ESTUDIO SUSTANCIAL Y PROBATORIO EN EL DERECHO COLOMBIANO DE LOS DELITOS INFORMÁTICOS COMETIDOS A TRAVÉS DE LA INTERNET

JAIME ENRIQUE ACOSTA ORDOSGOITIA
EVA MARIA ANGULO SOLEDAD

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS HUMANAS
ESCUELA DE DERECHO Y CIENCIA POLÍTICA
BUCARAMANGA
2004

ESTUDIO SUSTANCIAL Y PROBATORIO EN EL DERECHO COLOMBIANO DE LOS DELITOS INFORMÁTICOS COMETIDOS A TRAVÉS DE LA INTERNET

JAIME ENRIQUE ACOSTA ORDOSGOITIA
EVA MARIA ANGULO SOLEDAD

Proyecto de grado para optar al título de Abogado.

Directora
MARIA ISABEL AFANADOR
ABOGADA ESPECIALISTA EN DERECHO PENAL

Codirector
LUIS CARLOS GÓMEZ FLOREZ
INGENIERO DE SISTEMAS

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS HUMANAS
ESCUELA DE DERECHO Y CIENCIA POLÍTICA
BUCARAMANGA
2004

AGRADECIMIENTOS

Los autores expresamos nuestros más sinceros agradecimientos a:

Doctora María Isabel Afanador, Directora del presente trabajo de grado por su disposición y valiosas orientaciones.

Ingeniero Luís Carlos Gómez, Codirector del presente trabajo de grado por su disposición y valiosa colaboración.

A nuestras familias, por su incondicional compañía.

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

TITULO: ESTUDIO SUSTANCIAL Y PROBATORIO EN EL DERECHO COLOMBIANO DE LOS DELITO INFORMÁTICOS COMETIDOS A TRAVÉS DE LA INTERNET[*]

AUTORES: Jaime Enrique Acosta Ordosgoitia, Eva Maria Angulo Soledad[**]

PALABRAS CLAVES: Delito informático, internet, información, evidencia digital

DESCRIPCIÓN: El avance tecnológico de los medios de comunicación y la informática propicia la creación y evolución de conductas criminales que vulneran derechos humanos. Un análisis sustancial y probatorio al sistema jurídico penal colombiano facilita al legislador prevenir, regular y sancionar los delitos informáticos. El análisis sustancial determina los objetos en que recaen las conductas criminales informáticas cometidas por una clase especial de sujetos; afectando bienes jurídicos como la intimidad y la información. El análisis probatorio es necesario para proporcionar la certeza de los hechos, la búsqueda de la verdad material y el resultado del juicio para sancionar a los sujetos responsables de estas conductas.

En torno al principio de legalidad y a la ausencia de disposiciones normativas en el estatuto penal colombiano se propone la modificación y la creación de tipos penales, bajo la técnica legislativa de un sistema ortopédico, que permitan describir las conductas criminales informáticas en especial aquellas cuyo medio de comisión es la internet.

El trabajo de grado bajo la perspectiva de la dogmática penal, en un enfoque descriptivo, técnico jurídico y propositivo, contribuye a la comunidad académica en el estudio claro y sencillo de los delitos informáticos en Colombia, con el fin de fortalecer los procesos de conocimiento en el derecho informático.

[*] Trabajo de Grado

[**] Facultad de Ciencias Humanas, Escuela de Derecho y Ciencias Políticas, Carrera de Derecho. Dirigida por la Doctora Maria Isabel Afanador.

SUMMARY

TITLE: SUBSTANTIAL AND PROBATIVE ANALYSIS IN THE COLOMBIAN LOW ABOUT COMPUTER CRIMEN ALTHOUGH OF THE INTERNET[*].

AUTHORS: Jaime Enrique Acosta Ordosgoitia, Eva Maria Angulo Soledad[**]

KEY WORDS: Computer, crimen, internet, information, digital evidence

DESCRIPTION: The technological advance of the media and the computer science cause the creation and evolution of criminal behaviors that harm human rights. A substantial and probative analysis to the system juridical Colombian facilitates to legislator to prevent, regulate and penalty the computer crimen. The substantial analysis determines the objects affected with the computer criminal behaviors made by a special class of subject affecting rights as the intimacy and the information. The probative analysis is necessary for provide the fact's certainty, search of the material truth and the result of the trial for penalty to the subjects responsible for these behaviors.

Around the legality's principle and the absence of normative dispositions in the Colombian penal statute, purpose the modification and the creation of penal types, with the technical legislative of an orthopedic system that describe the computer criminal behaviors especially those by internet.

The degree project low the penal dogmatic, with a descriptive focus, juridical technician and propositive, contributes to the academic community in the clear and simple study of the computer crimes in Colombia, with the purpose of strengthening the processes of knowledge in the computer low.

[*] Work of Grade

[**] Ability of Human Sciences, School of Right and Political Sciences, Career of Right. Directed by the Doctor María Isabel Afanador.

INTRODUCCIÓN

La informática a través de sistemas computacionales y telemáticos permite procesar y poner a disposición una cantidad creciente de datos de información de naturaleza variada en las diversas esferas del conocimiento humano desarrollando nuevos y diversos comportamientos que inciden tanto de manera positiva como negativa en las sociedades.

El derecho, ciencia del saber humano, instituida para la regulación de los comportamientos humanos en sociedad, fue creada en un mundo predigital o analógico; ahora con el progreso de la era informática debe adecuarse a las nuevas tecnologías y su impacto en los derechos fundamentales.

La ausencia de preceptos o normas, que no incriminan acciones realizadas por los individuos en un ámbito situacional dado, permite a estos realizar cualquier actividad sin temor de ser objeto de represión punitiva; no obstante, la no prevención, regulación y penalización de las conductas que afectan a bienes jurídicos como la información y la intimidad personal, conllevan al freno y colapso de los sistemas de información ofrecidos en las relaciones de intercambio cultural, social y económico entre los habitantes del mundo.

Lo anterior ha promovido el interés de presentar una monografía que busca, a partir de un análisis sustancial y probatorio de las conductas criminales informáticas, presentar una propuesta en el ordenamiento jurídico para la sanción de las acciones que constituyen una amenaza para la convivencia social en una sociedad de la información y así proteger los intereses y derechos constitucionales afectados.

El objetivo propuesto en la monografía está constituido por dos ejes fundamentales, a saber:

- El análisis del estado en el cual se encuentra el ordenamiento jurídico Colombiano respecto de los delitos informáticos cometidos a través de la internet, determinando de qué manera dichas conductas delictivas que se comenten a través de la Internet vulneran derechos fundamentales.

- La delimitación de los comportamientos y acciones desplegadas por las personas dentro de los sistemas computacionales y telemáticos tipificando en el ordenamiento penal Colombiano las conductas que atentan contra los bienes informáticos.

Este trabajo contribuye a la comunidad académica en el estudio claro y sencillo de los delitos informáticos en Colombia, bajo la perspectiva de la dogmática penal. Esta monografía es descriptiva, por orientación del problema, es técnico jurídica y de fin propositivo; estructurada en cinco capítulos ordenados de la siguiente forma:

- El capítulo primero desarrolla los conceptos y clasificación de la informática jurídica y el derecho informático, disciplinas formadas por la interrelación del derecho y la informática. En la informática jurídica se describe los conceptos de: Informática jurídica documental, informática jurídica de gestión e informática jurídica analítica. Por su parte en el derecho informático se indican las fuentes temáticas principales que afectan a las ramas del derecho tradicional: Los contratos informáticos, la protección del software, el comercio electrónico, la libertad informática, el flujo internacional de datos y los delitos informáticos.

- El capitulo segundo presenta de manera breve, la pluralidad de definiciones que conforman el mapa semántico de la expresión delito informático, a partir de las diversas formas en que la doctrina informática lo describe; esto con el fin de proporcionar claridad conceptual sobre los delitos informáticos; así mismo presenta

- La clasificación doctrinal de las conductas que afectan la información, finalizando con la descripción del funcionamiento de la internet.

- El capitulo tercero contiene una caracterización de los sujetos que actúan en las conductas criminales informáticas, las principales acciones que realizan y el objeto material en que recaen. De otro lado estudia el concepto, reconocimiento jurídico y relación de los bienes jurídicos de la intimidad y la información; seguidamente se examina la atipicidad relativa y absoluta de los delitos informáticos, y por ultimo se analiza y clasifican los tipos penales considerados informáticos consagrados en el actual código penal.

- El capitulo cuarto aborda un análisis probatorio partiendo del concepto de prueba, continuando con el análisis de los medios de prueba tradicionales y la relación que puede tener con los delitos informáticos en su aplicación y fin, para terminar con el concepto de la evidencia informática y los principios que le dan validez.

- El capitulo quinto parte de un cuadro cronológico de los antecedentes normativos regulatorios del derecho de la información; continúa con la descripción de las técnicas legislativas utilizadas para tipificar, regular y sancionar las conductas que afectan la información, finalizando con la propuesta legislativa para incluir una tipificación básica de los delitos

informáticos que afectan el interés social y los bienes jurídicos reconocidos constitucionalmente en la Carta de Derechos.

1. LA INFORMÁTICA Y EL DERECHO

La sociedad de la información plantea la necesidad de establecer nuevos criterios que permitan establecer un diálogo entre DERECHO e INFORMÁTICA, en aras de solucionar y dar respuesta a problemas y factores surgidos en su interacción. Entre Informática y Derecho existen dos formas de catalogar su interrelación; la primera de carácter instrumental, se conoce como INFORMÁTICA JURÍDICA, en cuyo caso la INFORMÁTICA está al servicio del DERECHO; la segunda se denomina DERECHO INFORMÁTICO, el cual estudia LA INFORMÁTICA en todos sus aspectos, como objeto del DERECHO.

1.1 LA INFORMÁTICA JURÍDICA

La Informática jurídica tiene por objeto la aplicación de la tecnología de la información al DERECHO; consiste en la utilización de conceptos, categorías, métodos y técnicas propias de la informática en el ámbito de lo jurídico[1]. Por tanto, es una disciplina que enlaza una metodología tecnológica con su objeto jurídico, tendiente a socializar el conocimiento del Derecho, para hacerlo más común a todos los ciudadanos, mediante una racionalización lógica y tecnológica[2]. El derecho como tecnología, supone que éste se halle fundado necesariamente en conocimiento científico orientado a obtener eficientemente resultados prácticos, puesto que la tecnología no es sino la aplicación práctica del conocimiento científico. En suma, LA INFORMÁTICA JURÍDICA estudia el tratamiento automatizado de las fuentes del conocimiento jurídico, las fuentes de producción jurídica y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho.

[1] JORDAN Fernando, Informática Jurídica, Bogotá, Universidad de los Andes, 1983 pag.23.
[2] CACERES, Nieto. *Logica jurídica e información jurídica,* Revista Universidad Complutense de Madrid. Facultad de Derecho, 1986, pag. 33.

Con base en clasificaciones realizadas por los doctrinantes Fernando Caicedo[3], Abelardo Rivera Llano[4] y Antonio Enrique Pérez Luño[5], se destacan diversas disciplinas de la INFORMÁTICA JURÍDICA; así:

1.1.1 Informática Jurídica Documental. Su objeto es el uso de técnicas para el análisis, organización y tratamiento de la información jurídica, a través de sistemas de documentación legislativa, jurisprudencial y doctrinal.
Su desarrollo podría aminorar la crisis de desinformación y gran documentación en el Derecho Colombiano, producto de la avalancha de legislación, jurisprudencia y doctrina que hace materialmente imposible su discernimiento, interpretación y aplicación por los operadores y usuarios jurídicos, ya que esta disciplina busca restablecer un equilibrio entre el incesante flujo de datos jurídicos y la capacidad para asumirlos y aprovecharlos; generando certeza en el derecho y propiciando el valor de la seguridad jurídica, pilar del ordenamiento jurídico.

1.1.2 Informática Jurídica de Gestión. Su objeto son los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho. Registra un gran desarrollo y se le conoce también como la Ofimática o la Burótica, donde se inscriben los avances tendientes a la automatización de las tareas rutinarias que se llevan a cabo en oficinas y despachos jurídicos, mediante soportes informáticos o telemáticos de operaciones destinadas a recibir y transmitir comunicaciones de cualquier tipo, de leer y escribir textos; de formar, organizar y actualizar archivos y registros; exigir y recibir pagos; estipular condiciones y controlar su cumplimiento. Esta disciplina que hasta ahora se da aplicación en los despachos judiciales genera resultados más uniformes, imparciales, transparentes, rápidos y económicos, conllevando a que los

[3] CAICEDO, Fernando. *Curso de informática jurídica,* Bogota, Editorial Tecnos, 1988. pág. 22
[4] RIVERA Llano, Averaldo, Dimensiones de la Informática en el Derecho, Ed. Jurídica Radar, Bogotá, 1995, pag. 15-17
[5] PEREZ Luño, Antonio, Ensayos de Informática Jurídica, Biblioteca de Etica, Filosofia del Derecho y Política, México, 1996, pag. 41 – 44.

administradores de Justicia se dediquen exclusivamente a labores que exijan una actividad creadora. La Informática Jurídica de Gestión de acuerdo a la forma en que esté siendo utilizada se clasifica en:

♦ Informática Jurídica de Gestión Operacional: Cuando se utiliza para la elaboración de escritos, documentos, la gestión y seguimiento del archivo de actuaciones, permitiendo el control de los pasos de una clase de proceso específico para dar cumplimiento a las etapas del asunto de conocimiento.

♦ Informática Jurídica de Gestión Registral: Se ocupa de todas las clases de registros (públicos o privados) a fin de facilitar a los usuarios datos exactos en todos los registros oficiales con rapidez y facilidad de acceso, a diferencia de los métodos tradicionales.

1.1.3 Informática Decisional o Metadocumental. Su objeto son los procedimientos dirigidos a la sustitución o reproducción de las actividades del jurista; a proporcionarle decisiones, dictámenes, y ofrecerles soluciones de problemas. La evolución de esta disciplina se manifiesta en la aplicación en el Derecho de la inteligencia artificial y los sistemas expertos, ya que emplea el ordenador, en la ayuda de toma de decisiones a través de la solución de casos, mediante la elaboración informática de los factores lógico formales que concurren en el proceso legislativo y en la decisión judicial[6]. Esta disciplina aportaría al Derecho Colombiano prototipos y proyectos de sistemas jurídicos en materias como: Liquidaciones tributarias, cálculo de indemnizaciones por accidentes laborales o de tráfico y predicción de las consecuencias jurídicas de impacto medio ambientales; sin embargo se puede advertir que el desarrollo y evolución de esta disciplina puede conllevar a que las máquina de cómputo procese

[6] PEREZ Luño, Antonio, Ensayos de Informática Jurídica, Biblioteca de Etica, Filosofia del Derecho y Política, México, 1996, pag. 41 – 44.

informaciones y establezca inferencias lógicas, cuyo fin generaría la suplantación plena del razonamiento jurídico del juez o del abogado, hecho que puede ocasionar una laguna jurídica en torno a: ¿ Quién asume la responsabilidad por decisiones judiciales erróneas, debido a la inferencia de análisis lógico – matemático realizado por un ordenador?

1.1.4 Informática Jurídica Analítica. su objeto es poner a prueba las hipótesis jurídicas, aplicando la informática a la investigación de la teoría Jurídica y a la enseñanza del Derecho, con el fin de reflexionar los temas jurídicos como ayuda a la práctica forense. Esta disciplina es necesaria pues: ¿Cómo puede el jurista pretender juzgar las múltiples controversias que la informática presenta, si no posee conocimientos científicos, técnicos, filosóficos, políticos y culturales sobre la informática?

1.2 DERECHO INFORMÁTICO

El Derecho informático es el conjunto de normas que deben regir aspectos y conflictos jurídicos originados por el desarrollo y utilización de la informática[7]. Está integrado por proposiciones normativas que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la Telemática.

El contenido de las disciplinas que conforman el derecho informático es muy variado, como distintas son las especialidades del derecho en las cuales el impacto tecnológico las afecta y las incluye. El carácter interdisciplinario del Derecho informático genera un debate teórico sobre si se trata de un Derecho con normas dispersas y pertenecientes a diferentes disciplinas jurídicas o un Derecho unitario de normas dirigida a regular un objeto bien delimitado; siendo este el

[7] SALAZAR CANO, E. Cuadernos de Informática Jurídica y Derecho Cibernético. Venezuela, 1997, Pag. 48

criterio que más se ajusta a los fenómenos que la información y sus medios de transmisión han creado en el derecho tradicional.

Las fuentes temáticas del Derecho informático afectan a las ramas del Derecho tradicional, como se presenta en una enumeración tentativa, no exhaustiva en la siguiente tabla :

Tabla 1. Disciplinas Jurídicas tradicionales VS Temáticas del Derecho Informático.

RAMAS TRADICIONALES DEL DERECHO	FUENTES TEMÁTICAS
Derecho civil	Contratos informáticos
Derecho comercial	Protección del software – Comercio Electrónico.
Derecho constitucional	Libertad Informática (Habeas Data)
Derecho internacional publico	Flujo internacional de datos
Derecho penal	Delitos informáticos

Destacándose las ramas del Derecho, base de las normas y preceptos valorativos que rigen nuestro actuar, se observa que la evolución de los instrumentos tecnológicos como apoyo a la información, está irrumpiendo en todas las disciplinas jurídicas; es así que a continuación se explican someramente, las diferentes fuentes temáticas indicadas en la tabla No.1, con el fin de ilustrar como el desarrollo del la Información no solo afecta el Derecho Penal.

1.2.1 Contratos Informáticos. El Código civil Colombiano en el artículo 1602 define el contrato como: un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa, definición que puede proyectarse a los contratos informáticos, con importantes peculiaridades. Los Contratos informáticos se definen como un acuerdo de dos o más personas que crea, modifica o extingue

derechos y obligaciones de contenido informático, ya sea porque su objeto son bienes o servicios informáticos, o porque el acuerdo de voluntades se realizó en forma informática.

Las modalidades de contratos informáticos obedecen a dos perspectivas de enfoque: la objetiva y la subjetiva. La objetiva, parte de la naturaleza de la actividad a cumplir por el ordenador; y la subjetiva, contempla la posición y naturaleza jurídica de las relaciones de los contratantes en el intercambio de productos y servicios.

La complejidad "objetiva" de los contratos informáticos procede de la inevitable implicación del equipo físico y de los programas que definen la estructura del ordenador, entre los que podemos distinguir contratos de hardware, contratos de software, contratos de instalación llave en mano y contratos de servicios auxiliares los cuales implican la compra, venta y mantenimiento de ordenadores, y a su vez, de los programas que le permitan cumplir las funciones.

La complejidad "subjetiva" de los contratos informáticos viene determinada por el hecho de que este tipo de contratos son plurilaterales; es la intervención de dos o más usuarios de la informática. En la dimensión subjetiva de estos contratos, tiene especial importancia aquellos negocios jurídicos de compraventa, de arrendamiento, de prestación de servicios, de préstamo y de depósito de bienes informáticos.

Es así que la contratación de bienes y la prestación de servicios informáticos no tiene una calificación uniforme que la pueda situar, en cada caso, en un modelo o tipo de contrato de los que figuran en nuestro ordenamiento; por ello se hace necesario una normatividad adecuada a los mismos bienes informáticos, y su redacción debe tener en cuenta un equilibrio de prestaciones y evitar en lo posible la existencia de cláusulas oscuras.

1.2.2 Protección Jurídica del Software. Es el tema del Derecho informático que se refiere a los distintos medios para la protección jurídica del software. Los intereses que se manifiestan en la protección jurídica de los programas o soportes lógicos son: Intereses por parte de la empresa distribuidora del software, pues esta se dedica a la elaboración de programas para defender sus inversiones; el interés del programador, dedicado a que se le reconozca la paternidad de la creación del sistema lógico a efectos de un reconocimiento profesional o académico.

Los diferentes medios de tutela jurídica del software pueden agruparse en cuatro modalidades que han evolucionado a través del derecho informático y son:

- ✓ Instrumento de protección jurídica general: Tiende a evitar la competencia desleal, tutelar el secreto industrial y la creación de cláusulas de protección del software, estos instrumentos son rudimentarios y no garantizan efectivamente la importancia económica del software.

- ✓ Protección mediante del Derecho de patentes: En este punto se busca la manera de tutelar los soportes lógicos a través del derecho de patentes, reconociéndole a este bien inmaterial su vinculación al equipo físico que hace parte, y en otras, por su propia condición de invento industrial; esta protección asegura al autor del programa un monopolio temporal para su explotación garantizándole que durante dicho periodo nadie podrá producir, comercializar o utilizar el programa sin su consentimiento. Sin embargo presenta dificultades pues para que el software pueda ser patentado debe reunir las siguientes características: novedad, materialidad e industrialidad.

- ✓ Protección a través del derecho de autor: Consiste en la protección jurídica de los aspectos morales y patrimoniales de las creaciones originales del ingenio humano. Esta modalidad se inició en la década de los sesenta dándole reconocimiento a esta disciplina, aquí el software se tutela

condicionando la protección al carácter original del programa y prohibiendo no solo la reproducción sino también la utilización. En todo caso existen controversias sobre si el derecho de autor puede ser una disciplina jurídica restringida a los programas aplicativos, o si puede extenderse a los programas de bases escritos en código de máquina.

- ✓ Protección relacionada con medios específicos: Se trata de las disposiciones para la protección del software promulgadas en 1978 por la Organización Mundial de la Propiedad Intelectual (OMPI) que constituye un modelo de referencia para cualquier iniciativa de política legislativa en este sector. Esta disposición no excluye la aplicación de principios generales del derecho u otras disposiciones referentes a los Derechos de Autor, Derecho de patentes o competencia desleal.

1.2.3 Comercio Electrónico. Se fundamenta en el uso de redes para las actividades relacionadas con la gestión de negocios: Oferta y demanda de productos y servicios, pedidos, remesas, selección de transporte y seguros, pagos, publicidad, información, servicio postventa, entre otras. Por lo tanto, no sólo hace referencia a la compra y venta electrónica de bienes o servicios, sino también a otras actividades previas o posteriores.

En Colombia el Comercio electrónico abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden las siguientes operaciones: operación comercial de suministro o intercambio de bienes o servicios; acuerdo de distribución; operación de representación o mandato comercial; operaciones financieras, bursátiles y de seguros; construcción de obras; de consultoría; de ingeniería; de concesión y licencias; acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o

comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera según lo regulado en la ley 527 del 18 de agosto de 1999, mediante la cual se definió y reglamentó el acceso y uso de los mensajes de datos, el comercio electrónico y la firma digital.

1.2.4 Libertad Informática. Se trata de una de las principales fuentes que integran el derecho informático. Aparece como nuevo derecho de auto-tutela de la identidad informática; es el derecho de controlar, conocer, corregir, quitar o agregar los datos personales inscritos en las tarjetas de un programa electrónico. La libertad informática forma parte del núcleo de derechos denominados de tercera generación, en los cuales se incluyen el derecho a la paz, los derechos de los consumidores, el derecho a un medio ambiente sano y el derecho a una calidad de vida, derechos éstos dirigidos a potenciar la esfera de libertades del individuo en la era tecnológica.

En la Constitución Política Colombiana, las disposiciones que tienen relación directa con la Libertad Informática son las consagradas en el artículo 15 [8] y el artículo 20[9]. Tales derechos se ven vulnerados debido a la injerencia del ordenador en las diversas esferas y relaciones que conforman la vida cotidiana, por ello resulta apremiante se de reconocimiento jurídico a la libertad informática; avance que nuestro ordenamiento, gracias a la jurisprudencia Constitucional y a la doctrina informática la reconoce con el concepto de Habeas Data.

---

[8] 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 archivos de entidades públicas y privadas (Art 15 C.N)

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

El Habeas Data debe entenderse como un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas para: conocer y acceder a las informaciones que les conciernen, archivados en bancos de datos, controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su trasmisión. Dentro de nuestra Historia Constitucional se destaca que en la Constitución de 1886 no se contemplaba el habeas data, pero sí se estipulaban algunas garantías que tenían que ver con la privacidad personal, como lo consagró el Art. 23 (nadie podrá ser molestado en su persona o familia ni su domicilio registrado) y el Art. 38 (inviolabilidad de correspondencia).

En el proyecto de creación de la Constitución de 1991, se contempló el derecho a la intimidad personal y familiar, en términos similares a la norma existente hoy en día, incluyendo el habeas data y con un inciso específico acerca de que "la ley reglamentará el uso de la informática y de otros avances tecnológicos para garantizar la intimidad personal y familiar y el pleno ejercicio de otros derechos."
En la actualidad, la consagración de la libertad informática y el derecho a la autodeterminación informativa, en el marco de los derechos de la tercera generación, ha determinado que se postule el estatus de Habeas Data concretando con normativas y pronunciamientos judiciales sobre las garantías de acceso y control a las informaciones procesadas en bancos de datos.

1.2.5 Flujo internacional de Datos. Es un tema de preocupación para el derecho internacional informático; pues el flujo internacional y transnacional de datos ha suscitado un conflicto de intereses entre los países productores y los países consumidores de datos informáticos; conflicto originado en los países desarrollados quienes mantienen una posición decidida a favor de una libertad ilimitada de intercambio de información entre todos los países sin obstáculo ni limitaciones, mientras los países subdesarrollados, carentes de tecnología

informática, exigen el reconocimiento de facultades para ejercer control sobre los datos que pueden recogerse en su territorio.

Este tema es de vital importancia pues en el intercambio electrónico de datos se dan las diversas modalidades de contratación y que a efectos de oponibilidad y prueba presentan la ausencia de: firma manuscrita, registro en soporte de papel y formas simplificadas del acuerdo.

1.2.6 El Delito Informático. El Derecho Penal Informático tiene como objeto de estudio los delitos informáticos. La pregunta: ¿Existen los Delitos informáticos?, genera en la doctrina del derecho Penal informático dos tesis antagónicas: Tesis negativa de la existencia de Delitos informáticos y Tesis positiva de la existencia de Delitos informáticos. La tesis negativa aduce que no existen delitos informáticos sino simplemente conductas no éticas y antijurídicas cuyos medios de ejecución se verifican con modernos sistemas; es así, que todas las conductas catalogadas como delitos informáticos son asimilables o están tipificadas en los estatutos penales; en sentido contrario, la tesis positiva acepta la existencia de delitos informáticos con estructura propia y carentes de reconocimiento penal.

Como quiera que la presente investigación tiene por objeto realizar un análisis sustancial y Probatorio de los delitos informáticos dentro del sistema jurídico Colombiano, se abordará en el siguiente capítulo el concepto de Delito informático finalizando con una breve ilustración del medio de propagación de los delitos informáticos que más reviste importancia: la Internet.

2. DELITO INFORMÁTICO

En la doctrina Penal informática se observa una pluralidad de definiciones y conceptos en torno al término DELITO INFORMÁTICO, creando un asunto bastante controvertido para determinar un concepto universal y único de Delito Informático.

De allí que la doctrina Penal en materia informática recalque diferentes términos intentando definir el delito informático destacándose como denominación genérica y apropiada, en el Derecho penal informático Continental el término: Criminalidad informática[10] y en el Derecho penal informático anglosajón la denominación de Computer Crime[11].

En aras de proporcionar claridad conceptual sobre los delitos informáticos, es pertinente comentar una breve reseña de la pluralidad de definiciones que conforman el mapa semántico de la expresión Delito Informático a partir de las diversas maneras en que la doctrina informática lo describe.

[10] BAÓN RAMÍREZ (Delincuencia Informática .promociones y Publicaciones Universitarias. Barcelona, 1992) define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software .TIEDEMANN ., citado por Molina A. Introducción a la Criminología., Ed. Biblioteca Jurídica, Medellín, 1988) considera que con la expresión "criminalidad mediante computadoras", se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

[11] SARZANA, Carlo. (Criminalita e tecnología en computers crime: Rassagna Penitenziaria e criminología. Nos. 1-2 Ano 1. 1979. Roma, Italia) establece que los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

2.1. DEFINICIÓN DE DELITO INFORMÁTICO:

Por lo que se refiere a las definiciones que se esbozan en torno al delito informático, Julio Téllez Valdés señala: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de delitos en el sentido de acciones típicas, se requiere que la expresión delitos informáticos esté consignada en los estatutos penales"[12]; que en el caso Colombiano, al igual que en muchos otros no ha sido objeto de tipificación aún; sin embargo se destaca como las definiciones utilizadas para conceptualizar el delito informático, parte de diferentes criterios, entre otros:

Definición amplia: Define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".[13]

Definición simple: Según la cual el delito informático constituye cualquier acto violatorio de la ley penal para cuya comisión exitosa es esencial el conocimiento y utilización de la tecnología de las computadoras"[14]

Definición técnica: El delito informático es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin "[15] Por lo tanto, se entiende como delito informático las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin.

---

[12] TELLEZ VALDEZ, Julio, Derecho informatico, Editorial Mc Graw Hill, México, 1997, pag. 98.
[13] CALLEGARI, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985. P.115.
[14] Quiñones G.,G. Cibernética Penal El Delito Computarizado, Caracas, Editorial Gráficas Capitolio, Caracas, 1999, pág. 22.
[15] LIMA Maria de la Luz, El Delito Electronico, Ed Ariel, México, 1999.pag 67.

Definición analítica: El Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución [16]. Es acción dolosa que provoca un perjuicio a personas o entidades y en la que se hacen intervenir dispositivos o programas informáticos[17] o como acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin [18].
Igualmente se puede clasificar las diversas definiciones que se presentan de delitos informáticos, así:

- En torno al elemento material que sirve de medio para la comisión: El delito informático comprende comportamientos criminales en los cuales la computadora ha estado involucrada como material o como objeto de la acción criminógena, "[19].

- En torno al bien jurídico afectado: Los delitos informáticos comprenden todas aquellas conductas que revisten características delictivas y atentan contra el soporte lógico de un sistema de procesamiento de información" [20]; o aquellos delitos que se realicen contra los bienes ligados al tratamiento automático de datos"[21].

Vista la pluralidad de definiciones sobre Delito informático, para efectos de dar mayor claridad respecto del tema de la presente investigación, es pertinente manifestar que la realización de las conductas catalogadas como Delitos

[16] CASABONA Romero, Hacia un concepto de delito Informático, Ponencia presentada al XI Congreso Internacional de Informática, Buenos Aires, Agosto, 1991.
[17] GARCIA, Barcelo Miguel, Ponencia presentada al: Congreso sobre "Derecho Informático", celebrado en la Universidad de Zaragoza, España: en junio de 1989.
[18] LIMA Maria de la Luz, El Delito Electrónico, Ed Ariel, México, 1999.pag 20.
[19] SARZANA, Carlos. *Criminalita e tecnología en Computers crime.* Rassagna Penitenziaria e criminología. Nos 1-2. Año 1979. Roma. Pág. 53.
[20] ARTEAGA S., Alberto. El delito informático: Algunas implicaciones jurídico penales, Revista de la Facultad de ciencias jurídicas y políticas. Universidad central de Venezuela, 1989, pag. 11
[21] TIEDEMANN, K., citado por Molina A. Introducción a la Criminología., Ed. Biblioteca Jurídica, Medellín, 1988, Pág. 307

informáticos pueden hacerse a través de medios de comunicación e información como las redes, señales y ondas, las cuales en su mayor parte se canalizan mediante instrumentos u objetos materiales e inmateriales como son: El computador, el Teléfono, la televisión y la Internet; esta ultima medio inmaterial con mayor uso a nivel mundial permitiendo el intercambio, distribución , e interacción de datos de todo tipo y forma, e información personal o colectiva en tiempo record y espacios ilimitados.

Es así, que hoy día, ninguna persona es ajena a los efectos de la Internet; pues esta llegando a todos los sitios sin control y barrera alguna, conllevando al crecimiento acelerado de su uso; como se demuestra en el acápite 2.2.4

En el presente trabajo se asumirá la definición de delitos informáticos como aquellas conductas ilícitas susceptibles de ser reguladas y sancionadas por el derecho penal, que utilizan la Internet como medio de comisión y recaen sobre bienes intangibles afectando el derecho de la información, concepto útil para comprender los efectos sustanciales y probatorios de las conductas delictivas realizadas por medio de la Internet. De allí que antes de entrar al desarrollo de otros de los objetivos propuestos, es necesario conceptuar y entender qué es la Internet, su origen, funcionamiento y aplicaciones para tener una mayor comprensión de la comisión de los delitos informáticos.

2.2 DEFINICIÓN DE LA INTERNET

La Internet es un conjunto de redes independientes que se encuentran conectadas entre sí. Sus principales características son: la interactividad, la libre elección de contenidos y la ausencia de una autoridad de control. Es importante destacar su origen y funcionamiento para hacernos una idea mas clara del objeto de la presente investigación.

2.2.1 Origen de la Internet. La internet comenzó como un proyecto de la Agencia de Proyectos Avanzados de Investigación del Departamento de Defensa Norteamericano (DARPA) , quien diseñó específicamente el protocolo de comunicaciones TCP/IP[22]. El Departamento de Defensa de los Estados Unidos creó la ARPA con la finalidad de llevar a cabo el objetivo estratégico, de asegurar el envió de la orden de abrir fuego desde el centro de control a bases de misiles , aún después de que las redes de comunicaciones hubieran quedado en parte destruidas por un ataque. La red se denominó ARPAnet. Esta tecnología fue creada inicialmente con propósitos militares ya que deseaba iniciar un programa de investigación que desarrollara técnicas y tecnologías para conectar redes de varios tipos y protocolos de comunicación, que permitiera a las computadoras conectadas comunicarse libremente a través de diferentes plataformas. ARPAnet en principio interconectaba cuatro grandes ordenadores en localizaciones secretas de EEUU. Prontamente las universidades y centros de investigación se unieron a esta red para compartir información científica y tener acceso a grandes centros de cómputo. Es así que en 1972 ya existían 40 hosts o nodos de red y se organizo la Conferencia Internacional de Comunicaciones entre Ordenadores con la demostración de ARPAnet entre estos 40 equipos. En 1973 se inician las primeras conexiones internacionales con ARPAnet: Inglaterra y Noruega como medio de intercambio de datos de investigación, así mismo los usuarios comienzan a comunicarse mediante buzones personales de correo electrónico. En 1976 se desarrolla la tecnología UUCP en los laboratorios Bell de AT&T. Un año después se distribuye con Unix. En 1986, la Fundación Nacional para las ciencias (NSF National Science Foundation de Estados Unidos, inicio el desarrollo de NSFnet que constituye un factor decisivo para el desarrollo de Internet al crear cinco importantes centros de calculo equipados con supercomputadoras, con el fin de permitir a toda la comunidad científica tener acceso a la información almacenada. Entonces, cada centro universitario importante estableció una conexión con la red

[22] HANCE, Oliver. Leyes y negocios en la Internet. Origen de la Internet. México D.F. McGraw- Hill. 1996. Pág. 12.

constituida por la NSF, la cual fungió como esqueleto (o circuito principal) para todo el tráfico de esas subredes. De ahí en adelante fue posible ingresar a cualquier punto en la red desde cualquier sitio universitario conectado , en 1991 , la red empieza alejarse de Uníx y otros lenguajes de aplicación, y se inicia el uso de la interfase basada en Windows mas fácil para el usuario. Poco tiempo después apareció American On Line, Compusever y otros proveedores de servicio de Internet, quienes se enfocaron más en el usuario final en lugar de enfocarse en lo científico.

2.2.2 Aspectos técnicos del funcionamiento de la Internet. La Internet funciona bajo unas redes llamados protocolos, que son conjuntos de reglas y convenciones que han de adoptarse para ser entendido por los otros computadores de la red[23]. Cada uno de los computadores que son parte de la Internet no está conectados directamente con todos los demás; sólo con los más cercanos. Existe un organismo central llamado el Network Information Center (NIC) que se encarga de asignar direcciones Internet (números IP) diferentes a cada usuario, y la ICANN que es la encargada de asignar los nombres de dominio.

Para tener acceso a una máquina alejada, se hace a través de las demás formando una especie de cadena. Para esto se utilizan los paquetes.[24] Esta identificación se realiza mediante una Dirección IP, de este modo si un computador recibe un paquete que no es para él, lo reenvía al destinatario, o en su defecto, al computador más cercano a éste al que pueda acceder.

[23] Los dos protocolos más importantes son el *Protocolo de Control de Transmisión* (*Transmission Control Protocol*) y el Protocolo de Internet (Internet Protocol*")* Usualmente se trata a estos dos protocolos como uno solo, llamándolos TCP/IP. Un computador -sin importar que sistema utiliza, Linux, Windows u otro, o si es una PC o una Mac - puede comunicarse con cualquier otro si maneja estos protocolos."

[24] Un paquete es un trozo de información (texto, imágenes, voz o cualquier otro) que está marcado, indicando quién lo envía y para quién es.

Sin embargo, no todos los computadores que están conectados a Internet tienen el mismo propósito o poseen las mismas capacidades. Una gran parte ni siquiera es parte de la red de manera permanente (por ejemplo, si está conectado vía MODEM). Por esto la Internet opera según el llamado modelo cliente – servidor.
Los servidores forman el esqueleto de la Internet. Un servidor es un gran computador dedicado a atender las peticiones de otros computadores, de allí viene su nombre. Estas peticiones pueden ser el envío de una página web o un archivo que se encuentra en su base de datos, o el establecimiento de una conexión con otra máquina.

Por lo general, el computador donde se encuentra un usuario es un cliente. Los clientes son los computadores que realizan las peticiones a los servidores y reciben la información. Por eso los programas que reciben los clientes a través de la red como programas de correo electrónico, FTP, CLAT o navegadores web, son conocidos como *Aplicaciones del lado del Cliente* (*Client-side Applications*), y es a través de estos que se materializan los delitos informáticos.

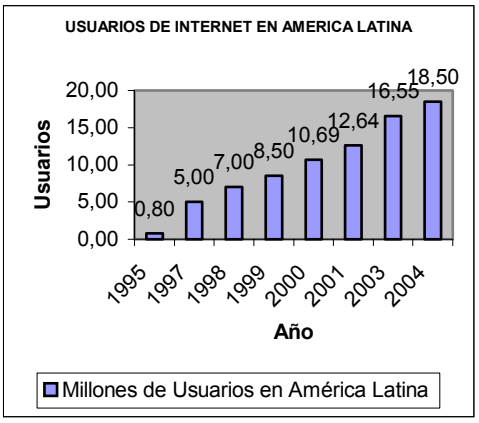
2.2.3 Usuarios de la Internet. La internet implica un cambio en el paradigma tradicional del intercambio de información y en las diferentes formas de relación entre los individuos que conforman una sociedad.

Tabla 2. Usuario de la Internet a nivel Mundial.

AÑO	NUMERO DE USUARIOS A NIVEL MUNDIAL
1997	Diez millones de Usuarios
1998	Ciento cincuenta y nueve millones de usuarios
1999	Doscientos doce millones de usuarios
2000	Doscientos setenta y dos millones de usuarios
2001	Trescientos setenta y nueve millones de usuarios
2002	Cuatrocientos cincuenta y nueve millones de usuario
2003	Quinientos diez millones de usuarios

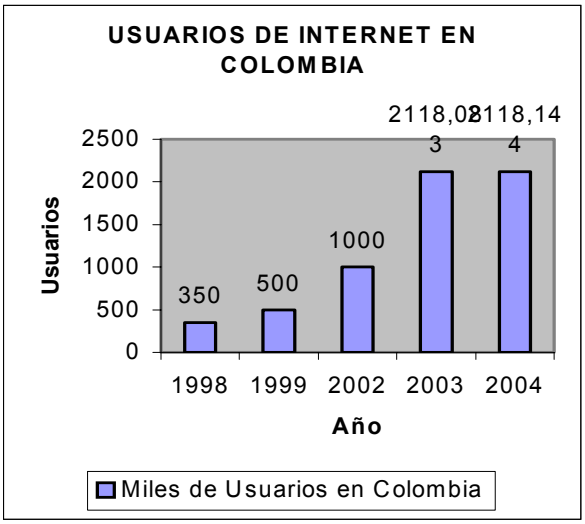
Fuente: http://www.Nielse/NetRatings.com

Gráfica 1. Usuarios de Internet en América Latina.



Fuente: IDC y Emarketer,

Gráfica 2. Usuarios de la Internet en Colombia.



Fuente: IDC y Emarketer

2.2.4 Aplicaciones de la Internet en las comunicaciones. Una vez se adquiera la conexión a la Internet, el usuario tiene acceso a los varios servicios y aplicaciones disponibles en la Internet entre los cuales se destaca el Correo electrónico, WWW, Telnet, FTP, Gopher, Listas de correo, Grupos de discusión y charla IRC.

Tabla 3. Ocho aplicaciones de la Internet en las comunicaciones.

APLICACIÓN EN LA INTERNET	***FUNCIONALIDAD***
CORREO ELECTRÓNICO	Permite a los Usuarios con una dirección electrónica comunicarse entre si de la misma manera en que lo hacen a través del servicio postal convencional. En términos prácticos, el mensaje del emisor del correo electrónico se envía a su servidor de correo electrónico (para un usuario o para una compañía pequeña, por lo general el proveedor de acceso a la Internet), el cual, a su vez, lo envía por la red al servicio de correo del destinatario, quien a su vez, abre su servidor de correo, consulta su buzón electrónico y recibe el mensaje.
WORLD WIDE WEB (W.W.W)	Se trata de un medio de divulgación de datos; fue creado por el CERN y permite hacer una consulta simple de recursos gracias a los enlaces de hipertexto (diferentes estilos, dibujos, sonidos, videos) insertados en el texto por el autor. El Web es entonces una aplicación de búsqueda para el usuario, pues le permite navegar en la Internet haciendo uso de varios servidores en segundos.

TELNET	Es el principal protocolo de la Internet para crear una conexión con el servidor remoto. Le permite al usuario estar en un computador y realizar trabajo en otro, el cual puede estar cerca o a distancia. Cuando el usuario ejecuta una sesión Telnet , su computadora es parte del servidor, esto significa que el usuario tiene acceso a los servicios, memoria y capacidad del procesamiento del servidor.
FTP (File Transfer Protocol, Protocolo de transferencia de archivos)	Es una versión reducida de Telnet. Puede utilizarse para transferir archivos, de texto o de programas, entre computadoras distantes. FTP es interactivo, esto significa que el usuario presenta los comandos cuando los digita en la terminal. FTP mantiene la conexión entre el cliente y el servidor y envía los comandos en texto ordinario. Cuando los datos se van a transferir, el cliente y el servidor abren una conexión de datos. Esta conexión se mantiene hasta que el usuario digita otros comandos.
GOPHER	Es un servicio interactivo que permite acceder información usando menús sencillos, el gopher constituye el primer intento para integrar varios recursos en la red explotando el modelo cliente – servidor.
LISTAS DE CORREO	Se trata de una lista de usuarios que desean intercambiar información o ideas sobre un tema específico. Cualquier usuario puede crear una lista de este tipo, tratándose como un foro para la colección y difusión de información. El principio en el que descansan estas listas es sencillo: cada

	mensaje enviado por un correo electrónico a la lista se distribuye automáticamente a la dirección electrónica de todos los suscriptores; por lo tanto es un correo dirigido a un gran auditorio.
GRUPOS DE DISCUSIÓN	Su objetivo es intercambiar información e ideas sobre un tema en particular; a diferencia de las listas de correo no implica el correo electrónico para enviar o recibir información pública. A lo que los usuarios tienden a referirse con el término grupo de interés esta fuera del contexto de la Internet y constituye una enorme red de información interconectada con la mayoría de los servicios telemáticos, incluyendo los de la Internet.
LA FUNCIÓN DE CHARLA O IRC	A diferencia de los grupos de discusión, la comunicación por charla se lleva a cabo directamente entre computadoras entre computadoras interconectadas y por lo tanto, solo pueden acceder a ella quienes estén conectados durante la sesión.

Dado que ya se analizó el concepto de delito informático y su relación con la Internet, es menester estudiar la clasificación de los delitos informáticos que la doctrina ha formulado, para así separar aquellas conductas que se escapan al tema de este trabajo.

2.3 CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Para clasificar el delito informático la doctrina tiene en cuenta tres criterios fundamentales: El subjetivo, el Objetivo y el Funcional.

2.3.1 Criterio subjetivo. Se centra en lo distintivo de los delincuentes informáticos, pues observa a los sujetos y a sus características; clasificándolos si es delito de cuello blanco, o si es un delito común, donde la persona no tiene una posición destacada en la sociedad; así mismo de acuerdo a si el criminal informático posee conocimientos técnicos en sistemas lógicos de información o desconoce por completo técnicas y lenguajes de información.

2.3.2 Criterio Objetivo. Este criterio clasifica los delitos informáticos acorde con el objeto material contra el cual recae o se dirige el comportamiento criminal informático y los agrupa de la siguiente manera:

Los fraudes Informáticos: Entendidos como aquellas actividades ilícitas que se cometen a través de la manipulación del sistema contra los programas de procesamiento de datos, entre ellas pueden citarse:

- Los daños engañosos – Datta diddling: Son las conductas referentes a las distintas formas de alteración de los datos contenidos en el ordenador, antes, o, durante su proceso informático.

- Los caballos de Troya: Consiste en insertar instrucciones de unificar terminología de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal, es decir, ejecuta funciones distintas a las previstas pues da instrucciones distintas a la computadora, de forma encubierta.

- La técnica del Salami: Es la desviación fraudulenta de céntimos de diversas cuentas bancarias a otra de la cual dispone el autor.

EL Sabotaje informático: Es el acto de borrar, suprimir o modificar sin autorización, funciones o datos de computadora con intención de obstaculizar el

funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

- Bombas lógicas: Son aquellas introducciones lógicas que se realizan en un programa informático que se activará ante determinada circunstancia (fecha, orden, etc.), dañando o destruyendo los datos informáticos contenidos en el ordenador[25] o modificando datos en un momento dado del futuro.

-Virus informáticos: Constituyen una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos, convirtiéndose en situaciones secuenciales de efectos previsibles, con capacidad de reproducción en el ordenador y su expansión y contagio a otros sistemas informáticos[26]. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

El espionaje informático: Debe entenderse como la obtención de datos o la copia de los mismos con el ánimo lucrativo. Dentro de esta clasificación se destaca:

- La Fuga de datos: modalidad informática de las prácticas de espionaje industrial, aparece en tanto todas las empresas y entidades custodian sus informaciones más valiosas en los archivos informáticos, posibilitándose su sustracción

El acceso no autorizado a servicios informáticos: Es el acceso no autorizado a sistemas informáticos por motivos diversos va desde la simple curiosidad, como en el caso del hacker, hasta llegar a actividades criminales de mayor repercusión informática. Se presenta de las siguientes maneras:

[25] PEREZ Luño, Antonio Enrique, Ensayos de Informática Jurídica, Biblioteca de Etica y Filosofia del Derecho, México, 1998, pag. 20.
[26] Ibidem. Pág. 32.

-Las puertas falsas: (Trap Doors) Conducta consistente en la introducción a los sistemas informáticos a través de accesos o "puertas" de entrada no previstas en las instrucciones de aplicación de los programas, aunque, como bien ha subrayado Pérez Luño, estas conductas puedan ser verificadas sólo por quienes tengan un conocimiento cualificado de los sistemas informáticos víctimas[27].

-La llave maestra: (Superzapping) Se trata del uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en los sistemas de información; su denominación se debe a un programa denominado "superzap", que a modo de "llave maestra" permite ingresar a cualquier archivo, así se encuentre reservado.

-Pinchado de líneas: (Wiretapping) Esta modalidad consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se transmiten las informaciones procesadas[28].

2.3.3 Criterio Funcional. Desde este criterio los delitos informáticos son aquellas conductas que tienen por objeto el funcionamiento de los sistemas informáticos. Esta categoría mira el proceso informático o de procesamiento de datos, y a partir de este se propone la clasificación de los delitos así:

- Delitos contra la fase de entrada del sistema: o sustracción de datos"[29], consiste en tomar algunos de los datos procesados por la computadora sustrayéndolos a través del medio magnético, óptico o magnético – óptico, para luego ser leídos, manipulados o simplemente mantenidos en otra computadora.

[27] Ibidem, pág. 20.
[28] Ibidem, pág. 21
[29] Peña Helen, Delitos informáticos. División de estudios de posgrado. Facultad de Derecho. UNAM., México, 1999, pag. 68

- Atentados contra la fase de salida del sistema: Se efectúa fijando un objetivo al funcionamiento del sistema informático, creando instrucciones falsas o fictas las cuales la computadora recibe y asume como ciertas, ejecutando la instrucción normalmente. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

- Atentados contra los programas del sistema: Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en "modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas"[30], al programa computacional. Con esto se busca desorientar las funciones del programa para buscar un beneficio o aprovechamiento propio[31]

[30] Ibidem, Pág. 72.
[31] Soler, José A. El delito Informático. Revista Protección y seguridad, mayo – junio de 1996, España, Pág. 29

3. ANÁLISIS SUSTANCIAL DE LOS DELITOS INFORMATICOS

El capitulo realiza un análisis sustancial de los delitos informáticos en torno a la legislación penal Colombiana para determinar si el ordenamiento jurídico tipifica los delitos informáticos, en especial, los cometidos a través de la internet, caso contrario, se da la necesidad de incluir en el derecho penal vigente una tipificación de los delitos informáticos, creando tipos penales nuevos o modificando los existentes.

Los delitos informáticos no serán sancionados si no existe previamente una descripción típica de estas conductas en el estatuto penal, de lo contrario es imposible establecer sanciones penales a los infractores, debido al principio de legalidad vigente en el derecho penal colombiano. El principio de legalidad enseña que no todas las conductas ejecutadas por los sujetos son de interés para el derecho penal , solo las acciones que afectan principios, valores y derechos aceptados de manera universal , imprescindibles para la convivencia humana; por tal motivo, la ausencia de preceptos o normas que no incriminan conductas realizadas por los sujetos , permite realizar cualquier actividad sin temor de ser objeto de represión punitiva. No obstante, la no incriminación de conductas que afectan a bienes jurídicos como la información y la intimidad personal, conlleva al freno y colapso de los sistemas de información y las garantías ofrecidas para las relaciones de intercambio cultural, social y económico entre los habitantes del mundo, de ahí la necesidad de tipificar las conductas que atentan contra los bienes informáticos en la legislación Colombiana.

El principio de legalidad, circunscrito en la máxima *nullum crimen, nulla poena sine lege*, adquirió carácter fundamental en el derecho penal Colombiano, como principio constitucional, independiente de cualquier teoría de la pena, reconocido

por el artículo 29, inciso segundo de la Carta Política y acogido en el artículo 6 de la ley 599 de 2000, actual código penal de Colombia [32] , el cual ha de interpretarse armónicamente con el artículo 10 (ibidem) que consagra el principio de tipicidad.

La tipicidad, concepto dinámico y funcional, presupone la adecuación entre un hecho existente en la vida real y una descripción normativa, ante un nexo de dependencia temporal o personal.[33]. Sugerida, por vez primera en 1906 como elemento integrante del delito por E. Von Beling, este principio da nacimiento a la figura jurídica del tipo penal.

El tipo, sustantivo, proveniente del latín typus, significa, símbolo representativo de una cosa figurada o imagen principal de algo a lo que se otorga una fisonomía propia; por tanto, el tipo es la descripción de la conducta o actos (acciones u omisiones) considerados delictivos por el legislador, encargado de otorgar relevancia penal a los diversos comportamientos ,quien las representa para su sanción, mediante técnicas legislativas, en proposiciones o figuras lingüísticas escritas, denominadas tipo penal, descripción típica, figura legal o figura típica; por ello, el tipo penal es un instrumento legal, lógicamente necesario y de naturaleza descriptiva, cuya función es la individualización de conductas humanas. [34]

En consideración al aspecto objetivo, abordará entonces el examen de los sujetos que actúan en las conductas criminales informáticas, en especial, las cometidas a través de la Internet., posteriormente se mencionan las principales acciones realizadas por el sujeto activo de las conductas criminales informáticas, se analiza el objeto material en que recaen las acciones y se estudia el concepto,

[32] El Art. 6 ley 599 de 2000 establece: Ninguna persona podrá ser sancionada por actos u omisiones que no fueren previstos como delitos, faltas o infracciones en leyes preexistentes.

[33] VELAZQUEZ, Fernando. Manual de Derecho Penal, Ed Temis. Bogota 2002, Pág. 250

[34] SAFARONNI, Eugenio Raúl. Manual de Derecho Penal, parte general. Ediar, Buenos Aires, 1979, Pág. 56

reconocimiento jurídico y relación de los objetos jurídicos de la intimidad y la información; consecutivamente se analiza la atipicidad tanto relativa y absoluta de los delitos informáticos , y por último se analiza los tipos penales considerados informáticos ,consagrados en el código penal vigente (Ley 599 de 2000).

3.1 SUJETOS JURÍDICOS DE LOS DELITOS INFORMÁTICOS

Existen dos clases de sujetos que intervienen en la ejecución de toda conducta punible: El sujeto activo y el sujeto pasivo. La teoría del derecho penal distingue como sujeto activo del delito aquella persona que lleva acabo la conducta tipificada en la ley y al sujeto pasivo como la persona titular del bien jurídico que el legislador protege en el respectivo tipo legal y que resulta afectada por la conducta del sujeto activo[35].

3.1.1 Sujeto Activo en el delito Informático. Es necesario determinar el sujeto activo de los delitos informáticos para garantizar seguridad jurídica en el momento de imputar responsabilidad penal, pues debe dejarse claro que la teoría general del delito no ha visto la posibilidad de imputar responsabilidad penal a las máquinas o a entes colectivos, en los hipotéticos casos de asociaciones de piratas informáticos o empresas dedicadas a divulgar el terrorismo y pánico informático y financiero.

Edwin Sutherland [36]determina que la definición de delitos informáticos no es de acuerdo al interés protegido, como sucede en los delitos convencionales; sino de acuerdo al sujeto activo que los comete; a su vez señala que el sujeto activo de los delitos informáticos presenta características de ser una persona de status socioeconómico alto, por tanto su comisión no puede explicarse por pobreza ,

[35] VELAZQUEZ, Fernando. Manual de Derecho Penal. Ed Temis. Bogota 2002, Pág. 263
[36] SUTHERLAND, Edwin H. El delito de Cuello Blanco. Ediciones Endimión. 2000, Pág. 157.

mala habitación, carencia de recreación, falta de educación, poca inteligencia o inestabilidad emocional.

Los autores de esta clase de delitos son considerados respetables, existiendo indiferencia en la opinión pública, sobre los daños ocasionados a la sociedad por las transgresiones que cometen. Los sujetos que realizan los delitos informáticos son personas que poseen habilidades en el manejo de sistemas informáticos, pues generalmente su situación laboral los lleva a estar en lugares estratégicos donde se opera información de carácter sensible, a su vez, son hábiles en el uso de sistemas lógicos-computacionales.

Los sujetos activos de los delitos informáticos son diversos, diferenciándolo entre sí: la naturaleza de los delitos cometidos de esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes. Algunos individuos que cometen delitos informáticos son los seducidos por la oportunidad, ejemplo, los engañadores de datos, tipo común de delincuente por computador, se trata de personas que cometen fraudes cambiando los datos que serán procesados.

En la década de los años 90 los criminales informáticos se clasificaron con los siguientes apelativos:

- Sombrero Negro: Calificados como terroristas y mercenarios, usaban sus conocimientos para acceder a bases de datos que luego vendían.

- Sombrero Gris: Calificados como piratas, dedicaban a demostrar su capacidad para vulnerar sistemas informáticos, su acción no estaba encaminada a causar daño.

- Sombrero Blanco: Calificativo dado a las personas dedicadas a detectar errores y fallas en los sistemas de seguridad, las cuales advertían cómo remediar el problema.

La distinción, según el grado de conocimiento, de los sujetos activos de delitos informáticos determina la forma, espacio y tiempo de actuar. Los doctrinantes Julio Téllez Valdez, y María Luz Lima[37] señalan como grupos originarios de sujetos activos de delitos informáticos a los hackers, crackers y phreakers ; los cuales dirigen su actuar en violentar la información almacenada en sistemas computacionales y la transmitida en la internet.

El hacker es la persona interesada en el funcionamiento de sistemas operativos; es aquel curioso que llega a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. La palabra hacker es un término ingles que caracteriza al delincuente silencioso o tecnológico. El hacker es capaz de crear su propio software para entrar a los sistemas de información; para él su actividad es un reto intelectual que no pretende producir daños justificándose en un código ético, que se caracteriza por: El acceso a los ordenadores y a cualquier cosa le puede enseñar como funciona el mundo, toda la información deberá ser libre y gratuita, la autoridad se desconoce y promueve la descentralización de la información.

- El cracker es la persona que se introduce en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, en general a causar problemas. Tiene dos pautas de comportamiento: a) Penetrar en un sistema informático para robar información y b) Desproteger

[37] TELLEZ VALDEZ, Julio, Derecho informático, Editorial Mc Graw Hill, México, 1997. Pág.13 y LIMA Maria de la Luz, El Delito Electrónico, Ed Ariel, México, 1999. Pág. 22.

todo tipo de programas con el objeto de hacerlos plenamente operativos como los programas comerciales que presentan protecciones anti-copia. El cracker es aquel hacker fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas, técnica que es difundida en la internet.

- Phreaker o cracker de teléfono es el especialista en telefonía, posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles; así mismo, conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Los phreakers buscan burlar la protección de las redes públicas y corporativas de telefonía, cuyas redes de comunicaciones son soportadas y administradas desde sistemas de computación con el fin de poner a prueba conocimientos y habilidades, pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de hacking a sus servidores.

- Lammers: Son los sujetos que aprovechan el conocimiento adquirido y publicado por los expertos, son despreciados por los hackers por su falta de conocimiento y herramientas propias para la realización de conductas informáticas.

- Gurus: Calificativo dado a los sujetos considerados maestros y orientadores para enseñar o sacar de cualquier duda al joven hacker. Son personas adultas, de amplia experiencia sobre sistemas informáticos o electrónicos El guru no esta activo, pero absorbe conocimientos; practican conocimientos propios enseña las técnicas básicas.

- Trashing: El objetivo de este sujeto es la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Las acciones realizadas corresponden a una desviación del procedimiento conocido como reingeniería social.

3.1.2 El Sujeto Pasivo en el Delito Informático. El sujeto pasivo del delito, para el estudio de los delitos informáticos, "es sumamente importante, ya que mediante él se pueden conocer los diferentes ilícitos cometidos por los delincuentes informáticos."[38]

Una entidad bancaria puede ser sujeto pasivo de delitos cometidos mediante operaciones computarizadas, así mismo los ahorradores pueden llegar a ser sujetos pasivos y al mismo tiempo los perjudicados con la acción delictiva que recae sobre los depósitos bancarios.[39]

Es necesario conocer a la víctima de estos delitos para así prever un sinnúmero de modalidades comisivas, puesto que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de sus sujetos activos. Directa o indirectamente todos somos víctimas del delito por computador afirmaba Bloom Becker[40]. Mientras el delito por computador sea visto como un espectáculo, se verá como un hecho que no concierne o que no pone en peligro ningún interés, pero una vez que se considere que todos son víctimas, se pensara que ya no es posible ignorar los retos sobre la seguridad de los sistemas.

---

[38] TELLEZ, Valdez, Julio. Derecho Informatico. México. Ed. Mc Graw Hill 1996 Pág. 48.

[39] . GUERRERO, Mateus. María Fernanda. Fraude informático en la Banca, aspectos criminológicos. Ediciones jurídicas 1995,Pág 49.

[40] BLOOM BECKER, Buck. Grandes estafas por computador. Ed. Ediciones jurídicas, Bogotá 1995, pág. 92

3.2 OBJETO MATERIAL

La situación de impunidad en los delitos informáticos aumenta de manera acelerada, en especial los que afectan la parte lógica de los sistemas computacionales debido a que no se tiene la claridad sobre la naturaleza jurídica del objeto material en esa modalidad de delitos.

El objeto Material: "es aquello sobre lo cual se concreta la vulneración del interés jurídico que el legislador pretende tutelar en cada tipo y hacia el cual se dirige la conducta del sujeto agente"[41] ; el objeto material puede ser una persona, una cosa o un fenómeno.

Dentro del estudio de las conductas criminales informáticas se observa que estas recaen sobre objetos materiales reales y en el fenómeno de la información.

3.2.1 Objetos materiales reales. Las conductas informáticas en los que el objeto de la acción es un objeto material relacionado con la informática ya están tipificadas y atentan contra bienes jurídicos definidos; por ejemplo, destruir un ordenador a golpes (delito de daños), robar disquetes (delito de hurto en su caso en concurso con un delito contra la intimidad); o cualquier medio electrónico diseñado o adaptado para emitir o recibir señales ; vale decir, con medios informáticos, electrónicos o telemáticos, tanto de hardware (equipos computacionales o unidades periféricas: Modem, impresoras, videocámaras, scanner, tableros ópticos, multimedia, cámaras digitales, etc.) como de software (programas de computador utilitarios, educativos, publicitarios, chats room, páginas de web, www –world word web-- hipertexto, correo electrónico, tableros electrónicos, lúdicos, etc.) y sean idóneos para el tratamiento o procesamiento de datos desde la recolección, almacenamiento, registro, procesamiento, utilización

[41] LOPEZ, Escobar. Derecho Penal Básico. Tomo I, Edit leyer, Bogotá 2000, Pág. 23.

hasta la transmisión de datos personales visuales, de texto o de sonido, o todos a la vez, o el envío y recepción de mensajes de datos o el intercambio electrónico de datos o documentos.

3.2.2 El objeto fenomenológico de la información. La información es un medio idóneo para afectar la intimidad, la libertad, el patrimonio económico individual, e incluso la vida o integridad personal. Esta última hipótesis podría presentarse con la modificación fraudulenta de los tratamientos médicos efectuados a un paciente o de los medicamentos suministrados, cuando obren en la base de datos de un hospital; o la tragedia que podría presentarse para los pasajeros de un navío, cuando un terrorista o un psicópata se introduce al computador de ésta y modifica la ruta, las condiciones de navegación o la presencia de otros medios de transporte. Con esta conducta se afecta el derecho individual a la inviolabilidad de las comunicaciones; con lo cual se ponen en peligro los derechos individuales a la intimidad e inviolabilidad de comunicaciones privadas.

La información como objeto material ha llevado al doctrinante Rivera Llano[42] a clasificar los delitos informáticos en:

-Delitos contra la información por creación.
-Delitos contra la información por destrucción.
-Delitos contra la información por el uso indebido.
-Delitos contra la información por sustracción.

3.3 BIENES JURÍDICOS EN LOS DELITOS INFORMATICOS

[42] RIVERA LLANO. Dimensiones de la Informática en el Derecho, Ed. Jurídica Radar, Bogotá, 1995.Pág. 25

Los bienes jurídicos tutelados y afectados por los delitos informáticos pueden ser numerosos, tales como: El honor, la propiedad y la fé pública[43]; para algunos autores como Molina Arrubla: " El bien jurídico tutelado es el patrimonio económico, ya que la mayoría de forma delictiva que se comete con computadoras oscilan entre el hurto, la estafa, fraude, abuso de confianza y el daño sobre la información, como algo que reviste por sí solo un valor económico o ideal suficientemente interesante[44]. El profesor Romero Casabona[45]. en un estudio sobre el delito informático, respecto de los bienes jurídicos que pueden resultar afectados con los delitos informáticos, afirma: la cuestión de sí la delincuencia informática supone la aparición, en el mundo de la dogmática penal, de un nuevo bien jurídico protegido merecedor de protección específica, se convierte como tantas otras cuestiones jurídicas, en algo relativo. Pues, si la novedad de la mencionada delincuencia radica fundamentalmente en los medios utilizados ,que ciertamente pueden hacer más dificultosa la averiguación y la prueba de los hechos, el bien jurídico protegido en cada caso será el que corresponda a la naturaleza de la infracción cometida: la intimidad, la propiedad, la propiedad intelectual o industrial, la fe pública, el buen funcionamiento de la Administración, la seguridad exterior o interior del Estado; ahora bien, si, por el contrario, se trata de delitos que recaen sobre objetos informáticos propiamente dichos como: aparatos, programas y datos ; podremos considerar, la aparición de un bien jurídico nuevo: La información.

En aspectos generales se cree que el bien jurídico afectado y que por tal es el que debe tutelarse por el ordenamiento jurídico Colombiano es la información, en tratándose de conductas cometidas que se valen de medios informáticos. La profesora española Gutiérrez Francés,[46] da entender que el bien jurídico afectado

[43] FERNÁNDEZ, Castro Juan Diego. Abogacía e Informática, El delito informático, en: Revista del Colegio de Abogados Penalistas del Valle, Volumen IX, Página 208 – 218.
[44] MOLINA, Arrubla Carlos. Introducción a la Criminología. Editorial Biblioteca Jurídica, Medellín, 1981, Pág. 32.
[45] CASABONA Romero, Hacia un concepto de delito Informático, Ponencia presentada al XI Congreso Internacional de Informática, Buenos Aires, Agosta, 1991. Pág. 21.
[46] GUTIERREZ Francés, Informática y derecho, Madrid, Editorial Alianza, 1999.Pág. 43.

con el delito informático es la información: almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos; posición que los autores del presente trabajo comparten; ya que este es un bien jurídico correlativo con los actos, hechos y omisiones que lo vulneran. De allí que se diga que los delitos informáticos podrán vulnerar derechos personales, sociales o familiares utilizando aparatos físicos tales como el hardware, computador u ordenadores con todos sus componentes materiales: Cpu, monitor, teclados, unidades periféricas de salida y entrada: Impresora, modem, tele transmisión, mouse, lápiz óptico, tablero electrónico; e igualmente los programas o software que están contenidos en los soportes físicos: Discos flexibles y duros, que constituyen lo que se conoce como la parte lógica del computador.

En síntesis, resaltan dos bienes jurídicos valiosos que se destacan como los más vulnerados por los delitos informáticos, estos son: La intimidad y la información.

3.3.1 La intimidad. La intimidad como derecho está previsto en la Carta Política al establecer: "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 reconocer, a actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades publicas y privadas" [47] ; entendido por nuestra corte constitucional como una norma que no es una simple retórica de derecho, sino un derecho constitucional y multicomprensivo al expresar "…cuando la doctrina se refiere a la intimidad bajo la forma de protección de la vía privada lo hace tanto en un sentido amplio como en un sentido estricto. En los primero, la expresión designa todas las reglas jurídicas que tienen por objeto proteger la vida personal y familiar; en un sentido más estricto la expresión se emplea también para designar exclusivamente un conjunto

[47] CONSTITUCION POLÍTICA DE COLOMBIA. ARTICULO 15. Colección códigos Brevis, Editorial Leyer, 2001.

de normas que tiene por fin la protección de las personas contra atentados que afectan particularmente el secreto o la libertad de la vida privada.."[48]

La intimidad es un derecho previsto en legislaciones consuetudinarias anglosajonas y en ordenamientos jurídicos escritos de donde se nutrió el constituyente de 1991 para elevarlo a rango constitucional; este derecho se reconoce a finales del siglo XIX en los Estados Unidos, plasmándose luego en la Constitución de 1958 de Francia, en 1972 en Alemania, y en 1978 en España. En Colombia el proyecto de ley No. 73 de 1986 por medio del cual se crea el estatuto de protección de la intimidad de las personas frente a los sistemas de información y a los bancos de datos"[49], fue un antecedente de demostración sobre la preocupación de las conductas criminales, que hoy día, denominamos delitos informáticos; es dicho estatuto donde se torna la idea de: Facultar al legislador para delimitar el uso de la información y garantizar bienes jurídicos como el honor, la intimidad personal y familiar de los ciudadanos y el legítimo derecho; para así: Evitar la posible utilización de conductas que atenten contra la informática con técnicas de recolección y almacenamiento de datos en los que se puede exponer la privacidad de las personas.[50]

La Constitución Colombiana de 1991 estableció en su artículo 15 el derecho a la intimidad personal y familiar, el derecho al buen nombre, y el derecho a la rectificación de datos , el segundo y el último son derechos de proyección exterior, es decir, buscan proteger la imagen de cada persona, de manera que se pretende que por mala información no se dañe el buen nombre y no se genere un yo distinto al real en las bases de datos, o sea que éste es el derecho protector del yo virtual; estos últimos derechos, pertenecen a la esfera pública de la persona.

---

[48] CORTE CONSTITUCIONAL DE COLOMBIA, Sentencia de Junio 16 de 1992. En Revista Legis Santa Fe de Bogota 1994.
[49] Anales del Congreso No. 92, Septiembre 16 de 1986, página 1-4
[50] RIASCOS GOMEZ, Libardo. La Constitución de 1991 y la informática Jurídica. Universidad de Nariño 1997, Pág. 45

En el derecho constitucional colombiano han surgido múltiples opiniones respecto del derecho a la intimidad. En el texto de Vladimiro Naranjo[51], se toma el derecho a la intimidad o privacidad desde la doctrina francesa de Montesquieu, quien estableció dos aspectos fundamentales dentro del derecho a la seguridad personal; el primero, es el que garantiza las no detenciones arbitrarias, es decir, el respeto al debido proceso, y cuya garantía es el habeas corpus; el segundo, es el derecho a la intimidad o privacidad, que garantiza la inviolabilidad de la correspondencia y de domicilio, garantías que se quedan cortas en tiempos contemporáneos; pero que por vía analógica histórica podrían abarcar lo que actualmente consideramos espacios íntimos.

La intimidad o privacidad se considera parte del derecho a la seguridad personal y, junto con los derechos a la seguridad económica y a la seguridad social, se enmarcan dentro de los derechos de la seguridad, los cuales garantizan la libertad pues son su garantía de protección. En una visión , poco profunda, se estudia el derecho a la intimidad como derecho fundamental, donde la intimidad es el espacio de la personalidad de los sujetos que no puede llegar a ser por ningún motivo, salvo la propia elección, de dominio público; entonces ,la intimidad busca proteger el espacio privado, y se estructura como un derecho protector frente a las injerencias del Estado y de los particulares en la esfera privada; de este modo hace parte de la vida intima, la vida familiar, la vida sexual, las anomalías físicas y síquicas, los secretos sobre el estado civil y la filiación, los escritos privados, la correspondencia de cualquier tipo y las situaciones de angustia, dolor y abatimiento; así pues es un derecho protector de la personalidad.

Para el análisis de la intimidad o privacidad se expresa que la intimidad como concepto se estructura a partir de la noción de privacidad. Lo privado es la expresión de la no intromisión del Estado en los asuntos personales, de ahí que en la intimidad se encuentra un espacio de doble libertad, libertad de la intrusión

[51] VLADIMIRO, Naranjo. Teoría Constitucional Colombiana, Temis, Bogota , Pág. 93.

del Estado y de la economía, y libertad de revelar lo que se quiere de sí, sólo a quien cada cual quiere . Es lo privado un concepto que se desarrolla en contraposición a lo público y, aunque suene obvio, se desarrolla a partir de tal concepto ,es por esto, por lo que el derecho a la intimidad se ha desarrollado como un derecho fundamental, junto con el desarrollo de la prensa y en general de las tecnologías de la información; pues la expresión y la información como libertades suelen inmiscuirse con la vida y la persona de personajes públicos, y es por tal motivo que, en reacción a tales actitudes humanas comunicativas, se creó la conciencia social de un derecho que protegiese la intimidad y el espacio personal.

El problema de la intimidad se halla en la autonomía; puesto que desde Kant es claro que el hombre goza del derecho a autodeterminarse, derecho previo a cualquier otro derecho dentro de una democracia liberal. Uno de los aspectos sobre los cuales se puede determinar es respecto de cuán grande es su esfera privada y cuán grande es su esfera pública, pues como se ve, es el hombre el que revelando o limitando la información que aparece de él en bases de datos y demás sistemas informativos, puede en teoría establecer cuál será el perfil de su vida que es parte del dominio público y cuál es parte de su dominio privado. Sólo a partir de la autonomía que su condición humana le concede, el hombre puede o no ampliar su privacidad.

Referente a las posiciones de la Corte Constitucional en torno al derecho de la intimidad, se encuentra que la primera sentencia fue la T-414 de 1992 [52] , donde se demuestra un perfil iusnaturalista, al establecer los siguientes aspectos:

[52] Corte Constitucional, sentencia No. T-414 de 1992, Magistrado Ponente Dr. Ciro Angarita Barón, Santafé de Bogotá, D.C.

- La intimidad se protege como una forma de asegurar la paz y la tranquilidad que exige el desarrollo físico, intelectual y moral de las personas, vale decir, como un derecho de la personalidad.

- La intimidad es un derecho general, absoluto, extrapatrimonial, inalienable e imprescriptible frente al Estado como a los particulares por ser un derecho de la personalidad. ; por lo tanto, toda persona es titular a priori de este derecho y el único legitimado para emitir la divulgación de datos concernientes a su vida privada.

- La intimidad se protege para asegurar la paz y la tranquilidad, pues, las tecnologías de la información están llevando a limitar la privacidad, la intimidad, y debido a esto se necesitan mecanismos jurídicos nuevos de protección.

En sentencias posteriores la Corte Constitucional afianzó esta teoría sobre la naturaleza del derecho a la intimidad, de manera que, características tan controvertibles como su absolutividad, se plasmaron teniendo como fundamento la dignidad humana, elemento kantiano incluido en el discurso constitucional moderno, que lleva a la convicción de la existencia de derechos absolutos; pero la absolutividad del derecho a la intimidad ,se vino a menos, luego de las sentencias SU-086 de 1995 y T-696 de 1996, donde se asentó que la intimidad no puede ser tomada como fundamento de excusa para que una central de información no establezca en sus bases de datos el incumplimiento de un deudor; así la Corte le quitó absolutividad al derecho a la intimidad, haciéndolo ceder ante casos en los que el titular del derecho tuviera obligaciones no cumplidas para con otros sujetos.

3.3.2 La información. Para la Real Academia de la Lengua Española, información es enterar, dar noticia de algo y que en términos jurídicos hubiera significado tan sólo una simple acumulación de datos, no obstante se ha ampliado,

transformándose como advierte Gutiérrez Francés: "En un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía." [53]

La Información es jurídicamente un activo más respecto del que se pueden ejercer prerrogativas patrimoniales y morales y debe ser entendida como un proceso en el cual se englobe tres supuestos como son: almacenamiento, tratamiento y transmisión de datos[54]; como bien jurídico, merece especial protección del Estado, pero no es considerado por la legislación tan importante como para merecer la existencia de ese cuerpo intencionalmente dirigido a protegerlo. El Profesor Riascos Gómez manifiesta que no es un bien jurídico; de ser un bien jurídicamente tutelado se consideraría como de interés para toda la sociedad; con implicaciones en lo económico, en la intimidad, en la libertad y en otros órdenes pero sin perder su propia identidad de bien jurídico de interés público o social. [55]

La seguridad jurídica en el bien jurídico de la información, es inexistente debido a que la información no es considerada un bien jurídico que por sí mismo merezca la protección del Estado y porque las conductas que constituyen incidentes de seguridad no han sido tipificados como delitos.

Desde el punto de vista económico y jurídico la información es un bien, el cual económicamente permite ser transado a través del mercado, siendo tanto de factor de producción como producto; jurídicamente, también es considerado como objeto de la propiedad, pues como bien económico, es objeto del poder y el mejor mecanismo para sustentarlo y mantenerlo.

---

[53] GUTIERREZ Frances, Informática y derecho, Madrid, Editorial Alianza, 1999.Pág. 32.
[54] BENEYTO Juan, Información y sociedad, Madrid, Alianza Editorial, 1999.Pág. 45.
[55] RIASCOS GOMEZ, RIASCOS GOMEZ, Libardo. La Constitución de 1991 y la informática Jurídica. Universidad de Nariño 1997.Pág. 54.

La concepción jurídica del bien información se da por ser un bien fenomenológicamente incorporal, pero jurídicamente no se ajusta dentro de la definición de bien incorporal hecha por la legislación; por otro lado considerarlo un bien mueble es imposible ya que la analogía es imperfecta pues no comparten los bienes que se llaman muebles ninguna característica común con la información, en tanto los muebles son corpóreos, es decir , son entidades físicas determinables, cosa que no sucede con la información misma. Para dar una salida jurídica se plantea que el reconocimiento del bien jurídico información se da a través del derecho de propiedad; así pues, dado que sobre los bienes se genera el reconocimiento del derecho de propiedad, la existencia de un reconocimiento de la propiedad sobre la información es necesariamente un reconocimiento de la calidad de bien que tiene la información.

El derecho de la información fue regulado junto al derecho de libertad de expresión y de opinión en la Carta Política colombiana en el artículo 20 [56], de la libertad de expresión se desprende la libertad de información donde se desenvuelve como facultad humana para recibir información y como práctica humana para difundir información.

La jurisprudencia de la Corte Constitucional en materia del derecho de la información ha sido muy variable; inicialmente la sentencia que puso de plano la presencia del derecho a la información y su importancia fue la T-414 de 1992 [57] donde se considera a la información como un bien, con la sentencia T- 473 de 1992 se menciona que el derecho de la información no es solamente el derecho

[56] CONSTITUCIÓN POLÍTICA DE COLOMBIA ARTICULO 20: “Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y de recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

[57] Corte Constitucional, sentencia No. T-414 de 1992, Magistrado Ponente Dr. Ciro Anganta Barón, Santafé de Bogotá, D.C.

de informar, sino también el derecho a estar informado.[58] Esta dualidad del derecho a la información se representa perfectamente en el articulo 20 de la Constitución Nacional, ratificado por la sentencia T-512 de 1992 al mencionar que el derecho a la información es un derecho de doble vía, en cuanto no esta contemplado, ni en la constitución, ni en ordenamiento, ni declaración alguna, como la sola posibilidad de emitir informaciones, sino que se extiende necesariamente al receptor de las informaciones.[59] En sentencia posterior se expuso la diferencia que existe entre estas dos libertades al decir que la libertad de expresión es una figura jurídica más amplia que la del derecho a la información. Abarca una generalidad que admite múltiples especies y, en virtud de la libertad de opinión y de pensamiento, no tiene tantas limitaciones como las que tienen el derecho a la información y el derecho de informar[60]. Limitaciones como se pone de plano en el texto constitucional resaltada en sentencias, como la T-332 de 1993 al exponer que el derecho a la información es de doble vía, característica trascendental cuando se trata de definir su exacto alcance: no cobija únicamente a quien informa -sujeto activo- sino que cubre también a los receptores del mensaje informativo -sujetos pasivos-, quienes pueden y deben reclamar de aquél, con fundamento en la misma garantía constitucional, una cierta calidad de la información. Ésta debe ser, siguiendo el mandato de la misma norma que reconoce el derecho, veraz e imparcial[61]; en sentencia posterior, el doctor Naranjo Mesa estableció que el derecho a la información es un derecho que expresa la

[58] Corte Constitucional, sentencia T- 473 de 1992, MP. Dr. Ciro Angarita Barón, Santafé de Bogota, D.C; 14 de Julio de 1992.

[59] Corte Constitucional, sentencia T-512 de 1992, Magistrado ponente Dr. José Gregorio Hernández Galindo, Santafé de Bogotá, D.C., nueve (9) de septiembre de mil novecientos noventa y dos (1992).

[60] Corte Constitucional, sentencia C-488/93, Magistrado ponente Dr. Vladimiro Naranjo Mesa, Santafé de Bogotá, D.C., veintiocho (28) de octubre de mil novecientos noventa y tres (1993).

[61] Corte Constitucional, sentencia T-332/93, Magistrado ponente Dr. José Gregorio Hernández Galindo, sentencia aprobada en Santafé de Bogotá, D.C., mediante acta del día doce (12) de agosto de mil novecientos noventa y tres (1993),

tendencia natural del hombre hacia el conocimiento donde el ser humano está abierto a la aprehensión conceptual del entorno para reflexionar y hacer juicios y raciocinios sobre la realidad y en virtud de esta tendencia ,toda persona se le debe la información de la verdad, como exigencia de su ser personal. La nueva aproximación de la Corte al derecho a la información es epistemológica al definir el derecho a partir de la tendencia del hombre por conocer; aun así, no lo define, puesto que exalta una de las cualidades que tiene el hombre, el acceso al conocimiento, y cómo este derecho es una manera de proteger tal característica resaltada por el juez constitucional como natural del hombre. En sentencia posterior se dice: "...el derecho a la información es una manifestación de la tendencia natural del hombre hacia el conocimiento de la verdad[62];en otras sentencias trata de clarificar dicha característica diciendo que "el derecho a la información expresa la propensión innata del hombre hacia el conocimiento de los seres humanos con los cuales se interrelaciona y de su entorno físico, social, cultural y económico, lo cual le permite reflexionar, razonar sobre la realidad, adquirir experiencias, e incluso transmitir a terceros la información y el conocimiento recibidos.[63] En sentencia del año 1995, se dio otra de las características del derecho a la información relacionada en cuanto a los sujetos intervinientes, al decir que "el derecho a la información no solamente cobija a los particulares, y en especial a los medios de comunicación y a los periodistas, sino que, como derecho constitucional fundamental, también cubre a las instituciones públicas y privadas. [64] ; Para 1996; la Corte hace una aproximación seria respecto del derecho a la información diciendo que:"El derecho a la información implica la posibilidad de recibir, buscar; investigar, almacenar, procesar,

[62] Corte Constitucional, sentencia T-563/93, Magistrado ponente Dr. Vladimiro Naranjo Mesa, Santafé de Bogotá, D.C., siete (7) de diciembre de mil novecientos noventa y tres (1993),
[63] Corte Constitucional, sentencia No, SU-056 de 1995, Magistrado ponente Dr. Antonio Barrera Carbonell, Santafé de Bogotá D.C., febrero diez y seis (16) de mil novecientos noventa y cinco (1995).
[64] Corte Constitucional, sentencia No. T-552 de 1995, Magistrado ponente Dr. José Gregorio Hernández Galindo, sentencia aprobada en Santafé de Bogotá, D.C., a los veintisiete días del mes de noviembre de mil novecientos noventa y cinco (1995).

sistematizar, analizar, clasificar y difundir informaciones, concepto éste genérico que cubre tanto las noticias de interés para la totalidad del conglomerado como los informes científicos, técnicos, académicos, deportivos o de cualquier otra índole y los datos almacenados y procesados por archivos y centrales informáticas. Se trata de un verdadero derecho fundamental, que no puede ser negado, desconocido, obstruido en su ejercicio o disminuido por el Estado, cuya obligación, por el contrario, consiste en garantizar que sea efectivo[65] ; pronunciamiento que develó el contenido del derecho, estableciendo su alcance al decir que "no es absoluto ni puede alegarse la garantía de su pleno disfrute como argumento para desconocer derechos de los asociados ni para evadir los necesarios controles estatales sobre la observancia del orden jurídico o sobre la prestación de los servicios que permitan canalizar informaciones al público. Por tanto, nada impide, a la luz de la Constitución, que el Estado contemple requisitos para recibir, manejar, difundir, distribuir o transmitir informaciones, ni que establezca restricciones o limitaciones por razón del imperio del orden jurídico, para hacer efectivos los derechos de las demás personas -tales como la honra, el buen nombre o la intimidad o con el objeto de preservar el interés colectivo[66].

3.4 ATIPICIDAD DE LOS DELITOS INFORMÁTICOS

Para precisar el concepto de atipicidad, es necesario tener de presente el concepto de juicio de tipicidad : entendido como la valoración que se hace con miras a determinar si la conducta objeto de examen coincide o no con la descripción típica en la ley"[67] ; es así que si una vez realizado el juicio de tipicidad,

[65] Corte Constitucional, sentencia No, C-073 de 1996, Magistrado sustanciador Dr. José Gregorio Hernández Galindo, sentencia aprobada según consta en acta del veintidós (22) de febrero de mil novecientos noventa y seis (1996).

[66] Corte Constitucional, sentencia No. C-073 de 1996, Magistrado sustanciador Dr. José Gregorio Hernández Galindo, sentencia aprobada según consta en acta del veintidós (22) de febrero de mil novecientos noventa y seis (1996).

[67] LÓPEZ, Escobar. Derecho Penal Básico. Tomo I, Edit LEYER , Bogotá. 2000, Pág. 36.

la acción examinada no encaja o no coincide con los caracteres imaginados por el legislador en el tipo concreto, se dirá entonces que no hay adecuación típica,[68] esto es lo que se conoce como atipicidad. La categoría en estudio tiene una faz positiva y otra negativa, dependiendo de los resultados a que lleve el juicio de las alternativas para el intérprete y el mismo juez ,al encontrarse ante la situación de ajustar el tipo de conducta a la normatividad existente, pueden ser: "que el concreto comportamiento se encuadre directa e inmediatamente en uno de los tipos de la parte especial, y que ante la imposibilidad de adecuación directa, encontrarse la falta total de adecuación al no haber tipo penal que consagre la conducta o porque al tratar de subsumirla adolece de por lo menos uno de los elementos constitutivos del tipo que en el caso concreto, de ser afirmativos puede conducir a afirmar la congruencia típica por presentarse los elementos objetivos y subjetivos de la figura; o, caso contrario, negarla, cayendo entonces en el terreno de la no tipicidad, que a su vez puede ser de carácter absoluto (cuando la conducta examinada no es subsumible en ningún tipo penal) o relativo (por no aparecer alguno o algunos de los elementos de la descripción, pudiendo ser comprendida por otro tipo penal[69].

Atipicidad relativa de los delitos informáticos

Como bien lo anota, Maria Clara Fernández,[70]tratar de averiguar si las conductas relacionadas con ilícitos informáticos tiene cabida en los tipos penales de la parte especial del código penal colombiano nos proporcionan un margen posible de reglamentación o de atipicidad relativa digna de tener en cuenta; ya que la falta de adecuación típica que distingue este fenómeno puede referirse a uno de los elementos que integran el tipo. Habrá tipicidad en relación al objeto, cuando este reúne las características señaladas en el respectivo tipo, como en el fraude

[68] FERNÁNDEZ, Carrasquilla Juan. Derecho penal Fundamental, Temis, Bogota 1989. Pág. 52.
[69] VELAZQUEZ, Fernando. Manual de Derecho Penal. Ed Temis. Bogota 2002, Pág. 245.
[70] FERNÁNDEZ, Maria Clara. Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos. Universidad Sergio arboleda. Santa Marta,2001. P.79

informático donde las probabilidades de adecuación se manifiestan en una atipicidad relativa respecto a los delitos contra el patrimonio económico, pues podría concretarse en tipos penales como en daño en bien ajeno, abuso de confianza, estafa, hurto simple o calificado ; de otra parte, puede también tener ocurrencia conductas que impliquen falsedad. Igualmente sucede en los ilícitos sobre bienes informáticos que por su naturaleza se perciben por los sentidos, como el hardware, al no presentar complicación en su adecuación. Todo entonces se define en función de la naturaleza del objeto material sobre el que se concreta la vulneración de un interés que el legislador está llamado a tutelar y sobre la propia conducta del agente que está gobernada por el verbo rector con algunos ingredientes descriptivos. Ahora bien, las implicaciones jurídicas que pueden surgir de la adecuación típica pueden o no ser una circunstancia de cierta gravedad, con esto se quiere decir que en los ilícitos sobre bienes informáticos que por su naturaleza se perciben por los sentidos, como es el hardware no presenta mayor complicación en su adecuación, en cambio, con los bienes intangibles como es el caso del software, la situación es totalmente diversa.

3.4.2 Atipicidad absoluta de los delitos informáticos. Es una forma de atipicidad donde existe ausencia de tipo penal en las conductas que ontológicamente se observan, en este evento la conducta examinada no resulta ubicable en ningún tipo penal, simplemente porque no esta descrita por la ley como conducta punible. Se presenta por la falta o ausencia del tipo y, por ende, imposibilidad de imponer sanción alguna, conforme al principio que no hay delito sin tipicidad. Tal sucede con los delitos informáticos cometidos a través de la internet y que atentan contra los aparatos lógicos, como:

Fraudes cometidos mediante la manipulación del computador, entre los que se destacan: Manipulación de los datos de entrada y salida, manipulación de programas y el fraude efectuado por manipulación informática.

Falsificaciones informáticas que comprende los daños o modificaciones de programas o datos computarizados como: El sabotaje informático, virus, gusanos, bombas lógicas o cronológicas

3.4.3. Conductas que revisten atipicidad absoluta.

La manipulación de programas.

La manipulación de programas es realizada por sujetos con altos conocimientos técnicos en informática, especialmente en programación, las manipulaciones al programa llevan consigo otras tareas que hacen imposible descubrir su identidad. La conducta consiste en modificar los programas existentes en el sistema de la computadora o en insertar nuevos programas o nuevas rutinas al programa computacional, con el fin de desorientar las funciones del programa y buscar un beneficio o aprovechamiento propio.

Los métodos para la manipulación de programas, entre los que se destaca el caballo de troya, consiste en la manipulación de un programa destinado a cumplir una función determinada y el cual, al ser inicializado ejecuta funciones distintas de las previstas pues da instrucciones distintas a la computadora, de forma encubierta . La única manera de encontrar tales manipulaciones es mediante controles externos específicos sobre los programas, controles que generan costos a las empresas que necesitan de un sustento tecnológico computacional para evitar y descubrir los fraudes por manipulación; sin embargo la prevención es menos costosa, ya que con un simple procedimiento de catalogación/descatalogación de programas podrán quedar bloqueados los programas y no se podrá acceder a las librerías de archivos sino con permisos.

Manipulación de los datos de salida

La manipulación de los datos de salida se efectúa fijando un objetivo al funcionamiento del sistema creando instrucciones falsas, las cuales la computadora recibe y asume como ciertas, ejecutando la instrucción normalmente. La manera más simple de manipular los datos de salida, es a través de cajeros automáticos y tarjetas de crédito un modo de operar es mediante el credit carding, donde en toda tarjeta de crédito existen por lo menos tres elementos de seguridad los cuales el común de la gente no debe saber. Estos están insertos en el número de cuenta, el panel para la firma y la banda magnética.

El número de cuenta completo de una tarjeta de crédito común tiene veinte dígitos., a pesar de sólo son necesarios ocho para mantener la seguridad. Las manipulaciones para la comisión de este delito se dan en áreas del comercio electrónico y telefónico, en las ventas de artículos por televisión donde se paga por medio de una tarjeta de crédito. El panel para la firma si alguien roba una tarjeta de crédito, lo peor que puede hacer es borrar la firma, pues la mayoría de las tarjetas tienen un sistema para detectar si la firma fue borrada, el diseño de fondo que tiene el panel está hecho de manera tal que el borrar la firma daña el fondo, lo que hace la tarjeta inservible. La banda magnética elemento de seguridad dispuesto en la parte posterior de la tarjeta, tal banda es el número de cuenta o identificación similar y la expiración de la tarjeta. La información contenida en la banda se puede borrar únicamente con pasarle un imán sobre ella o a través del entrampado de datos que consiste en la introducción de información falsa al ordenador o la eliminación de datos reales cuyo destino es introducirlos en el ordenador.

La manipulación de cajeros automáticos se puede hacer de dos maneras; una es robar las tarjetas y sus claves para así usar el cajero automático, la otra es a través de una línea telefónica con la cual se conecta a la línea del banco.

Fraude efectuado por manipulación informática

Este tipo de fraude busca manipular los datos que se repiten constantemente en los procesos de cómputo, es decir, aprovecha las repeticiones automáticas de los procesos de cómputo. Existen varias técnicas especializadas, como la llamada salami o redondeo de cuentas, la cual consiste en la introducción o modificación de algunas instrucciones en determinados programas con el fin de reducir de forma progresiva los saldos. Esa reducción y redistribución, hace casi indetectable estos millonarios hurtos informáticos pues en el redondeo de la cuenta individual la pérdida es tan pequeña que el titular de ésta no se preocupa por tal disminución o aumento, de tal forma que nunca se denuncia la disminución o aumento injustificado; así pues, quien efectúa el hurto está seguro de que individualmente nadie se va a quejar; asimismo, los delincuentes, para evitar ser descubiertos, encubren las sumas acumuladas en cuentas de la misma entidad para que no se vean afectados los balances en general, y haciéndolos en sumas tales de forma que se eviten los controles del banco de cada cuenta, como los que se hacen en materia de lavado de activos.

Falsificaciones por vía informática.

La falsificación, en términos no jurídicos, es la acción o efecto de falsificar. Falsificar significa, imitar algo fraudulentamente; mediante las computadoras se pueden efectuar dos tipos de falsificaciones, según sea la computadora y los datos almacenados en el objeto de la falsificación o sea la computadora, instrumento de la falsificación: Como objeto la computadora es objeto de la falsificación cuando se alteran datos de los documentos almacenados en forma computarizada y como instrumentos cuando las computadoras son utilizadas para efectuar la imitación fraudulenta. Se pueden imitar mediante computadoras desde un documento de tipo mercantil como un cheque o hasta un billete. La computadora, para hacer dichas falsificaciones, necesita de cierto hardware para optimizar el resultado del

procedimiento, normalmente se utilizan scanner, impresoras, cámaras digitales, lectores y escritores de discos compactos.

Daños o modificaciones de programas o datos computarizados

Los daños o modificaciones de programas afectan al software o los datos almacenados por una computadora, son las conductas en que los sujetos activos destinan su tiempo, ya que, la principal función de dichos programas es quebrar una barrera de seguridad para destruir todos los datos que alberga otra computadora o simplemente acabar con datos específicos que la competencia tiene para el desarrollo de cierto nuevo producto; esta conducta describe múltiples tipos de conductas, lo cual es imposible conocerlas todas ya que siempre habrá alguien creando una nueva manera de romper un sistema de seguridad o simplemente una nueva manera de destruir los datos que contienen múltiples computadoras; los modos de operar comunes y que en cierto modo pueden llegar a afectar a cualquier persona son los sabotajes informáticos, es decir, los actos de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema; los cuales se cometen de las siguientes maneras:

Virus: Son muy conocidos dentro del mundo de la computación. Los primeros virus fueron detectados a principios de los años setenta, cuando la computación y la informática apenas estaban comenzando su desarrollo, fueron inventados y aplicados al sistema financiero, donde su intención era permitir la comisión de fraudes, ya que su función principal era cambiar ciertas órdenes del programa de tal manera que se pudieran desviar dineros de la entidad financiera a otras entidades. Ahora los virus son definidos de múltiple maneras, la más conocidas establecen que un virus de computadora es un programa encargado de ejecutar mandatos en el ordenador, transgrediendo los sistemas de seguridad y con la aptitud de ser propagados de computador a computador por medio de un código

que se une por sí mismo a los programas o filas del computador. Los virus se propagan en computadores personales pues son expuestos al contagio por obvias razones, ya sea el intercambio de filas, las cuales pueden contener virus, los préstamos de programas o a través de la red por medio del e-mail; y sus consecuencias van de la simple inserción temporal de una pequeña gráfica o de un mensaje, hasta llegar a destruir información contenida en la computadora o alterar las funciones de éste.

Gusanos: Su fin es buscar infiltrarse en la computadora y ejecutar ciertas órdenes, se diferencian de los virus ya que no se propagan o regeneran dado que su destino es específico; así el programa gusano se destruye después de introducir los códigos de instrucciones al ordenador.

Los correos electrónicos bombas: Son mensajes que causan daño a quien los recibe, de manera que destruye los datos dentro de un ordenador con el sólo hecho de mirar el mensaje; existen varios tipos de bombas para el correo electrónico, algunas van atadas al mensaje, el cual puede ser un programa, un virus o cualquier otra cosa que cause daños al computador, un tipo de correo electrónico bomba es la que se ejecuta con sólo seleccionar un mensaje enviado, con el efecto de paralizar el sistema al intentar ver el mensaje, pues quien lo envió deja intacto el encabezado pero borra algún código inserto en éste; otro tipo de carta bomba es la que tiene como función estresar el servidor del correo, pues se sobrecarga la fila y el servidor y estos fallan usualmente se da cuando alguien envía más de mil correos electrónicos con el mismo mensaje. Esta técnica es útil para quien la comete, ya que nunca se sabe quién envía el mensaje pues la operación hace colapsar al servidor por la sobrecarga de datos y no permite ver el mensaje. Otro tipo de correo electrónico bomba es la llamada mancha o goteo se da cuando alguien envía un correo electrónico tan largo que se estropea la fila y el archivo perteneciente al destinatario del correo, pues se sobrecarga de

información de manera que el servidor tiene como única solución borrar la carpeta del usuario.

Bombas lógicas o cronológicas : Son de las manipulaciones informáticas, las que poseen el mayor potencial de daño ;pues están destinadas específicamente a destruir o modificar datos por medio de ciertas instrucciones, órdenes que el sistema recibe de manera inesperada Se suele denominar bomba lógica o cronológica como el conjunto de instrucciones, o rutinas, que en un momento dado obliga al programa a ejecutar acciones no previstas con el fin de ocasionar daños ; a pesar de ser mecanismos de fácil ejecución pues son simples instrucciones al sistema, para su preparación se necesitan conocimientos técnicos específicos pues requiere de elementos avanzados en programación de las órdenes a ejecutar en cierto programa, además que el delincuente debe saber en qué momento explotara la bomba puesta en el sistema. Así pues, las bombas lógicas se suelen clasificar según las condiciones de tiempo o de modo necesarias para desencadenar el conjunto de instrucciones que la bomba desencadenaría. Estas son de varios tipos:

Fijas: Aquéllas en que se toma como referencia una fecha fija en la que se desencadenará la reacción esperada.

Variables: Aquellos que se activan con el cumplimiento de condiciones variables, es decir, el programa se activa en el momento en que se cumplan las condiciones que el programador ha exigido para que explote la bomba lógica. Pueden ir desde un simple número de registros hasta una cantidad determinada de iniciaciones consecutivas de un programa.

Aleatorias: También se le llaman mixtas; pues combinan las condiciones de tiempo, es decir, las fijas, y las condiciones de modo, es decir, las variables; así pues, se

ejecuta la bomba en la fecha y hora previstas si previamente se han cumplido las condiciones de ejecución en él preestablecidas.

3.5 TIPOS PENALES QUE ATENTAN CONTRA LA INFORMACIÓN.

En este acápite se analiza aquellos tipos penales consagrados en el código penal colombiano vigente; los cuales contienen conductas que atentan contra la información; sin embargo dentro del esquema que presenta el código se conocen como tipos protectores de los bienes jurídicos de la intimidad, libertad e integridad y formación sexual y libertad de trabajo; estos son:

Acceso abusivo a un sistema informático.

El acceso abusivo a un sistema informático está consagrado en el articulo 195 del C.P, tipifica la introducción en un sistema informático que se encuentre protegido con alguna medida de seguridad; la conducta descrita es de peligro concreto para el bien jurídico individual de la intimidad, pero es de lesión para el bien jurídico de la información teniendo en cuenta el criterio de la confidencialidad.
El ingrediente normativo de la conducta que se concreta en lo abusivo, implica que el sujeto activo usa mal, excesiva, injusta, impropia o indebidamente tal derecho. La conducta se tipifica cuando el sujeto activo se introduzca a sistemas informáticos de acceso restringido; confirma esta afirmación el que la norma haga referencia a introducirse en un sistema informático protegido con medida de seguridad. Las medidas de seguridad de un sistema no se limitan a las claves o login para acceder al mismo; sino que pueden incluir horarios de acceso o permanencia para las personas autorizadas; tiempos de uso; y áreas restringidas de acceso para usuarios.

La conducta contiene dos verbos rectores, alternativos; el primero, introducirse, es de mera conducta y de ejecución instantánea; el segundo, consiste en mantenerse en el sistema contra la voluntad de quien tiene derecho a excluirlo, es de ejecución permanente, aunque también de mera conducta y de peligro.

El sujeto activo de la conducta es no calificado, o indeterminado; este tipo en especial ha tenido como fin sancionar las conductas de los hackers o piratas informáticos. El sujeto pasivo puede ser cualquier persona que sea dueña de un sistema de procesamiento de información; así las cosas, puede ser perjudicado todo aquél que tenga en sus haberes un computador, o una agenda electrónica.

El objeto jurídico de la conducta en sentido amplio es la información privada; ya que el acceso a sistemas informáticos no afecta la intimidad sino en contados casos, como por ejemplo cuando se introduce en un sistema de información en el que se almacena la hoja clínica o historia clínica de los pacientes.

La conducta es antijurídica debido a que se accede a un conjunto de datos almacenados por el titular de la base de datos, o por aquél que ha generado dicho registro de datos para su uso personal o para el uso autorizado de terceros. Así, toda la información contenida en ésta, y protegida en éste, es en principio lo que el derecho busca proteger.

El elemento normativo del tipo, que califica la acción del sujeto, es la palabra abusivamente, noción normativa mixta; pues tiene un contenido jurídico y extrajurídico. La palabra abusivamente viene de abusivo, término que ha sido definido como aquél que se introduce a una práctica por abuso, y abuso, que viene de abusar, se define como su acción o efecto. El vocablo abusar significa usar mal, excesiva, injusta, impropia o indebidamente de algo o de alguien ; de este modo, cuando alguien abusivamente se introduce a un sistema informático, tiene que estarlo haciendo en exceso de las facultades que se la han conferido, de

manera antijurídica, debido a que la ley no le autoriza para hacerlo, de manera impropia, pues no está usando las vías adecuadas para realizar tal acción, o de manera indebida, ya que teniendo el deber de no hacerlo, lo hace.

El delito es autónomo; ya que el agente de la conducta simplemente acceda al sistema informático sin realizar ningún otro acto como dañar, modificar o destruir la información en él contenida y es considerado un delito de poder, ya que sólo unos cuantos tienen la capacidad para ejecutar este tipo de conductas.

Violación ilícita de comunicaciones

La violación ilícita de comunicaciones, regulada en el artículo 192 del C.P, tipifica las conductas de sustracción, ocultamiento, extravío, destrucción, interceptación, control o impedimento de comunicaciones privadas dirigidas a persona diferente de quien despliega esta conducta; adicionalmente tipifica la acción de enterarse indebidamente del contenido de las comunicaciones privadas y la revelación de las mismas. Por su parte el art{iculo 196 de Código Penal tipifica la violación ilícita de comunicaciones o correspondencia de carácter oficial, cuyas conductas consisten en la sustracción, ocultamiento, extravío, destrucción, interceptación, control o impedimento de comunicaciones, definiendo que estas deben recaer sobre las comunicaciones de carácter oficial; este tipo es una derivación del delito de violación de comunicaciones privadas, su principal característica es la calificación que se le da a la información, es decir, determinar que cierto tipo de información es de carácter oficial; no obstante la categorización de información como carácter oficial no quiere decir que la misma sea pública, pues esto llevaría a un contrasentido, dado que constitucionalmente no hay comunicaciones públicas que sean objeto del secreto o reserva , ya que la información oficial reservada no es pública en tanto no se esté en frente del proceso judicial, las etapas previas son de carácter privado y sólo se hacen públicas después de la resolución de acusación.

El sujeto activo es indeterminado al igual que en la violación ilícita de comunicaciones privadas, no puede ser sujeto activo, el autor de la comunicación o el destinatario de la misma, debido a que el proceso informativo ocurre entre estos sujetos. Aparte los sujetos pasivos de la conducta son el emisor y el receptor de la información, pudiendo ser uno o varios emisores y uno o varios receptores, estos deben ser oficiales, es decir, para que la conducta afecte al bien tutelado es necesario que el emisor o el receptor, o los dos, sean personas consideradas servidores públicos.

El objeto jurídico, en sentido estricto, son las comunicaciones oficiales y, en sentido amplio, es la información caracterizada como oficial. El objeto material de la conducta es la comunicación oficial, dirigida a otra persona determinada; es decir la información que es dirigida al funcionario o persona jurídica oficial.

La conducta, al igual que en el tipo de interceptación ilícita de comunicaciones privadas, es compuesta, ya que contiene varios verbos rectores, estos son: sustraer, ocultar, extraviar, destruir, interceptar, controlar, impedir y enterarse. Sustraer es apropiarse de la comunicación interceptada; ocultar es esconder o dejar fuera del alcance; extraviar significa desviar de su curso regular ,destruir es deshacer, extinguir ,eliminar, dañar; interceptar implica la simple detección de la información a través del medio de propagación; controlar es someter la comunicación, o la información al dominio del sujeto activo; impedir significa atacar o detener la información o la comunicación haciendo que el receptor no la reciba; así mismo la conducta tiene un elemento normativo, el cual se introdujo con el vocablo ilícitamente; esto implica que existe una interceptación de comunicaciones oficial licita, como la que se ejecuta con autorización de funcionario competente.
Existen muchos medios para la comisión de la conducta, como ocurre con la interceptación de llamadas telefónicas a través de la inserción de mecanismos destinados directamente a la captura de la información que fluye a través del

cableado interceptado; de esta manera, se puede generar una interceptación funcional través y en contra de medios telemáticos, como la internet, donde para obtener la información se capturan las modulaciones generadas por el modulador del ordenador o sistema informático interceptado, y luego se desmodulan a través de módem, obteniendo el contenido de la información que recorre el cableado.
La interceptación del correo electrónico o e-mail, al igual que el correo normal, está protegidos por este tipo penal, ya que se enmarca dentro de la definición que hemos dado anteriormente de comunicación.

La punibilidad para el delito de interceptación de comunicaciones privadas, y el delito de interceptación de comunicación privada oficial, es totalmente distinta, ya que para los primeros la punibilidad es simple multa, mientras, para los segundos es prisión de 3 a 6 años.

Utilización ilícita de equipos transmisores o receptores.

La utilización ilícita de equipos transmisores o receptores está consagrada en el artículo 197 del C.P .El sujeto activo de este tipo de conductas es cualquier persona, ya que, es indeterminado o no cualificado el sujeto.El sujeto pasivo de la conducta es el Estado, ya que lo que pretende proteger es el espectro electromagnético, y la utilización de éste sin su autorización le causa un detrimento patrimonial, ya que no puede explotar adecuadamente su monopolio.

El objeto material es todo aparato adaptado para recibir o transmitir señales de radio, televisión, etc. En este tipo, el objeto material no es la información sino los instrumentos que permiten generar ciertos procesos de comunicación personal regulados.

Los verbos rectores de la conducta son poseer y usar. Poseer implica, en este caso, la tenencia, la posesión propiamente dicha, y la propiedad.

El tipo alude a ciertas consideraciones respecto del papel del Estado y de las comunicaciones, cuyo medio de transmisión es el espectro electromagnético. Dentro de estos comportamientos, encontramos conductas como la de los grupos insurgentes que tienen en su poder aparatos sofisticados e telecomunicaciones, con los cuales se les facilita el traslado de información. ,también se encuentra la conducta de aquellos grupos de personas que compran una antena parabólica y transmiten tal señal a un conjunto de personas, o aquellos que con el ánimo de montar una emisora de corto alcance dentro de una población alejada, compran aparatos necesarios para tal fin y operan dicha emisora.

Sabotaje.

El sabotaje consagrado en el artículo 199 del C.P, se determinó como una conducta que simplemente protegía materialmente los elementos de trabajo necesarios para realizar la labor. El nuevo código adoptó la propuesta según la cual era necesario ampliar el tipo de sabotaje debido a la necesidad de incluir los sistemas informáticos; planteamiento acertado, ya que es de común ocurrencia que en el lugar de trabajo se utilicen sistemas informáticos para desempeñar la labor.

El sujeto activo es no calificado o indeterminado; además, el tipo contiene un ingrediente subjetivo consistente en la intención de suspender o paralizar el trabajo o actividad laboral, elemento que guarda concordancia con el título y bien jurídico que pretende proteger, debido a que la intención del agente tiene que ser desestabilizar la actividad laboral de manera que la paralice o la suspenda, ya que siendo otra la intención del autor, el delito que se adecuaría típicamente sería el de daño.

El Sujeto Pasivo se considera a partir de dos puntos de vista, según el daño que genera la conducta. Desde una visión estricta el objetivamente afectado con la

conducta es el empleador, sea, el Estado o un particular. Es el empleador por ser éste un delito de daño calificado por el objeto material dañado, el que sufre el detrimento patrimonial con la consumación de la conducta, es aquél que ha destinado sus bienes para el desarrollo de la labor que se pretende interrumpir, esto es, el empleador. Desde el punto de vista genérico el sujeto pasivo es el Estado, ya que el bien jurídico tutelado y dañado no es el patrimonio económico, sino la libertad de trabajo, valor considerado como fundamental por la Constitución en los artículos 2, 53 y 54, el es protegido por el Estado, como quiera que el trabajo es considerado como la labor humana por excelencia y, por lo tanto, parte de la dignidad humana que, según el constituyente, ha de ser garantizada en todo caso; también se ha dicho que este tipo constituye una de las conductas que van en contra de bienes de utilidad pública, debido a la gran importancia que para el desempeño de cualquier labor tiene la información, y sobre todo el procesamiento automatizado de información, de manera que se lesiona el orden económico y social del cual es en parte titular el Estado, ya que, este tipo de bienes sólo son protegidos en razón de la utilidad que de ellos se deriva.

El objeto jurídico puede ser, o el patrimonio económico, o el orden económico social o la libertad de trabajo, sin ser excluyentes mutuamente, puesto que este tipo es pluriofensivo, por cuanto se afectan varios intereses jurídicos con la consumación de la conducta.El objeto material del tipo penal es la información y los equipos de procesamiento informático cuando es analizado desde el punto de vista informático. El tipo es de los llamados compuestos, debido a que contiene varios verbos rectores; estos son: destruir, inutilizar, desaparecer y dañar. Destruir alude a deshacer, arruinar o asolar una cosa material o inmaterial; inutilizar, significa hacer inútil o nula una cosa, y útil es aquello que trae o produce provecho, comodidad, fruto o interés, de manera que inutilizar es hacer que una cosa material o inmaterial no pueda producir algún provecho, fruto o interés; desaparecer, es ocultar, quitar de la vista con presteza una persona o cosa; dañar, es causar detrimento, perjuicio, menoscabo, dolor o molestia.

Pornografía con menores.

La Pornografía con menores se consagra en el artículo 218 del C.P, Es un tipo penal de resultado, pues no penaliza el incitar a la pornografía y demás conductas que generen el daño al bien sexual .El tipo establece una circunstancia agravante por ser integrante de la familia de la víctima, lo cual es confuso, ya que, en la determinación de la familia no se dice hasta qué grado de consanguinidad o de afinidad se es parte de tal familia y en cuál no. El objeto de este tipo va destinado a reprimir todas estas conductas que generan un mercado alrededor de una práctica sexual desaprobada, ya que ésta va en contra de la libertad y formación sexual. La expresión gráfica de la prostitución, o llamada pornografía, es uno de aquellos modos de expresión humanos que, por la controversia que generan en las discusiones respecto de la moral social, han sido limitadas en sus posibilidades y alcance de expresión. Claro está, que dichas limitantes no han sido en modo alguno fruto del concepto de moral pública, pues, el constituyente, eliminó de su léxico tal acepción y permitió que el hombre se desarrollara como a bien le pareciera y de ese modo, tal como lo ha advertido la Corte Constitucional, el hombre tiene para sí el derecho de formarse sexualmente, y el acceso a la pornografía es parte de tal libertad.El verdadero problema de la expresión pornográfica está en el tipo, en el sujeto emisor y receptor de la pornografía. La pornografía de mayores de edad y para mayores de edad no puede ser limitada, ya que el adulto puede ser tanto emisor, receptor u objeto de la expresión pornográfica, puesto que constitucionalmente no se limita su participación en tal tipo de procesos expresivos. El problema jurídico-penal está en la participación de emisores, receptores u objetos de personas consideradas por el derecho como menores de edad; así, en lo sexual, esa aptitud de disposición sólo se adquiere a los 18 años de edad y por tanto, el acceso a pornografía y la disposición del cuerpo para expresar la pornografía se tiene únicamente al cumplir dicha edad. De esta manera, la expresión pornográfica únicamente puede lícitamente ser emitida y recibida por mayores de edad; por lo anterior, la existencia de pornografía en la

que menores de edad son objeto de dicha expresión implica que durante el proceso del consentimiento se dio en contra vía de lo previamente dictaminado por las leyes, pues aunque el menor consienta su acto este consentimiento no es válido, además de afectarse el libre desarrollo de la personalidad.

El sujeto activo no es calificado, por lo tanto es indeterminado, el tipo no tiene ningún elemento subjetivo o normativo que califique la actividad del sujeto activo, puede ser una persona natural o una persona jurídica. El sujeto pasivo del comportamiento es calificado por la edad, es decir, el sujeto sobre el cual recae el comportamiento son los menores de dieciocho años, calificación hecha debido a que el derecho nacional tomó una presunción que establece que el hombre y la mujer tienen la suficiente madurez sexual para disponer del cuerpo a los dieciocho años; y sólo pueden ser sujeto pasivo las personas naturales.

El bien jurídico tutelado es la libertad sexual como el derecho de toda persona para disponer de su cuerpo, en lo erótico, como a bien tenga; aun así, el bien jurídico es la libertad y formación sexual, como una de las libertades que surgen de la autodeterminación consagrada en el artículo 16 de la Constitución.

El objeto material es el medio por el cual se transmite la expresión pornográfica, noción ambigua; pues que puede ser considerado material pornográfico y qué no puede ser considerado como tal; la solución a esto depende del criterio que se tenga de la decisión judicial, pues será el juez quien determine si algo es o no pornográfico, ya que el derecho no da las herramientas para determinarlo jurídicamente; aún así, en sentido genealógico, la palabra alude a la expresión gráfica de la prostitución o el tratado respecto de la prostitución ,otra definición involucra lo obsceno, definido esto como lo impúdico, torpe u ofensivo al pudor., la expresión de la pornografía es cierto tipo de información que el Estado limita a cierto grupo de personas, de modo que será pornográfico el material que el juez considere como tal.

Los verbos rectores de la conducta son fotografiar, filmar, vender, comprar, exhibir o comercializar. Fotografiar significa tomar fotografías; filmar es impresionar una película cinematográfica con imágenes ;vender, según la legislación, significa celebrar como contrato de compraventa obligándose a dar el bien a cambio de una cantidad de dinero; comprar significa, según el sistema legal colombiano, el celebrar contrato de compraventa obligándose a pagar un precio en dinero a cambio de un bien; exhibir alude a manifestar o mostrar en público ; comercializar significa dar a un producto condiciones y organización comerciales para su venta . El tipo penaliza la conducta de aquél que introduce al menor en la pornografía, puesto que le deja prestar su cuerpo para ejecutar un acto que el menor, según la ley, no está preparado intelectual y psicológicamente. Con todo, la ley se queda corta, porque protegiendo la formación sexual no enfoca su atención a los demás intervinientes en el proceso de comunicación, y no determina los efectos para con aquellos que se ven afectados en su correcta formación sexual por el acceso a la pornografía, sea de menores sea de adultos. En principio, el menor no puede acceder a pornografía de adultos ni infantil, pues su formación sexual se ve afectada por no ser lo suficientemente “maduro”. Siendo coherentes, el adulto debería ser penalizado por demandar la pornografía infantil, ya que está fomentando el mercado que se pretende eliminar. Así, nos encontramos con un tipo penal corto; pues no penaliza a aquél que permite el acceso del menor a la pornografía, ni siquiera hay sanciones administrativas específicas hasta lo que conocemos en contra de los servidores de la internet que permitan la publicación de contenidos ilícitos como éste.

Delitos contra la integridad moral

Los delitos contra la integridad moral protegen la honra y el buen nombre de los individuos estos son el aspecto psicológico y el concepto revelador de la personalidad; estos se convierten en el objeto jurídico de delitos informáticos debido a que la información almacenada de una persona, cuando no respeta los

principios de integridad y veracidad, afecta la probidad de ésta, puesto que la honra, considerada constitucionalmente como valor jurídico que merece protección, es el sentimiento o la conciencia de la propia dignidad, y es también el más valioso atributo que pueda tener la persona frente a los demás. Lo mismo sucede con el buen nombre que, como derecho, pretende defender el desarrollo del estatus de la persona dentro de lo público, dado que el sujeto de derechos, sea persona natural o jurídica, no debe verse sin herramientas para proteger la imagen que constituye el nombre.

Estos comportamientos son destructores de la integridad moral, ya que la honra y el buen nombre reflejan la dignidad esencial y valor de todo ser humano, un concepto que ha de hallarse en la raíz de cualquier sistema decente de libertad ordenada, pues para el respeto mismo de la democracia liberal y el Estado Social de Derecho, es necesario encontrar protección a tales valores. El contexto constitucional califica la honra como derecho fundamental y objeto de especial garantía para la persona por parte del Estado; así las cosas, la ley 599 de 2000 tipificó la calumnia y la injuria en los articulos 220 y 221 respectivamentes, modificando la punibilidad, cambiando la pena de prisión por pena de multa, haciendo, según el criterio adoptado por la corte constitucional, que puedan ser sujetos de acción penal personas jurídicas.

4. ANÁLISIS PROBATORIO DE LOS DELITOS INFORMÁTICOS

En el lenguaje jurídico, la palabra prueba ,tiene varios significados, no solo se llama así a lo que sirve para proporcionar la convicción de la realidad y la certeza del hecho o cosa, sino también al resultado mismo y el procedimiento que se sigue para obtenerlo, donde su objeto es la obtención de la verdad material, esto es, llegar a conocer lo que en realidad ocurrió en el mundo fenoménico, cómo y de qué manera se desarrollaron los acontecimientos, de forma que el resultado del juicio sería un calco de lo ocurrido en el momento de la comisión.

La característica más conocida de los delitos informáticos es en la consumación de la conducta, en su perfeccionamiento instantáneo en una sola acción o con varias acciones en tiempos distintos, repetitivos y prolongados. Dicha posibilidad de comisión con intervalos, generalmente largos hace más compleja su investigación y su detención [71] ; conllevando a que uno de los puntos más controvertidos en la doctrina del derecho informático, sea la demostración de la existencia de los delitos informáticos.

Este capítulo estudia la prueba referente a los delitos informáticos, toda vez que por medio de la ciencia de las pruebas en el proceso penal, podemos obtener un acercamiento cierto a la verdad material, para lo cual se hace necesario incorporar al acervo probatorio todo aquello que resulta de la ciencia, la técnica y todo lo correspondiente al análisis de los delitos informáticos, como el documento electrónico, el dictamen del perito informático, entre otros; siendo evidente que el

[71] FERNÁNDEZ, Maria Clara. Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos. Universidad Sergio arboleda. Santa Marta, 2001. P.94.

resultado del juicio, la condena o la absolución dependerán en gran medida de lo demostrado en el desarrollo del proceso.

La prueba en materia informática es al mismo tiempo el medio empleado para la averiguación de la verdad y el resultado de la actuación jurisdiccional en el caso concreto de los delitos informáticos. Por un lado, es la actividad que tiende a obtener la verdad material de lo ocurrido, y se ocupa por lo tanto de acreditar más allá de toda duda sobre: El hecho incriminado, la participación del involucrado, su grado de responsabilidad, su personalidad, sus motivaciones y la razón de su actuar. Por el otro, los instrumentos utilizados con el fin de probar.

En los delitos informáticos existe dificultad en la obtención de los medios que sirvan de prueba de las infracciones cometidas a través de tecnologías informáticas; ya que los jueces y fiscales desconocen la forma de valorar y recepcionar este tipo de pruebas; por lo tanto se hace difícil seguir las huellas del infractor y obtener las pruebas para la investigación. De esta manera es erróneo afirmar que la carga de la prueba en materia de delitos informáticos se invierta al usuario, puesto que bajo la responsabilidad del ente investigador existe el deber de probar.

4.1 RECOLECCIÓN, ASEGURAMIENTO Y OBTENCIÓN DE LA PRUEBA INFORMÁTICA.

Los métodos tradicionales de búsqueda y el hallazgo de la prueba en todas las investigaciones no resultan suficientes para el éxito en los procedimientos por delitos informáticos. Aquello que se halló en el lugar del hecho, debe ser exactamente lo que llegue al ámbito del funcionario judicial, para su análisis y dictamen. Los procedimientos internacionalmente aceptados para recolección aseguramiento, análisis y reporte de la prueba informática no están previstos en el código penal vigente, ya que solo se mencionan las actividades mínimas

requeridas para aportar evidencia a los procesos ordinarios. En la recolección, aseguramiento y obtención de la prueba informática existen iniciativas internacionales como las de IOCE (International Organization of Computer Evidence), la Convención de Cybercrimen presentada por la comunidad europea, el Digital Forensic Reseach Workshop, donde se establecen lineamiento de acción y parámetros que cobijan el tratamiento de la evidencia en medios electrónicos.
Cuando se tiene acceso a pruebas informáticas por medios no autorizados y no existen medios para demostrar su autenticidad, confiabilidad y suficiencia, los elementos aportados carecerán de la validez requerida y serán tachados de ilegales. La evidencia obtenida de esta manera, no ofrece maneras para comprobar las posibles hipótesis que sobre el caso se hayan efectuado, dadas las irregularidades que enmarcan su presentación.

La labor de asegurar la prueba consiste fundamentalmente en establecer que el contenido de las unidades de almacenamiento, al momento de procederse a su secuestro se pueda confirmar y que sean idénticas al que se utilizó para realizar la conducta criminal informática[72]; es así, que el código de procedimiento penal, ley 906 de 2004, en su articulo 236, faculta al fiscal, realizar la aprehensión de computadores , disquetes , servidores y demás medios de almacenamiento físico; para que, expertos en informática forense descubran, recojan, analicen y custodien la información que recuperen.

El método utilizado para el aseguramiento de la prueba en el estatuto procesal penal vigente, es la cadena de custodia, definida como el procedimiento a través del cual se establece una relación directa de la evidencia con la escena del crimen o con el momento en que la prueba es aprehendida. La cadena de custodia nace de la necesidad de que cada funcionario que tenga a su cargo las evidencias físicas de un hecho presuntamente punible, asuma la responsabilidad de su

[72] RAMÍREZ, Baon. Delincuencia Informática.promociones y Publicaciones Universitarias. Barcelona, 1992, pag. 36.

aseguramiento y por lo que pueda suceder con ellas en caso de alteración, sustitución, deterioro, destrucción o pérdida.

El código de procedimiento penal colombiano, contiene disposiciones expresas, con el deber de aplicar la cadena de custodia a los elementos físicos, materia de prueba, para garantizar la autenticidad de los mismos, acreditando su identidad y estado original, las condiciones y las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos, así mismo, los cambios hechos en ellos por cada custodio"[73]

4.2 LOS MEDIOS DE PRUEBA EN LOS DELITOS INFORMÁTICOS

Es pertinente antes de abordar el conocimiento de los medios de prueba en los delitos informáticos tratar someramente acerca de la valoración de la prueba en el derecho penal.

En la valoración de la prueba, el ordenamiento penal ha abandonado los sistemas de la prueba legal o prueba tasada, donde la ley media cuantitativamente el valor de cada prueba, para que el juez la aplique. En la actualidad la prueba se valora bajo la libre valoración judicial o libre convicción, que supone, la comprensión del alcance y valor de la actividad jurisdiccional, el reconocimiento de sus poderes discrecionales y la forma en que los hombres pueden llegar a adquirir un conocimiento adecuado y firme sobre cosas que no han presenciado con sus ojos; por lo que deben pasar por las representaciones de los demás hasta formarse un juicio de culpabilidad o inculpabilidad respecto de un individuo concreto en una situación específica de vida humana todo ello basado en el principio de la sana crítica.

[73] Ley 906 de 2004 Artículo 216. Aseguramiento y custodia. Cada elemento material probatorio y evidencia física recogido, será asegurado, embalado y custodiado para evitar la suplantación o la alteración del mismo.

Los medios de prueba son el instrumento, la actividad, el procedimiento que se sigue para conocer procesalmente un hecho, un objeto o materia de prueba[74]. Según la función que cumple en el proceso, la prueba puede ser: Prueba representativa y prueba racional; la primera se caracteriza por el cómo se lleva al juez a la convicción a través de los recuerdos de lo que otro vio o escuchó, donde toman valor destacable los criterios de tipo psicológico y físicos de la percepción, del valor de los sentidos, de sus posibilidades engañosas, de los prejuicios de las gentes, de sus valores lingüísticos y de traducción en un discurso de lo que fue una fugaz experiencia vital en el pasado, o la prueba racional , consiste en el razonamiento lógico, según los principios de la filosofía, y de la común experiencia vital de los seres humanos, en cuyo entorno pasan las demás pruebas, formándose un juicio crítico, racional, reconstructor de un hecho del pasado, del cual el juzgador no tuvo noticias más que por la recreación que se ha operado ante sus ojos a través del proceso.

4.2.1 El documento. La noción de documento puede resultar de mucha importancia a la hora del análisis que se hace del acervo allegado o presentado en un proceso penal y de la valoración realizada por el funcionario judicial encargado de dictar sentencia; sin embargo resulta incuestionable que el desarrollo y avance de la tecnología han ido determinando una adecuación de los regímenes jurídicos, que permitan dar el fundamento legal que requiere el intercambio electrónico de datos, cuya velocidad trasciende incluso al concepto de jurisdicción, con incidencia en las relaciones y situaciones personales, contractuales, comerciales, financieras, que en un momento determinado deban ser objeto de prueba en el escenario judicial, y que deben interesar en la medida en que la informática es utilizada para la consumación de actividades delictivas. Prueba de la incidencia del desarrollo tecnológico en la modificación del concepto de documento, se encuentra en la ley de comercio electrónico, firma digital y entidades de certificación (ley 527 de 1999).

[74] ALZATE NOREÑA, Luis, Pruebas Judiciales, Bogotá, Ed. Temis 1954. p. 207

La legislación Colombiana definió el documento en el Código de Procedimiento Penal de 1987, en su artículo 279 [75], norma no muy diferente al texto del artículo 277 del Decreto 2700 de 1991 ya derogado, en el cual se pretendió establecer reglas para el reconocimiento de documentos auténticos. Las mencionadas normas eran parecidas a la del artículo 251 del Código de Procedimiento Civil, el cual sólo es más explícito, en cuanto a la aptitud probatoria,[76]ya que luego, de una relación similar de cosas, a las que les reconoce el carácter de documento, dice que también lo es todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.

El código de procedimiento penal ley 600 de julio 24 de 2000 se eliminan los apartes con aspecto de definición y la relación de las cosas u objetos que pueden constituir documento, argumentando que dicha relación se da en el código penal, ley 599 de 2000, en el capítulo correspondiente a los delitos de falsedad en documento en el articulo 294.[77] En síntesis, todo lo que se hizo, fue llevar la

[75] Código de Procedimiento Penal de 1987, artículo 279. Es documento toda expresión de persona conocida o conocible, recogida por escrito o por cualquier medio mecánico o técnicamente impreso como los planos, dibujos, cuadros, fotografías, radiografías, cintas cinematográficas, y fonópticas y archivos electromagnéticos que tengan capacidad probatoria.

[76] Código de Procedimiento Civil, artículo 251.Distintas clases de documentos. Son documentos los escritos, impresos, planos, dibujos, cuadros, fotografías, cintas cinematográficas, discos, grabaciones magnetofónicas, radiografías, talones, contraseñas, cupones, etiquetas, sellos y , en general todo objeto mueble que tenga carácter representativo o declarativo, y las inscripciones en lápidas, monumentos, edificios o similares.
Los documentos son públicos o privados. Documento público es el otorgado por el funcionario público en ejercicio de su cargo o con su intervención. Cuando consiste en un escrito autorizado o suscrito por el respectivo funcionario, es instrumento público; cuando es otorgado por un notario o quien haga sus veces y ha sido incorporado en el respectivo protocolo, se denomina escritura pública. Documento privado es el que no reúne los requisitos para ser documento público.

[77] Artículo 294. Documento. Para los efectos de la ley penal es documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, soporte material que exprese o incorpore datos o hechos, que tengan capacidad probatoria.

definición del estatuto adjetivo al sustantivo y amplió el concepto de documento al considerar como tal cualquier soporte material con capacidad para expresar o incorporar datos, con el fin de permitir la calificación a cualquier elemento utilizado para esos fines por la informática. En la ley 906 de 2004 no se define el concepto de documento, solo menciona elementos que constituyen documentos, como: Las grabaciones magnetofónicas, discos de todas las especies que contengan grabaciones, grabaciones fonópticas o vídeos, películas cinematográficas, grabaciones computacionales. mensajes de datos, télex, telefax y similares, fotografías, radiografías, ecografías, tomografías, electroencefalogramas, electrocardiogramas.

Una modalidad del documento en los sistemas informáticos, a la vez que constituye un medio de prueba idóneo en materia informática, es el documento electrónico, definido como aquel proveniente de la elaboración electrónica, u objeto físico dirigido a conservar y transmitir informaciones mediante mensajes en lenguaje natural, realizado con la intermediación de funciones electrónicas.

Prueba de la incidencia del desarrollo tecnológico en la modificación del concepto de documento, se encuentra en el artículo 5º de la ley 527 de 1999, al disponer que no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos. Los mensajes de datos son entendidos como la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI)[78], internet, el correo electrónico, el telegrama y el telefax. El carácter de documento

[78] Electronic Data Interchange (EDI): Intercambio electrónico de datos, es la transmisión electrónica de información de un computador a otro, estando estructurada la información conforme a alguna norma técnica o protocolo convenida al efecto. HANCE, Olivier. Leyes y Negocios en Internet. México D.F. McGraw-Hill.1996.Pág. 25.

que tiene los mensajes de datos, la Corte Constitucional colombiana, al revisar la constitucionalidad de la ley 527 de 1999 se pronunció en los siguientes términos:

> *"El mensaje de datos como tal debe recibir el mismo tratamiento de los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento. Dentro de las características esenciales del mensaje de datos encontramos que es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse; es un documento legible que puede ser presentado ante las entidades públicas y los tribunales; admite su almacenamiento e inalterabilidad en el tiempo; facilita la revisión y posterior auditoria para los fines contables, impositivos y reglamentarios; afirma derechos y obligaciones jurídicas entre los intervinientes y es accesible para su ulterior consulta, es decir, que la información en forma de datos computarizados es susceptible de leerse e interpretarse".* [79] .

La importancia de disposiciones como la citada, reside en el hecho de que las transacciones financieras entre establecimientos y personas distantes, la comunicación y las nuevas formas de delinquir se ven facilitadas por el uso de la red cibernética que permite realizarlas casi en tiempo real, con la consecuencia lógica de una mayor dificultad para que las autoridades puedan hacer el seguimiento en caso de que esas transacciones y comunicaciones se estén utilizando para cometer delitos informáticos.

En un ordenamiento jurídico que recoja el sistema de prueba legal, es necesario que la ley considere expresamente al documento electrónico como medio de

[79], GUERRERO, María Fernanda. Comentarios sobre la ley de comercio electrónico y firmas digitales. Cámara de Comercio de Bogotá Octubre de 2001. P.19.

prueba idóneo. En cambio, según el principio del libre convencimiento del juez, las partes podrán acompañar documentos electrónicos y el juez no tendrá obstáculos para admitirlos como medios de prueba, en la medida en que no exista norma alguna que lo inhiba para utilizar los documentos electrónicos como medios de prueba, admitiéndolos en subsidio de otros, imponiéndoles una determinada eficacia probatoria[80] .Esto no significa que el juez debe necesariamente atribuirle plena atención al documento electrónico, sin valorar antes su autenticidad y su seguridad; así, el documento será auténtico cuando no haya sufrido alteraciones, cuando ha sido realmente otorgado y autorizado por la persona y de la manera que en él se expresa, y será tanto más seguro cuanto más difícil sea alterarlo y cuanto más fácil sea verificar la alteración y reconstruir el texto originario.

4.2.2. Sistemas de seguridad informática en los documentos electrónicos. Esta admitido, dividir las técnicas modernas de autenticación de un documento electrónico en dos grandes técnicas; el código secreto y la criptografía.

El código secreto es la técnica más difundida y asociada a la canalización de la informática y la telemática de gran público; consiste en una combinación de cifras o letras, que el sujeto conoce y digita sobre el teclado del sistema que va a utilizar. Comúnmente se recurre a otro procedimiento, que consiste en combinar este uso del P.I.N;[81] con la introducción dentro de la misma máquina, de una carta a pista magnética, o de una carta a memoria, que verifica la validez del código dado, sin que sea necesario poner en juego el cerebro central del sistema.

[80] GUERRERO, María Fernanda. Breves consideraciones a cerca del documento electrónico: Su problemática jurídico procesal. Boletín Jurídico de la Asociación Bancaria. No. 642 – 2 de Febrero 15 de 1992.

[81] Apelativo anglosajón que significa: Personal identificación number, número de identificación personal.

La criptografía es la técnica utilizada para hacer efectivos numerosos mecanismos de seguridad informática. Su alcance excede la operación de autenticación, tocando las funciones que se remiten a la fiabilidad de una comunicación automática (integridad de los datos, confidencialidad, conservación; es decir, se trata de la codificación de un texto a transmitir con la ayuda de claves y de algoritmos[82]. En los sistemas criptográficos simétricos, la misma clave permite efectuar el ciframiento y el desciframiento del texto; el sistema es descifrado asimétrico, cuando hacen falta dos claves diferentes para estas dos operaciones; por lo demás, las claves pueden ser secretas, privadas o públicas, según el grado de accesibilidad. Los métodos criptográficos más conocidos son el D.E.S (Data Ecription System) y el R.S.A., sigla dada por los nombres de los tres inventores (Rivest, Shamir y Adleman).[83]

Un listado de cosas u objetos que pueden constituir documentos con aptitud probatoria en investigaciones o juicios por delitos informáticos son: Soportes informáticos, como los discos duros de computadoras, discos blandos (diskettes), discos compactos, discos de compactación de información , discos ópticos, impresoras, agendas digitales y electrónicas, teléfonos celulares, cassettes de audio y video, discos de DVD, cámaras digitales y dispositivos de memoria paralela, los cuales es necesario inspeccionar detalladamente con todas las seguridades, para recuperar la información, relacionada con la conducta criminal informática.

[82]El algoritmo es un conjunto finito de reglas determinadas que sirven para resolver un problema por medio de un número finito de operaciones según descripción de la norma ISO 2382.

[83] CH. DAUMD. Security withthout identification: card computers to make big brother obsolete, edición de Digi Cash, 2002. P. 35

4.2.3 Peritaje informático. El peritaje es el medio de prueba, de suma importancia para cualquier actuación judicial o arbitraje que precisen conocimientos científicos o técnicos especializados. A medida que transcurre el tiempo se encuentran diferentes maneras de hacer peritazgos debido a los cambios de la tecnología y la ciencia.

El perito informático debe ser un profesional del peritaje informático, no un experto en una sola área de la informática. Es decir, un informático preparado, idóneo en varias disciplinas, y sobre todo, eficaz perito en la materia.

En el año 2001, la Policía General de la Nación creo un grupo de apoyo técnico informático, mediante la Resolución 2762 del 30 de Julio de 2001,denominado grupo de delitos informáticos, basándose en el crecimiento cuantitativo y cualitativo de la delincuencia informática en los últimos años; por lo que consideró, contar con funcionarios dotados de la capacidad técnica, que permitan resolver los requerimientos que, en esta materia de delitos informáticos, le efectúen los funcionarios judiciales.

El código procesal penal, ley 906 de 2004, en el artículo 406 afirma que el servicio de peritos se prestará por los expertos de la policía judicial, del instituto nacional de medicina legal y ciencias forenses, entidades públicas o privadas, y particulares especializados en la materia de que se trate. Ante la amplísima gama de eventos que pueden ser objeto de dictamen pericial en materia informática, es dable suponer que no existe una disciplina que resulte abarcativa de todas y cada una de las especialidades que pudieren requerirse; así, la designación puede hacerse extensiva a funcionarios públicos, en general fuerzas de seguridad o entes estatales con dependencias técnicas específicas habilitados en razón de su competencia o título profesional.

El perito debe ser muy cauto al momento de determinar si los puntos de pericia a resolver son o no de su especialidad, pues, por lo general se requiere la intervención conjunta de otros profesionales, tales como la participación conjunta o sucesiva de ingenieros, programadores, analistas de sistemas, técnicos en computación , en fin sea la naturaleza del requerimiento. De pretender efectuar el examen pericial sin contar con los conocimientos específicos, aún cuando se posea título habilitante, dada la enorme variedad de objetos que pueden caer bajo tratamiento pericial, correrá el riesgo de sufrir fundadas impugnaciones de los peritos o consultores técnicos de parte, toda vez que, en las pericias informáticas, su intervención se verifica casi permanentemente. En las pericias informáticas, hay que tener en cuenta, que no siempre se relaciona con delitos informáticos exclusivamente, es decir, no siempre que la informática forma parte de un asunto judicial es con motivo de un delito.

De la aplicación práctica del conocimiento específico se desprende la existencia de dos grandes campos de la labor pericial, reconocidas por la doctrina penal informática, y son:

Pericias de autenticidad: Son pericias con la necesidad de tener a disposición el patrón material de comparación, ya sea de hardware o software, entendido como indubitable; que permitirá el análisis comparativo determinante de la autenticidad o no, del elemento sospechado.

Pericias de contenido, funcionamiento y recuperación de datos: Son las pericias que abarcan el almacenamiento de datos, el análisis y determinación de estructuras de diseño de sistemas, los medios de comunicación y transferencia de datos, métodos de entrada, acceso, procesamiento y salidas; que en su conjunto requieren la colaboración interdisciplinaria de profesionales en la materia; así, puede requerirse al perito, la lectura del contenido de un diskette, la verificación de copia o adulteración de sistemas y aplicaciones de software, la impresión del

material secuestrado, la impresión del contenido de discos rígidos, establecer el uso indebido de marcas o la explicación de uso de utilitarios y sistemas de computación.

4.2.4 El informe pericial y su eficacia probatoria. La eficacia probatoria de los dictámenes informáticos radica fundamentalmente en la continuidad en el aseguramiento de la prueba desde el momento de su secuestro [84]; realizado ello en debida forma, es poco probable, en la investigación preliminar, que el material inspeccionado, no arroje elementos contundentes, para la prueba del delito.

El dictamen del perito debe contener una opinión fundada, exponiendo al juez los antecedentes de orden técnico que tuvo en cuenta para realizar el dictamen. La pericia no puede consistir en una mera opinión del experto, prescindiendo del necesario sustento científico, dada la increíble diversidad de aplicaciones, utilidades, sistemas operativos, etc. Normalmente, el perito informático ha de utilizar herramientas consistentes en software específicos que permita acceder a la información almacenada en las computadoras. Las pericias tendientes a establecer la autenticidad de marcas o aplicaciones de software, así como también de unidades lógicas, u elementos electrónicos que integran un procesador y que normalmente caen dentro del la esfera de incumbencia del perito informático, suelen ser dictámenes sencillos en la medida en que se cuenta con los correspondientes patrones de comparación o indubitables; distinto es que se someta a dictamen el modo de funcionamiento de un dispositivo, la obtención de información borrada o alterada en soportes magnéticos, la determinación de maniobras fraudulentas mediante el uso de aplicaciones informáticas, puertas falsas, intrusiones no autorizadas a sistemas de redes o bases de datos a través de la internet, violación de la correspondencia electrónica, práctica informática del caballo de troya, la técnica salami, los virus informáticos, las bombas lógicas etc. Es allí donde la prueba pierde su materialidad, para convertirse exclusivamente en

[84] NICOLIELLO Saúl, El Dictamen pericial, Ediciones Amalio, Montevideo, Uruguay, 1999, pag. 24

dato, en mera información traducida en desniveles de tensión eléctrica, es aquí donde la función del perito se vuelve compleja. Por un lado, debe suplir las limitaciones técnicas que dificultan la obtención del resultado pretendido y, por el otro, realizar la traducción de dichos resultados, en la inteligencia de que serán interpretados por quienes no poseen una visión tecnológica; para luego proceder a tener por acreditada o no la comisión de delitos.

La eficacia probatoria de los elementos informáticos, y su interpretación a través de los dictámenes periciales se deriva de los procesadores de datos que se haya obtenido de sistemas implementados a la luz de previsiones legales o reglamentaciones específicas y que resulta inevitable su cuestionamiento. De todos modos, ello obedece exclusivamente a la reticencia o retardo con que el derecho enfrenta los avances tecnológicos; pues, para desvirtuar la opinión de cualquier perito es imprescindible valorar elementos que permitan advertir fehacientemente el error o el insuficiente empleo de datos científicos, que deben conocer por su profesión.

No es la ausencia de método o fundamentos científicos lo que pone en tela de juicio la eficacia probatoria de los dictámenes, sino la tendencia a creer que todo aquello que escapa a la percepción directa de los sentidos requiere de un experto para dilucidar su existencia, es esencialmente falible; cuando en realidad, la pericia informática se funda en principios técnicos inobjetables.

4.2.5 Inspección judicial. Es la prueba de percepción por excelencia, con ella el juez aplica sus propios sentidos para conocer el hecho, aplica su observación personal y sensorial, es un medio de prueba directo. [85]; con el fin de constituir hechos indicadores a través de los cuales se llegue a establecer la

[85] RODRÍGUEZ, Gustavo. Derecho probatorio X edición, Ediciones Ciencia y Derecho, Bogotá, 1997.Pág. 23

responsabilidad de un individuo, o por lo menos aportar elementos de juicio para valorar la credibilidad que merece un imputado.

La volatilidad de los datos en lo que a prueba informática se refiere, exige las máximas precauciones a la hora de realizar la inspección judicial, dicha actividad comienza desde el momento de la inspección; cuando aquello que resulta de interés se halla almacenado en computadoras y sus operadores conocen las rutinas que deben llevarse a cabo rápidamente para eliminar los registros comprometedores o bien inutilizar completamente los sistemas. Por lo tanto, es menester, como primera medida, disponer el alejamiento de toda persona que se halle en presencia de las computadoras, servidores o tableros de suministro eléctrico, para proceder, inmediatamente a desconectar la totalidad de los teclados hasta que cada uno de los terminales sea examinados por los expertos; hecho esto, se procede al secuestro de las unidades; en principio carece de relevancia el traslado de la totalidad de monitores y teclados, toda vez que ellos no intervienen en el almacenamiento de información de interés para la causa, la cual si se halla en las unidades de control o CPU; no obstante ello, en función a la gran variedad de marcas, modelos, clones, es conveniente que el experto determine si resulta necesario trasladar tales elementos a fin de permitir su puesta en funcionamiento en laboratorio a los fines periciales. Básicamente, el tratamiento que debe darse al computador consiste en franjado de todas las conexiones de entrada y salida, ya sea de datos, periféricos o energía y los accesos a unidades de discos flexibles, rígidos removibles; finalmente, se debe franjear toda la periferia, evitando la posibilidad de que se desmonten sus partes componentes, todo ello con la rúbrica de funcionarios y testigos.

En síntesis, como resultado del acto procesal debe obtenerse un acta de la inspección judicial en donde conste la descripción unívoca del equipamiento inspeccionado y sus periféricos secuestrados, el modo en que se hallaba instalado; la descripción de los sistemas operativos que poseen; las operaciones técnicas

realizadas y el modo en que se procedió a asegurar, secuestrar y resguardar los objetos de interés. Para proceder a la práctica de la inspección judicial, en función de los puntos a tratar, ha de solicitarse nuevamente la presencia de testigos, asistencia de consultores técnicos o peritos de parte y realizarse las tareas técnicas con idéntica minuciosidad. En todos los casos, de resultar técnicamente viable, es aconsejable el trabajo sobre copias de la totalidad de los elementos secuestrados, asegurando previamente su identidad, a fin de no alterar el sustrato original.

4.2.6 Indicio. El indicio o prueba indiciaria es aquella que a través de un razonamiento lógico de orden racional, se genera una inferencia que permite descubrir un hecho desconocido de una serie de hechos conocidos. Se la define como una prueba de carácter indirecto, de tipo residual, real o personal, de la que se puede extraer una inferencia que permite formar un juicio de culpabilidad.

El código de procedimiento penal, define este medio de prueba en el artículo 284[86], definición que señala tres elementos integradores: Un hecho conocido, llamado usualmente indicio, indicante o indicador; un hecho desconocido que se pretende conocer y demostrar, llamado también hecho indicado y una inferencia lógica o razonamiento; por medio del cual, partiendo del hecho conocido, concluimos o deducimos, con probabilidad unas veces, con certezas otras, cual es el desconocido.

El indicio se puede definir, como las cosas, estados o hechos personales y materiales, ocurridos o en curso, aptos para convencer acerca de la verdad de afirmaciones o de la existencia de hechos objeto del proceso."[87]

[86] Código de procedimiento, artículo 284 .Todo indicio ha de basarse en la experiencia y supone un hecho indicador, del cual el funcionario infiere lógicamente la existencia de otro.

[87] ROCHA Antonio, La prueba indiciaria, Externado de Colombia, Bogotá, 1978. Pág. 18

Los indicios pueden ser genéricos, derivados de la conducta anterior del imputado, es decir de su modus operandi.; así por ejemplo, los antecedentes del sujeto, eventualmente de los registros policiales, de las denuncias recibidas con anterioridad que lo sindicaban como vinculado a tal tipo de actividades, pueden servir actualmente para configurar un indicio de que está reincidiendo en tal actividad.

Por indicios específicos se entiende los referidos especialmente al hecho de ser reconocido como hacker al tener un amplio y basto conocimiento de la red.

Como toda prueba, los indicios pueden ser negativos o de descargo y positivos o de cargos. Los requisitos indispensables para que sea válida la prueba indiciaria son:

Que estén relacionados con el hecho que se trata de probar, y que concurran en número suficiente para hacer plena prueba, esto es que deben ser variados y múltiples, no bastando uno solo.

Que sean de real envergadura o gravedad, de modo que refieran contundentemente al tema central objeto de prueba.

Que no se trate de minucias o asuntos colaterales o intrascendentes, o de detalle; que resulten inequívocos, concordantes, no contradictorios entre sí, no colindantes unos de otros.

Que sean precisos y lleven a una misma conclusión; que haya entre ellos una concatenación, o ligazón lógica que permita realizar la inferencia sin dificultad y sin artificio de ninguna especie, como conclusión que fluye natural y libremente de la simple acumulación de prueba.

Que estén plenamente probados cada uno de ellos, y que en su articulación se pueda afirmar que cada uno de ellos constituye una prueba material.

La inmensa mayoría de personas que navegan por la red consideran que lo hacen como anónimas o clandestinas, sin embargo, en la red el anónimo y la clandestinidad no existe; pues cada paso por ella deja tal número de rastros que son posibles reconstruirlos uno a uno, y en cualquier tiempo dan lugar al reconocimiento o al manejo de sus claves o datos de seguridad.

Los indicios sobre la intervención de personas en aras de efectuar actos encaminados a la realización de delitos informáticos suelen darse con la ayuda de accesorios comercializados para tal fin, por compañías proveedoras de servicios de computación tales como *NOD32v2 Probably Unknow NewHeur_PE Privacy Foundation, una ONG estadounidense de defensa de la privacidad y del derecho a la intimidad en Internet, lanzó un singular programa gratuito, el Bugnosis 1.0, para detectar los denominados "Bugs", pequeñas imágenes colocadas en sitios Web, cuyos códigos permiten "espiar" nuestros hábitos de navegantes.*

4.3 LA EVIDENCIA DIGITAL

La evidencia digital es pieza probatoria básica para el funcionario judicial; el cual debe conocer , acerca de cómo se crea, cómo se recolecta, cómo se asegura y cómo se presenta en el juicio[88]; con el fin de aportar con claridad y precisión factores que orienten las decisiones sobre casos donde ésta evidencia sea parte fundamental. La evidencia digital al ser un objeto relativamente fácil de manipular, generado por dispositivos electrónicos, de los cuales no sabemos nada sobre su funcionamiento, la susceptibilidad a las fallas, entre otras características, advierte que es un campo de investigación delicado y formal, donde el conocimiento

[88] Carlos S. Álvarez Cabrera .División de seguridad legal de la información, en: Asociadoscarlos.alvarez@geoabogados.com

técnico, es tan fundamental como, el conocimiento computacional y de técnicas probatorias.

La evidencia digital está soportada en medios electrónicos [89] que si bien, físicamente pueden presentar fallas y que, lógicamente pueden ser manipulados, son la vía requerida para presentar las pruebas de los hechos ocurridos en sistemas o dispositivos electrónicos.

La evidencia digital está frecuentemente sometida a errores, fallas y pérdidas, eventos que hay que analizar y profundizar, para tratar de disminuir el nivel de incertidumbre en torno a los delitos informáticos. Mientras mayor sea la incertidumbre alrededor de la evidencia digital identificada, recolectada y aportada a un proceso, menor será la fortaleza de su admisibilidad y capacidad probatoria sobre los hechos presentados al funcionario judicial.

Los errores asociados con los medios de almacenamiento y configuraciones de los sistemas de cómputo son frecuentes, generalmente se encuentra que los diskettes, discos duros, cintas, Cd-roms, DVD (Digital video disk), entre otros, tienen errores de fábrica; los cuales no son identificables previo su uso, haciendo que las posibles evidencias allí residentes, no cuenten con características confiables y verificables, dada las condiciones defectuosas del medio inicial, muchas veces los atacantes o intrusos en los sistemas, con amplios conocimientos de los programas de almacenamiento de archivos pueden manipular las estructuras de datos de dichos sistemas y esconder información valiosa en sectores de los discos que aparentemente reflejen fallas del medio de almacenamiento.

Las fallas del software pueden generar inconsistencias o imprecisiones sobre los archivos generados; en este sentido, el afinamiento de la instalación del sistema

[89] AZPILCUETA, Tomas, Derecho Informático, Buenos Aires, Ediciones Alianza, 1987.Pág. 73.

operacional, la sincronización de tiempo de las máquinas e instalación de actualizaciones del software se convierten en actividades críticas para disminuir la posibilidad de funcionamiento inadecuados del software base y por ende, de las aplicaciones que se ejecuten en las máquinas; contrario a esto se puede generar que los eventos registrados no correspondan a la realidad de los mismos, abriendo la posibilidad de mayor incertidumbre alrededor de los hechos, favoreciendo la posición del posible intruso y generando una duda razonable sobre las acusaciones efectuadas.

De manera complementaria al presentarse una falla en el sistema operacional, la cual puede ser provocada por el atacante o producto del sistema mismo, puede involucrar elementos técnicos de admisibilidad de las pruebas, que no favorezcan la veracidad de las mismas, desviando el proceso judicial.

4.4.1 Principios de la evidencia digital. La evidencia digital se sustenta en tres principios principales que son la autenticidad, la confiabilidad y la suficiencia.

La autenticidad

La autenticidad es la característica que muestra la no alterabilidad de los medios originales y que busca confirmar que los registros aportados corresponden a la realidad demostrada en la fase de identificación y recolección de evidencia.
La autenticidad de la evidencia sugiere ilustrar a las partes que la evidencia ha sido generada y registrada en lugares o sitios relacionados con el caso, particularmente en la escena del posible ilícito o lugares establecidos en la diligencia de levantamiento.

En medios no digitales, la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto por el artículo 11 de la ley 446 de 1998 [90], en este sentido, todas las pruebas que se aporten por las partes se entenderán como válidas.

Verificar la autenticidad de los registros digitales requiere, el desarrollo y configuración de mecanismos de control de integridad de archivos; es decir, la autenticidad requiere una arquitectura que ostente mecanismos que aseguren la integridad de los archivos y el control de cambios de los mismos.

Confiabilidad.

La confiabilidad, como principio, es factor relevante para asegurar la admisibilidad de la evidencia. La confiabilidad señala si efectivamente los elementos probatorios aportados vienen de fuentes que son creíbles y verificables, y que sustentan elementos de la defensa o del fiscal en el proceso penal que se adelante.

En medios digitales, se relaciona el concepto de confiabilidad, con la configuración de la arquitectura de computación; en cómo se diseñó la estrategia de registro; cómo se diseñó su almacenamiento; cómo se protegen; cómo se registran y se sincronizan; cómo se recogen y analizan, preguntas, cuyas respuestas buscan demostrar que los registros electrónicos poseen una manera confiable para ser identificados, recolectados y verificados.

[90] Ley 446 de 1998, artículo 11. Autenticidad de los documentos, En todos los procesos, los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos emanados por terceros.

Cuando se logra que una arquitectura de cómputo, ofrezca mecanismos de sincronización de eventos y una centralización de registros de sus actividades, los cuales de manera complementaria, soportan estrategias de control de integridad, se avanzará en la formalización de la confiabilidad de la evidencia digital. La confiabilidad de la evidencia en una arquitectura de cómputo, estará en función de la manera como se sincronice el registro de las acciones de los usuarios y de un registro centralizado e íntegro de los mismos, lo cual reitera la necesidad de un control de integridad de los registros del sistema, para mantener la autenticidad de los mismos.

Suficiencia.

La suficiencia es la presencia de toda la evidencia necesaria para adelantar un caso, característica que es factor de éxito en las investigaciones adelantadas en procesos judiciales. Frecuentemente la falta de pruebas o insuficiencia de elementos probatorios ocasiona la dilación o terminación de procesos que podrían haberse resuelto de manera breve y rápida; en este sentido, se reconoce que mientras mayores fuentes de análisis y pruebas se tengan, habrá posibilidades de avanzar en la defensa o acusación en un proceso judicial. Desarrollar esta característica en arquitecturas de cómputo, requiere afianzar y manejar destrezas de correlación de eventos en registros de auditoria; es decir, contando con una arquitectura con mecanismos de integridad, sincronización y centralización, es posible establecer patrones de análisis que muestren la imagen completa de la situación bajo revisión.

La correlación de eventos, definida como el establecimiento de relaciones coherentes y consistentes entre diferentes fuentes de datos para establecer y conocer eventos ocurridos en una arquitectura o procesos, sugiere una manera de probar y verificar la suficiencia de los datos entregados en un juicio. En posibilidad, es viable establecer relaciones entre los datos y eventos presentados, canalizando

las inquietudes y afirmaciones de las partes sobre comportamientos y acciones de los involucrados, sustentando dichas relaciones con hechos o registros que previamente han sido asegurados y sincronizados; es decir, que la correlación de eventos como una función entre la centralización del registro de eventos y el debido control de integridad de los mismos, se soporta en una sincronización formal de tiempo y eventos que deben estar disponibles por la arquitectura de cómputo para asegurar la suficiencia del análisis de la información presente en una arquitectura de cómputo.

5. TÉCNICA LEGISLATIVA EN RELACIÓN CON LA TIPIFICACIÓN DE DELITOS INFORMÁTICOS.

Los tipos contenidos en la legislación Penal son obra exclusiva del legislador, quien es el encargado de delimitar el contenido y el alcance de las figuras delictivas en virtud de los principios de reserva legal y tipicidad, derivados del artículo veintinueve de la carta política que consagra, entre otros, el principio de: Legalidad sustantiva y procesal; por ello el legislador asume la función de describir y señalar explícitamente las conductas que lesionen o pongan en peligro el bien jurídico tutelado. El principal problema que surge para el legislador, cuando selecciona y describe las conductas que intenta criminalizar, es precisar qué opción de técnica legislativa debe asumir para ofrecer una adecuada política criminal.

Las tendencias respecto a la penalización de la criminalidad informática en países similares al Colombiano, han sido la de descodificar o penalizar conductas , modificar normas del código legal vigente, promover la expedición de una ley especial, o un criterio unificador de desarrollar una norma tipo en las cuales se incluya la parte sustantiva y procesal.

A la luz del derecho comparado las conductas criminales informáticas se han tipificado en dos principales sistemas, a saber:

Sistema ortopédico: Este sistema busca corregir, agregar o modificar las normas existentes. lo encontramos en la legislación italiana[91].

[91] Dicho sistema se adoptó con la ley numero 547 de 1993 Por la cual se reformo el código penal Italiano.

Sistema de ley especial: Mediante el cual se regula un tema específico en una ley especial y por tanto genera nuevos efectos ante los hechos que se presenten.

Las propuestas en torno a: ¿Qué sistema adoptar en la legislación Colombiana?, son: Tipificar las conductas criminales realizadas a través de sistemas informáticos o telemáticos modificando tipos penales existentes en el estatuto penal y así mismo crear nuevas figuras dentro de dicho marco jurídico adicionándole reformas al código adjetivo penal; propuesta enmarcada dentro del sistema ortopédico ya referenciado, el cual se guía por el principio de la subsidiaridad que invoca la extrema ratio del derecho penal, donde los diversos tipos penales informáticos deben ser encasillados en los diferentes capítulos del código penal dependiendo del interés jurídico que con ellos resulte afectado, propuesta que conllevaría a una reforma parcial del mencionado código penal como lo reitera Albero Araujo: *"*Este aspecto es el relativo a sí los diversos tipos penales informáticos deben ser encasillados en los diferentes capítulos del Código Penal dependiendo del interés jurídico que con ellos resulte afectado, lo cual conllevaría a una reforma parcial del mencionado Código Penal".[92]

Esta posición es compartida por diversos autores entre ellos Grisanti,[93] quien ha sostenido que: Cierto es, que allí donde, se acepta el principio de la legalidad de los delitos y de las penas, está excluida la analogía como medio de creación de nuevos tipos legales, pero no es menos cierto que las leyes penales admiten, cuando sea necesario, la interpretación extensiva, esto es, la que amplia el sentido meramente lexicográfico del texto legal para adecuar este al espíritu de la ley. Además, la interpretación de la ley penal ha de ser progresiva.

[92] ARAUJO; Alberto Daniel .La informática en el proceso de administración de justicia .En: Revista Derecho y Tecnología Informática, Bogota 1990, Pág. 16
[93] GRISANTI A., Lecciones de Derecho Penal. Ed Móbil Libros, Caracas 1989, Pág. 44

Otro autor partidario de subsumir las acciones antijurídicas informáticas en los tipos penales ya preexistentes en la legislación penal vigente es Lidia Callegari[94] señalando: Que tratar de legislar para crear una parte del Código Penal que trate del delito informático o hacer una ley especial al respecto es muy peligroso. Al manifestar que: "debe caerse en la trampa de sentirse obligado a crear toda una infraestructura de carácter legislativo en aspectos que solamente tienen incidencia en el campo instrumental o, para, ser mas claros en el ámbito de los medios de comisión de los delitos"[95]. Por lo tanto no hay que crear una norma separada, especial, autónoma para regular los mencionados delitos porque los instrumentos normativos vigentes en el caso de Colombia pueden amparar por sí solos, o con ciertas modificaciones, las conductas realizadas a través de las computadoras o restantes medios similares. Esta posición en palabras de Libardo Riasco[96] se determina en: "no se deben crear nuevos tipos penales si los actuales delitos pueden encuadrarse entre ellos; solo basta la aclaración del verbo rector para la ampliación de los eventos que la doctrina mundial ha llamado delitos informáticos"

Por otra parte, encontramos las posiciones según las cuales el legislador normativiza las conductas que han de subsumirse en los nuevos tipos penales; debido a que los tipos penales descritos en el Código Penal y aplicables supuestamente a tipificar delitos informáticos, resultan insuficientes frente a las nuevas necesidades de la colectividad, dado que en Derecho Penal está expresamente prohibida la aplicación analógica de los tipos debido al reconocimiento del principio de legalidad. Es así, que de no producirse la creación de nuevas figuras delictivas, numerosas conductas continuarían quedando impunes puesto que las conductas ilícitas hechos punibles creados por el

[94] CALLEGARI, Lidia. "Delitos informáticos y legislación" en Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985.

[95] Ibidem

[96] RIASCOS Gomez Librado, La Constitución de 1991 y la informática jurídica, Publicación Universidad de Nariño, 1997.Pág. 35.

nacimiento del fenómeno tecnológico no se pueden encuadrar en descripciones típicas exactas , sumado a que no existe como en el caso de nuestra legislación, la protección de un bien jurídico multicomprensivo como es el de la información y además estas conductas violatorias a la intimidad no se encuadran o subsumen dentro de verbos rectores que comprendan los hechos transgresores.

Los textos legales vigentes no pueden adaptarse a las novedosas conductas delictivas informáticas, sin violar el principio de prohibición de la analogía. Es importante destacar que la analogía es una de las fuentes del Derecho. La analogía consiste en la solución de un caso no previsto en la ley recurriendo a una norma de la ley que regula un caso semejante.[97] Pero en el caso especifico del Derecho Penal, no tiene cabida la analogía tomando en cuenta las exigencias del principio de legalidad, en virtud del cual se prohibe la creación de delitos y penas por analogía pues toda la materia penal está reservada a la ley y las conductas antijurídicas y las sanciones penales deben estar expresamente previstas en ella, de acuerdo al principio de taxatividad.

En tal sentido Nuñez[98] plantea cómo muchos sistemas penales confrontan considerables dificultades en la aplicación de sus normas penales tradicionales ya que no puede realizarse una interpretación extensiva de los tipos penales existentes en el Código Penal del 2000 .La verdad es que la variedad y alcance de hechos delictivos que se pueden cometer con la ayuda de la tecnología moderna tales como las computadoras, obliga a un estudio detallado donde se puedan establecer los tipos penales, las características, categorías, y clasificaciones de los delitos En tal sentido, varios autores proponen avanzar y profundizar hacia la promulgación de normas jurídicas que protejan y defiendan los bienes, acciones y derechos de los usuarios de sistemas informáticos.

[97] GRISANTI A., Lecciones de Derecho Penal. Ed Móbil Libros, Caracas 1989, Pág. 35
[98] NUÑEZ T., E. Los Elementos del Delito en la Dogmática Jurídico – Penal. Librería Destino. Caracas 1.998, Pág. 52

En el caso colombiano como en otros ordenamientos, la situación se muestra incontestable, ya que no se castigan dichos comportamientos ilícitos, porque no se tiene la claridad sobre la naturaleza jurídica de los bienes objetos materiales de los delitos ni del interés jurídico protegido.

Ahora bien, en relación al sistema de técnica legislativa en Colombia para prevenir los delitos informáticos que afectan el sistema operativo de las computadoras y que se realizan a través del medio de la internet, proponemos un estatuto ortopédico, compartiendo algunos preceptos del archivado proyecto de ley estatutaria numero 223 de 2001 que pretendió modificar y adicionar algunos tipos penales en el código penal.

5.1 PROPUESTA PARA LA PENALIZACIÓN DE LOS DELITOS INFORMÁTICOS

Considerando que:

Los cambios y avances de la informática, las innovaciones tecnológicas y científicas, el auge de la Internet, han generado nuevas conductas delictivas y una nueva clase de delincuentes

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

Los delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella.

Los recursos tecnológicos que emplean estos delincuentes, logran borrar en muchos casos la evidencia de sus actividades, a pesar de que los perjuicios

económicos causados a sus víctimas son de gran consideración, y en ocasiones pueden llegar a comprometer la seguridad del Estado, el orden económico y social así como la vida y demás derechos de las personas.

Se debe legislar en forma orgánica en nuestro Código Penal, brindando mayor seguridad jurídica y promover una importante campaña de prevención de eventuales hechos delictivos informáticos.

Se propone:

Modificar algunos artículos contemplados en el titulo III capitulo VII del Libro II de la ley 599 de 2000.

Crear un título nuevo en el actual código penal para los delitos informáticos, lo cual permitirá la tutela penal de un nuevo bien jurídico: La información, destinado a precaver la lesión o puesta en peligro de los derechos que tienen las personas a que el procesamiento, la conservación y la transmisión de datos informáticos que usan o les pertenecen.

La protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

Tipificar como delitos autónomos el espionaje informático, el sabotaje informático, la introducción de virus informático y nuevas conductas sancionables penalmente atentatorias del bien jurídico penal de la información.

Con el fin de que:

La autonomía de la información como bien jurídico y el tratamiento de las conductas punibles de manera integral bajo el mismo, permita implementar una técnica jurídica eficaz para que los funcionarios judiciales actúen con mayor claridad ante una conducta que realizan personas instruidas, estudiosas y muy hábiles intelectualmente.

Exista una regulación de medidas preventivas de carácter penal para mantener la seguridad jurídica y los principios del orden social y el bien común.

PROPUESTA LEGISLATIVA N 2004-09-
Proponentes: EVA MARIA ANGULO SOLEDAD
JAIME ENRIQUE ACOSTA ORDOSGOITIA

"La cual se adicionan y modifican tipos penales y se tutela el bien jurídico información en la ley 599 de 2000 con el fin de contrarrestar los delitos informáticos."

Artículo xx. El artículo 16 de la ley 599 de 2000 se adicionará de la siguiente manera:

La ley penal colombiana se aplicará a:

El que cometa en el extranjero delito contra el bien jurídico de la información si dentro del territorio de la República hubiere producido efectos la conducta punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo xx. Responsabilidad de las personas jurídicas. Las personas jurídicas serán sancionadas en los casos en que por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o

preferente cometan delitos informáticos o en aquellos casos en que se atente contra el bien jurídico de la información.

La sanción aplicable a las personas jurídicas por los delitos será de multa, por el doble del monto establecido para el referido delito y la pérdida del registro comercial por el término de cinco años.

Artículo xx El capitulo III de la ley 599 de 2000 tendrá un nuevo articulo del siguiente tenor: El servidor público que en ejercicio de sus funciones falsifique, suprima o oculte un documento público electrónico se sancionara con la perdida de empleo o cargo publico, la inhabilitación para el ejercicio de derechos y funciones publicas por el termino de tres años y la privación del derecho a manejar sistemas de información por el termino de doce meses.

Artículo xx El Titulo VII, capitulo I de la ley 599 de 2000 tendrá dos nuevos Tipos penales del siguiente tenor:

Hurto mediante tecnologías de la información**:** El que mediante el uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años , multa de tres unidades multa de segundo grado y la privación del derecho a manejar sistemas de información por el término de cinco años.

Obtención indebida de bienes o servicios. El que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será sancionado con prisión de dos a seis años, multa de

tres unidades multa de segundo grado y la privación del derecho a manejar sistemas de información por el término de tres años.

Articulo xx. El articulo 192 de la ley 599 de 2000: quedara así: Violación ilícita de comunicaciones privadas El que ilícitamente por cualquier medio acceda, intercepte, interfiera, impida, desvié, elimine, modifique mensaje de datos, señal de transmisión o comunicación de carácter privado y ajeno, será sancionado con prisión de dos a tres años , la privación del derecho a manejar sistemas de información y el decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos durante el tiempo de cumplimiento de la pena.

Articulo xx. El articulo 193 de la ley 599 de 2000: quedará así: El que, sin permiso de autoridad judicial competente, importe, fabrique, ofrezca, posea, distribuya, comercialice o preste servicios de equipos, dispositivos, programas o instrumentos destinados a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información o interceptar la comunicación privada entre personas incurrirá en: Inhabilitación para el ejercicio de profesión en sistemas informáticos, industria o comercio por el término de tres años, privación del derecho a manejar sistemas de información por el término de 12 meses, el comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos, durante el tiempo de cumplimiento de la pena y multa de uno a tres unidades multa de segundo grado.

Artículo.xx- El articulo 194 de la ley 599 de 2000. Quedara así: Divulgación de información reservada: El que sin autorización de autoridad judicial competente, divulgue*,* copie datos o información reservada o confidencial que se encuentre en ficheros, archivos, bases de datos, sistemas informáticos o telemáticos, públicos o

privados, incurrirá en prisión de tres a diez meses y a tres unidades multa de segundo grado y trabajo comunitario por el término de uno a cinco años.

Artículo xx. El articulo 195 de la ley 599 de 2000. Quedara así: Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información incurrirá en la privación del derecho a manejar sistemas de información por el término de cinco años, trabajo comunitario por el término de hasta tres años y multa de uno a tres unidades multa de segundo grado.

TITULO XXX
DE LOS DELITOS CONTRA LA INFORMACIÓN

Artículo xxx. Espionaje informático. El que sin autorización del titular ingrese, intercepte, interfiera, base de datos, programas o documentos electrónicos ajenos contenidos en red, soporte o sistemas informáticos y telemáticos con el ánimo de, usar, revelar, comercializar, divulgar, difundir o apoderarse de la información o datos en tránsito o contenido en ellos, se sancionara con inhabilitación para el ejercicio de profesión en sistemas informáticos, industria o comercio por el termino de tres años, privación del derecho a manejar sistemas de información por el término de veinticuatro meses, y multa de tres a seis unidades multa de segundo grado.

Artículo xxx. Sabotaje informático El que destruya, dañe, modifique, altere, inutilice obstaculice, borre el funcionamiento de sistema informático, base de datos, programas o documentos electrónicos y telemáticos se sancionara con prisión de cuatro a siete años, la privación del derecho a manejar sistemas de información por el termino de cinco años y multa de tres a seis unidades multa de segundo grado.

Artículo xxx. Sabotaje informático culposo El que destruya, dañe, modifique, altere, inutilice obstaculice, borre el funcionamiento de sistema informático, base de datos, programas o documentos electrónicos y telemáticos por falta al deber objetivo de cuidado, incurrirá en pena de trabajo comunitario por el término de dos años, la privación del derecho a manejar sistemas de información por el termino de un año y multa de uno a tres unidades multa de segundo grado.

Artículo xxx. Fraude Informático. El que, mediante el uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones o datos falsos o fraudulentos que produzcan un resultado que permita obtener un provecho ilícito en perjuicio ajeno será sancionado con prisión de dos a cinco años, la privación del derecho a manejar sistemas de información durante el término de cinco años y multa de tres unidades multa de segundo grado.

Artículo xxx. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos**.** El que por cualquier medio, grabe, copie, altere, clone, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines como tarjetas de crédito, celulares y demás, incurrirá en prisión de tres meses a diez meses y a cuatro unidades multa de segundo grado y trabajo comunitario por el término de uno a cinco años.
La misma pena se establecerá cuando el objeto de la conducta consista en incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos.

Artículo xxx**.** Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante tecnologías, instrumentos o medios de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de dos a cinco años, la privación del derecho a

manejar sistemas de información durante el término de cinco años y multa de tres unidades multa de segundo grado.

Artículo xxx. Creación de virus informático. El que sin el permiso del Gobierno Nacional cree, diseñe, o fabrique programas, códigos, documentos de datos o información que contengan virus o gusanos informáticos se sancionara con multa de tres unidades multa de segundo, trabajo comunitario por el término de uno a cinco años y la privación del derecho a manejar sistemas de información durante el termino de cuatro años.

Artículo xxx Circunstancias de Agravación comunes a los artículos anteriores. Las penas correspondientes a los delitos previstos aumentaran a la mitad cuando:

Se ponga en peligro la seguridad de un medio de transporte público de personas o de cargas, el normal funcionamiento de las comunicaciones, de la provisión de agua, del suministro de electricidad, de la prestación del servicio de salud o de cualquier otro servicio público.

Se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones jurídicas y financieras o resultare algún perjuicio a personas naturales o jurídicas que ostenten la calidad de comerciante

La Conducta hubiere sido cometida mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.
La conducta se realizare por empleado o contratista del propietario del sistema informático o telemático.

La conducta la realizare un servidor público, con provecho para sí o para un tercero.

El autor de la conducta fuese el responsable de la custodia, administración, operación, control, mantenimiento o seguridad de un archivo, registro, sistema o dato informático.

El propósito o fin perseguido por el agente sea de carácter terrorista o daño a la comunidad en general.

CONCLUSIONES

La interacción de la ciencia del derecho y la informática da existencia a las disciplinas de la informática jurídica y del derecho informático. La informática jurídica estudia el tratamiento automatizado de las fuentes del conocimiento, producción y medios instrumentales con los que se gestiona el derecho. El derecho informático estudia los aspectos y conflictos jurídicos originados en el desarrollo, uso y disposición de la informática.

El contenido de las disciplinas que conforman el derecho informático es variado, como distintas son las especialidades del derecho en las cuales el impacto tecnológico las afecta.

Dentro de la variedad de saberes que conforman el derecho informático, es el derecho penal informático, la disciplina encargada del estudio de los delitos informáticos.

La expresión delito informático comprende una pluralidad de significados generando dificultad para establecer un concepto universal y único; sin embargo, con el fin de superar la dificultad aludida, la doctrina informática ha planteado tres criterios de definición, a saber: Los criterios de definición son: El criterio subjetivo, el criterio objetivo y el criterio funcional; así mismo, se encuadra la pluralidad de definiciones de delito informático en torno al elemento material que sirve de medio para la comisión de estos delitos, y en torno al bien jurídico afectado.

La realización de las conductas catalogadas como delitos informáticos pueden hacerse utilizando medios de comunicación e información como redes, señales y

ondas, los cuales se canalizan mediante instrumentos u objetos, como: Computadoras , teléfonos o la Internet.

La Internet es el medio inmaterial de comunicación de mayor uso a nivel mundial que permite el intercambio, distribución, interacción y recolección de información de manera rápida, sin limitación de espacios. La Internet es un conjunto de redes independientes, que se encuentran conectadas entre si; creada inicialmente con propósitos militares, rápidamente, se convirtió en un medio para compartir información científica y acceder a grandes centros de cómputo; hasta convertirse en un medio masivo de información, de toda tendencia y disciplina. La Internet ofrece variedad de servicios y aplicaciones disponibles entre los que se destacan los correos electrónicos, los medios de divulgación de datos, las listas de discusión y charla.

Con base en el principio de legalidad debe existir previamente en el ordenamiento penal una descripción típica de los delitos informáticos con el fin de que estas conductas sean sancionadas. Es necesario tipificar estas conductas que afectan bienes jurídicos como la información y la intimidad con el fin de evitar el colapso de los sistemas de información y la vulneración de derechos fundamentales.

Por otra parte , se hace necesaria la determinación del sujeto activo de los delitos informáticos, en aras de garantizar seguridad jurídica en el momento de imputar responsabilidad penal.

La diversidad de los sujetos activos en los delitos informáticos con variados apelativos, ha llevado a enumerar esta clase de sujeto en: Hacker, cracker, phreakers, lammers, gurus y trashing; situación diferente se presenta en el sujeto pasivo donde se determina que de manera directa e indirecta todos somos víctimas de los delitos informáticos.

Respecto al objeto material sobre el cual recaen las conductas informáticas, se encuentran objetos materiales reales como ordenadores , disquetes, instrumentos electrónicos del hardware, sistemas lógicos como el software y el objeto fenomenológico de la información; que ha llevado a clasificar los delitos informáticos en delitos contra la información por creación, por destrucción, por uso indebido y por sustracción.

Los bienes jurídicos tutelados y afectados por los delitos informáticos son variados, como, la honra, el patrimonio económico, la fe pública, la propiedad intelectual, la seguridad del Estado; sin embargo, se destacan la intimidad personal y la información como los bienes jurídicos mas afectados por los delitos informáticos.

La intimidad como derecho es reconocido en nuestra Carta Política en su artículo 15 y en posición de la Honorable Corte Constitucional es un derecho de la personalidad de carácter general, absoluto, inalienable e imprescriptible.

La información como fenómeno político, económico y jurídico ha suscitado dentro de la doctrina informática la inquietud de ser considerado como un bien jurídico a tutelar; el cual merece protección especial por parte del Estado. La información como derecho es regulado junto al derecho de libertad de expresión y de opinión en el artículo 20 de la Carta Política, donde se describe como facultad humana para recibir información y como práctica humana para difundir información.

En torno al análisis de determinar si las conductas criminales informáticas coinciden o no con las descripciones típicas señaladas en el estatuto penal (ley 599 de 2000) se concluyo que estas acciones revisten un carácter atípico tanto relativo como absoluto, veamos:

La atipicidad relativa se da en función de la naturaleza del objeto material sobre el que se concreta la vulneración de un interés que el legislador está llamado a tutelar y sobre la propia conducta del agente dada por el verbo rector con algunos ingredientes normativos.

La atipicidad absoluta se denota en los delitos informáticos cometidos mediante la Internet y en especial los que atentan contra los aparatos lógicos como: Fraudes cometidos a través de la manipulación del computador, donde se desarrollan las conductas de: Manipulación de los datos de entrada y salida, manipulación de programas y el fraude efectuado por manipulación informática; así mismo , las falsificaciones informáticas que comprende los daños o modificaciones de programas o datos computarizados como: El sabotaje informático, virus, gusanos, bombas lógicas o cronológicas.

Respecto a los tipos penales consagrados en la ley 599 de 2000 que expresan conductas atentatorias contra el bien jurídico de la información que se considera necesario proteger, se presentan tipos penales que actualmente solo buscan tutelar bienes jurídicos como la intimidad , libertad e integridad, formación sexual y libertad de trabajo; estos tipos penales son: Acceso abusivo a un sistema informático, violación ilícita de comunicaciones , utilización ilícita de equipos transmisores o receptores, sabotaje y pornografía con menores.

El análisis probatorio de los delitos informáticos es necesario para proporcionar la certeza de los hechos y la búsqueda de la verdad material ante el fenómeno delictual informático y el resultado del juicio que sancionará a los sujetos responsables de estas conductas; puesto que una característica sobresaliente de los delitos informáticos es su perfeccionamiento instantáneo en una sola acción o varias acciones en tiempos distintos, repetitivos y prolongados; hecho que hace compleja su demostración e investigación .

En la obtención de los medios que sirvan de prueba de las infracciones cometidas por medio de tecnologías informáticas existe dificultad, pues los operadores judiciales, desconocen la forma de valorar y recepcionar las pruebas.

Cuando se tiene acceso a pruebas informáticas por medios no autorizados y no existiendo medios para demostrar su autenticidad, confiabilidad y suficiencia; conllevaría a que los elementos aportados carecerán de la validez requerida y serán tratados de ilegales.

Respecto a los medios de prueba que sirven para el conocimiento de los fenómenos criminales informáticos, se destacan la modalidad del documento electrónico; el cual cobra relevancia jurídica a partir de la ley 527 de 1999; conllevando a que los operadores de justicia valoren su autenticidad y su seguridad.

Actualmente dos grandes técnicas existen para demostrar la autenticidad de los documentos electrónicos; estas son el código secreto y la criptografía. El código secreto es la técnica mas difundida, consiste en una combinación de cifras o letras que el sujeto conoce y digita sobre el teclado que va utilizar .La criptografía es la técnica utilizada para hacer efectivos números mecanismos de seguridad informática.

Los objetos que pueden constituir documentos con virtud probatoria en investigaciones o juicios por delitos informáticos son: Soportes informáticos, como los discos duros de computadoras, discos blandos (diskettes), discos compactos, discos de compactación de información , discos ópticos, impresoras, agendas digitales y electrónicas, teléfonos celulares, cassettes de audio y video, discos de DVD, cámaras digitales y dispositivos de memoria paralela, los cuales son necesarios inspeccionar detalladamente con todas las seguridades, para recuperar la información, relacionada con la conducta criminal informática.

El peritaje informático reviste diversas maneras de realizarlo, debido a los cambios de la tecnología y la ciencia; pero dentro de la aplicación práctica existen dos grandes campos de la labor pericial, reconocidos por la doctrina penal informática: Las pericias de contenido, funcionamiento y recuperación de datos, y las pericias de autenticidad.

La eficacia probatoria de los elementos informáticos, y su interpretación a través de los dictámenes periciales se deriva de los procesadores de datos que se haya obtenido de sistemas implementados a la luz de previsiones legales o reglamentaciones específicas.

No es la ausencia de método o fundamentos científicos lo que pone en tela de juicio la eficacia probatoria de los dictámenes de los peritos informáticos; sino, la tendencia a creer que todo aquello que escapa a la percepción directa de los sentidos no se podrá dilucidar su existencia.

Los indicios sobre la intervención de personas en aras de efectuar actos encaminados a la realización de delitos informáticos, suelen darse con la ayuda de accesorios comercializados para tal fin, por compañías proveedoras de servicios de computación.

La evidencia digital es pieza probatoria básica para el funcionario judicial, constituyéndose en la vía requerida para presentar las pruebas de los hechos ocurridos en sistemas informáticos o dispositivos electrónicos.

La evidencia digital está soportada en medios electrónicos; y es el funcionario judicial el cual debe conocer, acerca de cómo se crea, cómo se recolecta, cómo se asegura y cómo se presenta en el juicio, con el fin de aportar con claridad y precisión, factores que orienten las decisiones sobre casos donde ésta evidencia sea parte fundamental.

La evidencia digital se sustenta en tres principios fundamentales, como son la autenticidad, la confiabilidad y la suficiencia.

La autenticidad es la característica que muestra la no alterabilidad de los medios originales y busca confirmar que los registros aportados corresponden a la realidad demostrada en la fase de identificación y recolección de evidencia; la confiabilidad es el principio que señala si efectivamente los elementos probatorios aportados vienen de fuentes creíbles y verificables; en tanto que el principio de la suficiencia indica la presencia de toda la evidencia necesaria para adelantar una investigación sobre delitos informáticos.

Los tipos contenidos en la legislación Penal son obra exclusiva del legislador, en virtud del principio de reserva legal, no obstante, el principal problema que surge para el legislador, cuando busca señalar y describir las conductas constitutivas de delitos informáticos, es precisar qué opción de técnica legislativa debe asumir para ofrecer una adecuada política criminal.

Las tendencias respecto a la penalización de la criminalidad informática, han sido, la de descodificar o penalizar conductas, modificar normas del código penal, promover la expedición de una ley especial, o de desarrollar una norma “tipo” en las cuales se incluya la parte sustantiva y procesal.

Es necesario adoptar como ley, el proyecto en consideración, para mantener los principios de seguridad jurídica, justicia y bien común; principios pilares de un Estado Social de Derecho.

El proyecto de ley que se presenta como parte propositiva del presente trabajo busca adicionar nuevos tipos penales a bienes jurídicos ya tutelados en el ordenamiento penal como lo es el patrimonio económico; en los delitos de hurto mediante tecnologías de la información y obtención indebida de bienes o servicios;

así mismo, modifica de manera parcial los tipos penales consignados en el titulo de los delitos contra la libertad y otras garantías.

El proyecto de ley en mención eleva a rango de bien jurídico penal la información; conllevando a incorporar tipos penales como: Espionaje, fraude, sabotaje informático; oferta engañosa y creación de virus informáticos; y crea la responsabilidad penal a las personas jurídicas que por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente cometan delitos informáticos o acciones que busquen vulnerar la información.

BIBLIOGRAFÍA

ACTAS JORNADAS MARCO LEGAL Y DEONTOLÓGICO DE LA INFORMÁTICA VOLÚMENES I Y II. En Revista Iberoamericana de derecho Informático. Serie informática y derecho. Extremadura: UNED. 1998.

ACTAS II CONGRESO INTERNACIONAL DE INFORMÁTICA Y DERECHO. Volúmenes I y II. Serie informática y Derecho. Extremadura UNED. 1996.

ACTAS II JORNADAS INTERNACIONALES SOBRE EL DELITO CIBERNÉTICO. Revista Iberoamericana de Derecho Informático. Informática y derecho. Extremadura: UNED. 1998.

ALZATE NOREÑA, Luis, Pruebas Judiciales, Bogotá, Ed. Temis 1954.

ARAUJO; Alberto Daniel .La informática en el proceso de administración de Justicia. En: Revista Derecho y Tecnología Informática, Bogota 1990.

ARTEAGA S, Alberto. El delito informático: Algunas implicaciones jurídico penales, Revista de la Facultad de ciencias jurídicas y políticas. Universidad central de Venezuela, 1989.

AZPILCUETA, Herminio Tomas, Derecho Informático, Buenos Aires, Ediciones Alianza, 1987.

BAÓN RAMÍREZ Delincuencia Informática. Promociones y Publicaciones Universitarias. Barcelona, 1992.

BENEYTO Juan. Información y sociedad, Madrid, Alianza Editorial, 1999.

BLOOM BECKER, Buck. Grandes estafas por computador., ediciones jurídicas, Bogotá 1995.

CACERES, Nieto. Lógica jurídica e información jurídica, Revista Universidad Complutense de Madrid. Facultad de Derecho, 1986.

CAICEDO, Fernando. Curso de informática jurídica, Bogota, Editorial Tecnos, 1988.

CALLEGARI, Lidia. Delitos informáticos y legislación, en: Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana. Medellín, Colombia. No. 70 julio-agosto-septiembre. 1985.

CARRASCOSA LOPEZ, Valentin. El derecho de la prueba y la informática, problemática y perspectivas. Informática y Derecho II. Extremadura: UNED. 1997.

CASABONA Romero, Hacia un concepto de delito Informático, Ponencia presentada al XI Congreso Internacional de Informática, Buenos Aires, Agosto, 1991.

CÓDIGO DE PROCEDIMIENTO PENAL, Colección código brevis, Editorial Leyer, 2003.

CÓDIGO DE PROCEDIMIENTO CIVIL, Colección código brevis, Editorial Leyer, 2003

CÓDIGO PENAL LEY 599 DE 2000. Colección código brevis, Editorial Leyer, 2003.

CONSTITUCION NACIONAL DE COLOMBIA, Editorial la Nueva Ley, Santanfe de Bogota, 1996.

COLOMBIA. CORTE CONSTITUCIONAL, sentencia de Junio 16 de 1992. En Revista Legis Santa Fe de Bogota 1994.

COLOMBIA. CORTE CONSTITUCIONAL, sentencia T-512 de 1992, Magistrado ponente Dr. José Gregorio Hernández Galindo, sentencia aprobada en Santafé de Bogotá, D.C., mediante acta de nueve (9) de septiembre de mil novecientos noventa y dos (1992).

COLOMBIA. CORTE CONSTITUCIONAL, sentencia T-696 de 1996, Magistrado ponente Dr. Fabio Morón Díaz, Santafé de Bogotá D.C., diciembre cinco (5) de mil novecientos noventa y seis (1996).

COLOMBIA.CORTE CONSTITUCIONAL, sentencias Corte Constitucional, sentencia T-414 de 1992, Magistrado ponente Dr. Ciro Angarita

COLOMBIA. CORTE CONSTITUCIONAL, sentencia T-066 de 1998, Magistrado ponente: Dr. Eduardo Cifuentes Muñoz, marzo 5 de 1998.

COLOMBIA. CORTE CONSTITUCIONAL, sentencia T- 473 de 1992, MP. Dr. Ciro Angarita Barón, Santafé de Bogota, D.C; 14 de Julio de 1992.

CORTE CONSTITUCIONAL, sentencia C-488/93, Magistrado ponente Dr. Vladimiro Naranjo Mesa, Santafé de Bogotá, D.C., veintiocho (28) de octubre de mil novecientos noventa y tres (1993).

COLOMBIA. CORTE CONSTITUCIONAL, sentencia T-332/93, Magistrado ponente Dr. José Gregorio Hernández Galindo, sentencia aprobada en Santafé de Bogotá, D.C., mediante acta del día doce (12) de agosto de mil novecientos noventa y tres (1993),

COLOMBIA CORTE CONSTITUCIONAL, sentencia T-563/93, Magistrado ponente Dr. Vladimiro Naranjo Mesa, Santafé de Bogotá, D.C., siete (7) de diciembre de mil novecientos noventa y tres (1993),

COLOMBIA. CORTE CONSTITUCIONAL, sentencia No, SU-056 de 1995, Magistrado ponente Dr. Antonio Barrera Carbonell, Santafé de Bogotá D.C., febrero diez y seis (16) de mil novecientos noventa y cinco (1995).

COLOMBIA. CORTE CONSTITUCIONAL, sentencia No. T-552 de 1995, Magistrado ponente Dr. José Gregorio Hernández Galindo, sentencia aprobada en Santafé de Bogotá, D.C., a los veintisiete días del mes de noviembre de mil novecientos noventa y cinco (1995).

COLOMBIA. CORTE CONSTITUCIONAL, sentencia No, C-073 de 1996, Magistrado sustanciador Dr. José Gregorio Hernández Galindo, sentencia aprobada según consta en acta del veintidós (22) de febrero de mil novecientos noventa y seis (1996).

COLOMBIA. CORTE CONSTITUCIONAL, sentencia No. C-073 de 1996, Magistrado sustanciador Dr. José Gregorio Hernández Galindo, sentencia aprobada según consta en acta del veintidós (22) de febrero de mil novecientos noventa y seis (1996).

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. Contenidos ilícitos y nocivos en Internet. Bruselas, 16.10.1996 COM (96) 487 final.

COMISIÓN DE LAS COMUNIDADES EUROPEAS. Comunicación de la Comisión. Seguimiento del Libro Verde sobre Derechos de Autor y Derechos afines en la sociedad de la información. Bruselas, 20.11.1996 COM (96) 568 FINAL.

DICCIONARIO DE LA LENGUA CASTELLANA USUAL, Santafé de Bogotá, Planeta 2001

DUARTE CALDERÓN, Carlos Arturo y otros. Informática Jurídica en el Derecho Procesal Penal, UNAB, Facultad de Derecho, Bucaramanga, 1991.

ENCICLOPEDIA DE INFORMÁTICA, MacGraw Hill, Madrid 1996.

FERNANDEZ, Carrasquilla Juan. Derecho penal Fundamental, Temis, Bogota 1989

FERNÁNDEZ, Castro Juan Diego. Abogacía e Informática, El delito informático, en: Revista del Colegio de Abogados Penalistas del Valle, Volumen IX.

FERNÁNDEZ, Maria Clara. Atipicidad relativa en los delitos de falsedad, hurto, estafa y daño informáticos. Universidad Sergio arboleda. Santa Marta, 2001.

GARCÍA, Barcelo Miguel, Ponencia presentada al: Congreso sobre "Derecho Informático", celebrado en la Universidad de Zaragoza, España: en junio de 1989.

GIRALDO ÁNGEL, Jaime. Informática Jurídica Documental. Bogotá: Temis. 1990.

GUERRERO, María Fernanda. Comentarios sobre la ley de comercio electrónico y firmas digitales. Cámara de Comercio de Bogotá Octubre de 2001.

GUERRERO, María Fernanda. Breves consideraciones a cerca del documento electrónico: Su problemática jurídico procesal. Boletín Jurídico de la Asociación Bancaria. No. 642 – 2 de Febrero 15 de 1992.

GUERRERO, María Fernanda. Fraude informático en la Banca, aspectos criminológicos. Ed. Ediciones jurídicas 1995.

GUTIÉRREZ Francés, Informática y derecho, Madrid, Editorial Alianza, 1999.

HANCE, Oliver. El derecho de los negocios en internet, MacGraw Hill, Madrid 1998.

JORDAN FLORES, Fernando, Informática Jurídica, Bogotá, Universidad de los Andes, 1983

LIMA Maria de la Luz, El Delito Electrónico, Ed Ariel, México, 1999.

LÓPEZ, Escobar. Derecho Penal Básico. Tomo I, Edit Leyer, Bogotá. 2000

MÁRQUEZ, Carlos Pablo. El delito informático. Edit Leyer, Bogotá. 2002

MOLINA, Arrubla. Carlos. Introducción a la Criminología. Editorial Biblioteca Jurídica, Medellín, 1981.

NACIONES UNIDAS. Revista Internacional de Política Criminal. Manual de las Naciones Unidas sobre Prevención del Delito y Control de delitos informáticos.

Oficina de las Naciones Unidas en Viena. Centro de Desarrollo Social y Asuntos humanitarios. Nos.43 y 44. Naciones Unidas, Nueva York.1994.

NACIONES UNIDAS. Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana. 27 de agosto a 7 de septiembre de 1990. (A/CONF. 144/28/Rev.1) Nueva York, Naciones Unidas. 1991.

PEREZ LUÑO, Antonio Enrique, Ensayos de Informática Jurídica, Biblioteca de Ética y Filosofía del Derecho, México. Distribuciones Fontamara S.A., 1998.

PEÑA Helen, Delitos informáticos. División de estudios de postgrado. Facultad de Derecho. UNAM., México, 1999.

QUIÑONES G.,G. Cibernética Penal. El Delito Computarizado, Caracas, Editorial Gráficas Capitolio, Caracas, 1999.

RAMÍREZ, Baon. Delincuencia Informática. Publicaciones Universitarias. Barcelona, 1992.

RIASCOS GOMEZ, Libardo. La Constitución de 1991 y la informática Jurídica. Universidad de Nariño 1997.

RIVERA LLANO. Dimensiones de la Informática en el Derecho, Bogotá, Ed. Jurídica Radar, 1995.

ROCHA Antonio, La prueba indiciaria, 1978, Externado de Colombia,

SAFARONNI, Eugenio Raúl. Manual de Derecho Penal, parte general. Ediar, Buenos Aires, 1979.

SALAZAR CANO, E. Cuadernos de Informática Jurídica y Derecho Cibernético. Venezuela, 1997

SARZANA, Carlos. Criminalita e tecnología en Computers crime. Rassagna Penitenziaria e criminología. Nos 1-2. Ano 1979. Roma.

SOLER, José A. El delito Informático. Revista Protección y seguridad, mayo – junio de 1996, España.

TELLEZ VALDEZ, Julio, Derecho informático, Editorial Mc Graw Hill, México, 1997.

TIEDEMANN, K., citado por Molina A. Introducción a la Criminología., Ed. Biblioteca Jurídica, Medellín, 1988.

VELAZQUEZ, Fernando. Manual de Derecho Penal, Ed Temis. Bogota 2002,

VIEGA, Rodríguez, Maria. Delitos Informáticos, Revista electrónica de Derecho informático, Nº 09- Abril de 1999.