipótesis de control social; algunos países han adoptado la creación de normas que limitan el acceso a la web; lo que ha generado como consecuencia la afectación e inobservancia de los derechos fundamentales, de quienes están en permanente contacto con la tecnología; como por ejemplo en Estados Unidos de América con la creación de la ley S.O.P.A<sup>1</sup> o en España con la ley SINDE<sup>2</sup>, leyes encargadas de regular estos temas que no son problemas de nivel local de cada país, sino que por el contrario es un problema que abarca al continente entero;

---

<sup>1</sup> Ley Stop Online Piracy Act, también conocida como HR3261, es un proyecto de ley presentado en la cámara de representantes de estados unidos el 26 de octubre de 2011, por el representante LAMAR SMITH y un grupo bipartidista de 12 copatrocinadores iniciales.

<sup>2</sup> Ley para la protección de los derechos de autor en la internet.

pero estos son temas que apenas están abriendo la ventana de la discusión; lo que nos concierne es analizar ¿qué ha hecho y que está haciendo nuestro país al respecto? ¿Qué tan eficaz es la protección de la información en nuestro país?; bueno efectivamente en Colombia el legislador ha implementado la protección jurídica y material de los derechos informáticos y las bases donde reposan los datos personales, claro que lo importante es la creación de esos bienes jurídicos para poderlos proteger entonces veamos que es un bien jurídico:

A lo largo de la evolución del derecho penal se han distinguido diversos conceptos de bien-jurídico.- en efecto la noción acuñada por Birnbaum a mediados del siglo S. XIX, se refiere a los que son efectivamente protegidos por el derecho; esta concepción, sin embargo, es demasiado abstracta y por ello no cumple con la función delimitadora del *ius puniendi* que persigue un derecho penal de inspiración democrática<sup>3</sup>.

Pero, esta concepción de bienes jurídicos tutelados a cambiado y ha sido tratado por otros doctrinantes de una manera diferente, siempre persiguiendo la protección de los bienes jurídicos de los asociados según Von Liszt, *“bajo una concepción material del bien jurídico, su origen reside en el interés de la vida existente antes del Derecho y surgido de las relaciones sociales. El interés social no se convierte en bien jurídico hasta que no es protegido por el Derecho”*<sup>4</sup>.

Claro que al gobierno local le ha preocupado intensamente las construcción de medidas jurídicas que contrarresten las conductas desviadas de los infotraficantes, máxime cuando es la obligación del mismo estado la efectiva protección de los derechos de sus representados, pero el problema no radica en su reglamentación interna, el problema va mucho más allá, pues es evidente que la tecnología desborda los límites de la globalización y por eso debemos acudir a los estudios adelantados en el extranjero, ahora bien, todos los estudios sobre materia de delincuencia informática ha sido acogida como ejemplo de los demás países, que no solamente tiene la oportunidad, sino que su implementación ha sido desde el oriente, y que por obvias razones son países más desarrollados en estos temas.

Las conductas criminales mediante la utilización de medios de comunicación y el atropellamiento de las bases de datos que suministra un proveedor, es la base fundamental para que exista una serie de conductas que son relevantes para el derecho penal, y de ahí su importancia para el estudio del derecho, sobre la ciberdelincuencia, pues se ha dicho al respecto que:

---

<sup>3</sup> RINCON, Ríos Jarvey, Delitos informáticos, edición Universidad Santiago de Cali, año 2009, pág. 9

<sup>4</sup> *Ibíd.* Pág. 10

*Cada vez más, se hace necesario el respaldo legal como la mejor y más adecuada forma de reprimir y castigar estos delitos, tal como se expondrá en el capítulo de la conveniencia de su incriminación y el sistema más adecuado para Colombia, según su tradición jurídico- legal. Las conductas reprochables, resultan en la mayoría de los casos impunes debido a la inidoneidad de las figuras incriminatorias tradicionales, al no ser castigados dichos comportamientos ilícitos, debido a la carencia de claridad sobre la naturaleza jurídica de los bienes objeto material de los delitos ni del interés jurídico protegido, como se verá en el capítulo de atipicidad relativa de la acción<sup>5</sup>.*

Claro que como bien lo señala Jarvey Rincón Ríos, en su texto primero está la solución en las otras ramas del derecho, pues recordemos que el derecho penal es la ultima ratio, y por eso su mínima intervención debe ser estudiada, además que no solamente es un problema interno sino un factor tecnológico que afecta a toda la comunidad mundial, pues podría decirse que la regulación de la utilización de la información y la web, debería ser estudiada por parte de una organización mundial donde haya representantes de cada país y así generar un reglamentación acorde con el problema social que viven todas las sociedades.

En materia de tecnología, las comunicaciones y por ende las relaciones comerciales hay mejorado considerablemente y su avance trae consigo indudables consecuencias para el control social, en derecho, pues evidentemente los negocios jurídicos y la información en los despachos judiciales, como por ejemplo se están digitalizando, es decir que esto implica para el gobierno en cabeza del ministerio de telecomunicaciones adelantar la regulación sistemática de estos medios; la firma digital también es una nueva figura considerada como una de las herramienta puestas a disposición de los cibercontratantes, como medio de pruebas para perfeccionar sus negocios jurídicos, además de la autenticidad de los correos electrónicos etc.

Entonces, vemos la necesidad de tipificar las conductas que afectan la informática y la base de datos que quedan en las computadoras y las plataformas de los servidores de internet; lo que se ha pretendido es la regulación de las conductas hipotéticas en las que puede incurrir un individuo, conductas que deben ser relevantes para el derecho penal, es así la incorporación de ideas para categorizarlas, y posteriormente castigarlas, siempre que infrinjan la información de manera indebida y afectado interés particulares de otras personas, claro está la afectación de la intimidad virtual de las entidades financieras, gubernamentales,

---

<sup>5</sup> FERNÁNDEZ María Clara, Tesis de Grado Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos, Universidad Sergio Arboleda Escuela de Derecho - Santa Marta 2001.

inclusive de las mismas personas, etc.; figuras que se deben adecuar a un tipo penal creado por el legislador.

Al respecto:

*La cifra negra de la criminalidad, en materia de delitos informáticos, no puede seguir en la penumbra, de allí la necesidad imperiosa para el derecho penal y organismos gubernamentales la investigación de una nueva modalidad comisiva de amplias repercusiones sociales y económicas. Existe una necesidad urgente de incluir en el derecho penal vigente una tipificación básica de los delitos informáticos que afecten el interés social y el patrimonio público. En primer término en lo que concierne a las conductas punibles, sería imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes<sup>6</sup>.*

No es extraño para nadie, que la dinámica de la sociedad y la realidad social a la que se ven expuestos los individuos con la aparición de nuevos instrumentos para la convivencia; tales como la informática y por supuesto las computadoras, instrumentos que han evolucionado, para facilitar los negocios, la economía o simplemente una relación social a través de estos medios de comunicación, porque no son más que eso, unos instrumentos puestos a disposición de la comunidad para mejorar sus relaciones; pero eso no termina aquí, ya que siempre tendrá unas consecuencias en el entorno social; es aquí donde entra el derecho penal para tipificar ciertas conductas en las cuales pueden incurrir los individuos cuando hacen uso inadecuado de estas herramientas, y por supuesto cuando contribuyen una mala utilidad de los sistemas de datos, en fin unas cuantas hipótesis delictivas; es por esto que es fundamental los estudios de este nivel, avanzando y contribuyendo a llenar las penurias de la sociedad en estos temas, tal como lo dice el autor RINCON, Ríos Jarvey, en su texto sobre los delitos informáticos: *“Un bien jurídico nace de la necesidad de protección de ciertos y cambiantes bienes inmanentes a las personas como tales”<sup>7</sup>*; y por ende protegiéndolas a través de una ley o mejor un compendios de normas penales desvaloradas en conductas punibles, y en consecuencia sancionarlas; Por su parte el texto del director de Rincón Ríos es una verdadera aproximación a los problemas que se presentaran en la sociedad por el surgimiento de nuevas tecnologías; por tal razón se ha creado en Colombia un nuevo bien jurídico tutelado llamado **“LA PROTECCIÓN DE LA INFORMACIÓN”**

---

<sup>6</sup> Ibíd.

<sup>7</sup> Ibíd. Pág. 11.

Por otra parte, los tratadistas han hecho una aproximación a lo que se podría denominar delitos informáticos, pues se ha dicho que se clasifican en:

*“a) Las Manipulaciones que una persona realice en las actividades de entrada y salida de información o de datos computarizados; b) El Espionaje económico, teniendo en cuenta que la información se almacena en soportes electromagnéticos, la transferencia de datos de un lugar a otro por cualquier medio sistematizado es lo más usual actualmente este espionaje económico se utiliza por empresas rivales, así como con finalidades políticas por Estados Extranjeros; c) Sabotaje. Se produce daño, destrucción, inutilización en el procesamiento de datos o información automatizada, en programas o software total o parcialmente; y, d) Hurto de tiempo. Tiene cabida en la indebida utilización, sin autorización de equipos computacionales o salas informáticas. Se penaliza el uso indebido y el tiempo de procesamiento de información o de datos perdido por el propietario con las inapropiadas actividades<sup>8</sup>.*

Entre estas posiciones sobre lo que es el delito informático, es importante saber que parte del avance de la humanidad, que ha permitido posicionar a la tecnología como eje central de las actividades cotidianas, cambiando notoriamente la manera de registrar nuestra intelectualidad, esta migración cultural ha traído por supuesto el uso de la Informática como pilar fundamental en el esclarecimiento de conductas delictivas relacionadas con dispositivos digitales; es por esto que, en un estado social y democrático de derecho el interés final es la protección de este tipo de conductas que se han presentado en la actualidad, y además amparado en las condiciones de vida social. Obviamente sin olvidar que el derecho penal debe ser visto como la ultima ratio, es decir que también se puede proteger estas conductas con las demás aristas del derecho.

Por su parte el procedimiento o tratamiento sistematizado de la información o datos personales, está configurado por diferentes fases o etapas: la recolección, selección, almacenamiento, registro, utilización, transmisión, bloqueo y cancelación de datos. El acceso a la información se presenta en las fases de utilización, transmisión, bloqueo y cancelación de datos. Las personas autorizadas para ellos son los titulares de los bancos de datos o ficheros, los administradores, ejecutores o usuarios del sistema. Cuando no es ninguno de ellos o no están autorizados para hacerlo se dice que el acceso a la información es ilegal o abusivo. Ahora bien, para que se configure el delito de intrusión informático en el derecho Colombiano, se requiere además que el sistema informático esté protegido con *medida de seguridad*. Este requisito adicional resulta superfluo, pues se entiende que un sistema informático con o sin medida de seguridad puede

---

<sup>8</sup> ARRUBLA Molina. siguiendo a Tiedemann, profesor del Instituto de Criminología y Derecho Penal de Friburgo (Alemania)



ser objeto de vulneración por medios informáticos<sup>9</sup> y para los depredadores (hackers o Craker) de sistemas informáticos son más atractivos los sistemas con seguridad que los que no la tienen.

En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online supera los 200 millones, comparado con 26 millones en 1995<sup>10</sup>.

A medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, la trata de niños con fines pornográficos<sup>11</sup> entre otros que veremos a lo largo de este trabajo.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en «paraísos informáticos» - o sea, en países que carecen de leyes o experiencia para seguirles la pista<sup>12</sup>.

Según datos recientes del Servicio Secreto de los Estados Unidos, se calcula que los consumidores pierden unos 500 millones de dólares al año debido a los piratas que les roban de las cuentas online sus números de tarjeta de crédito y de llamadas. Dichos números se pueden vender por jugosas sumas de dinero a falsificadores que utilizan programas especiales para codificarlos en bandas magnéticas de tarjetas bancarias y de crédito, señala el Manual de la ONU<sup>13</sup>.

Otros delincuentes de la informática pueden sabotear las computadoras para ganarles ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión. Los delincuentes manipulan los datos o

---

<sup>9</sup> Por informática entendemos la transformación y transferencia de la información a través de las computadoras, con la finalidad de realizar los procedimientos cotidianos de manera más eficiente, sin embargo la UNESCO, ofrece otra definición si se quiere, más amplia, "ciencia que tiene que ver con los sistemas de procesamiento de información y sus implicaciones económicas, políticas y socioculturales. Delitos Informáticos en Colombia; Jarvey Rincón Ríos.

<sup>10</sup> Disponible en la web: <http://www.emagister.com/curso-delitos-informaticos/impacto-delitos-informaticos-impacto-nivel-general>, visto el 14 de junio de 2012.

<sup>11</sup> Disponible en la web: <http://www.wattpad.com/5423587-delitos-inform%C3%A1ticos?p=12>, visto el 14 de junio de 2012.

<sup>12</sup> Disponible en la web: <http://www.un.org/spanish/conferences/Xcongreso/prensa/2088hs.htm>, visto el 14 de junio de 2012.

<sup>13</sup> Disponible en la web: <http://delitosinformaticosndn.blogspot.com/>, visto 16 de junio de 2012.

los computadores, ya sea directamente o mediante los llamados «gusanos» o «virus», que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro. Algunos virus dirigidos contra computadoras elegidas al azar; que originalmente pasaron de una computadora a otra por medio de disquetes «infectados»; también se están propagando últimamente por las redes, con frecuencia camuflados en mensajes electrónicos o en programas «descargados » de la red<sup>14</sup>.

En 1990, se supo por primera vez en Europa de un caso en que se usó a un virus para sonsacar dinero, cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la «cura»<sup>15</sup>.

Los delincuentes cibernéticos al acecho también usan el correo electrónico para enviar mensajes amenazantes especialmente a las mujeres. De acuerdo al libro de Barbará Jenson «Acecho cibernético: delito, represión y responsabilidad personal en el mundo online», publicado en 1996, se calcula que unas 200.000 personas acechan a alguien cada año<sup>16</sup>.

Los delincuentes también han utilizado el correo electrónico y los «chat rooms» o salas de tertulia de la Internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños online y luego concertado citas reales con ellos para explotarlos o secuestrarlos. El Departamento de Justicia de los Estados Unidos dice que se está registrando un incremento de la pedofilia por la Internet<sup>17</sup>.

Además de las incursiones por las páginas particulares de la Red, los delincuentes pueden abrir sus propios sitios para estafar a los clientes o vender mercancías y servicios prohibidos, como armas, drogas, medicamentos sin receta ni regulación y pornografía<sup>18</sup>.

Informa CyberCop que varios autos que se habían anunciado en la página electrónica no se vendieron en ese plazo, pero los dueños no pudieron encontrar a ninguno de los autores del servicio clasificado para que les reembolsaran el

---

<sup>14</sup> Ibíd.

<sup>15</sup> Disponible en la web: <http://www.monografias.com/trabajos6/delin/delin2.shtml>, visto el 18 de junio de 2012.

<sup>16</sup> Ob cit.

<sup>17</sup> Ibíd.

<sup>18</sup> Ibíd.

dinero. Desde entonces, el sitio en la Red de este «servicio» ha sido clausurado<sup>19</sup>.

Por último la naturaleza jurídica sobre el bien tutelado de la informática, hace referencia a tres teorías, según los tratadistas: “primero, se considera que el delito informático representa solo la comisión de otros delitos mediante el uso de computadoras; segundo, se considera que este tipo de delitos tiene un contenido propio, lo que lo lleva a afectar un nuevo bien jurídico tutelado “la información” y por último una corriente considera que el delito debe ser observado desde un punto de vista triple; a) el computador puede ser el objeto de la ofensa, al manipular o dañar la información contenida en él; b) como herramienta, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito tradición; c) como objeto de prueba; así se concluye con la naturaleza del bien jurídico tutelado de la “informática” por tanto el bien jurídico se justifica, puesto que es una categoría límite al poder punitivo del Estado, una protección capaz de impedir arbitrariedades, distorsiones o confusiones en la elaboración de la estructura penal; en consecuencia hoy se reconoce que la función del ordenamiento jurídico-penal, es de más amplio alcance, pues no solamente se limita a asegurar las condiciones fundamentales de la vida en común, sino también a proveer el desarrollo y el mejoramiento de la sociedad, partiendo de las necesidades que se presentan con el manejo de estas nuevas tecnologías”<sup>20</sup>.

En Colombia la ley “Ileras” era una de las aproximaciones que pretendía evitar la violación de derecho de autor, pero como un mecanismo que posiblemente agravaría aun más la situación de las comunicaciones, en tanto que decía:

*Los “castigos” que propone la norma para quienes publiquen contenidos protegidos con derechos de autor y sin permisos generaran muchas inquietudes.*

*Para el caso de una persona que aloja en su blog o página web un material no autorizado y se lucra de él a través de pauta o cobro por su visualización o descarga, podría pagar con cárcel. De aprobarse el proyecto, se incluiría en el artículo 271 del Código Penal este nuevo delito que, según el código, impone una pena de 4 a 8 años de cárcel y multas de 26.66 a 1.000 salarios mínimos para los delitos de violación a los derechos patrimoniales de autor y derechos conexos. Ahora bien, si alguien hace la publicación de un material no autorizado, pero no tiene fines comerciales o de lucro, esa persona “podría asumir eventualmente una responsabilidad civil, pero no penal”, explica Juan Carlos Monroy.*

---

<sup>19</sup> Ibid.

<sup>20</sup> Página 13, Delitos Informáticos en Colombia; Jarvey Rincón Ríos.

*Este punto es tal vez el más polémico y el motivo de preocupación de los jóvenes, en particular de los estudiantes<sup>21</sup>.*

En la actualidad tenemos incluida una reforma al código penal del 2.000, toda vez que se introdujeron algunos tipos penales que pretenden contrarrestar la criminalidad con la utilización de computadoras e internet:

En Colombia, la ley 1273 de enero de 2009, sancionada por el Presidente Álvaro Uribe Vélez, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico denominado 'De la protección de la información y de los datos', se establece que el ciudadano que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP (Protocolo de Internet) diferente, en la creencia de que acceda a su banco o a otro sitio personal o de confianza. En su primer capítulo, la norma dicta medidas penales de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. La norma tiene en cuenta:

\*Acceso abusivo a un sistema informático: habla del acceso parcial o completo a un sistema informático protegido o no con una medida de seguridad.

\*Obstaculización ilegítima de sistema informático o red de telecomunicación: quien obstaculice el normal funcionamiento o acceso a un sistema informático o a una red de telecomunicaciones.

\*Interceptación de datos informáticos: quien sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

\*Daño informático: quien destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

\*Uso de software malicioso: quien distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

---

<sup>21</sup> Disponible en la web, Artículo de la revista semana del 13 de abril del 2011, <http://www.semana.com/nacion/pros-contras-ley-llerias/155071-3.aspx>

\*Violación de datos personales: quien 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. Con esta reglamentación Colombia da un paso muy importante en este tema legal, pero no se debe olvidar que en el mundo de la tecnología hay tanta dinámica, que si con esta modificación del Código Penal no se consideran las posibles nuevas modalidades que van a surgir y se permita que queden sin castigo, este proyecto de ley quedará a medias. Es importante que sea lo suficientemente flexible para poder acoger lo que viene en el futuro del cibercriminalismo. Si no lo es, en poco tiempo quedará obsoleta<sup>22</sup>.

Importante determinar cuáles son los vacíos de la legislación informática en materia de modalidades y participación de las conductas desvaloradas por el legislador por delitos categorizados, en respuesta que dio un periodista sobre la actual ley de información y protección de datos personales, dijo:

***¿Cuáles son los mayores vacíos en la legislación colombiana frente al delito informático?***

*En materia normativa, los mayores vacíos están relacionados con las restricciones generales y abstractas que tiene el Juez para procurar y analizar las diferentes fuentes informáticas que colaborarían en gran medida en emitir una decisión más rápida y justa. Otro aspecto que se ha entendido como “vacío” es la no existencia exhaustiva y taxativa de normas<sup>23</sup>.*

Como medio de prueba, utilización como instrumento, como objetivo donde recae la conducta punible, los delitos informáticos se pueden clasificar de varias formas, entre ellas podemos dividir en criterios de instrumentos o herramientas y también como fin u objeto para la comisión de los ilícitos, la informática es catalogado como una serie de información digitalizada, por ende su ordenación de manera sistematizada tomando como herramienta un ordenador, es decir una maquina conocida como computadora que se encarga de recibir y procesa **datos** para convertirlos en información útil, aquí radica la importancia para el derecho penal y en general para todo el derecho, habida cuenta que la información y las bases de datos es lo principal que se pretende proteger por parte de un gobierno.

La información legalmente obtenida, no puede ser objeto de manipulaciones indebidas, por ejemplo la información privada de una empresa, las bases de datos

---

<sup>22</sup>Uniderecho.comdisponibleen:[http://www.uniderecho.com/leer\\_ley\\_Ley-En-Colombia\\_19\\_1459.html](http://www.uniderecho.com/leer_ley_Ley-En-Colombia_19_1459.html)

<sup>23</sup> GALLARDO, Sara M. Periodista, comunicadora, Universidad Jorge Tadeo Lozano. Disponible en: <http://www.acis.org.co/index.php?id=455>

de las entidades gubernamentales, las cuentas de las personas en redes sociales, los servidores de las empresas e instituciones, aquí radica el derecho a la intimidad y a la reserva, nadie tiene permiso de acceder de manera fraudulenta a manipular los datos e información de nadie, es por ello que se afecta de manera directa algunos aspectos importantes en la sociedad, y raya de manera indirecta con otros derechos como la libertad de expresión y los derechos intelectuales.

Ahora bien, a través de esta indebida apropiación de información, se tipifican una serie de conductas delictivas como lo son, el hurto, la estafa, las amenazas, el constreñimiento ilegal, la extorsión, el sabotaje, la competencia desleal, la injuria, la calumnia, la inducción a la prostitución, el proxenetismo, en fin una serie de conductas punibles que necesitan su propia regulación.

Aquí radican varias cosas, *primero* lo referente a la parte probatorias de las conductas punibles, y *segundo* la participación de las mismas, con distintas modalidades, en efecto hablamos de accesos abusivo a sistemas de información, que podría ser en redes sociales, servidores privados, paginas institucionales, etc.; pero en realidad el problema radica en que la información, puede afectar otros derechos fundamentales como la honra, la vida, la intimidad, y la dignidad humana como eje principal de una estado social y democrático de derecho.

Claro que detrás estos derechos esta la protección de la infamación y los datos personales, es aquí donde ha entrado el estado a intervenir y regular la conductas criminales, como control social dentro de la política criminal actual.

## 7. MARCO JURIDICO

- Artículo 15 de la Constitución Política de Colombia
- Ley 1273 de 2009
- Ley 1288 de 2009
- Ley 1266 de 2008
- ISO 27.000 – 2700, Seguridad de la Información Congreso de Ciberterrorismo de Budapest 2001
- Ley 527 de 99, comercio electrónico, valor probatorio a la evidencia digital.
- Ley 679 de 2001, proveedores de internet

## 8. CRONOGRAMA

Meses	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.
<b>Actividades</b>									
Seleccionar tema de investigación									
Recolección de información									
Elaboración de borradores									
Primera etapa elaboración de Anteproyecto									
Segunda etapa elaboración de anteproyecto									
Tercera etapa elaboración anteproyecto									
Correcciones y ajustes									
Impresión y Sustentación									



## 9. MODALIDADES PARA LA COMISIÓN DE DELITOS INFORMÁTICOS

### 9.1. DATOS MALICIOSOS

Los avances Tecnológicos demuestra la evolución del hombre y su relación con la tierra donde albergan e interrelacionan con el mundo exterior, esto se constata a través de los medios que permiten el almacenamiento, la transmisión y la administración de la información; avances de vital importancia que sencillamente han cambiado la vida diaria de las personas y organizaciones reflejado esto, con el aumento de los negocios y sus actividades; como por ejemplo: en transacciones comerciales (cajeros automáticos, banca virtual), venta y compra de bienes y servicios a través de correos electrónicos, comunicaciones en línea, sistemas de información y almacenamiento, etc., actividades que han permitido mejorar ostensiblemente la relaciones de las personas y la tecnología para su vida diaria; pero así mismo, se han generado una serie de conductas ilícitas que pretenden sacar provechos ilícitos por medio del conocimiento tecnológico lo cual se denomina “**DELITOS INFORMÁTICOS**” generando como consecuencia necesaria la “**CIBERDELINCUENCIA**”.




















Dentro de las nociones de delito informático encontramos entre otros:

***Delito informático**, crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.*

*Existen actividades delictivas que se realizan por medio de estructuras electrónicas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información (borrado, dañado, alteración o supresión de data crédito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía*

*infantil, pedofilia en Internet, violación de información confidencial y muchos otros*<sup>24</sup>.

Encontramos varias modalidades para perpetrar sus cometidos utilizando por contera los conocimientos tecnológicos y las herramientas que la ciencia pone a sus manos, para cometer actividades ilícitas, es decir aprovechando esos medios tecnológicos y conocimientos para afectar la vida social, comercial, laboral de las personas que buscan *a priori* mejorar sus niveles de vida; conductas por si solas reprochadas por la sociedad; los delincuentes buscan varias formas para afectar los bienes jurídicos de las personas, a través de estas nuevas herramientas; a continuación haré un análisis de cada una de las conductas utilizadas por los delincuentes para conculcar derechos, como una nueva forma de cometer delitos; pero antes quisiera recordar que el rastreo es indudablemente de una combinación de términos informáticos con una apreciación de carácter jurídico; máxime cuando se ha convalidado por la ley como delitos informáticos algunas de estas categorías, haciendo una desvaloración de ciertas actividades hipotéticas en las que frecuentemente incurren los delincuentes y finalmente tipificándolas en el Código Penal, a través de la ley 1273 de 2009.

-  Virus.
-  Gusanos.
-  Bomba lógica o cronológica.
-  Infiltración de información. "Data leakage"
-  Carroña. "Scavenging"
-  Martillo. "Hacking"
-  Intercepción. "Eavesdropping"
-  Redondeo. "Round Down"
-  Botnet(IRC – Internet Relay Chat)
-  Acceso no autorizado a servicios y sistemas informáticos.
-  Piratas Informáticos o hackers.
-  Reproducción no autorizada de programas informáticos.
-  Fishing.
-  Hoax.
-  Keylogger.
-  Spyware.
-  Ingeniería Social.
-  Cartas Nigerianas.
-  Grooming.

---

<sup>24</sup> Disponible en la web: <http://johamartinez23.blogspot.com/2010/01/hola-soy-leidy-johana-martinez-y-este..>, visto el 29 de junio de 2012. Artículo sobre delitos virtuales del 19 de julio de 2010.

**Virus:** Denominado técnicamente como malware que se encarga de contaminar los archivos o destruir los programas de una manera inesperada y sin consentimiento de los administradores de sus bases de datos y usuarios; una definición más técnica desde el punto de vista de la informática y la tecnología es:



*Un **virus informático** es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad<sup>25</sup>.*

Por su parte, dentro de los datos maliciosos encontramos **los gusanos** que pueden ser utilizados por los cibernautas encargados de afectar o destruir las bases de datos de manera premeditada y son intención, pero que finalmente son maliciosos y dañinos; sistema éste que pretende dañar o destruir bases de datos; lo que hace este dato es simplemente entrar a los archivos y propagarse causando daños en los computadores y generar bloqueos a las redes informáticas causando verdaderos perjuicios; modalidad que puede ser con dolo o con culpa, habida cuenta que quienes los generan pueden ser autores materiales de estas conductas, pero también puede suceder que otros con negligencia no se percatan de su peligro y los ponen a circular, bien sea por publicidad engañosa o nombre muy llamativos Ej.: “ver quién te ha te ha eliminado del mns” y nombre similares que hacen caer fácilmente a una persona en error; en fin, una descripción mas técnica la encontramos desarrollada de la siguiente forma: “El gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil<sup>26</sup>”.

<sup>25</sup> Disponible en la web descargado el 01 de Jun 2012: [http://es.wikipedia.org/wiki/Virus\\_inform%C3%A1tico](http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico).

<sup>26</sup> *Ibidem*.

Los virus y los gusanos pueden tener las mismas características pero las diferencias ciertas particularidades, pero estos están clasificados dentro de los llamados datos maliciosos.

*El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.*

Finalmente, los efectos los efectos dañinos que traen los gusanos pueden ser lanza virus o lanza gusanos que logran destruir la información que se encuentra en un medio de almacenamiento como un disco duro, se propaga destruyendo recursos tecnológicos.

Todos los anteriores son códigos maliciosos.

**Bomba lógica o cronológica:** Catalogada como una modalidad para destruir las bases de datos lo importante de esta modalidad de delincuencia se basa en la activación a una hora y fecha determinada, para que se consume el daño y como consecuencia la afectación de las bases de datos y la información.

## **9.2. INFILTRACIÓN DE INFORMACIÓN**

Este tipo de modalidad utilizada por la delincuencia, consiste en la posibilidad de conectar en una red un computador instalar un programa y poder observar que información fluye por la misma.

Lo que fluye por la red es igual que la infamación que enviamos por medio de otros sistemas tradicionales como las mensajerías, con las mismas características en el encabezado.

Tratándose de información que viaja por la red, lo que hace el delincuente es atrapar ese contenedor de información y abrirlo, mirarlo, y modificarlo, lo cierra y lo envía a su destinatario, temas que casi no se ve por los sistemas de seguridad actuales utilizados por las empresas; modalidad que puede ser utilizada por un mecanismo llamado Snifer que cumple el siguiente procedimiento afectando de manera directa el tráfico normal de la información en la web y como consecuencia modificándola.

**SNIFER:** *Supone una amenaza grave para la seguridad no sólo de una máquina sino también de toda una red. Gran cantidad de tráfico confidencial viaja en claro, sin ningún tipo de cifrado, por las redes de la mayoría de las empresas. Ese es el entorno ideal para un sniffer, que puede acceder de forma transparente a esa información, y permitir que alguien abuse de su conocimiento. Por eso es muy importante realizar búsquedas periódicas de sniffers dentro de las redes de cualquier empresa, no sólo por el daño que puedan causar, sino también porque encontrarlos es señal de que se ha producido y explotado una grave brecha y hay que tomar medidas inmediatas.*

*Existen casos en los que un sniffer no es peligroso. A veces, explorando una red en busca de sniffers se detectará que hay algunos, por ejemplo, en máquinas que dependen del departamento de administración de redes. Esto puede ocurrir porque, en realidad, un sniffer no se diferencia demasiado de una herramienta de monitorización y diagnóstico del tráfico de red que puede estar siendo legítimamente utilizada por personal encargado de la administración de la red. Otros dispositivos, especialmente routers y hub, suelen producir falsos positivos que hay que tener en cuenta<sup>27</sup>.*

**Carroña:** Basura que se deja en las papelera de reciclaje de un computador que en realidad no se eliminan, pueden ser utilizadas por los delincuentes para recoger información y hace ingeniería criminal, como mirar, nombres, teléfonos y todo tipo de datos que permitan la ideación de la conducta punible, esta es una técnica muy utilizada y que además puede servir para encontrar evidencia digital.

**La Técnica del martillo:** Consiste en golpear, hacer que se caiga un servidor y como consecuencia directa la entrada al sistema; modalidad desplegada principalmente por unos individuos identificados técnicamente en la informática como los Crackers; categoría encargada de entrar a una base de datos, en un gran número de veces y de manera simultánea generando la denegación del servicio; y por ende forjando la caída del sistema, y del servidor; es así como se penetra la información; para contrarrestar esta modalidad existen actualmente las barras de seguridad, para ingresar a una página web, son signos, números, letras

---

<sup>27</sup> Disponible en el siguiente enlace: [http://es.wikipedia.org/wiki/Detecci%C3%B3n\\_de\\_sniffer](http://es.wikipedia.org/wiki/Detecci%C3%B3n_de_sniffer).

que debe escribir el visitante y deben coincidir para permitirle el ingreso, esto con el objeto de detectar, que quien está ingresando es una persona y no se está haciendo a través de computadores; es así como estructura una seguridad, para evitar la vulnerabilidad de las paginas y sus bases de datos.

El artículo 269A del C.P, es un claro ejemplo de esta modalidad de delito, pues al respecto señala que *“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 (...)”*<sup>28</sup>, es así como la técnica del martillo efectivamente se adecua al tipo, cuando se accede sin permiso al sistema protegido con seguridad, para efectuar el daño.

**Técnica interceptación:** Este tipo de modalidad es utilizada por los delincuentes para encontrar contraseñas o información que permita infiltrarse y recoger datos para hurtar cuentas, o simplemente dañar el sistema, es similar a la técnica de la infiltración de la información, pero con el ingrediente de que se atrapa ese contenedor de información, se abre y extrae lo que se interesa, puede ser que por allí este fluyendo la contraseña de una cuenta administradora de un banco, y el ciberdelincuente la utilice para desplegar sus ideas criminales; el artículo 269C, tipifica esta modalidad como delito, la interceptación de datos personales, *“El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión (...)”*<sup>29</sup> en reciente pronunciamiento de la jurisprudencia de la Corte Suprema de Justicia, se condenó a un servidor público por interceptar datos personales, para suministrar información personal a un tercero, valiéndose de su condición de trabajar en la Fiscalía General de la Nación, y tener acceso a las bases de datos, que en este caso presentaría modalidad concursal con la violación de datos personales del Artículo 269F; al respecto dijo:

*3. A través de la Ley 1273 de 2009, el legislador estableció un nuevo bien jurídico “de la protección de la información y de los datos” encaminado a que “se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones...”.*

*4. El artículo 269F “violación de datos personales”, en su aspecto típico contiene un elemento subjetivo que se concreta en la intención de quien indebidamente obtiene el dato, de perseguir un provecho para sí o un tercero, y como elemento*

---

<sup>28</sup> Artículo 269A del Código Penal Colombiano, Ed. Leyer 2009.

<sup>29</sup> Artículo 269F del Código Penal Colombiano, Ed. Leyer 2009.

normativo, la condición de que el autor no se encuentre autorizado para acceder a la información<sup>30</sup>.

Siguiendo lo anterior evidencia que estas modalidades pueden afectar varios tipos penales como el caso de interceptar datos y como consecuencia la violación de los mismos.

**Redondeo “Round Down”:** Es conocida como una de las primeras técnicas empleadas en Colombia, que consiste en logra hacer transacciones por un valor determinado, pero lo que hace el delincuente es desviar valor muy pequeño a su cuenta, lo que sería irrisorio; pero multiplicado ese valor por las miles de transacciones y por varios años, sería una suma muy considerable que evidentemente aumentaría el patrimonio económico de alguien; penalmente una técnica que permite hurtar mucho dinero y que ahora está tipificada en el código penal como una modalidad de delincuencia cibernauta, que protege los datos y la información, esta modalidad es muy complicada de detectar, con las trasferencias que se realizan en los bancos, las consignaciones etc. Que observándolo detenidamente sería capaz de enriquecer a un tercero con el desvío de pequeñas cantidades de dinero; esta modalidad de delincuencia es muy utilizada y se encuentra tipificada como hurto por medios informáticos y semejantes consagrado en el Artículo 269I: *“El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código (...)*”<sup>31</sup>.

En definición encontrada en la web se dice:

#### **Redondeo o técnica del salami**

*Consiste en introducir al programa unas instrucciones para que remita a una cuenta determinada los céntimos de dinero de muchas cuentas corrientes TECNICA ESPECIALIZADA consiste en las cantidades de dinero muy pequeñas se va sacando repetidamente de una cuenta y se transfieren a otra, se realiza muy fácil y es muy difícil de detectar*<sup>32</sup>

**Botnet (IRC-Internet Relay Chat):** Esta modalidad es conocida como ataque de los zombis, modalidad de delito informático que consiste en enviar muchos correos

<sup>30</sup> CORTE SUPREMA DE JUSTICIA, SALA DE CASACIÓN PENAL, M.P. AUGUSTO J. IBÁÑEZ GUZMÁN, APROBADO ACTA No. 189- Proceso nº 36208, Bogotá, D.C., dieciséis (16) de mayo de dos mil doce (2012).

<sup>31</sup> Artículo 269I del Código Penal Colombiano, Ed. Leyer 2009

<sup>32</sup> Disponible en la web: <http://www.buenastareas.com/ensayos/DelitosInformaticos/89422.html>, visto el 18 de junio de 2012.

con un archivo adjunto, que como consecuencia al abrir el documentos, inmediatamente se instala un software malicioso, con el ingrediente que el usuario no tiene un antivirus actualizado, lo que permite que se instale sin ningún problema; y lo que hace el delincuente una vez el software está instalado, es activarlo y ponerlo en uso, sin que se note, lo que por contera puede ser instalado en varios computadores y ponerlos a funcionar al mismo tiempo, atacando un servidor o una página, generando la denegación del servicio, equipo que está siendo utilizado por delincuentes sin que el dueño se percate, podría decirse que es una especie de “autoría mediata”, utilizando a una persona como instrumento, pero lo que pasa en este caso, es que se utilizan varios computadores como instrumentos para perpetrar su ataque y ejecutar la conducta criminal; finalmente estos computadores sirven solo para efectuar los análisis y actos de indagación por parte de la fiscalía y los forenses en delitos informáticos; como es razonable estos dueños de los computadores utilizados por los ciberdelincuetes no tienen ningún tipo de responsabilidad penal.

**Fishing:** Otra modalidad más común y de mayor incidencia en la actualidad que consiste en la suplantación de sitios web, en español traducida “pesca“, modalidad encaminada a enviar de un correo electrónico con la imagen de una entidad financiera, donde se induce en error al usuario con fines engaños para que este facilite o suministre sus datos o los actualice, y finalmente ha sido víctima de un ataque por parte de estos delincuentes que desbancan sus cuentas bancarias sin que estos se percaten que fueron engañados y robados. Ejemplo: la Fiscalía General de la Nación fue víctima de esta modalidad de conducta, donde suplantaron su página de web y vulneraron su lock de seguridad, haciendo incurrir en error y sustrayendo información confidencial y personal, situación que en la actualidad es objeto de investigación por parte de las autoridades y está tipificada en el Artículo 269G del C.P., “El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión (...)”<sup>33</sup>.

**Hoax:** Modalidad, emprendidas para defraudara las personas, utilizando señuelos falso, y aspectos de credibilidad inherentes a las personas, como sus creencias personales, consistente en enviar correos electrónicos con imágenes de situaciones subjetivas que rodeas las creencias de los individuos, como por ejemplo: “envíe este correo y recibirá bendiciones, o dinero por cada reenvió a cambio”; conocidas en la web como las famosas cadenas electrónicas, lo que pretende es alimentar las bases de datos de los delincuentes con las cuentas de correos electrónicos que aparecen en los email enviados, con el objeto de filtrar sus listas de posibles víctimas; se conocen como los “SPAM”, correos no deseados, y lo que hacen es vender las cuentas a entidades de mercadeo; y por

---

<sup>33</sup> Artículo 269G del Código Penal Colombiano, Ed. Leyer 2009



contera los usuarios van a ver, como les llegan correos electrónicos que ofreciéndoles bienes y servicios que ellos nunca han buscado, de aquí que son víctimas de estas ventas de sus cuentas para estos fines, utilizándolas como mercadeo sin su consentimiento.

**Keylogger:** Es un programa que se instala en el computador local, mediante un dispositivo USB, o de forma remota a través de un correo electrónico, se instala y captura todas las pulsaciones que se hagan en un PC; como las contraseñas, de las paginas sociales o contraseñas de las cuentas bancarias, lo que hace es un análisis de los movimientos desplegados por los usuarios y robar sus datos, este tipo de programas denominados como venenosos, lo que hacen es guardad las contraseñas o actividades hechas en un computador y sus actividades en la web, y por ende lo que permite es enviar esta información capturada a un correo electrónico previamente configurado, una vez se logra el cometido, este programa está diseñado para autodestruirse sin dejar rastro. Dentro de sus principales víctimas están las personas que utilizan los medios electrónicos para hacer trasferencias de grandes valores, como puede ser de una persona hasta una entidad financiera; utilizando estos medios con fines ilícitos y hacer trasferencias electrónicas afectando el patrimonio por medio de estas técnicas criminales.

**Cartas nigerianus,** Técnica consistente en enviar un correo electrónico, donde se manifiesta que ha sido el ganador de un premio y que para hacerlo efectivo debe consignar cierta cantidad de dinero, esta técnica es muy frecuente a través de llamadas telefónicas, con un discurso muy fuerte, cargado de artimañas y actos histriónicos que pretenden enredar a sus víctimas y por contera que caigan en error, una especie de estafa por medios electrónicos, que efectivamente terminan entregando contraseñas, dinero, dando información confidencial y posteriormente ser extorsionados, lo que podría generar la configuración de modalidad heterogenia de tipos penales; a través de esta simple técnica, que es utilizada por delincuentes profesionales que previamente han diseñado una estructura criminal, muy bien elaborada.

**Grooming,** Técnica de carácter clandestino, utilizados por delincuentes de delitos sexuales que manipulan la web para hacerse pasar como menores de edad, hablando como tal y engañando a sus víctimas que por lo general son también menores, utilizado artimañas y señuelos hasta que inducen a estos menores hacer actos sexuales a través de los sitios web, o lo que es más grave acordar una cita, para encontrarse de manera física y así satisfacer su cometido.

Finalmente, estas modalidades son las más utilizadas por los delincuentes, a pesar de que existen otras, que pueden ser encajadas en las conductas que actualmente están desvaloradas por el legislador en el Código Penal Colombiano, pero, en la actualidad los estudiosos de estos tipos de delitos han catalogado, las

anteriores modalidades en grandes grupos de conductas ilícitas, al respecto se ha manifestado:

*El delito informático incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos: Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos (Spam), ataque masivos a servidores de Internet y generación de virus. Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc. Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores<sup>34</sup>.*

Después de hacer un acercamiento a las modalidades de los delitos informáticos, encontramos que estos delitos revisten ciertas características, así:

### **CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS**

- *Son conductas criminales de cuello blanco, en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.*
- *Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.*
- *Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.*
- *Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de siete cifras a aquellos que las realizan.*
- *Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.*
- *Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.*
- *Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.*
- *Ofrecen facilidades para su comisión a los menores de edad.*
- *Tienden a proliferar cada vez más, por lo que requieren una urgente regulación<sup>35</sup>.*

---

<sup>34</sup> Disponible en la web: <http://johamartinez23.blogspot.com/2010/01/hola-soy-leidy-johana-martinez-y-este>., visto el 29 de junio de 2012. Artículo sobre delitos virtuales del 19 de julio de 2010.

<sup>35</sup> Disponible en la web: <http://www.angelfire.com/la/LegislaDir/Carac.html>, visto el 03 de julio de 2012.

## **10.FORMA DE PARTICIPACIÓN EN LA COMISIÓN DE DELITOS INFORMÁTICOS**

### **10.1. AUTORÍA EN LA COMISIÓN DE DELITOS INFORMÁTICOS.**

Tratándose de las conductas que pueden incurrir los delincuentes en este tipo de delitos informáticos, el código penal colombiano atiende los postulados de la teoría finalista en materia de autoría y participación, tal como ha sido dividida en los artículos 28, 29 y 30 de la ley 599 de 2000, pues la distinción es fundamental a la hora de realizar la proposición jurídica, en atención a la intervención en sentido amplio, que como se dijo puede ser a título de autor o participe en los delitos tipificados en la ley colombiana; por eso en éste capítulo se hará en primera medida un recuento de éstos de conceptos, que en la vida práctica han tenido un sin número de percepciones, inclusive tratadas por la Corte Suprema de Justicia en varias ocasiones, es decir lo que se pretende es enfatizar en cada una de las modalidades de intervención en las conductas punibles y hacer una relación en materias de Delitos Informáticos, siempre que las existan.

Como se dijo en los artículos 28, 29 y 30, se define de manera escueta quienes pueden ser realizadores de las conductas punibles así:

**ARTICULO 28. CONCURSO DE PERSONAS EN LA CONDUCTA PUNIBLE.** *Concurren en la realización de la conducta punible los autores y los partícipes.*

**ARTICULO 29. AUTORES.** *Es autor quien realice la conducta punible por sí mismo o utilizando a otro como instrumento.*

*Son coautores los que, mediando un acuerdo común, actúan con división del trabajo criminal atendiendo la importancia del aporte.*

*También es autor quien actúa como miembro u órgano de representación autorizado o de hecho de una persona jurídica, de un ente colectivo sin tal atributo, o de una persona natural cuya representación voluntaria se detente, y realiza la conducta punible, aunque los elementos especiales que fundamentan la*

*penalidad de la figura punible respectiva no concurran en él, pero sí en la persona o ente colectivo representado.*

*El autor en sus diversas modalidades incurrirá en la pena prevista para la conducta punible.*

**ARTICULO 30. PARTICIPES.** *Son partícipes el determinador y el cómplice.*

*Quien determine a otro a realizar la conducta antijurídica incurrirá en la pena prevista para la infracción.*

*Quien contribuya a la realización de la conducta antijurídica o preste una ayuda posterior, por concierto previo o concomitante a la misma, incurrirá en la pena prevista para la correspondiente infracción disminuida de una sexta parte a la mitad.*

*Al interviniente que no teniendo las calidades especiales exigidas en el tipo penal concurra en su realización, se le rebajará la pena en una cuarta parte.*

Como es bien sabido, el código divide la realización de las conductas punibles en autores y partícipes; los primeros que pueden ser tanto autor materia o inmediato y autor mediato, también conocido como el hombre de atrás, y como una modalidad de autoría esta la coautoría cuando quienes realizan la conducta punible es un numero plural de personas, aquí habría que distinguir de qué tipo de coautoría se trata si es propia o impropia, según el desarrollo teórico que ha existido por décadas, pero como este trabajo esta ceñido a caracterizar estas modalidades en los delitos informáticos, no se hará un análisis detenido sobre las teorías existentes, pero a lo largo del trabajo se anunciara someramente si lo fuere necesario.

Ahora bien, como se ha tratado por los doctrinantes, la división consiste en si el hecho ilícito se desplegó por un individuo o por varios, se asume la conducta como propia, es decir es autor; pero si por el contrario se actúa con el convencimiento de que participa en un hecho ajeno será simplemente partícipe, es decir será autor quien domina finalmente la comisión del hecho punible, que como se dijo podrá ser autor o coautor dependiendo el número de personas según el caso.

Al respecto la jurisprudencia ha manifestado:

*(...) que si en la ejecución del hecho, a pesar de la intervención de un numero plural de sujetos asume la conducta como propia, es autor, pero si tiene el convencimiento de que participa en un hecho ajeno, solamente será partícipe, por lo tanto será autor quien domina finalmente la realización del delito abarcando las hipótesis de la autoría mediata y coautoría. Frente a la coautoría cada participante realiza, en unión con otros, la conducta típica, previa celebración de un acuerdo en virtud del cual se busca una contribución objetiva en la que cada uno tiene el dominio del hecho de tal manera que la tarea asumida individualmente se torna indispensable para la total realización del plan (...)<sup>36</sup>.*

En materia de delitos informáticos, los ciberdelincuentes podrán ser considerados como tales dependiendo de la forma en que intervengan en la comisión del delito; en primera medida, observaremos la modalidad de autoría inmediata o material en estos delitos y sus diferentes nombres técnicos; que no distorsionan para nada la denominación jurídico penal que se debe dar, a la hora de individualizarlos y hacer la proposición jurídica para que respondan.

Los delincuentes informáticos que pueden participar a título de autor inmediato o material, son los que por propia mano realizan el hecho punible, entre ellos tenemos los llamados **Hackers**; quienes en últimas despliegan la conducta punible por sí mismos y se caracterizan por las habilidades en tecnología, es decir hacen todo por medio de computadores, y dentro de sus preferencias en lo posible se rodean de personas con las mismas características que manejen la misma información, estos delincuentes buscan un reconocimiento en su entorno, por lo general no lo hacen por dinero ni para sí, ni para un tercero.

Dentro de las defunciones de Hackers encontramos la siguiente:

*En informática, un **hacker**<sup>1</sup> es una persona que pertenece a una de estas comunidades o subculturas distintas pero no completamente independientes:*

- Gente apasionada por la *seguridad informática*. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet ("Black hats"). Pero también incluye a aquellos que depuran y arreglan

---

<sup>36</sup> Sentencia 30 de enero de 2008. rad. 23898. M.P. Julio Socha Salamanca.

errores en los sistemas ("White hats") y a los de moral ambigua como son los "Grey hats".

- Una comunidad de entusiastas programadores y diseñadores de sistemas originada en los sesenta alrededor del *Instituto Tecnológico de Massachusetts* (MIT), el *Tech Model Railroad Club* (TMRC) y el *Laboratorio de Inteligencia Artificial del MIT*.<sup>2</sup> Esta comunidad se caracteriza por el lanzamiento del movimiento de *software libre*. La *World Wide Web* e *Internet* en sí misma son creaciones de hackers.<sup>3</sup> El *RFC 1392*<sup>4</sup> amplía este significado como "persona que se disfruta de un conocimiento profundo del funcionamiento interno de un sistema, en particular de computadoras y redes informáticas"
- La *comunidad de aficionados* a la informática doméstica, centrada en el hardware posterior a los setenta y en el software (juegos de ordenador, crackeo de software, la *demoscene*) de entre los ochenta/noventa<sup>37</sup>.

Los delincuentes en este tipo conductas se caracterizan por vulnerar los sistemas de seguridad, y manejar los sistemas con gran propiedad, que como se dijo infringen de manera abusiva el código penal accediendo a sistemas informáticos en Colombia ésta conducta está tipificada como delito; a título de ejemplo encontramos el artículo 269 A:

*ARTÍCULO 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. <Artículo adicionado por el artículo 1 de la Ley 1273 de 2009. El nuevo texto es el siguiente:> 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.*

Como vemos es una conducta que atenta con el bien jurídico de la protección de la informática y de los datos personales; y es realizada por una persona que interviene a título de autor material, directo en la comisión del hecho punible; ahora bien, sería interesante verificar si es viable la comisión en términos de autoría mediata entendida que quien actúa dominando el hecho es el hombre de atrás que utiliza a otro como instrumento para su cometido o si es posible la comisión en la modalidad de coautoría, pero esto será objeto verificación más adelante.

---

<sup>37</sup> Disponible en la web <http://es.wikipedia.org/wiki/Hacker>, visto el 2 de agosto de 2012.

Siguiendo con el tema de la autoría inmediata o material y los denominados ciberdelincuentes encontramos los llamados **Crakers**, otro tipo de delincuente, caracterizados por ser infosociables, también se reúnen con personas de la misma estirpe, pero se encargan de destruir las barras de seguridad de los sistemas y se identifican por ser motivados por dinero o sacar provecho económico con su conducta, lo que en realidad tampoco para la calificación jurídica tiene relevancia jurídica, pues también puede actuar como autor metería o directo.

Una definición que encontramos es la siguiente:

*El término **cracker** (del inglés crack, romper) se utiliza para referirse a las personas que rompen algún sistema de seguridad.<sup>1</sup> Los crackers pueden estar motivados por una multitud de razones, incluyendo fines de lucro, protesta, o por el desafío<sup>38</sup>.*

El ciberpunk es otro reconocido delincuente en metería de delitos informáticos, pues éste tiene una particularidad y es que genera códigos maliciosos, tales como virus, troyanos que pueden ser utilizados para destruir sistemas informáticos, estos también pueden considerarse como autores materiales a pesar de que éste tipo de conductas necesita de la ayuda de otras personas para propagar su conducta delictiva, pero en términos de autoría metería es éste considerado como tal, habida cuenta que a pesar de utilizar a otras personas como instrumentos para hacer efectivo su cometido y utilizando medios informáticos, es en últimas quien realiza la conducta de propia mano.

El ciberpunk se define así:

*Los personajes del cyberpunk clásico son seres marginados, alejados, solitarios, que viven al margen de la sociedad, generalmente en futuros distópicos donde la vida diaria es impactada por el rápido cambio tecnológico, una atmósfera de información computarizada ubicua y la modificación invasiva del cuerpo humano.*

Los infotraficantes son otros tipos de delincuentes que radica en lo mismo afectar la protección de la información y las bases de datos, que el código penal consagra, éste tipo de delincuentes se encarga de manipular información que puede ser íntima o restringida y de venderla al mejor postor.

---

<sup>38</sup> Disponible en la web: <http://es.wikipedia.org/wiki/Cracker>, visto el 7 de agosto de 2012.

Definición encontrada en la web:

### 33). **Infotraficante**

*Actividad: manejo ilegal de la información, amparado en la libertad de expresión.*

*Conocimiento: habilidad tecnológica básica.*

*Motivación: competitividad, intereses de todo tipo, lucro.*

*Socialización: grupos pequeños o personas individuales*

*Cronología: cualquier edad*

*Su visión: lucro, hacer daño, odios<sup>39</sup>.*

Dentro de la modalidad delictiva de este tipo de personas se enmarca en la calidad de autor inmediato o material, es decir la perpetración del hecho ilícito está desplegada de manera directa al ataque de la información que circula por la web o en aparatos informáticos, y por ende la materialización del delito está en cabeza propia; algunos de los tipos penales que señalan esta modalidad pueden estar en los artículos 269 A (Acceso abusivo a un sistema informático), artículo 269 C (Interceptación de datos informáticos), y el artículo 269 F (Violación de datos personales).

Entre otros delincuentes existen los llamados **Piratas Informáticos** y los **Lamers**, los primeros con una gran habilidad en la informática es uno de los más peligrosos, porque su actividad radica en la copia ilegal de software, que causan grandes pérdidas en la industria de la tecnología e informática, al respecto se dice que estos delincuentes tiene varias habilidades:

*La práctica habitual de la copia ilegal de software, tanto en el terreno doméstico como en el ámbito empresarial, ha relegado este término a ciertos personajes con alguna aureola capaces de penetrar en bases de datos de centros clave. Sin embargo, el término alude precisamente a esta práctica no por extendida menos reprobable, que ocasiona cuantiosísimas pérdidas a la industria informática.*

*Aunque la palabra pirata es evocativamente romántica, este apelativo es atribuido a las personas que hacen uso del software creado por terceros, a través de copias obtenidas ilegalmente, vale decir, sin permiso o licencia del autor. Al software no original se le denomina "copia pirata", pero en términos reales y crudos deber llamarse un software robado.*

*La palabra pirata, asociada al uso ilegal del software, fue nombrada por primera vez por William Gates en 1976, en su "Carta abierta a los Hobistas" mediante la*

---

<sup>39</sup>Disponible en la web: <http://bioandres.galeon.com/>, visto el 7 de agosto de 2012.



*cual expresó su protesta debido a que muchos usuarios de computadoras estaban haciendo uso de un software desarrollado por él, sin su autorización. En todo el mundo el uso del software ilegal está sujeto a sanciones y penalidades, que se agravan cuando el pirata se convierte en un comercializador de software copiado ilegalmente para lucrar en beneficio propio. En el Perú la pena por este delito varía de 1 a 4 años de prisión condicional para los usuarios finales y con un máximo de 8 años de prisión efectiva para los comercializadores.*

*ACTIVIDAD: Comercio ilegal.*

*CONOCIMIENTO: Habilidad tecnológica limitada.*

*MOTIVACIÓN: Inconscientes, sin compromiso.*

*SOCIALIZACIÓN: Sólo grupos pequeños.*

*CRONOLOGIA: Cualquier Edad.*

*SU VISIÓN: Diversión, lucro fácil<sup>40</sup>.*

Los Lamers modalidad de delincuentes encargados de descargar programas de la red con el fin de buscar información de datos personales, tales como contraseñas, claves, la defunción de estos delincuentes es:

*Lamer es un anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez considerada un incompetente en una materia, actividad específica o dentro de una comunidad, a pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un lamer. Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender. Un hacker sería el opuesto de un lamer al tener gran cantidad de conocimientos y no presumir de ello<sup>41</sup>.*

*ACTIVIDAD: Una persona que alardea de pirata informático, cracker o hacker y solo intenta utilizar programas de fácil manejo realizados por auténticos hackers, sin obtener los resultados que pretendía; incluso llegando a perjudicarse a él mismo. PARA MAS INFORMACION HAGA CLICK AQUÍ [http://tu.tv/videos/homero-rey-de-la-internet\\_1](http://tu.tv/videos/homero-rey-de-la-internet_1)*

*CONOCIMIENTO: Una persona que realmente se cree ser un entendido o tener grandes conocimientos, siendo en realidad un inepto en la materia.*

*MOTIVACION: Una persona con intención de molestar a los demás usuarios*

---

<sup>40</sup> Disponible en la web: <http://bioandres.galeon.com/>, visto el 8 de agosto de 2012.

*SOCIALIZACION: se mueve en grandes grupos sociales como salas de chat, juegos en línea y descargas P2P.*

*CRONOLOGIA: Cualquier edad.*

*VISION: son personas que creen ser hackers pero no pueden recibir esta "denominación" debido a que utilizan programas creados por otras personas. Frecuentemente insultan a los programadores y se creen los mejores por saber utilizar programas hechos por otros<sup>41</sup>.*

Estos son los ciberdelincuentes mas reconocidos, a pesar de que existen otros con similares formas de atacar la información y las bases de datos, pero inclusive en la países más desarrollados existen estos delincuentes que se caracterizan por realizar sus delitos de forma poco convencional para nosotros, pero con gran expansión en otros países y con un incremento inimaginable que afectan la tranquilidad y buen funcionamiento de los sistemas informáticos y las plataformas que suministran y almacenan información.

En materia de autoría material, estas modalidades son permanentes y con mucha frecuencia en la criminalidad informática, su judicialización en Colombia está enmarcada así, sin embargo no se descarta la modalidad de autoría mediata o la coautoría habida cuenta que es posible que existan estas modalidades.

#### **10.1.1. Coautoría en la comisión de delitos informáticos.**

La coautoría como una modalidad de autoría tiene sus requisitos para que pueda configurarse, pues es un concurso de personas que participan en la comisión del delito, haremos una descripción de esta modalidad en términos generales y sus consideraciones jurídicas tanto legales como doctrinales, y después la relacionaremos con las conductas punibles que afectan la protección de la información y las bases de datos; entonces veamos una definición muy clara:

*COAUTORÍA, es la ejecución de varios conductas punibles por medio de varias personas, que se han concretado sobre el designio criminal (TEORÍA DEL DOMINIO FUNCIONAL), todos asumen el delito como propio, independientemente de que haya distribución de trabajo o no. Según DERECHO PENAL CASUÍSTICO se exige cuatro presupuestos que son, concertación previa, co-dominio funcional, se excluyen las conductas no acordadas, diseño de un plan criminal, principio de*

---

<sup>41</sup> Ibídem.

*ejecución independiente de que se haya consumado o no, imputación recíproca, lo que hace que todos responda por cualquier que cometa el ilícito. Según LECCIONES DE DERECHO PENAL de la UNIVERSIDAD EXTERNADO DE COLOMBIA, se necesitan tres requisitos que son: previo común, división de trabajo e importancia de trabajo. Es importante saber si los intervinientes responde como autor o como participe ya que puede haber un actuar mancomunado, por lo tanto además del acuerdo común que también lo tiene los partícipes es necesario distinguir la IMPUTACIÓN RECÍPROCA, así como actué al autor se le achaca de la misma manera al participe, la división del trabajo es importante para saber de la importancia de cada uno de estos, por lo que en final para ser coautor se necesitan los mismo requisitos que para ser autor, por manera que en tratándose de delitos de infracción de deber o especiales, nadie que no tenga la cualificación o este especialmente vinculado con esa relación de deber puede ser coautor, la contribución del extraneus siempre constituiría participación(...)42.*

En atención a las cibercriminalidad, por medio de la tecnología y con la utilización de medios informáticos, éstas personas pueden cometer delitos con la intervención de varias conductas atendiendo un plan común, asumiendo el hecho ilícito como propio, el caso sería un grupo de crackers que se conciertan para delinquir, como lo puede ser con la técnica del martillo que consiste en golpear, y hacer que se caiga un servidor, como consecuencia directa la entrada al sistema; modalidad desplegada principalmente por varios individuos identificados técnicamente en la informática como los Crackers; categoría encargada de entrar a una base de datos, en un gran número de veces y de manera simultánea generando la denegación del servicio; y por ende forjando la caída del sistema y del servidor; es así como efectivamente existiría en términos de proposición jurídica frente a la modalidad de coautoría, siempre y cuando exista en co-dominio funcional, acuerdo previo, y aporte o división de trabajo, en la realización de la conducta punible.

Entonces es factible que se presente la coautoría en materia de delitos informáticos, habida cuenta que efectivamente pueden haber varias personas en la afectación de la información, lo que sería interesante es la revisión detenida de la coautoría propia o impropia según el caso, atendiendo los postulados del dominio funcional que se desprende de aquellas y su grado de participación en el fin común acordado previamente y su efectiva materialización.

---

<sup>42</sup> DAZA Pérez Mario Felipe, ESTUDIO SOBRE AUTORIA, PARTICIPACION, INTERVINIENTE Y COMUNICABILIDAD DE CIRCUNSTANCIAS, pg. 15.

## 10.2. PARTICIPACIÓN EN LA COMISIÓN DE DELITOS INFORMÁTICOS.

El artículo 30 del Código Penal Colombiano, define al determinador y al cómplice como forma de intervenir en la realización del tipo penal, el determinador es quien instiga a otro a realizar la conducta antijurídica y se sanciona con las misma pena prevista por el tipo penal, mientras que el cómplice es quien presta una ayuda previa, concomitante o posterior a la conducta antijurídica, se le sanciona con una pena reducida en una sexta parte a la mitad.

Se habla en éste artículo de los intervinientes con calidades especiales que por vía legal, según el código penal colombiano (ley 599 de 2000) se encuentra en la categoría de los partícipes, pero por vía jurisprudencial en la actualidad en tratándose de delitos especiales, como lo son contra la administración pública existe un cambio significativo, pues el intervinientes en este tipo de conductas pasa a ser un coautor y será sancionado como tal, siempre que concurra en la comisión del delito, pero también lo pude hacer en calidad de cómplice o determinador, con las consecuentes sanciones y disminuciones; lo que no pasa en los delitos comunes; al respecto la sala penal a reseñado:

*Pero al coautor, pues necesariamente el inciso final tiene como supuesto el concurso de sujetos, que realizando como suyo obviamente el verbo rector del tipo penal especial, no cuente sin embargo con la cualidad que para el sujeto activo demanda la respectiva norma, la pena que le corresponderá será la prevista para la infracción disminuida en una cuarta parte, de conformidad con el inciso final del precitado artículo 30. Así, vr.gr., si con un servidor público, un particular, concurre a apropiarse en provecho suyo o de un tercero de bienes del Estado, la pena que le corresponderá será la del peculado, por conservarse la unidad de imputación, disminuida en una cuarta parte, he ahí el trato diferencial, por no poseer la cualidad exigida para el sujeto activo<sup>43</sup>.*

En materia de delitos informáticos estas figuras, resultan aplicables sin ningún tipo de cuestionamiento, habida cuenta que respecto al determinador éste puede instigar, inducir, influenciar a otra persona para desplegué la conducta criminal, ya puede ser por consejo o mandato, pero finalmente se afecta un bien jurídico, como lo puede ser la información o los datos personales; un ejemplo sería que un hacker aconseje a un principiante para que vulnere un lock de seguridad de una empresa con el fin de que adquiriera reconocimiento en el gremio de los ciberdelincuentes, este sería el caso donde efectivamente se determino a otro para que se produzca

---

<sup>43</sup> CORTE SUPREMA DE JUSTICIA, SALA DE CASACIÓN PENAL, M.P. Dr. CARLOS AUGUSTO GÁLVEZ ARGOTE, Aprobado: Acta No. 78, Proceso No 20704, Bogotá, D.C., ocho (8) de julio de dos mil tres (2.003).

el hecho ilícito; el cual deberá probarse si el inductor logró perpetrar en la psiquis del inducido.

Frente al determinado se dice:

***DETERMINADOR***, llamado autor intelectual, es la persona mediante un mandato, inducción, instigación, consejo, coacción, orden y cualquier otro medio idóneo consigue que otra (autor material), lleve a cabo en forma material y directa una conducta típica mediante (acción u omisión). EL HILO CONDUCTOR ENTRE DETERMINADOR Y DETERMINADO ESTA DADO POR EL CONOCIMIENTO CONCRETO QUE EL SEGUNDO TIENE DE LA ACTIVIDAD DELICTIVA POR REALIZAR, SITUACIÓN QUE LA DISTINGUE DE LA DENOMINADA AUTORIA MEDIATA. El determinador se sirve de tercero para llevarlo a cabo, por lo que no lo realiza de manera directa por eso es que la doctrina lo ha llamado autor intelectual<sup>44</sup>.

Como vemos es factible la modalidad de determinador en la comisión de delitos informáticos, pues no existe incompatibilidad alguna, simplemente que resultaría muy complejo en el plano probatorio su configuración, habida cuenta que por tratarse de un tema muy complejo en materia informática resultaría prudente enmarcarlo como tal, pero a mi juicio sería posible esta modalidad, en vista de que el código penal lo consagra en su parte general.

En la jurisprudencia se ha tratado así:

*El determinador lo ha dicho la corte desde antaño que es la persona que induce, instiga, manda, orden o cualquier medio idóneo, logra que otra realice material y directamente conducta de acción u omisión descrita en un tipo penal, por lo tanto el determinador y el cómplice, pues ninguna de estas personas realiza materialmente la conducta descrita en el tipo, aquel que determina a otro a obrar y el cómplice contribuye a la realización del hecho punible pero ninguno de ellos debe recorrer con su acción u omisión la legal descripción comportamental.*

*La Corte ha distinguido los requisitos para la determinación que son los siguientes: Que el inductor genere en el inducido la definitiva de resolución de cometer un delito o refuerce la idea con efecto resolutorio de la idea preexistente,*

---

<sup>44</sup> Ibidem.

*no basta con realizar la cooperación moral. Debe de realizarse el injusto típico, que al menos alcance la tentativa. Debe de existir un nexo de causalidad entre la acción del inductor y el hecho principal, de manera que es el hecho antijurídico (jurídicamente relevante). Inductor actué con conciencia y voluntad inequívocamente dirigida a producir en el inducido la resolución de cometer el hecho y la ejecución del mismo. Y el instigador debe carecer del dominio del hecho pues este pertenece al autor que lo ejecuta a título propio ya que si aquel despliega una actividad esencial en la ejecución del plan global ya no sería determinante sino verdadero coautor material del injusto típico<sup>45</sup>.*

### **10.2.1. El cómplice en los delitos informáticos.**

Debemos establecer previamente en qué consiste la modalidad de complicidad en el delito, toda vez que como se conoce es la participación previa, concomitante o posterior a la comisión del hecho punible, y que además éste no tiene dominio del hecho, pues su contribución no es necesaria para perpetrar el punible, porque estaríamos frente a otra modalidad, entonces en cómplice si debe tener conocimiento de la realización de la conducta típica y accede a la contribución del delito principal.

Veamos como lo define la doctrina:

**COMPLICIDAD**, es la colaboración delictiva consciente y voluntaria que un tercero realiza al autor de una conducta punible dolosa, para actuar de manera antecedente, concomitante o subsiguiente, obedeciendo a un acuerdo previo, por lo que el cómplice no domina el hecho, el legislador le da menor pena. Elementos. Conocimiento de la contribución en la realización de una conducta punible dolosa, colaboración por acción u omisión, no dominación del hecho, principio de la ejecución del acto para sanción y que se considere delictivo, se consideran tres tipos de complicidad según la doctrina y la jurisprudencia.

**COMPLICIDAD PREVIA O ANTECEDENTE**, cuando es producto o se despliega cuándo la actividad física o intelectualmente se idea con anterioridad de la ejecución. Ejemplo. El médico que le presta su consultorio para que aborten, el amigo que le dice a la otra que se preste para sacar a la víctima para después apuñalearla etc...

---

<sup>45</sup> SENTENCIA FEBRERO 25 DE 2004. RAD. 19866. MP. MARINA PULIDO & JORGE LUIS QUINTERO.

*COMPLICIDAD CONCOMITANTE, se caracteriza por la colaboración que presta el tercero (cómplice) al momento justo de la ejecución de la conducta punible por parte del autor, como es el caso del tipo que le pide a su novia que le pase el revólver para ultimar a la víctima, o en el momento justo del que se viola a una mujer le pido a un compañero que le abra la puerta y le colabore.*

*COMPLICIDAD POSTERIOR O SUBSIGUIENTE, se concreta después del autor haya cometido la conducta punible, como había acordado, sin importar su grado de perfección, este tipo de complicidad suele confundirse con los delitos de favorecimiento y receptación radicando su diferencia en que las dos formas de encubrimiento se presentan con posterioridad a la comisión de la conducta punible y SIN QUE EXISTA ACUERDO PREVIO. Favorecimiento Art. 446 (el que tenga conocimiento de la comisión de la conducta punible y ayude eludir la acción o entorpecer...) o Receptación Art. 447 (el que sin haber tomado parte en la ejecución de la conducta punible adquiere, posea, convierta o transfiera bienes muebles o inmuebles que tenga su origen en un delito...)Ejemplo. Juan le pide a Pedro que después de matar a Carlos, le pide ayuda para movilizar el cuerpo hasta incinerarlo, el que pesca ilegalmente y le pide a alguien que se lo guarde los peces (pesca ilegal) o el juez que le pide al secretario que le diga al abogado que le dinero para que falle a favor<sup>46</sup>.*

Como vemos existen tres tipos de complicidad, que en materia de delitos informáticos, se dan, pues resulta claro que para acceder de manera abusiva a un sistema de información es factible que por ejemplo: otra persona preste su computador o contraseña para ingresar a una página y hacer un desfalco a una entidad financiera, estaríamos en presencia que esta persona actuó en la modalidad de complicidad previa, para hacer efectiva la conducta punible, por parte del cibercriminal.

Por otra parte encontramos que se puede dar la complicidad cuando, una persona guarda unos dispositivos de almacenamiento donde el autor tiene una información que acabo de descargar de la web, respecto a unos software maliciosos, y éste (el cómplice) sabe que es producto de un ilícito y finalmente termina prestando su ayuda.

Lo que se pretendía era analizar la modalidad de participes, tal como lo consagra el código penal colombiano en el artículo 30, al referirse que son participes tanto el cómplice como el determinador, y que cada uno de éstos puede fácilmente ser

---

<sup>46</sup> Ob cit. Pág.22.

participes en los delitos informáticos, tanto en materia de complicidad y determinación en vulneración de la protección de información y datos personales.

### **10.2.2. El interviniente en los delitos informáticos.**

Como se dijo renglones atrás el interviniente debe tener unas calidades especiales, para que se estructure su modalidad, en materia de delitos especiales como por ejemplo los que son contra la administración pública, el que concurra a su realización, por vía jurisprudencial se considera coautor, cuando participa cumpliendo los requisitos de esta; pero en tratándose de delitos comunes simplemente seguirá las pesquisas de interviniente como determinante o cómplice, es decir la figura del interviniente no opera en los delitos comunes; para hacer mayor claridad frente a este tipo de modalidad y definir si finalmente se estructura su participación en los delitos informáticos, miremos la jurisprudencia reciente referente interviniente, y posteriormente la relación con los delitos informáticos.

*EN SENTENCIA DEL 20 DE MAYO DE 2009. RAD. 31654. MP. MARIA DEL ROSARIO GONZALES DE LEMOS, comenta que el termino interviniente no lo hace como un símil de participes, ni como un concepto que congloba a todo aquel que de una u otra forma concurre en la realización de la conducta punible, valga decir determinadores, autores, coautores y cómplices, sino lo hace en sentido restrictivo de coautor de delito especial sin cualificación, , todo esto entorno a la principio de unidad de imputación, Ejemplo, si un servidor público, un particular concurre a apropiarse en provecho suyo o de un tercero de bienes del estado, la pena que le corresponderá será la del peculado, por conservarse la unidad de imputación, disminuida en una cuarta parte, de ahí el trato diferencial, por no poseer la cualidad exigida para el sujeto activo. SEGÚN ESTA JURISPRUDENCIA Y COMO EN MUCHOS OTRAS DETERMINA QUE AL INTERVINIENTE QUE ACTUA EN CONDICION DE COAUTOR SE HACE ACREEDOR A LA PENA PREVISTA EN EL RESPECTIVO TIPO PENAL DSIMINUIDA EN UNA CUARTA PARTE, ACORDE CON LOS ESTABLECIDO EN EL INCISO FINAL DEL ART. 30 AL DETERMINADOR POR LO TANTO A SU TURNO, CON O SIN LA REFERIDA CONDICION, SE LE APLICA LA SANCIÓN CONTENIDA EN LA NORMA INFRINGIDA SIN NINGUN TIPO DE DISMINUCION, MIENTRAS QUE AL COMPLICE CARECIENDO O NO DE LA CONDICIN EXIGIDA SE LE RECONOCE LA REBAJA DE PENA UNA SEXTA PARTE A LA MITAD<sup>47</sup>.*

---

<sup>47</sup> En sentencia del 20 de mayo de 2009. rad. 31654. M.P. María del Rosario Gonzales de Lemos.



Por lo tanto se desprende que el interviniente con calidades especiales es el sujeto activo que concurre en la participación en los delitos especiales, tales como los de la administración pública.

## 11. SANCIÓN EN LOS DELITOS INFORMÁTICOS

### 11.1. ANTECEDENTES LEGISLATIVOS.

#### 11.1.1. Marco Constitucional

Lo encontramos en el artículo 15:

*Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.*

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

*La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley<sup>48</sup>.*

En la constitución de 1991, se consagra como un derecho fundamental, la información y las bases de datos que además tienen una protección inviolable que solo admite su interceptación mediante orden judicial y que tiene control previo y posterior de conformidad a las reglas del estatuto procesal penal; entonces de aquí radica su protección por parte del estado y su garantía efectiva, enhorabuena y atendiendo los postulados de la política criminal del estado, el legislador colombiano hace efectiva la protección a través de leyes que garanticen y respeten el buen funcionamiento de los medios de comunicación que eviten la afectación de la información privada y los datos personales suministrados en la web, con el fin de evitar la trasgresión de la intimidad de las personas.

---

<sup>48</sup> Artículo 15 Constitución Política de 1991, edición Leyer 2009.

### 11.1.2. Marco legal

A lo largo de la legislatura tanto nacional como internacional se ha promulgado diferentes herramientas para limitar y proteger la información entre ellas encontramos las siguientes:

- 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***, ley que pretendía la protección y regulación de la información, en materia de inteligencia y contrainteligencia, que se generaría con sus actividades y límites; esta ley fue declarada inexecutable por la corte constitucional mediante sentencia C-913 de 2010, dentro de los argumentos se consideraron que para regular estas actividades se debe hacer por medio de una ley estatutaria habida cuenta que se trata de un derecho fundamental y entre otros esta la violación del derecho fundamental a la intimidad.

#### ***3.4. La materia tratada por la Ley 1288 de 2009 debe ser desarrollada mediante ley estatutaria***

*Según resulta de los anteriores planteamientos y de la jurisprudencia que ha sido reseñada, el análisis de constitucionalidad de la Ley 1288 de 2009 deberá abordar los siguientes aspectos: i) cuáles son los elementos estructurales o esenciales del derecho fundamental a la intimidad, a partir de lo cual deberá determinarse en qué medida la ley acusada versa sobre tales aspectos; ii) si en razón a su contenido, las disposiciones de esta ley pueden entenderse como una actualización o una nueva configuración normativa de este derecho fundamental; iii) si la regulación en ella contenida se encuadra en alguno(s) otro(s) de los criterios cuya presencia obliga a que la respectiva normatividad esté contenida en una ley estatutaria<sup>49</sup>.*

---

<sup>49</sup> Sentencia C-913 de 2010, Referencia: expediente D-8057, Magistrado Ponente: Dr. NILSON PINILLA PINILLA, Bogotá, D. C., dieciséis (16) de noviembre de dos mil diez (2010).

En materia de afectación a la intimidad dijo:

El derecho a la intimidad: elementos estructurales y definitorios:

La Corte ha analizado el derecho a la intimidad de que trata el artículo 15 superior, desde muy diversas perspectivas de la vida social. De manera general ha señalado que este derecho consiste en la posibilidad de preservar del conocimiento público determinados actos o situaciones de la vida personal que no tienen por qué trascender a otros, salvo que el propio interesado decida revelarlas, o que sean conocidas como consecuencia de un acto de autoridad debidamente fundamentado.

Respecto del contenido o elementos estructurales de ese derecho fundamental, dijo esta corporación en sentencia [T-696 de 1996](#) (M. P. Fabio Morón Díaz):

*“La intimidad, el espacio exclusivo de cada uno, es aquella órbita reservada para cada persona y de que toda persona debe gozar, que busca el aislamiento o inmunidad del individuo frente a la necesaria injerencia de los demás, dada la sociabilidad natural del ser humano. Es el área restringida inherente a toda persona o familia, que solamente puede ser penetrada por extraños con el consentimiento de su titular o mediando orden dictada por autoridad competente, en ejercicio de sus funciones y de conformidad con la Constitución y la ley<sup>50</sup>.”*

- La ley 1266 de 2008, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones, esta ley regula de una u otra forma la información en las centrales de riesgos para las personas que adquieren créditos financieros y aplica una sanción a aquellos que se atrasan en sus pagos, por lo que se reportaran sus datos en unas bases que atenderán información sobre su obligación crediticia.
- Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones; esta le abarca temas de gran importancia como los mensajes de datos, la firma digital, y los correos electrónicos, esta ley se encuentra vigente.

---

<sup>50</sup> Ibídem.

- Ley 679 de 2001, por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo [44](#) de la Constitución, esta ley consagra el uso global en redes respecto de menor de edad.

### 11.1.3. Marco Internacional

Normas que regulan y fijan estándares internacionales en materia de seguridad de la información y la creación de directrices que se deben tener presentes para su reglamentación interna en procura de suministrar estándares generales de seguridad en materia de tecnología, encontramos entonces las siguientes:

- *ISO/IEC 27000-series*

*La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC).*

*La serie contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). La mayoría de estas normas se encuentran en preparación e incluyen:*

*ISO/IEC 27000 - es un vocabulario estándar para el SGSI. Se encuentra en desarrollo actualmente.*

*ISO/IEC 27001 - es la certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005<sup>51</sup>.*

- **Congreso de ciberterrorismo budapest 2001**, donde se hacen precisiones en materia de criminalidad informática y sirven como referente internacional para la aplicación de normas y estrategias de seguridad en materia de delitos

---

<sup>51</sup> Disponible en la web: [http://es.wikipedia.org/wiki/ISO/IEC\\_27000-series](http://es.wikipedia.org/wiki/ISO/IEC_27000-series), vista el 13 de agosto de 2012.

informáticos, al respecto encontramos una guía EL CIBERDELITO: GUÍA PARA LOS PAÍSES EN DESARROLLO<sup>52</sup>.

#### **11.1.4. Ley 1273 de 2009.**

En la actualidad está vigente la ley 1273 de 2009, por medio de la cual se creó la protección a los datos y la información, como un nuevo bien jurídico tutelado, así: *“De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos (...)”*<sup>53</sup>.

La sanción de este tipo de conductas esta sancionada de una forma proporcional y necesaria, en base a la política criminal del estado; las modalidades y su participación pueden influir directamente en su tasación, aparte de las circunstancias de agravación y atenuación genéricas para todos los delitos tipificados en el código penal.

Antes de entrar a señalar la sanción de pena de prisión que consagra estos delitos informáticos, cabe recordar que en la praxis jurídica en materia de hechos ilícitos por medio de la informática, sus modalidades, para la comisión y por ende la participación de los delincuentes en su realización; es muy compleja, primero por la poca frecuencia en la vida normal de la sociedad, es decir en la actualidad los servidores públicos tienen poco conocimiento de su participación y las diferentes modalidades de perpetración y afectación de los bienes jurídicos protegidos con la ley 1273 de 2009; segundo por tratarse de técnicas novedosas, tercero por tratarse de situaciones que pueden adecuarse a otros tipos penales diferentes, como por ejemplo, el hurto, la injuria, la calumnia, en fin varias conductas que son de preferencia de los fiscales a la hora de imputar cargos; en conclusión lo que se pretende aclarar es que en materia de sanción estos delitos tienen su propia pena que debe ser analizada con cuidado por las partes en un proceso penal.

En esta ley encontramos que hay varios delitos tipificados, entraremos a revisar la forma de sanción y las penas de la siguiente manera según sus tipos penales:

---

<sup>52</sup> EL CIBERDELITO:GUÍA PARA LOS PAÍSES EN DESARROLLO División de Aplicaciones TIC y Ciberseguridad, Departamento de Políticas y Estrategias, Sector de Desarrollo de las Telecomunicaciones de la UIT, Proyecto de abril de 2009, Para mayor información póngase en contacto con la División de Aplicaciones TIC y Ciberseguridad del UIT-D en [cybmail@itu.int](mailto:cybmail@itu.int) Disponible en la web: [http://www.itu.int/dms\\_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf](http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf), visto el 20 de agosto de 2012.  
<sup>53</sup> Ley 1273, Diario Oficial N° 47223 de 5 de enero 2009.

El artículo 269A, respecto del acceso abusivo a un 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.*

Esta se enmarca en la modalidad de la **Técnica de interceptación, la Técnica del martillo**, entre ya analizamos en un capítulo anterior.

Como vemos esta técnica trae como pena de prisión de 48 a 96 meses, es decir de 4 a 8 años, lo que significa que es una pena excarcelable, que aplica la detención preventiva y no tiene el beneficio del Artículo 63 de código penal, toda vez que no es posible la suspensión condicional de la ejecución de la pena por no cumplir el requisito objetivo, es decir que la pena excede los 3 años consagrados en la norma.

El delito de obstaculización ilegítima de sistema informático o red de telecomunicaciones.

*Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, 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, siempre que la conducta no constituya delito sancionado con una pena mayor<sup>54</sup>.*

Este delito trae consigo la obstaculización que puede ser a través de virus, gusanos, Bomba lógica o cronológica; al igual que el anterior tiene una pena de prisión de 4 a 8 años, sin ningún tipo de beneficio, y delito que procede la detención preventiva en establecimiento carcelario de conformidad al artículo 313 del C.P.P.

Por otro lado está el artículo 269C, respecto de la interceptación de datos informáticos, así:

---

<sup>54</sup> Código Penal Colombiano, ley 599 de 2.000, modificado por la ley 1273 de 2009, artículo 269B, Ed. Leyer año 2009.

*Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses<sup>55</sup>.*

Modalidad esta que tiene la misma denominación en materia informática, que es utilizada por los delincuentes para encontrar contraseñas o información que permita infiltrarse y recoger datos para hurtar cuentas, o simplemente dañar el sistema, es similar a la técnica de la infiltración de la información.

Este delito tiene una pena de prisión de 3 a 6 años, es decir que puede ser susceptible de sustitución de detención preventiva por el lugar de residencia, pero no es posible la suspensión de la ejecución de la pena, porque no cumple el factor objetivo que la pena a imponer sea inferior a 3 años de conformidad con el artículo 63 de C.P.

El delito de Daño informático, está tipificado así:

*Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, 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<sup>56</sup>.*

Este tipo penal tiene una sanción con pena de prisión de 4 a 8 años, y no es susceptible de aplicar sustitución de detención preventiva y mucho menos la suspensión condicional de la ejecución de la pena, al tenor de los artículos 313 y 63 del Código Penal Colombiano respectivamente.

Las modalidades, según se ha hecho referencia en capítulos anteriores podría estar, los virus informáticos, los gusanos informáticos, la bomba lógica o cronológica, la técnica **Botnet (IRC-Internet Relay Chat)** y la técnica del martillo.

Por su parte el uso de software malicioso encontramos que está tipificado de la siguiente forma:

---

<sup>55</sup> Ibíd, artículo 269C.

<sup>56</sup> Ibíd., artículo 269D.



*Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, 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<sup>57</sup>.*

Este delito puede ser realizado por medio de la modalidad del “**SNIFER**” (Supone una amenaza grave para la seguridad no sólo de una máquina sino también de toda una red. Gran cantidad de tráfico confidencial viaja en claro, sin ningún tipo de cifrado, por las redes de la mayoría de las empresas), (...) <sup>58</sup>, este delito de 4 a 8 años, y no tiene beneficios de ningún orden.

El delito de violación de datos personales establece lo siguiente:

*Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes<sup>59</sup>.*

Este tiene la misma pena de 4 a 8 años de prisión y tampoco cumple con requisitos para beneficios procesales, por su parte este delito está determinado por varias modalidades delictivas y técnicas ciberdelictivas, como por ejemplo la técnica “**Fishing**”.

La suplantación de sitios web para capturar datos personales dice:

*Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, 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, siempre que la conducta no constituya delito sancionado con pena más grave.*

---

<sup>57</sup> Ibid., artículo 269E.

<sup>58</sup> Disponible en el siguiente enlace: [http://es.wikipedia.org/wiki/Detecci%C3%B3n\\_de\\_sniffer](http://es.wikipedia.org/wiki/Detecci%C3%B3n_de_sniffer), Visto el 15 mayo de 2012.

<sup>59</sup> Op.cit, ley 1273 de 2009, artículo 269F.

*En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.*

*La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito<sup>60</sup>.*

Este tipo penal consagra una modalidad como lo es la bomba lógica o cronológica y establece también una pena de 4 a 8 años de prisión.

Los anteriores tipos penal, además de las penas a imponer trae consigo unas circunstancias que agravan la pena a imponer así:

*Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:*

- 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.*
- 2. Por servidor público en ejercicio de sus funciones.*
- 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.*
- 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.*
- 5. Obteniendo provecho para sí o para un tercero.*
- 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.*
- 7. Utilizando como instrumento a un tercero de buena fe.*
- 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales<sup>61</sup>.*

Finalmente, el Código Penal Colombiano, modificado por la ley 1273 de 2009, establece otro capítulo que sintetiza las conductas con los atentados informáticos para la comisión de otros tipos penales, pero que igualmente los absorbe de manera específica:

---

<sup>60</sup> *Ibíd.*, artículo 269G.

<sup>61</sup> *Ibíd.*, artículo 269H.

## CAPITULO II

### *De los atentados informáticos y otras infracciones*

*Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.*

*Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad<sup>62</sup>.*

---

<sup>62</sup> *Ibíd.*, artículo 269I.

## 12. CONCLUSIONES

A lo largo del trabajo, en materia de delitos informáticos se pudo concluir que en Colombia se encuentran tipificadas algunas modalidades o técnicas para la realización material del delito, que afectan las bases de datos y la información, sin embargo existen ciertas técnicas que son de mucha tecnología que son de difícil comprensión en materia de ciberdelincuencia, es decir su tipificación positiva en una norma es ardua, inclusive su desvaloración jurídica de resultado en una norma que comprenda y sancione de manera específica un tipo de conductas que ponga en peligro los bienes jurídicos tutelados, es muy compleja, por el mismo sentido de ser algo novedoso en la actualidad, que se sale de las conductas tradicionales, utilizadas por los delincuentes.

De la misma forma, cabe mencionar que a pesar de su tipificación y sanción de las conductas que afecten las bases de datos y la información, el estado en materia de política criminal a procurado compilar las diferentes técnicas utilizadas por los delincuentes, con el fin de agrupar y proteger todo tipo de afectación a los derechos fundamentales como lo son la intimidad, la dignidad, la honra, el patrimonio y todos aquellos derechos que son potencialmente vulnerables a través de las herramientas tecnológicas, tal como vio a lo largo del trabajo.

En el mismo orden de ideas, por tratarse de conductas relacionadas con instrumentos tecnológicos para cometer ilícitos, se concluye que la apreciación de estas técnicas y la imputación de aquellas es más compleja por el desconocimiento y falta de preparación por parte de los actores de la justicia penal.

Es necesario que a nivel nacional, se procure con la inversión y preparación de políticas que instruyan a los funcionarios en materia de delitos informáticos, porque éstos pueden ser más peligrosos, habida cuenta que su materialización es a través de estos medios, imposibilitando significativamente la individualización de la participación de la conducta penal.

De lo anteriormente planteado, se puede concluir que las formas de participación en la comisión de un hecho punible es de mayor cuidado, toda vez que hay que presumir si se hace en la calidad de autor o participe en los delitos informáticos y su calificación jurídica es el tema.

En efecto, el problema principal es el poco conocimiento frente a estos temas, el desarrollo social, el cambio constante de la sociedad, el avance tecnológico sin medida, el cambio de generaciones y la actualización permanente de las normas al desarrollo inquebrantable, por parte de los actores jurídicos.

La escena virtual es una de las más apetecidas en la actualidad para cometer sus actividades delictivas, pues la delincuencia va en aumento, toda vez que es una modalidad de mayor facilidad para perpetrar sus cometidos, sin ser encontrados de manera inmediata y por ende pensaría que se torna más complicada la flagrancia de un ciberdelincuente, por el modus operandi en que operan, entonces se puede concluir que en materia de delitos informáticos va en aumento, y necesita un cuidado muy detenido por parte de la política criminal del estado, inclusive un consenso con los demás países.

## BIBLIOGRAFIA

*ARRUBLA Molina*. Siguiendo a *Tiedemann*, profesor del Instituto de Criminología y Derecho Penal de Friburgo (Alemania)

Código penal, edición Leyer 2010

FERNÁNDEZ María Clara, Tesis de Grado Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos, Universidad Sergio Arboleda Escuela de Derecho - Santa Marta 2001.

RINCON, Ríos Jarvey, Delitos informáticos, edición Universidad Santiago de Cali, año 2009, pág. 9

SENTENCIA 336/2007 modif. 244 C.P.P, Sobre las bases de datos.

## INTERNET

Ley Stop Online Piracy Act, también conocida como HR3261, es un proyecto de ley presentado en la cámara de representantes de estados unidos el 26 de octubre de 2011, por el representante LAMAR SMITH y un grupo bipartidista de 12 copatrocinadores iniciales.

Ley para la protección de los derechos de autor en el internet.

Disponible en la web, Artículo de la revista semana del 13 de abril del 2011, <http://www.semana.com/nacion/pros-contras-ley-lleras/155071-3.aspx>

Uniderecho.com disponible en: [http://www.uniderecho.com/leer\\_ley\\_Ley-En-Colombia\\_19\\_1459.html](http://www.uniderecho.com/leer_ley_Ley-En-Colombia_19_1459.html)

GALLARDO, Sara M. Periodista, comunicadora, Universidad Jorge Tadeo Lozano. Disponible en: <http://www.acis.org.co/index.php?id=455>.

Disponible: <http://johamartinez23.blogspot.com/2010/01/hola-soy-leidy-johana-martinez-y-este->, delitos informáticos en Colombia.

## GLOSARIO

**DIRECCION IP:** es una información que hay en el correo electrónico que me permite encontrar evidencia ej.: correo electrónico.

**ISP:** Proveedor de servicios de internet ej.: UNE, TELMES, el encargado de guardar la información de quien sale a internet.

**LOCK DE SEGURIDAD:** Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.