EL DELITO INFORMATICO Y SU INCIDENCIA EN EL NUEVO CÓDIGO PENAL

JAIRO EDMUNDO CABRERA PANTOJA

UNIVERSIDAD DE NARIÑO
FACULTAD DE DERECHO Y CIENCIAS POLITICAS
CENTRO DE INVESTIGACIONES SOCIOJURIDICAS
SAN JUAN DE PASTO
2004

EL DELITO INFORMATICO Y SU INCIDENCIA EN EL NUEVO CÓDIGO PENAL

JAIRO EDMUNDO CABRERA PANTOJA

Informe final de trabajo de grado para optar el título de Abogado.

Asesor :
Dr. JUAN CARLOS LAGOS MORA
DECANO DE LA FACULTAD DE DERECHO

UNIVERSIDAD DE NARIÑO
FACULTAD DE DERECHO Y CIENCIAS POLITICAS
CENTRO DE INVESTIGACIONES SOCIOJURIDICAS
SAN JUAN DE PASTO
2004

“Las ideas y conclusiones aportadas en la tesis de grado, son responsabilidad exclusiva de los autores”.

Artículo 1 del Acuerdo N° 324 de Octubre 11 de 1.996, emanada del Honorable Consejo Directivo de la Universidad de Nariño.

Nota de aceptación.

_____
_____
_____
_____
_____
_____
_____

_____
Firma del Jurado

_____
Firma del Jurado

_____
Firma del Asesor

San Juan de Pasto, 25 de Junio de 2004.

CONTENIDO

RESUMEN

Las nuevas tecnologías y más específicamente las tecnologías de la información, generan en el ser humano nuevas situaciones a las cuales ha tenido que adaptarse dando lugar a cambios en su manera de percibir su entorno , tal como el acceso rápido a la información, la agilización de transacciones bancarias y comerciales que influyen directamente en las concepciones culturales.

Con el paso del tiempo, hemos visto como el mundo se ha vuelto mucho más dependiente de la red global de información, por lo tanto cada día más se aumentan las posibilidades para que sea atacada la infraestructura no física, sino virtual de la información y conseguir la desestabilización tanto económica, social, política, jurídica o informática dentro de un país a través del uso de las armas de la info –guerra (guerra informática).

Doctrinariamente el Sabotaje Informático, propio de la conductas criminógenas de daños o modificaciones de programas o datos computarizados , mediante la cuales, el agente se introduce a los sistemas de información con la finalidad de obstaculizar su funcionamiento. Es la conducta que ejecutan los conocidos dark side hackers y crackers o intrusos. Las modalidades más conocidas son las siguientes: Las bombas lógicas (logic bombs), que se introducen en un sistema informático y se activan con un comando especial (fecha, números, etc.), para destruir o dañar datos contenidos en un ordenador; ejemplo de ello fueron los conocidos virus Sycam y Dragón Rojo. Los virus informáticos producen también destrucción o daño en el software o hardware del computador, pero a diferencia de las bombas lógicas, tienen capacidad de expansión y contagio a otros sistemas informáticos, sin que el operador legítimo sepa de ello (es un mero instrumento). Otros de los mecanismos que pueden impedir el acceso a un sistema de información por parte del usuario legítimo, son los conocidos como "spamm" o el "electronic-mail bombing"; que consisten en el envío de cientos o miles de mensajes de correo electrónico, no solicitados o autorizados, para bloquear los sistemas.

A pesar de lo anterior sólo nueve naciones han desarrollado leyes adecuadas para combatir la delincuencia en Internet. Esto demuestra que las normativas internacionales no están adaptadas a la nueva realidad al igual que nuestro país, razón por la cual pretendemos con éste estudio dar una solución jurídica aplicable en Colombia, para combatir los delitos a través de la red.

ABSTRACT

The new technologies and more specifically the technologies of the information, generate in the human being new situations to which has had to adapt giving place to changes in their way of perceiving their environment, just as the quick access to the information, the activation of bank and commercial transactions that they influence directly in the cultural conceptions.

With the step of the time, we have seen as the world he has become much more dependent of the global net of information, therefore every day more the possibilities are increased so that the non physics infrastructure will be attack.
The use of the weapons of the computer war, which don't have like fundamental base a chemical reaction, but rather they are inside a programming language and they can take place a lot but I damage that the conventional weapons that today knows.

The Computer Sabotage, characteristic of damages or modifications of programs or on-line data, by means of the one which, the agent is introduced to the systems of information with the purpose of blocking her operation. It is the behavior that the well-known dark side hackers and crackers or intruders execute. The better known modalities are the following ones: The logical bombs (logic bombs) that they are introduced in a computer system and they are activated with a special command (it dates, numbers, etc.), to destroy or to damage contained data in a computer; example of they were it the well-known virus Sycam and Red Dragon. The virus computer specialist also produce destruction or damage in the software or hardware of the computer, but contrary to the logical bombs, they have expansion capacity and infection to other computer systems, without the legitimate operator knows about it (it is a mere instrument). Then it is possible that the logical bombs and the virus computer specialist affect the readiness of the information transitorily, without destroying it. Others of the mechanisms that can impede the access to a system of information on the part of the legitimate user, are the acquaintances as " spamm " or the electronic-mail bombing"; that consist in the shipment of hundred or thousands of messages of electronic mail, not requested or authorized, to block the systems.

In spite of the above-mentioned nine nations have only developed appropriate laws to combat the delinquency in Internet. This demonstrates that the normative ones international they are not adapted to the new reality the same as our country, for this reason, our work will be give a new law for fight the crime inside in the world wide web of information.

INTRODUCCIÓN

Las sociedades se han visto envueltas dentro de un nuevo ordenamiento tecnológico, que influye directamente sobre las viejas concepciones culturales, sociales, e incluso legislativas, hace unos 30 años era prácticamente inconcebible realizar compras por un computador, mucho menos comunicarse a través de él, y a un menos impensable realizar terrorismo por una red. Dado lo anterior es necesario que la legislación se adapte a todos los nuevos precedentes tecnológicos con el fin de establecer parámetros básicos que no pueden ser violados.

Colombia pese a todo, ha avanzado lentamente en la implementación de leyes sobre estas nuevas estructuras informáticas, tal como lo fue la ley 527 de 1999 en donde se regula de manera muy superficial el comercio electrónico, es decir, el intercambio de bienes, servicios, ofertas, demandas y aceptación que se realicen por medios electrónicos.

En cambio a lo que respecta a delitos y seguridad en la Red, nuestro actual código penal Ley 599 de 2000, no hace alusión expresa a esta clase de delitos informáticos; sin embargo, en varias de sus normas recoge conductas que podrían subsumirse dentro de esta nueva modalidad delictual, entendiendo que éste delito informático[*], podría incluir aquellas conductas que recaen en las herramientas electrónicas tales como programas, computadores, etc, los cuales valiéndose de estos "medios" lesionen bienes jurídicamente tutelados, como la intimidad, el patrimonio económico, etc, pero que no podrían ser castigados como delitos informáticos , puesto que no existen dentro de nuestra legislación.

Dado lo anterior, el derecho no puede quedarse como una simple dogmática jurídica, es imperioso entonces que se cambie a un criterio eminentemente axiológico, que nos permita regular y hacer leyes con base en lo que ocurre en nuestro entorno y por ende, en adecuarnos a nuestras nuevas bases tecnológicas, más específicamente en lo que respecta a los actos que ocasionan daños o modificaciones de programas o datos computalizados. Entonces las autoridades deben afrontar la ausencia de leyes para combatir los novísimos métodos delictivos y la falta de formación técnica que les permita intuir el *modus operandi* de estos delincuentes cibernéticos. Es aquí donde el papel de la Psicología cumple una función muy importante, ya que su objetivo es el estudio del comportamiento del ser humano en diferentes campos. Desde la Psicología

[*] Es conocido también como "Sabotaje Informático", donde el agente se introduce a los sistemas de información con la finalidad de obstaculizar , dañar o entorpecer su funcionamiento. Es la conducta que ejecutan los conocidos Hackers o intrusos.

Criminal se pueden hacer diversos aportes en cuanto a la determinación de causas, tanto personales como sociales, del comportamiento delictivo y el desarrollo de principios válidos para el control social del delito.

El trabajo en conjunto entre la Psicología y el Derecho, permite un entendimiento integral con lo que se refiere a la criminalidad, no solamente desde el sentido legal sino una contribución de los diferentes factores causales que han llevado a una persona hacia un comportamiento criminal.

1. UNA APROXIMACIÓN A LA TEORIA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

1.1 GENERALIDADES

Con la aparición del hombre sobre la Tierra nace el pensamiento y se da el paso decisivo a la reflexión. Por primera vez un ser en la historia de la Vida , no sólo se conoce, sino que conoce. A pesar de los últimos descubrimientos del siglo XX, la Paleontología , aún no ha dado una respuesta definitiva a la aparición de la inteligencia en el hombre, pero lo que nadie duda es que desde el punto de vista orgánico del fenómeno se reduce al perfeccionamiento del cerebro. "*Gracias a que era bípedo pudo valerse de las manos con mayor independencia, el cerebro pudo desarrollarse y , gracias a éste, los ojos, al aproximarse a la cara más reducida, han podido converger y captar lo que las manos cogían , acercaban y presentaban en cualquier sentido y ser capaces de manifestar el gesto mismo de la reflexión*"[1].

Esto dio origen a un proceso evolutivo en el cual el hombre, empezó a desarrollar aún mas sus capacidades, impulsado cada día por la necesidad, pues suele decirse que toda acomodación completa de un grupo humano al medio ambiente en el que vive "*constituye un conjunto de tanto valor absoluto como cualquier otro, e incluso en aquellas formas de existencia que más se aproximan a la vida animal*"[2]. Los seres irracionales se detienen en las más sencilla forma de la adaptación de la naturaleza, en cambio la flexibilidad de la inteligencia humana obliga a reaccionar ante cada presión exterior, obedeciéndola u oponiéndose a ella.

La evolución del hombre , trajo con sigo que generaciones y generaciones de individuos construyan unas bases de conocimiento específico , para desarrollarlo y aplicarlo en su vida cotidiana. Este conocimiento debía ser transmitido entre ellos, lo cual origino la implementación de signos y señas que se convertirían en información y que hasta nuestros días el conocimiento y transmisión de éstos datos sigue vigente como parte esencial del ser humano.

Los avances tecnológicos, fueron posibles porque el ser humano registró sus experiencias en elementos materiales, los cuales sirvieron de base, para que otros los modifiquen o los complementen, mejorando sustancialmente el conocimiento inicial. Estos avances en principio fueron transmitidos bajo la oralidad, posteriormente se hicieron a través de medios rudimentarios como la escritura

[1] EL ALBA DE LA CIVILIZACIÓN. Bogotá; Círculo de Lectores, 1984. p. 25.
[2] HISTORIA UNIVERSAL. Medellín; Editorial Voluntad, 1977. p. 12.

cuneiforme ; luego con la imprenta; y ahora, con los sistemas electrónicos de información.

Este progreso técnico ha conducido al ser humano a sofisticar sus formas de producción de consumo y de ocio. A partir del siglo XVIII los desarrollos técnicos han comenzado a plantear dificultades en su efectivo control. Así mismo, la cantidad de información relativa a las personas, datos técnicos, estadísticas, documentación, ha ido creciendo considerablemente. Ha de tenerse en cuenta que la masa informativa no aumenta aritméticamente, sino con una progresión mayor e imparable. Tanto el control de las máquinas como la ordenación y el acceso directo a toda esa información ha exigido la invención de un aparato que sea capaz de reproducir algunos aspectos característicos de la capacidad mental humana para auxiliar al hombre. Este aparato es lo que conocemos con el nombre de computadora.

La palabra computadora designa una serie de máquinas que responden a una funcionalidad similar. Quiere ello decir que desde las primeras computadoras hasta las actuales se ha producido una evolución tan grande que materialmente resulta difícil reconocer su relación. La primera computadora electromecánica se construyo en 1944, se la llamó MARK I, resultaba inmensa, pesaba 5.000 Kg., poseía muy poca memoria y sólo sumaba, restaba, multiplicaba y dividía. A las computadoras de la década de los años cuarenta se las llamaba dinosaurios, por su condición prehistórica, su tamaño colosal y su poco cerebro. Las actuales son muy distintas, entre ellas las computadoras de bolsillo, las cuales adquieren mayor rapidez para el procesamiento de datos así como una amplia capacidad de memoria[3] , en donde no solo se almacena textos, sino también música y video, lo que se constituye en “información”.

1.2 LA TEORIA DE LA INFORMACIÓN

En primera instancia nos acercaremos a la definición de información, pues ésta a sido objeto de múltiples debates desde una perspectiva filosófica y científica. Así pues, desde un puntos de vista etimológico, la palabra información viene de la raíz latina *forma* y como talla información es, simplemente, un conjunto de datos transmitidos desde una fuente emisora hasta una fuente receptora. De este modo, la trasmisión de información no implica necesariamente la trasmisión de conocimientos, de tal manera que incluso las máquinas son capaces de informar, ya que la información únicamente es la unión coherente de datos que, sin tener en cuenta la interpretación de estos, constituyen formalmente la información.[4] Para otros, la información “parece admitir forzosamente la noción de conciencia y

[3] EL MUNDO DE LA COMPUTACIÓN. Barcelona, España; Editorial Océano, 1991. p.4.
[4] CROSSON, FREDERICK y SAIRE, Kenneth, Filosofía y Cibernética. México. Fondo de la Cultura Económica, 1982.

sentido"[5], de modo que, sólo puede haber procesos de información entre entes que tengan conciencia con la cual le puedan asignar a tales datos un sentido, en principio hombres, lo cual no nos puede llevar a descartas la posibilidad de la conciencia de las máquinas. Así pues , "algo sólo se convierte en información cuando algún agente cognitivo le asigna una significación, es decir lo interpreta como signo". Desde esta perspectiva, la información vista desde el sujeto, solamente puede ser percibida cuando tal sujeto puede asignarle sentido. Desde el punto de vista forma y objetivo, la información de datos, debido a que la estructura de los proceso informáticos se fundamenta en aquellas partículas, lo cual permite que sea trasmitida por un sujeto no consciente que dichos datos contienen una significación cognitiva [6]. Así lo dijo la Corte Constitucional Colombiana, en sentencia T –414 de 1992, en la cual reza:

En la teoría de la información el dato[*] es un elemento material susceptible de ser convertido en información cuando se inserta en un modelo que lo relaciona con otros datos y hace posible que el dicho dato adquiera sentido. En forma muy somera, se puede decir que el sentido en última instancia, lo producen una o varias mentes humanas y este sentido es un determinante de la acción social. Los modelos se plasman en forma de textos y mensajes que consisten en una serie de signos algunos de los cuales les llamaremos datos, organizados de acuerdo a sistemas de reglas o gramática. A través de los signos y mensajes los eventos adquieren realidad social. La realidad expresada a través de mensajes es la determinante de la acción social . El dato se constituye entonces en el elemento básico de información sobre eventos o cosas.

Es entonces que la teoría de la Información se sustenta en que todo tipo de información está compuesta de datos, y en que es el receptor consciente quien interpreta tales datos para que, al encasillarlos dentro de sus sistema mental, se conviertan en elementos con significado. Así, los datos se convierten en un elemento necesario en toda estructura de transmisión de información[7].

Tal como lo ha expresado la Doctrina, es importante completar el esquema para distinguir entre información y comunicación. En este sentido , determinamos que la comunicación es el género y la información es la especie, pues ésta última se encuentra inmersa en la primera. De este modo el mensaje que envía el emisor a través de un canal determinado es tomado por el receptor, instante en el cual se transforman en información. De esta manera pues, "el proceso de comunicación contiene el proceso de información, pero se diferencia de aquél en que hay una

[5] RUYER, Raymond, La cibernética y el origen de la información. México; Fondo de la Cultura, 1987
[6] MARQUES, Carlos. El delito Informático. Bogotá; Editorial Leyer, 2002. p. 21.
[*] La acumulación de varios datos se llaman "datos agregados", la unión de éstos se llaman "registros", la unión de varios registros se denominan "archivos", y la unión de éstos últimos con un único propósito se llaman "base de Datos".
[7] MARQUES, Op. Cit., p. 20.

trasmisión de respuesta a la información enviada , de modo que se da un proceso de alimentación externa de los datos enviados"[8].

En virtud de lo anterior y en el mundo actual globalizado, el acceso a la información es un derecho que puede ejercerlo libremente cualquier persona "*salvo cuando con él puedan afectarse otros como la intimidad, el patrimonio económico, la libre competencia o la seguridad de un Estado*".
Pero este acceso, esta cada vez mas saturado por la cantidad de información recibida, hoy por hoy es fácil enviar o recibir e-mail , fotos, audio, video a través de un teléfono celular, y sin pensar todo lo que se puede recolectar a través de la Web. Todos estos adelantos han sido atribuidos a la denominada "tecnología de la Información" , gracias a la cual , este conjunto de conocimientos han marcado una pauta importantísima desde la comunicación a caballo entre los pueblos a la comunicación en tiempo real satelital.

Hoy por hoy, estamos supremamente familiarizados con la palabra tecnología, entendida esta como el uso del conocimiento científico para especificar modos de hacer cosas de una manera reproducible; esto nos conduce a una definición aún más específica, que sería las Tecnologías de la información, que se podría definir como el conjunto convergente de tecnologías de la microelectrónica, informática y telecomunicaciones.

A pesar de tener diversas ventajas en nuestra sociedad, esta denominada "tecnología de la información", ha traído consigo nuevas formas de criminalidad, siendo denominada genéricamente por la doctrina como "delincuencia informática", la cual no ha tenido una mayor evolución legislativa, pero si ha tenido un amplio desarrollo doctrinal, puesto que la doctrina va a la par con el ingenio humano.

Las computadoras han adquirido un sinnúmero de aplicaciones que permiten facilitar las actuaciones diarias del ser humano, sin embargo, éstas en la actualidad se las utiliza como un medio eficaz para transmitir, obtener y almacenar la información, lo que nos permite concluir que se han transformado en un nuevo sistema de comunicación de la mano con la Internet, pues para acceder a la red mundial es necesario tener la computadora como un instrumento para tal fin, condicionando el desarrollo de la informática; "*a la creación, procesamiento, almacenamiento y transmisión de datos*"[9].
Esto ha permitido que todas las actividades por mas pequeñas que sean tengan la posibilidad de acceder a la tecnología de la informática para mejorar sustanciablemente sus tareas que hasta hace unas pocas décadas eran inimaginables hacerlas de una manera tan rápida y precisa. Así por ejemplo, los

[8] Ibid., p. 20.
[9] XXIII JORNADAS INTERNACIONALES DE DERECHO PENAL. Ponencia Derecho Informático. Bogotá; Universidad Externado de Colombia, 2002.

sistemas de construcción virtual han permito a los ingenieros prevé situaciones de riesgo para determinar que diseño se acomoda más a las expectativas del lugar, de igual manera la tecnología ha permitido a los médicos operar en tiempo real a un paciente que se encuentra a mas de 2000 kilómetros de distancia, entre otras muchas aplicaciones.

Este progreso tecnológico ha permitido que los sistemas computacionales pongan a disposición de millones de usuarios en todo el mundo, una cantidad inimaginable de información, de todas las áreas del conocimiento humano, desde las ciencias exactas hasta las metafísicas, desde una receta de cocina hasta la fabricación de una bomba[*], pues en la práctica cotidiana , no existen barreras para permitir que a través de este medio se acceda con suprema facilidad a un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas e investigaciones que para el hombre común era preferible no hacerlo, y si lo hacía, sólo tenía a sus disposición equipos auxiliares para transcribir sus resultados. En la actualidad, en cambio, "*ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de Responder casi toda la gama de interrogantes que se planteen a los archivos informáticos*"[10].

Este es el panorama de este nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro

---

[*] En Internet es fácil encontrar respuestas a preguntas tales como ¿Necesita la información sobre como construir un arma de pulso electromagnético, (EMPW) que pueda ser ocultada en un maletín?. Trate en la siguiente dirección electrónica de la WWW, (Internet): http:/ www.cs.monash.edu.au/~carlo/ ¿Desea interferir satélites de comunicaciones?. Pruebe en: http://www.spectre.com . Así como la Internet tiene su lado positivo, en donde las distancias y la información de bibliotecas, museos, etc se acorta, también está la información sobre indicaciones para causar terror. El ciberespacio maneja formas de transmitir y recepcionar la información, por lo cual nos permite percibir que es posible realizar con eficacia un acto de terror cuya exigencia esta delimitada por a la habilidad del individuo y conocimiento de la red. Nuestro mundo real sería todo lo físico conocido y por medio de los avances tecnológicos se encontraría íntimamente ligado al mundo virtual, el cual puede ser usado por una nueva generación de violentos para causar caos y obtener unos fines políticos, económicos, etc. determinados, estos serían los terroristas cibernéticos. Con el paso del tiempo, hemos visto como el mundo se ha vuelto mucho más dependiente de la red global de información, por lo tanto cada día más se aumentan las posibilidades para que sea atacada la infraestructura no física, sino virtual de la información y conseguir la desestabilización tanto económica, social, política, jurídica o informática dentro de un país a través del uso de las armas de la info –guerra (guerra informática), las cuales no tienen como base fundamental una reacción química para producir una explosión , sino que están dentro de un lenguaje de programación y pueden producir mucho mas daño que las armas convencionales que hoy conocemos. Libremente en la INTERNET encontramos las instrucciones para la fabricación de elementos ofensivos para llevar a cabo atentados explosivos o biológicos , esto se facilita por la aparición de manuales electrónicos sobre tecnología de bombas o armas químicas y bacteriológicas, tal como fue el caso de la bomba usada en el atentado de Oklahoma en Estados unidos, fue diseñada y fabricada según "El Manual del Terrorista" página de libre acceso en internet. Sin embargo el uso de las armas de la llamada Info-Guerra pueden brindar una capacidad mucho más sutil y efectiva de causar terror y paralizar a una sociedad

[10] CASTRO OSPINA, Sandra Janet. Delitos informáticos : la informacion como bien jurídico y los delitos informáticos en el nuevo Codigo Penal Colombiano. en: XXIII jornadas internacionales de Derecho Penal. Universidad Externado de Colombia, Bogotá. 2002.

consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Las nuevas aplicaciones de la informática, tales como la miniaturizaciones de los sistemas de almacenamientos, el desarrollo de la nanotecnología, el mejoramiento del proceso y almacenamiento de los chips no solo con fines industriales sino también militares, la agilización de los componentes tecnológicos de información, han demostrado que estas nuevas tecnologías, son un arma de doble filo, pues mientras mejoren y faciliten la calidad de vida de los humanos, también trae consigo problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Este nuevo orden tecnológico, trae consigo nuevos interrogantes, que obviamente nos predicen que debemos realizar reestructuraciones dentro de nuestro ordenamiento jurídico, que de una manera nos podrían traer ventajas , pero así mismo crearían situaciones que incluso aún no podrían ser previsibles, la Internet es un mundo inimaginable de conocimiento, que nos podría conducir incluso a desigualdades y conflictos por el acceso a la información . Debido a esta situación , el aumento de los delitos relacionados con los sistemas informáticos registrados en la última década en los países desarrollado tales como en Estados Unidos y Japón, representan una amenaza para la seguridad, para su economía e incluso para la sociedad en general.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la Organización para la Cooperación al Desarrollo a Paris en Mayo de 1983, el término *delitos relacionados con las computadoras* "*se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos"*. Y tal como lo ha manifestado la doctrina la "*amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales"*.

En la actualidad la informatización se ha implantado en casi todos los países. El acceso a la información se ha tornado en un derecho, aunque existen salvedades tales como en países del medio oriente, en donde se es prohibido el acceso a la información a través de Internet, puesto que generaría conocer nuevas ideas culturales que de una u otra forma atentaría con las raíces propias del Islam.

La informatización antes referida se ha desarrollado no solo en la organización y administración del Estado[*], sino que ha sido de vital aplicación en el sector privado, tal como la automatización de funciones, e incluso en la producción Industrial ; así mismo como en la investigación científica y en el desarrollo de la tecnología Espacial, pues para nuestra generación el uso de la informática se convierte en indispensable aunque no en muchas ocasiones conveniente, pues se empiezan a presentar comportamiento negativos, que desencadenan nuevas formas de criminalidad relacionadas directamente con la informática.

El sorprendente desarrollo de la tecnología informática ha dado nuevas pautas para desarrollar el ingenio del ser humano, que a la vez ha abierto las posibilidades de delinquir de formas impensables a través de una red. La manipulación fraudulenta de los computadores con fines económicos, tales como los mas sencillos , ingresar a un servidor de un plantel educativo con el fin de cambiar notas, hasta la mas complicadas, ingresar a entidades gubernamentales o bancarias con el objeto de borrar, modificar o sacar información , íntimamente ligadas a la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son solo algunos de los movimientos realizados por estos individuos que hasta hoy podemos determinar. Los alcances de esta clase de delitos nos permiten entender que a través de éstos procedimientos se pueden obtener grandes beneficios, que necesariamente pueden afectar a un individuo, a un grupo determinado de éstos o por el contrario a toda una sociedad en general.

Digamos además , que esta clase de delitos, son supremamente complicados de descubrirlos y más aún castigarlos, pues se trata de unos delincuentes "especialistas", con un amplio conocimiento de las tecnologías de la información , que en muchas ocasiones ni siquiera dejan huella ni rastro alguno de su posible autor, lo que nos lleva a pensar que en muchos casos son "crímenes perfectos".
En este sentido, el Tratadista Argentino Marcelo Manson determina que la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos. La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto

[*] En relación a lo anterior, Colombia se constituye como un Pionero en lo que refiere al Gobierno Virtual. Pues gracias a paginas Web, el gobierno nacional ha trato de estructurar el gobierno en línea, en donde los usuarios pueden conocer directamente los procesos de licitación con las entidades Públicas, así mismo hacer sugerencias, acceder a sentencias, a fallos judiciales e incluso interactuar en formas de veedurías Ciudadanas para el control de la corrupción por parte del pueblo. San Juan de Pasto, fue seleccionada como una de las ciudades pioneros en instaurar el gobierno local en línea, para tratar de agilizar todos los procesos propios de una mandato local, con el fin de facilitar los trámites a sus asociados

cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos*. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos."*

Para lo anterior, es a nuestro parecer que es importante estudiar las distintas modalidades delictivas , tal como la destrucción o violación del hardware y sofware , y qué mecanismos existen para poder evitarlos, pues esta guerra no solo es entre programas que ataquen y otros que se defiendan , sino que también es importante conocer los datos empíricos de estas conductas, para legislar y contrarrestar estas nuevas formas de criminalidad, de la par con la Ingeniería de Sistemas y el Derecho .

Igual es acertado el comentario de Mason, al indicar que "*si se tiene en cuenta que los sistemas informáticos, pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, provisionales y de identificación de las personas".* Y si a ello se agrega que existen Bancos de Datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares; se comprenderá que están en juego o podrían ha llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger. Esto nos permite dilucidar que no es la amenaza del computador como tal sobre el individuo, pues aún no se ha llegado a un desarrollo de la I.A[*], sino a la utilización real del hombre de estos instrumentos con fines delictivos .

Nuestra sociedad no está frente al peligro de la tecnología de la informática, sino frente a la posibilidad de que ciertos individuos con conocimientos técnicos específicos, la utilicen con fines delictivos para demostrar cierto poder, pues la humanidad esta orientada a convertir a la información como un símbolo de poder, a expensas de las libertades individuales como el Derecho a la intimidad, que conllevan obviamente al detrimento de las individualidades y de las colectividades de un determinado territorio, pues el peligro de estas amenazas serán directamente proporcionales a los avances tecnológicos venideros.

Para nuestro estudio en particular, abordaremos la protección de los sistemas informáticos desde una perspectiva penal, aunque deben estar complementadas por aspectos comerciales, civiles, sociológicos y psicológicos, los cuales no deben excluirse entre si, sino, todo lo contrario deben estar vinculados para tratar de dar

[*] Se conoce con el nombre de Inteligencia Artificial, al desarrollo de tecnologías que permiten a las computadoras pensar por si mismas y auto programarse para cumplir cualquier función que el medio le imponga. Este desarrollo tecnológico aún se encuentra en etapas experimentales.

una protección global a esta nuevas formas delictivas, puesto que la movilidad de la red, permite fácilmente, cometer un delito informático, utilizando un aparto conectado a Internet en Sud Africa , con un destinatario en los Estados Unidos a miles de kilómetros de distancia. Pues dadas las características de éstas problemáticas, solo a través de una Protección Mundial , desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

2. El DELITO INFORMATICO

Como ya lo hemos mencionado anteriormente , el desarrollo doctrinal del tema, ha sido de bastante amplitud, pues observamos que el concepto de "delito informático" comprende no solamente aquellas conductas que recaen sobre los sistemas computacionales como tal, es decir sobre los programas, equipos, etc, sino también sobre aquellas conductas que utilizando estos medios pueden lesionar un bien jurídico tutelado por la legislación Penal.

Es entonces que dar un concepto sobre delitos informáticos no una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico penales, se requiere que la expresión "delitos informáticos" este consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, no ha sido objeto de tipificación aún; sin embargo, muchos especialistas en derecho informático emplean esta alusión a los efectos de una mejor conceptualización.

Es importante entonces conocer que durante el Primer Congreso Andino de Derecho e Informática celebrado en marzo de 2001, fue presentada la ponencia de la profesora de Derecho Penal de la Universidad del Zulia, doctora Milagros Soto Caldera , acerca del concepto de delito informático, se hizo la siguiente síntesis de las definiciones que existen en la doctrina:
"En primer lugar, se presenta la definición establecida por Sarzana quien 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'" .
Lima dice que el delito electrónico en un sentido amplio “es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel como método, medio o fin.”

Zabale y otros definen los delitos informáticos como “toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, y el cual se distingue de los delitos computacionales o tradicionales informatizados”

Parker define los delitos informáticos como todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha, o habría podido sufrir una pérdida; y cuyo autor ha, o habría podido obtener un beneficio.

El autor mejicano Téllez conceptualiza el delito informático en forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin' y por las segundas 'actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”

Así mismo la legislación Española ha denominado a los delitos informáticos como “todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes”

Tales definiciones son suficientemente ilustrativas, por lo que tan solo agregaríamos que la categoría denominada "delincuencia informática", como tema de estudio doctrinal, es útil para determinar de lege ferenda qué conductas cometidas por medio de sistemas de procesamiento de datos, o en éstos, pueden lesionar bienes jurídicos vinculados a derechos individuales y así proceder a su tipificación; y de lege lata, permite al operador jurídico determinar cuándo se encuentra frente a una conducta antijurídica, por haber lesionado materialmente tales bienes jurídicos o haberlos puesto concretamente en peligro

2.1 CLASIFICACIÓN DE LOS DELITOS

Ha sido diversa la clasificación de los delitos informáticos por parte de la doctrina, sin embargo para nuestro estudio tomaremos la expedida por la Organización de las Naciones Unidas para esta clase de comportamientos, que está catalogada así:

2.1.1 Fraudes cometidos mediante manipulación de computadoras.

2.1.1.1 Manipulación de los datos de entrada. Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

2.1.1.2 La manipulación de programas. 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. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado

Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función norma

2.1.1.3 Manipulación de los datos de salida: Se efectúa fijando un objetivo al funcionamiento del sistema informático. 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. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

2.1.1.4 Fraude efectuado por manipulación informática. *A*provecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra

2.1.2 Falsificaciones informáticas.

2.1.2.1 Como objeto. Cuando se alteran datos de los documentos almacenados en forma computarizada.

2.1.2.2 Como instrumentos. Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos

2.1.3 ***Daños o modificaciones de programas o datos computarizados.***

2.1.3.1 ***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:

- **Virus.** Cronogramas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de ***VIRUS.*** Es una serie de claves programáticas que pueden adherirse a los soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya *Gusanos* Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

- **Bomba lógica o cronológica.** Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

2.1.4 Acceso no autorizado a servicios y sistemas informáticos. Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

2.1.4.1 Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema

2.1.4.2 ***Reproducción no autorizada de programas informáticos de protección legal.*** Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones moderna. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un *delito informático* debido a que el bien jurídico a tutelar es la propiedad intelectual

Por otra parte, es importante determinar las clasificaciones expuestas por la Doctrina, para lo cual, nos parece significativo citar al autor mexicano JULIO TELLEZ VALDEZ , quien define de una manera excepcional lo que a su parecer es el Delito informático , además de brindarnos una clasificación muy precisa de las conductas criminales derivadas de la tecnología de la información. Para éste tratadista los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)".

Según TELLEZ VALDEZ, este tipo de acciones presentan las siguientes características principales:

a) Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.

b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) En su mayoría son imprudenciales y no necesariamente se cometen con intención.

j) Ofrecen facilidades para su comisión a los menores de edad.

k) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

l) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.
Asimismo, este autor clasifica a estos delitos, de acuerdo a dos criterios: [11]

2.2 COMO INSTRUMENTO O MEDIO

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

d) Lectura, sustracción o copiado de información confidencial.
e) Modificación de datos tanto en la entrada como en la salida.

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

h) Uso no autorizado de programas de computo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

[11] TÉLLEZ VALDEZ, J.J. Derecho Informático. México; Editorial McGRaw Hill, 1997, p. 105.

j) Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

l) Acceso a áreas informatizadas en forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

2.3 Como fin u objetivo

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios.

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:

- Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- Espionaje: Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- Terrorismo: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
- Narcotráfico: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- Otros delitos: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

3. ALGUNAS APROXIMACIONES AL SUJETO ACTIVO DEL DELITO

3.1. SUJETO ACTIVO

Las personas involucradas en los delitos informáticos, son aquellas que manifiestan ciertas características que no poseen todos los individuos, pues son conocedores del manejo de sistemas informáticos, en algunos casos están ubicados a nivel laboral en situaciones estratégicas para manejar información de carácter sensible, Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos, “el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada”. Así mismo, otro reciente estudio realizado en América del Norte y Europa indicó que “el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.” Sin embargo; pueden presentarse otros casos en los que no necesariamente se encuentren en actividades laborales que faciliten realizar este tipo de delitos.

El nivel de capacidades del delincuente informático es tema de controversia ya que para algunos doctrinantes el nivel de aptitudes no es indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas con un nivel intelectual alto, con capacidades técnicas especiales y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un individuo especializado en carreras derivadas de la tecnología de la información, tales como sistemas, electrónica o mecatrónica.
Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", se llegó a denominar este tipo de actividad como “delitos de cuello blanco” término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

Asimismo, este criminólogo estadounidense afirma que tanto la definición de los "delitos informáticos como la de los delitos de cuello blanco no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen

ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional". Es decir que se requerían de conocimientos específicos, en este caso conocimientos de informática, y un cierto status socio-económico para actuar; debido a que en aquella época las personas tenían difícil acceso a computadoras, ya sea por sus costos y por la complejidad de su funcionamiento.

Sin embargo en la actualidad ya no sucede lo mismo, pues cualquier persona con suficientes conocimientos de informática puede acceder a los sistemas. De esta manera ya no se los llama como delitos de cuello blanco, sino "Delitos de cuello dorado" por las atribuciones que se le han hecho a este tipo de personas, es decir las características "especiales" que supone la sociedad poseen estos sujetos y además de la relevancia que les ha dado la sociedad en comparación con otros tipos de delincuentes.

Así mismo, comenzó a denominárseles hackers a aquellas personas relacionadas con actividades como violar y dañar programas de sistemas que se suponían impenetrables, comenzando así un nuevo tipo de crimen, un delincuente difícil de identificar.

Sin embargo debido a la falta de información en el denominador común, no se ha elaborado una clara distinción, pues es necesario tener claridad en las consecuencias de acto.

A comienzos de los noventas Internet era aún un tema lejano para la mayoría de personas, pues su acceso era muy restringido, debido a esto; la información confidencial atrajo a los primeros criminales informáticos. En aquella época se los catalogaba como:

Sombrero Negro: calificados como terroristas y mercenarios, usaban sus conocimientos para acceder a bases de datos que luego vendían
Sombrero Gris: este tipo de piratas se dedicaba a demostrar cuanto sabía y cuál era su capacidad para vulnerar sistemas. Su acción nunca fue con la intención de causar daño.

Sombrero Blanco: detectaban errores y fallas en los sistemas de seguridad y advertían como remediar el problema.
A medida que Internet se volvió mas asequible el pirateo se hizo mas fácil y la disposición de programas ya estaba en la red. Por lo tanto la distinción debe hacerse en función de los conocimientos y la manera de actuar, encontrando de esta manera Hackers y Crackers.

3.1.1 .Hacker

La palabra hacker es una expresión ideomática del ingles, cuya traducción literal tiene varios significados, el mas conocido es aquel que se refiere a “una persona contratada para un trabajo rutinario” y que por naturaleza del mismo trabajo es tedioso, entregado y hasta podría decirse maniático.

Este se crea a finales del siglo 19, cuando en EEUU hubo un gran movimiento migratorio, en donde las personas buscaban mejores oportunidades. Los hackers eran personas que bajaban equipajes de las familias que arribaban a San Francisco, New York, etc. Quienes se caracterizaban por ser personas infatigables, ya que trabajaban sin descansar, tratando de no perder ninguna oportunidad para ganar dinero.

Con relación al mundo de la computación , el hacker hace referencia a las personas que se dedican a la investigación y desarrollo de las computación, extendiendo esfuerzos más allá de lo convencional. Los hackers tienen “un saludable sentido de curiosidad... no sueltan ningún sistema que están investigando hasta que los problemas que se le presenten queden resueltos” Es decirse caracterizan por ser personas con mucho interés por el funcionamiento de los sistemas operativos, muy curiosos y que les gusta explorar todas las partes de estos para conocer el funcionamiento de cualquier sistema informático.

“Un hacker es una persona dedicada a su arte, alguien que sigue el conocimiento hacia donde este se dirija, alguien que se apega a la tecnología para explorarla, observarla, analizarla y modificar su funcionamiento, es alguien que no tiene límites para la imaginación y busca información para después compartirla, es alguien al que no le interesa el dinero con lo que hace, solo le importa las bellezas que pueden crear con su cerebro, devorando todo lo que le produzca satisfacción y estimulación mental... Un hacker es aquel que piensa distinto y hace de ese pensamiento una realidad con diversos métodos. Es aquel que le interesa lo nuevo y que quiere aprender a fondo lo que le interesa”

Inicialmente la palabra hacker hacía referencia a las personas aficionadas a las computadoras, programación y tecnología informática. Actualmente se relaciona con un término peyorativo para las personas que se conectan a la red para consultar o alterar programas o datos computarizados, atentan contra la propiedad de seguridad de las redes, autores de virus, intrusos y vándalos del ciberespacio, además de aquellos que disfrutan explorando los sistemas operativos.

Dentro del grupo de conocedores de la materia, los hackers se denominan como personas intelectualmente inquietas, llenas de curiosidad en cuanto a la tecnología de la informática, además; su motivación no se centra por obtener beneficios económico, pues no buscan que sus actos los lleven a obtener mayores

ganancias, sino más bien a obtener una satisfacción intelectual; por lo que no pretenden producir ningún tipo de daño, cuyas actividades se apoyan en un código ético:

El acceso a los ordenadores y a cualquier cosa le pueda enseñar como funciona el mundo, debería ser limitado y total
Toda la información debería ser libre y gratuita
Desconfía de la autoridad. Promueve la descentralización
Los Hackers deberán ser juzgados por sus hack, no por criterios sin sentido como calificaciones académicas, edad, raza o posición social.
Se puede crear arte y belleza en un computador
Los computadores pueden mejorar tu vida
La ética hacker defiende la libertad absoluta de información, libre acceso y distribución.

El código ético original, surge a mediados de los setentas, basado en lo que para ellos era un derecho (libertad de información) y sobre lo que era incorrecto (información restringida). Las ideas éticas de la comunidad hacker pretendían compartir su conocimiento con la gente para beneficiarla, y de esta manera lograr que la información pueda emplearse con mayor utilidad, en vez de dejarla perder en la confidencialidad.

El hacking significa " el pensamiento fuera de la caja para idear soluciones poco convencionales a los problemas", es decir la actividad del hacker estudia a profundidad los sistemas, para conocer cómo trabajan, descubriendo sus debilidades y características para ir más allá de sus límites. Sus principales armas son la creatividad e imaginación, puestas en práctica en el momento del hack.

La información confidencial, representa para los hackers un desafío intelectual, por lo que puede pasar días y noches enteras delante de una computadora; experimentando con diferentes técnicas hasta lograr su objetivo. Por lo tanto, no será posible encontrar una hacker que se desinterese de sus búsquedas, siendo constante, realizando el mejor trabajo para conseguir libertad en la información.

3.1.2 Cracker

El cracker es un término que aparece hacia 1985 dentro de la comunidad de los hackers, debido a la mala utilización del término, diferenciando a los crackers como las personas que rompen la seguridad de un sistema. Estos hacen parte de pequeños grupos organizados que se involucran en el terreno de lo ilegal. Un hacker tiene la habilidad suficiente para convertirse en un cracker, sin embargo la ética del hacker lo mantiene al margen de la legalidad. Cuando pasa los límites legales se convierte en un cracker o un dark side hacker.

Su intención es destruir los datos, impedir el servicio a usuarios legítimos, romper con la seguridad de programas comerciales, destrucción de programas a través de virus, el robo de datos y venta de éstos; con el propósito de sacar provecho en el mercado negro. Puesto que lo que pretende es romper los programas, debe conocer perfectamente buena parte de la programación de Software y Hardware, es decir la parte de programación y la parte física de la electrónica.

Usualmente es una persona que alardea de sus conocimientos sobre computación, que investiga la manera de bloquear protecciones hasta lograr su objetivo. Algunos utilizan programas propios o los que encuentran en la red para vulnerar las claves de acceso a sistemas. Otros usan herramientas hechas por ellos mismos o por otros crackers para identificar los paswords de los computadores, o introducir virus para destruir los datos en las mismas.

A los crackers se los identifican como personas rencorosas y frustradas de alguna empresa, cuya principal motivación es vengarse contra alguna compañía o persona, además de obtener beneficios económicos, pues los programas tienen precios elevados, permitiendo que la copia ilegal de programas de última generación se mantengan en el mercado.

Podemos así identificar las diferencias entre un hacker y un craker. El hacker crea sus propios programas, pues tiene bastos conocimientos en programación y lenguajes de programación, mientras que el cracker se basa en sistemas ya creados que puede obtener a través de la red. Además el cracker pretende romper programas en la red, destrozar la computadora de otra persona, introducir virus, etc, es decir crear problemas, a diferencia de los hackers que su objetivo es el de alertar a las personas de los fallos encontrados en un programa, buscando que se mejoren los problemas en la red.

3.2 PERFIL HACKER

A pesar de la atención que se ha focalizado en países extranjeros en cuanto a la conducta criminal de los hackers, es muy poca la información que se puede conocer de estas personas.

Existen estudios relacionados para encontrar la etiología o causa de la conducta criminal computarizada. Uno de ellos fue el de Skinner y Ream, quienes dirigieron una investigación basada en la teoría del Aprendizaje Social para explicar la etiología del crimen computarizado. Los resultados concluyeron que la asociación diferencial del grupo de pares era el mas fuerte predictor del crimen computarizado. Además que las racionalizaciones tienen una influencia significativa sobre la actividad computarizada en el estudio. Una hipótesis que no

fue apoyada en el estudio, se refería a la certeza del castigo, es decir en la medida en que estos sujetos se perciban como vulnerables a ser atrapados o castigados, la conducta se mantiene; pues no se encontró ninguna correlación significativa en el estudio realizado.

Un estudio de caso, además de otras investigaciones dan soporte a los resultados de Skinner y Freaman. Both Denning y Parker concluyeron que la asociación diferencial y el refuerzo diferencial juegan un papel importante en el crimen computarizado y en los hackers. Parker también concluyó con un estudio de caso de 25 años, en el cual plantea que los hackers son reforzados por sus conductas, más no son castigados. Citando casos en los que se condenó a hackers que habían sido pagados con altas remuneraciones por la industria de seguridad informática y fueron tratados como “estrellas” por los medios de comunicación.

Chantler dirigió una investigación mas profunda. El estudio intentó entender más profundamente el perfil de los hackers. El estudio tenía como objetivos describir el ambiente de los hackers, identificar las características y generar hipótesis de la génesis de los hackers.. El estudio era etnográfico en naturaleza e intentó examinar la cultura de los hackers de manera sistemática.

El estudio concluyó que debido a que había varios atributos podría usarse para categorizar a los hackers. Los atributos eran actividades de los hackers, sus proezas en el hacking, su conocimiento, su motivación y cuánto tiempo ellos habían estado hacking . Chantler usó éstos atributos para llegar a tres categorías; grupo élite, neófitos y perdedores y “lamers”

En el grupo élite exhibieron un nivel muy alto de conocimiento y fue motivado por el deseo de logro, auto descubrimiento, y por la excitación y desafío. Los neófitos mostraron un nivel de conocimiento razonable, pero la mayoría todavía estaba aprendiendo. Ellos eran seguidores y usualmente eran lo que el grupo de la élite habían sido. Los perdedores y “lamers” demostraron poca habilidad intelectual. Ellos estaban motivados por un deseo de ganancia, venganza, robo y espionaje. Chantler concluyó que solo el 30% de la comunidad de los hacker se sentían pertenecientes al grupo elite, 60% en los neófitos y un 10% a los perdedores y “lamers”.

El estudio concluyó además que nadie fuerza a los hackers para que entren al hacking, y que ellos mismos son automotivados y dedicados a estar a la vanguardia de la tecnología de la computadora. En el momento del estudio la comunidad hacker estaba dando inicio a su organización. Chantler concluyó que ninguna teoría real sobre su génesis era posible basado en sus resultados. El estudio también concluyó que aunque los hackers tienen atributos que deben ser aprovechados por las principales industrias de seguridad (ej. automotivación), su falta de límites éticos eran problemáticos. Chantler advirtió que los hackers eran

una amenaza potencial debido a su intenso interés y curiosidad en sistemas y su interés por lo que estos contienen.

Otros estudios sobre se basan sobre la conducta de los hackers. Uno de ellos consistió en el estudio de individuos considerados como cyber-puncks.

Los resultados arrojados, indicaron que se clasificaban como caucásicos, entre 12 y 30 años, de familias de clase media. Considerados como personas solitarias, con habilidades sociales limitadas y un desempeño pobre en el colegio. Estas personas generalmente no tienen orientación profesional, pero sí demuestran aptitudes en computación y otros sistemas electrónicos.

El computador comienza a ser un medio por el cual estos individuos intentan ganar control sobre cierta parte de sus vidas. El hacking es una actividad solitaria, en la cual estos individuos se convierten en los “amos” de sus máquinas. Como factor adicional el Internet y la computadora facilitan que los sujetos mantengan la anonimidad en sus actividades, pues no hay ningún tipo de comunicación cara a cara, permitiendo además que ellos creen sus propios personajes; pudiendo ser esta una oportunidad de ser alguien con poder y prestigio, reflejado en los nicknames de personajes de ciencia ficción y fantasía de la ciencia. Estos individuos no están felices de cómo son por lo tanto la computadora se convierte en su medio de escape.

Llamativamente estos individuos muestran por un lado ser personas solitarias, y por otro la fuerte necesidad de pertenecer a un grupo social grande. La comunidad de los hackers contiene diversos grupos o clubes a los cuales estos individuos pertenecen. La comunidad hacker organiza anualmente convenciones para discutir sus ataques y de los esfuerzos de las entidades legislativas para controlar su actividad. Además existen grupos específicos de hackers para noticias, canales de chat y periódicos.

Los cyber-punks tienden a alardear acerca de lo que son capaces de hacer. Esto puede sen en parte por el deseo de ser admirado por su grupo de hackers.

A pesar de los argumentos comunes de los hackers, la mayoría de ataques tienen una naturaleza malévola, indicando que estos individuos presentan sentimientos de ira y la necesidad de “dar un golpe” a alguien o a algo. Cuando estos individuos no se sienten cómodos con otras personas deciden “dar un golpe” a las computadoras y redes, argumentando que las corporaciones son inmorales y necesitan que alguien les de una lección.

Un estudio realizado por Post, indica que ellos se auto perciben como solitarios, con bajos logros y socialmente “ineptos”. La investigación con hackers afirma que estuvieron motivados por el desafío, la excitación por el éxito, y el deseo de aprender; ésta última íntimamente relacionada con la satisfacción intelectual.

Igualmente, algunos de los participantes en el estudio incluyeron categorías como venganza, sabotaje y el fraude como principales factores de motivación.

Planta además que los hackers tienen un sentido de ““flexibilidad ética”, que desde el momento en que se minimiza el contacto humano por medio de la computadora, el hacking comienza a parecer un juego, donde las consecuencias serias pueden ser fácilmente ignoradas.

Los resultados de la investigación del grupo de cyber-punk demuestran que estos individuos presentan características que son consistentes con los estereotipos que se manejan en los medios de comunicación. Las motivaciones de estos individuos no resultan tan altruistas como la sociedad lo suponía. Los principales factores que motivan sus acciones son la venganza, el poder y la codicia. A pesar de algunas demandas en cuanto una adicción psicológica al hacking, no existe mayor evidencia científica que la apoye.

Además de esto, también se identificaron características de conducta en estos individuos, una de ellas es que tienden a minimizar o interpretan equivocadamente las consecuencias de sus actividades, racionalizando que su conducta está realmente al servicio de la comunidad. Ellos también tienden a deshumanizar y culpar a las víctimas que ellos atacan.

Un estudio más reciente, se encontró que no existían diferencias significativas entre los cinco Factores de Rasgo (Autoreporte de personalidad basado en cinco factores: extraversión, conformidad, escrupulosidad, neuroticismo y abierto a la experiencia) entre individuos que han estado involucrados con conductas delictivas computarizadas y aquellos que nunca han estado involucrados en este tipo de actividades. Esto contradice muchos de los supuestos y mas aún contraria el estereotipo que actualmente se ha sostenido de los delincuentes computarizados.

Los resultados indicaron que los delincuentes computarizados son más explosivos y manipulativos. Siendo estas características comunes de los delincuentes, más no exclusivas de los delincuentes computarizados.

Los resultados tampoco apoyaron la hipótesis que los delincuentes computarizados tenderían a tomar sus decisiones morales basadas más en hedonismo que en moralidad interior o social. Nuevamente contradice investigaciones anteriores y estereotipos que normalmente se manejan en la sociedad. Se plantea que las decisiones morales basadas en el hedonismo serían equivalentes a encontrarse en la fase de moralidad pre convencional de Kholberg, que estudios previamente desarrollados afirman que los delincuentes computarizados tienden a encontrarse globalmente en la fase de moralidad pre convencional.

El cuatela debe tomarse cuando interpretando los resultados como los hallazgos son algo preliminares, el estudio es exploratorio, y dos de los instrumentos usaron es nuevo (CCI y MDKS).

A pesar de las limitaciones de este estudio, es un paso importante en la dirección de desarrollo un entendiendo mejor de delincuentes de la computadora
Skinner y Ream, dirigieron una investigación basada en la teoría del Aprendizaje Social para explicar la etiología del crimen computarizado. Los resultados concluyeron que la asociación diferencial del grupo de pares era el mas fuerte predictor del crimen computarizado. Además que las racionalizaciones tienen una influencia significativa sobre la actividad computarizada en el estudio. Una hipótesis que no fue apoyada en el estudio, se refería a la certeza del castigo, es decir en la medida en que estos sujetos se perciban como vulnerables a ser atrapados o castigados, la conducta se mantiene; pues no se encontró ninguna correlación significativa en el estudio realizado.

Estos estudios no son concluyentes y generalizables a la comunidad hacker, mas bien dan una información útil sobre las características de personas que han estado involucradas con actividades criminales a través de la red; la cual puede servir mas adelante para dar inicio a otras investigaciones que profundicen estos hallazgos.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

En lo que se refiere a delitos informáticos, OLIVER HANCE, considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

a) “Acceso no autorizado: Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, un correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.

b) Actos dañinos o circulación de material dañino: Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre se es clasificado como piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o

destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

c) Interceptación no autorizada: En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él" [12].

Es de advertir que las leyes estadounidense y canadienses , lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que "cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada". Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

a) Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.
b) Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
c) Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
d) No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
e) Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
f) Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En síntesis, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes locales tales como la Intranet así como la conexión de la computadora a Internet, aunque no son los únicos medios. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente en nuestro país, como son el caso de la red de fibra óptica, así mismo como la expansión de negocios de telefonía local hacia la transmisión de datos, como la implantación de nuevos operadores de telefonía celular denominada PCS en contraposición a los sistemas TDMA y GSM, conllevan también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto

[12] HANCE, Oliver. EL Derecho de los negocios en Internet. Madrid; Mac Graw Hill, 1998. p.57.

para los sectores afectados de la infraestructura crítica de un país, como para los legisladores y las autoridades judiciales encargadas de las investigaciones y sanciones de éstos delitos.

4. DAÑOS O MODIFICACIONES DE PROGRAMAS O DATOS COMPUTARIZADOS EN NUESTRO CÓDIGO PENAL (LEY 599 de 2000)

Es importante aclarar, que el bien jurídico afectado en esta clase de delitos es la información , situación que ha sido muy bien expuesta por el profesor FRANCISCO BUENO ARUZ quien 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 (aparatos, programas, datos), en algunos casos, aunque no siempre, podremos considerar, con el profesor ROMEO CASABONA, la aparición de un bien jurídico nuevo: la información sobre la información, como algo que reviste por sí solo un valor (económico o ideal) lo suficientemente interesante como para que la conducta correspondiente sea merecedora de una calificación jurídica y de una sanción atendiendo exclusiva y preferentemente a la importancia de la información sobre la información..."*

Así mismo, el profesor LUIS MIGUEL REYNA ALFARO, quien se desempeñaba como director de la Revista Electrónica de Derecho Penal de Perú, propuso en su ponencia dentro del Primer Congreso Andino de Derecho Informático, que se incorporara la "información" como objeto de tutela, pues afirma REYNA que "*cuando se trataba de conductas cometidas a través de medios informático....., , hoy en día no resulta suficiente poseer la información, para lo cual es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que "la información" deba ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión)"*
Así podemos decir que el interés social digno de tutela penal sería: la información (almacenada, tratada y transmitida a través de sistemas informáticos),

Existen un sinnúmero de conductas que se pueden realizar a través de medios computacionales, puesto que las conductas están ligadas a los avances en los sistemas electrónicos, que originan nuevas modalidades delictuales a la par con los adelantos tecnológicos, *"incluso últimamente los virus informáticos se están convirtiendo en enfermedades terminales para el hardware de un computador,*

pues ahora tales virus se alojan en lugares donde se hace imposible su eliminación". Muchas de éstas conductas, "*están destinadas simplemente a efectuar daños al software o los datos almacenados por una computadora."*
Estas son propiciadas, por personas expertas en el manejo de la computación, pues es aquí donde realmente se pueden medir sus conocimientos en informática, con el único objetivo de penetrar y violar la seguridad existente en una determinada base de datos, para que concomitante a ello, se puedan realizar un sinnúmero de actuaciones que serían de fácil ejecución una ves se haya ingresado al sistema. En este orden de ideas, simplemente se puede obtener una información clasificada, o por el contrario destruir, dañar o modificar los datos que ese alberga en esa computadora.

El sabotaje informático, es decir, "*el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento del sistema se comete de la siguiente manera":*

4.1 VIRUS

Los 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, Estos 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 múltiples maneras. La mas acomodada a nuestra historia reciente establecen que un virus de computadora es un programa encargado de ejecutar órdenes 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[13]. 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 a través de la red por medio de e-mail o simplemente a través de un disckette entre un computador y otro.
Los virus tienen múltiples consecuencias. Van de la simple inserción temporal de una pequeña gráfica o de un mensaje, hasta llegar a destruir información contenida en el computador o alterar las funciones de éste, Últimamente han venido saliendo unos virus llamados "praks", los cuales se pegan a los archivos de

[13] SOLER, José A, El delito informático. Revista protección y seguridad. España; mayo-junio 1996.

MSWord y pasan en cierto modo desapercibidos por los antivirus comunes, que únicamente revisan las filas de los programas ejecutables[14].

4.2 GUSANOS

Los gusanos o Worms, son parecidos a los virus pues buscan infiltrarse en el computador y ejecutar ciertas órdenes, pero se diferencian de éstos en que se propagan o regeneran dado que su destino es específico. Así, el programa o gusano se destruye después de introducir los códigos de instrucciones al ordenador.

4.3 E-MAIL "BOMBS"

El nacimiento de Internet trajo consigo el llamado correo electrónico. Éste fue diseñado para que una persona envíe a otra un mensaje a través de la red. Algunos delincuentes se las han ingeniado para que algunos de esos mensajes causen daño a quien los recibe, de tal manera que se destruyan los datos dentro de un ordenador con el sólo hecho de mirar el mensaje[15]".

Hay varios tipos de bombas para el correo electrónico, algunas van atadas al mensaje como un atachment, el cual puede ser un programa, un virus o cualquier otra cosa que cause daños al computador.

El segundo tipo de e-mail bomb es la que se ejecuta con sólo seleccionar el mensaje. Estas, a diferencia de los anteriores, simplemente paralizan el sistema al algún código inserto en éste. Estas bombas son inofensivas, son una simple broma que para solucionarla no necesita más que teclear ctrl. + Alt+ Supr para reiniciar el equipo.
Las bombas de e-mail son potencialmente peligrosa cuando están encubiertas en un attachment que puede ser un virus o un trojan horse. Otro tipo de carta bomba es la que tiene cmo función estresar el servidor del correo, pues se sobrecarga la fila y el servidor y estos fallan. Usualmente se tiene el efecto mencionado cuando alguien envía más de mil cartas con el mensaje. Esta técnica es útil para quien la comete, ya que nunca se sabe quien envía el mensaje pues la operación hace colapsar al servidor por la sobrecarga de datos y no permite ver el mensaje. Esta conducta es dañosa y siempre malitencionada, en el sentido de que no es común que alguien por broma se tome el trabajo de copias mil veces la

[14]-. VIRASES AND COMPUTER CRIMES. Aurora Computer technologies Inc. Nov. 1996, citado por MARQUES, Carlos. El delito Informático. Bogotá; Editorial Leyer. 2002, p. 279.
[15] Marques, Op. Cit., p. 280.

misma carta y luego se tome la molestia de enviar tal cantidad de bits[16]. Otro tipo de bomba es la mamada blob – mancha o goteo . SE ha sido blobbed, manchado o goteado cuando alguien envía un e-mail 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 de tal usuario. Esta conducta es a menudo intencionada, pero algunas veces es considerada por algunos como un ataque sano pues no daña nada más que el mensaje que se envió .

4.4 CABALLO DE TROYA

Estos son los que van destinados a causar daños a la información contenida en la computadora, de tal manera que su función no es modificar un programa sino destruir filas o información. Buen ejemplo de estos son aquellas dudosas filas *.zip que se encuentran en Internet y que usualmente son bajadas por personas que erróneamente consideraban que los efectos de su aplicación no son dañinos, ya que esperaban descomprimir un archivo y en realidad son programas cuya orden es destinada, por ejemplo, a borrar todas las filas *.bat del computador.[17]

4.5 BOMBA LOGICA O CRONOLOGICA – LOGIC BOMB

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”[18]. A pesar de ser mecanismos de facil ejecucion pues son simples instrucciones al sistema, para su preparación se necesitan de 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 que momento explotará 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 pueden ser:

[16] Ibid., p. 280.
[17] Ibid., P. 280.
[18] SOLER, José. El Delito Informático. España; Revista de Protección y Seguridad Social, Mayo-Junio de 1996. P. 28.

FIJAS. Son aquellas en que se toma como referencia una fecha fija en la que se desencadenará la reacción esperada. Algunos virus tiene este mecanismos[19].
VARIABLES . Estos son 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.[20]
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[21].

4.6 ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO

Tal como lo menciona el Doctor CARLOS PABLO MARQUEZ, "*en principio , el delito de acceso a sistema informático parecía haber sido tipificado en la ley 422, cuando se prohíbe el acceso a sistemas de comunicaciones, pero no es absolutamente típica la conducta que se pretende adecuar, puesto que los elementos no permiten la correcta estructuración de la conducta"*. De acuerdo a nuestro entender, este delito es propiamente el determinado para castigar las "incursiones electrónicas", es definido entonces por la doctrina como "*el comportamiento consistente en la introducción a sistemas de información o computadoras infringiendo medidas de seguridad destinadas a proteger los datos en ellas contenidas"*, lo que en pocas palabras da lugar a comprender que este delito únicamente castiga la intrusión al sistema, no siendo más otro el objeto de éste, es decir, que se obvia lo que podría el intruso informático realizar dentro del sistema, lo que para la fase inicial del crimen, sería la etapa crucial para el acceso a un determinado sistema y su posterior daño o modificación a un programa determinado.

Sin embargo, el Código Penal, tipificó esta conducta de la siguiente manera:
Art. 195- Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad , o se mantenga contra la voluntad de quien tiene derecho a excluirlo incurrirá en multa".
Si bien, la descripción de la conducta plante hacer una introducción a lo que denominaríamos delitos de modificaciones a programas, pues es obvio que para la comisión de éstos últimos, fue necesario realizar el primero. Lastimosamente el Código solo específica la sanción de multa, pues no es más explícito, dejando la norma penal en la deriva de diversas interpretaciones que a la larga no podrán ser

[19] Ibid., P.29.
[20] Ibid., p. 30.
[21] Ibíd., p. 30.

reprochadas, pues realmente no se está observando las verdaderas intenciones que pueda contener el autor. Por tal razón este delito será siempre cometido en virtud de realizar modificaciones a programas a través de Internet, pues lo convertiría en el medio idóneo para tales fines, pues una vez ingresado al sistema, podrá realizarse dichas cambios que afectarían de manera clara los intereses privados o públicos del dueño de la información. No utilizamos la palabra daño, pues este delito no se constituye necesariamente con la introducción a un determinado sistema, es decir no es necesario conocer el acceso o realizar la incursión sin autorización para dañar una determinada información , pues el daño no tiene un orden determinado, a diferencia de la modificación , ya que ésta última trata de cambiar el contenido de la información de una forma consciente , es decir que se sabe lo que se quiere cambiar o modificar, mientras que el daño esta íntimamente ligado al caos, al azar que pueda generar un virus , una logic bom o un troyan horses, pues como se sabe esta clase de ataques informáticos son realizadas con el fin de destruir la información contenida en el sistema, sin discriminar realmente lo que se quiere dañar, o se sabe que existe cierta información , pero para dañarla no importa hacerlo indiscriminadamente con la demás información. Otra diferencia abismal es que la modificación en cierta forma deja la información con sus mismos patrones, intacta, es decir si son base de datos de pagos en una determinada empresa la alteración radicaría que a través de medios fraudulentos, valga la redundancia, se altere esa información, dejando los mismos parámetros por la cual fue construida pero no como realmente se la construyó; en cambio los daños producirían una alteración de esos parámetros, es decir se formaron con base a sistemas que daban soporte a determinada operación, los cuales fueron alterados de forma tal que el daño altera abismalmente el normal desempeño del programa ejecutado.

Es importante aclarar que en esta clase de conductas, no es necesario que el individuo se introduzca “abusivamente”, pues para hacerlo tal y como se define la palabra es abusando del individuo, lo que esta clase de conductas darían lugar no a un abuso sino a un engaño, pues es necesario que para que se configure el abuso debe existir al menos una relación interpersonal entre los dos sujetos, mas sin embargo, estos delitos electrónicos, por su misma esencia y naturaleza es imposible la interacción de dos seres humanos, pues el medio para hacerlo es una computadora Ahora bien, si determinamos que este delito es con base a un engaño, desechamos de plano “el abuso”, pues el modus operandi estará dictaminado por la falsa identificación del usuario que le ha enviado al correo por lo general con avisos llamativos.

Es común en esta materia, que al ingresar al correo electrónico, se pueda observar que le han escrito varias personas que no conoce, pero que son nombres comunes de acuerdo a la zona y lugar del usuario, entonces para los servidores estadounidenses, quienes envía el mencionado correo se hará llamar MARK STUART o SAM SIMON, y para los servidores latinoamericanos serán DIEGO LOPEZ o MAURICIO CARDENAS, que no podrían levantar sospecha frente al

incauto usuario. Sin embargo, estos se encuentran cargados de programas que una vez ingresan al computador podrán dañar la información que éste almacena, pero única y exclusivamente con el "consentimiento pasivo" de quien se verá afectado con la infiltración del virus. Digo entonces, es pasivo, por cuanto, el usuario, que por lo general corresponde a la mayor parte de la población que no posee conocimientos avanzados en sistemas, abre el e-mail desatando de manera similar lo que ocurrió en la mitología Griega, en donde Pandora por mutuo proprio abre la caja desatando todos los males en el universo. Igual sucede con los usuarios de un sistema, pues no tiene el conocimiento ni muchas veces la tecnología necesaria para evitar llevar a su computador y por ende a su sistema a un mal inevitable. Lo que en cierta forma, daría a entender el consentimiento pasivo, como fase final de la conducta criminal, la que no se encontraría en el envío de una bomba lógica o de un troyan horses, pues si el usuario logra eliminarlas nunca podría configure el delito como tal "*el que destruya, modifique o altere"*, pues no pudo la conducta terminarse en virtud de la frustración de la fase final para su consumación, pues éste delito se consuma no solo enviando la información sino que el sujeto pasivo la active, lo cual sería mas lógico pensar en una tipificación de una conducta que sancione exclusivamente el envío de éste tipo de información.

Pero en este sentido el principal problema radicaría en el envío de FOWARDS, es decir la compilación de varios e-mails, que son enviados una y otra vez, convirtiéndose en cadenas de direcciones electrónicas, en virtud de lo anterior nos preguntamos entonces ¿Cómo saber que al enviar un FOWARD no estamos enviando un logic bomb?. Acaso deberá prohibirse el envío de FOWARD por INTERNET? Lastimosamente cada día los sistemas computacionales cambian y las posibilidades de nuevas modalidades de conductas para daños o modificaciones de programas computarizados lo hacen también. Lo importante aquí no sería determinar como lo sabemos, sino realmente que intención se tenía para hacerlo, pues si no existiere ningún motivo fútil para hacerlo estaríamos encaminándonos hacia la atipicidad.

Es importante en esta clase de conductas la comisión dolosa y estructurada de lo que realmente se quiere lograr y los fines que se tienen para su consumación. Es decir, el sujeto activo del delito, debe tener un amplio conocimiento en el área de la informática para determinar los alcances que podría ocasionar la información enviada a otro computador. Sin embargo, en la mayoría de las ocasiones, esta clase de delitos, no tiene un sujeto pasivo determinado para la comisión del ilícito, es decir, si frente a un delito de hurto, el individuo identifica al menos visualmente a la persona, sabe que sexo es, identifica su apariencia, etc. todo lo que se alcance a determinar con una buena observación, que al final otorga la conclusión de que es apta para ser atracada, pues gracias a la visualización determina que ese individuo será un buen "botín". Pero en lo que nos concierne a delitos electrónicos, el sujeto activo no tiene ningún sujeto pasivo determinado, simplemente lanza sus armas de info-delincuencia aleatoriamente a cualquier

cantidad de personas en el mundo, es decir no buscan un lucro determinado, sino más bien un reconocimiento en él circulo social que frecuentan o incluso en el ámbito de toda una sociedad, lo que deja de lado, el juicio de reproche y el disvalor de resultado que se le pueda endilgar, pues para muchas personas los hacker o intrusos cibernéticos no son delincuentes como tales sino mas bien héroes locales[*].

Siguiendo con nuestro análisis normativo, esta supeditado al SABOTAJE previsto en el Articulo ARTICULO. 199. que reza: "*El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de uno (1) a seis (6) años y multa de cinco (5) a veinte (20) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.*
Si como consecuencia de la conducta descrita en el inciso anterior sobreviniere la suspensión o cesación colectiva del trabajo, la pena se aumentará hasta en una tercera parte"

La conducta no puede ser endilgada de igual manera por cuanto se maneja el fin de suspender o paralizar, lo que en muchas ocasiones los hackers buscan mera diversión, reto o reconocimiento.

"El sabotaje se determinó como una conducta que simplemente protegía materialmente los elementos de trabajo necesario para realizar la labor. El nuevo código adoptó una nueva posición doctrinal, según la cual era necesario ampliar el tipo de sabotaje debido a que para ejecutar un sabotaje es necesario incluir también los sistemas informáticos." Situación que fue muy bien tenida para el desarrollo estructural de éste tipo, sin embargo, se observa que éste no está totalmente acorde a las nuevas estructuras informáticas, por cuanto su alcance se encuentra delimitado con el objeto de paralizar una labor. De esta forma el daño, desde cierto aparte del comportamiento, es contra la información. El tipo, como uno de aquellos que pertenecen a los llamados por la legislación francesa de sabotaje informático, está en general*, "dirigido a proteger los elementos que se hacen indispensables para laborar, pero, desde el punto de vista informático, está dirigido a proteger a la información puesto que es un bien privado fundamental para la ejecución de ciertas actividades"* [22] En este orden de ideas, la Doctrina francesa, ha optado por la ampliación del alcance de esta clase de delitos, puesto que lo que importa proteger realmente es la información que pueda tener el

[*] Dentro de la Investigación de campo que realizamos en la Universidad Nacional, logramos establecer por comentarios de varios estudiantes, que el hacker que ocasionó el colapso de la página web de la Universidad de los Andes, pertenecía a la Facultad de Ingeniería Electrónica de la Universidad Nacional, el cual no era reconocido como un delincuente, sino que tenía una amplia y favorable reputación entre sus compañeros, frente a los cuales no era rechazado sino todo lo contrario. Admirado.

[22] MARQUEZ, Op. Cit., p. 162.

usuario, independientemente de quien lo sea. Un problema de discusión podría plantearse, el de decidir hasta que punto la información guardada en un sistema computacional es de tal magnitud para el usuario, que la pérdida de ésta configure una acción típica. Nos preguntamos entonces, ¿la única foto de la abuela gravada en archivos adjuntos, será lo mismo que perder la información de un trabajo en particular?. Entonces se consideraría que esa información subjetivamente podría tener el mismo valor para un sujeto, lo que nos llevaría a concluir para nuestra investigación, que no importa que clase de información se sabotee sino que simplemente se castigue la acción que lleva a un resultado final de destrucción.

Tal como esta descrito el Sabotaje, se ha determinado que éste *"es de los llamados compuestos, debido a que contiene varios verbos rectores descritos. Estos son: destruir, inutilizar, desaparecer y dañar. Destruir alude a deshacer, arruinar o asolar una cosa material o inmaterial*[23]*, inutilizar, significa hacer inútil, vana o nula una cosa y útil es aquello que trae o produce provecho, comodidad, fruto o interés,*[24] *de manera que inutilizar es hacer que una cosa materia o inmaterial no pueda producir algún provecho, fruto o interés, desaparecer, como lo mencionamos, es ocultar, quitar de la vista con presteza una persona o cosa*[25]*, dañar, de nuevo, es causar detrimento, perjuicio, menoscabo, dolor o molestia*[26]
Sin embargo de la interpretación de la norma, no es posible desprender el Sabotaje informático a través de Internet, puesto que en primer lugar se ubica en los delitos "Contra la libertad de trabajo y asociación" además que se busca como objetivo la paralización de las labores, sin embargo, el tipo no diferencia como podría dañarse la base de datos, es decir, deja ampliamente abierta las posibilidades interpretativas para la ejecución de tales fines, sin embargo, debería una nueva disposición proteger toda clase de sistemas informáticos no con el objeto de proteger el normal desenvolvimiento de las actividades laborales sino de proteger el patrimonio inmaterial individual alojado en un sistema de computación. La doctrina corroborando lo anterior nos indica que "*El sabotaje informático también puede ocurrir de manera remota. Existe una gran cantidad de modus operandi adecuados para el desarrollo de estas conductas que van destinadas al saboteo de sistemas informáticos. Tales pueden ser los caballos de troya o las bombas de tiempo, los cuales son programas informáticos que se activan al interior del sistema informático haciendo que impida el procesamiento o se destruya la información impidiendo el desarrollo común de la actividad*[27]*"*

Esto nos lleva a concluir que en cuanto a la tipificación de sabotaje informático en relación a la "*inutilización, daño, destrucción y ocultamiento de información o*

[23] Ibid., p. 163.
[24] Ibid., P. 163.
[25] Ibid., P. 164.
[26] Ibíd., p. 165
[27] Ibid., p. 164.

sistemas informáticos" no es clara en nuestra legislación , lo que nos hace invocar urgentemente una penalización efectiva y concisa de esta clase de conductas.
Ahora bien, dentro del estudio realizado al código penal vigente, encontramos otra figura que podría vincularse al objeto de nuestra investigación , o que nos podría brindar nuevas pautas para tratar de "crear" una normatividad que proteja toda clase de información en un ordenador para evitar su daño, destrucción o modificación.

Podría pensarse entonces, que la destrucción en bien ajeno, encajaría en lo referente a la destrucción , daño o modificación de programas a través de Internet, pero que a la larga, tampoco estarían acordes para tipificar éstas conductas. El código Penal ha determinado en su artículo 265 el Daño a bien ajeno, de la siguiente manera:

"ARTICULO. 265.—Daño en bien ajeno. El que destruya, inutilice, haga desaparecer o de cualquier otro modo dañe bien ajeno, mueble o inmueble incurrirá en prisión de uno (1) a cinco (5) años y multa de cinco (5) a veinticinco (25) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.
La pena será de uno (1) a dos (2) años de prisión y multa hasta de diez (10) salarios mínimos legales mensuales vigentes, cuando el monto del daño no exceda de diez (10) salarios mínimos legales mensuales vigentes.
Si se resarciere el daño ocasionado al ofendido o perjudicado antes de proferirse sentencia de primera o única instancia, habrá lugar al proferimiento de resolución inhibitoria, preclusión de la investigación o cesación de procedimiento."

Se determina entonces, que en esta clase de delitos, el objeto jurídico es el patrimonio, mientras que el objeto material son los bines corporales sean estos muebles o inmuebles. Sin embargo en materia informática , el nuevo tipo omitió las consideraciones de los bienes informáticos, de manera que el objeto materia de estas conductas sea simplemente los bienes corporales, es decir, los bienes muebles e inmuebles. *Así, dentro de estos bienes podemos clasificar, desde la informática a aquellos que son parte de los procesos de soporte, recuperación y transmisión de información, pero no podemos incluir en ellos la información en si misma , ya que la doctrina, nos indica, que la información no puede ser objeto material del delito de daño, de la misma manera que no puede ser objeto del delito de hurto.* Se ha determinado que en materia penal, la noción de cosa mueble es mucho más amplia que en materia civil. Aparte de las consideradas como muebles por la doctrina tales como las losas del pavimento, también deben considerarse como cosas muebles en materia penal todas las demás que sean susceptibles de transportarse de un lugar a otro bien sea por no estar adheridas al suelo o porque pueden separase de el , como las plantas, los cuadros embutidos en la pared y muchas otras consideradas por la ley civil como inmuebles. De igual manera expresa el tratadista VICENTE ARENAS, *"igual deben considerase muebles otras cosas que tienen existencia material y que, aunque no son*

tangibles, pueden sustraerse con ánimo de aprovechamiento ilícito, como ocurre con el gas, el vapor, la energía electrica, etc. En términos generales son objeto material del delito de hurto todas las cosas corporales que puedan transportarse, aunque civilmente sean muebles[28]. Sin embargo, el ilustre penalista, hace la aclaración y a manera de conclusión, "*las cosas incorporales no pueden ser objeto de hurto porque no pueden sustraerse*[29]"

De esta manera el delito de hurto, se requiere necesariamente la materialidad de la información, es decir podría una vez materializada ser susceptible de hurto, sin embargo en lo que respecta al daño en bien ajeno, la doctrina ha considerado que la "*información no es un bien corporal y por tanto no es objeto material del delito." De esta manera, se hace sumamente difícil tratar de subsumir una conducta de ésta categoría en los articulados de nuestro código penal, pues no es posible clasificar la información de ser un bien incorpóreo a uno corpóreo para que encaje en la exigencia que como tal le haría la norma . Es por eso, que en nuestra norma penal* "sólo pueden ser objeto de tales delitos los elementos para el procesamiento informático, como el hardware de las computadoras, los sistemas magnéticos, ótpicos, etc, donde se almacena información y demás parnafernalia dedicada a la informática. Precisamente el comportamiento, en cuanto a la información se hace atípico. Esto es, que no existe norma que condene el daño de información.[30]

Surge entonces, un vacío en nuestra normatividad penal, pues no existe ninguna norma que trate sobre la destrucción de la información , lo cual hace importante nuestra investigación, pues gracias al análisis antes realizado podríamos proponer una nueva solución legislativa que planté soluciones a estos nuevos delitos informáticos cometidos a través de sistemas computacionales, lo cual da lugar a la atipicidad de las conductas, pues éstas no se encuentran catalogadas como delitos.

De acuerdo a estos nuevas modalidades delictuales, surgen nuevos planteamientos que nos llevan a dilucidar algunas nuevas formas de criminalización , sin embargo, se trata de observar hasta que punto , si se considera que la norma tomara como objeto la información , ciertas conductas estarían acordes a un ordenamiento jurídico o no?.

Carlos Marques, nos ilustra sobre los nuevos conflictos que pueden ser suscitados en razón del uso de sistemas computacionales , causando daños suponiendo que existiera en nuestra legislación una norma que tome a la información como objeto, es decir que pueda ser susceptible de ser dañada y que por ende esta conducta pueda ser castigada. Nos refiere el autor que en relación a los nuevos problemas

---

[28] ARENAS, Vicente. Compendio de Derecho Penal. 3ª Ed.. Bogotá; Editorial Temis, 1982. p. 277.
[29] Ibid. P.277.
[30] MARQUEZ, Op. Cit., p. 203.

tecnológicos planteados existen debates dentro de la academia en relación a ciertos comportamientos de los programadores de software. Pues estos, se caracterizarían por tener la capacidad para producir ciertos programas que pueden ser utilizados en un computador personal para uso tanto personal como laboral, sin embargo es fácil entender que los programas que se adquieren no son propiedad del usuario, es decir, en ningún momento el autor o programador esta transmitiendo el dominio sobre esta clase de bienes, pues lo que interesante del mundo de las computadoras, es que no se compra el bien en si, sino la licencia o autorización por parte del autor para utilizarlos.

De esta forma, es muy fácil encontrar un sinnúmero de programas en Internet, que han sido extraidos en contra de los intereses del autor, es decir , se encuentran en el ciberespacio esperando a ser bajados por cualquier cibernauta y utilizarlo sin el permiso de su creador. En virtud de estas circunstancias, muchos programadores en "*en aras de proteger sus creaciones, inventaron unos subprogramas llamados virus informáticos*[31]*".* Los cuales son tomados como medidas preventivas para evitar el uso ilegal de éstos, puesto que son presentados a los usuarios, quienes pueden ingresar u obtenerlos libremente, para simplemente mirar su aplicación y servicios a través de un DEMO, sin embargo, estos en estos se obliga o se exhorta al usuario para que se contacte con el proveedor de estos programas par obtener una licencia de funcionamiento, advirtiendo que de no hacerlo, el archivo tiene contenido una instrucción codificada que daría lugar a su autodestrucción. En este orden de ideas, no podría considerarse como delito dicha actitud, pues actúa en lo que se conoce como una "*legítima defensa privilegiada u offendiculae*[32]*",* que únicamente destruiría el software que se utilizaba sin licencia, que a la postre aún no era usado por el dueño del computador, por tanto quien lo destruye es el autor del mismo, que nos lleva a pensar, que no podría existir ninguna conducta por cuando esta actividad estaba revestida de antijuridicidad. Pero podría suceder una situación contraria, en donde el virus insertado en el Software estaba no destinado a dañar el programa utilizado sin licencia sino a toda la información de un sistema en general buscando su destrucción , daño o modificación. Las consideraciones que hace el autor son de otro talante. Él cree *"que se ha de mirar el tipo de virus, para así establecer cuál fue el resultado de la defensa y juzgar si en si el virus es de aquellos que van destinados a destruir toda la información del sistema informático, o a impedir el correcto funcionamiento del mismo, es claro que hay exceso en la defensa y, por tanto, se incurre en delito de daño. Si el virus simplemente va destinado a impedir el funcionamiento del sistema informático cuando se activa el programa mencionado, considera el autor que hay legítima defensa privilegiada*[33]*".*

[31] Ibid., P. 204.
[32] Ibid., P. 204.
[33] Ibid., P. 204.

De lo anterior, podríamos sacar una importante discusión, en la cual se trate de determinar que a la hora de realizar el daño a través de un sistema computalizado, y se dañe un programa determinado, en este caso, se dañe programas o software pertenencientes a una compañía de programación. Realmente a quien se estaría perjudicando? ¿Al dueño del programa, o a quien adquirió los derechos para utilizarlo? Y que tal si se daña unos archivos de suma importancia para el propietario del computador, que se encontraban inmersos en un software no autorizado por licencia? Será entonces que ante la ilicitud de la piratería no se configuraría el delito de daño?, puesto que muy fácil sería determinar el viejo adagio popular "ladrón que roba a ladrón..." que dados los avances tecnológicos sería "pirata informático que destruye a pirata informático".... ¿acaso por la ilicitud del primero, debe ser impune la ilicitud del segundo?.

Lo interesante para concluir, sería que una tipificación acorde con el delito de daños a programas , no estaría supeditada a determinar de quien es el programa, sino la afectación de toda clase de información que en un sistema computacional se encuentren, discriminando la autoría, es decir, lo que se busca es castigar la intromisión y posterior daño a la información contenida en un sistema computacional de manera general, pues el simple hecho de incursionar en un sistema en contra de la voluntad de su titular, es materia de reprochabilidad en una sociedad de Estado Social de Derecho como la nuestra.

De igual manera, nos podríamos encontrar, con modalidades delictivas cometidas a través de un computador, que no necesariamente afecte a la información , sino que constituye un daño directamente en los bienes materiales del computador. Tal como lo expresa en *su libro,* el autor nos indica que *"existen muchos tipos de virus, pero los avances en "seguridad" informática han llevado a que estos virus estropeen el funcionamiento de una computadora de por vida. Estos virus, indican a quien los detecta, que se alojan en la memoria RAM[*] de computador y se activan con el BOOT, y al formatearse el disco duro no desaparecen ya que su lugar verdadero de almacenamiento es la memoria ROM[*], la cual alimenta en la iniciación a la memoria RAM del computador, infectándose de nuevo el sistema al hacer el boot. Esta memoria ROM o ROS es industrialmente preestablecida y, por su importancia para el funcionamiento del sistema, no puede ser manipulada haciendo que el computador pierda su utilidad.[34]"*. Y una vez más aumentamos a nuestra conclusión , que no solo el daño debe estar supeditado a los programas, sino que mediante los virus u otras clases de incursiones pueden dañar físicamente la estructura del ordenador.

---

[*] Random access memory, es la que el usuario pueda usar libremente, es volátil, se puede cambiar la disposición de las cosas y la información que contiene.

[*] Random access memory, es la que el usuario pueda usar libremente, es volátil, se puede cambiar la disposición de las cosas y la información que contiene

[34] MARQUEZ, Op. Cit., p.162

Esta clase de comportamientos, tendientes a dañar, modificar programas a través de Internet, sería catalogado como delito "*mediante sistema informático"*, que necesariamente su modus operandi es compuesto por *"tecnologías informáticas*", por lo cual se hace relevante , "*que en la comisión del delito han de intervenir como medio las tecnologías utilizadas para el procesamiento de información."*
Es así, como esta clase de delitos podrán cometerse exclusivamente con el uso de medios informáticos, "*los cuales son todos aquellos métodos de transmisión, almacenamiento, recolección y recuperación de datos que tienen como receptor un sujeto capaz de conocer"* , ya sea de forma presente o remota (vía Internet), protegiendo la información y el objeto físico del ordenador .

Situación muy particular , es la Descrita en el Libro II, Parte Especial , Título Unico, de la Ley 734 de 2002, Código Disciplinario Unico, artículo 48 de las Faltas Gravísimas, Numeral 43 que reza "*Causar daño a los equipos estatales de informática, alterar, falsificar , introducir, borrar , ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos o en los que se almacene o guarde la misma, o permitir el acceso a ella a personas no autorizadas"*, pues bien, esta norma esta descrita de una manera sumamente clara en donde podría subsumirse la actuación de un intruso informático, específicamente un craker, puesto que busca la sanción ante el daño, modificación o alteración de la información de cualquiera de los sistemas de información oficial, lo cual nos permite identificar la administración como sujeto pasivo de la falta, específicamente la información, sin distinguir que clase, sino simplemente ingresar a una base de datos con el fin de introducir, alterar o dañar la información; verbos éstos, que nos abarcarían todas las modalidades delictivas antes estudiadas.

De igual manera y en el mismo enunciado se prohíbe el acceso abusivo a un sistema, es decir integrando las dos modalidades delictuales, con diferentes sujetos activos como lo son los hackers y los crakers.
Decimos entonces que es una situación muy peculiar, puesto que el mencionado estatuto, es el Código Disciplinario Unico, en donde se concede al Estado la Potestad Disciplinaria, haciéndola independiente de cualquier otra que pueda surgir de la comisión de la falta, para la cual única y exclusivamente serán sujetos disciplinables todos los servidores públicos, aunque se encuentre retirados del servicio y los particulares contenidos en el artículo 53 del Código[*]
Sin embargo es rescatable de la descripción de la falta, como un ejemplo en nuestra legislación para traspasar las fronteras del derecho disciplinario, profiriendo una norma penal para la eventual protección de los usuarios de la computación.

[*] Son sujetos disciplinables los particulares que cuplan labores de interventoría en los contratos estatales, que ejerzan funciones públicas, en lo que tiene que ver con estas; presten servicios públicos a cargo del Estado, de los contemplados en el artículo 366 de la Constitución política, administren recursos de este, salvo las empresas de economía mixta que se rijan por el régimen privado

5. DERECHO COMPARADO

En este orden de ideas se analizará legislaciones de varios paises referentes a los daños o modificaciones de programas, con el fin de tomar como punto de partida varias propuestas realizadas en estos lugares, para adoptar una legislación propia que castigue esta clase de actividades.

5.1 SITUACION EN ARGENTINA

En la Argentina, aún no existe legislación especifica sobre los llamados *delitos informáticos*. Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la Ley 11.723 de propiedad intelectual gracias al Decreto Nº 165/94 del 8 de febrero de 1994.

En dicho Decreto se definen:
Obras de software: Las producciones que se ajusten a las siguientes definiciones:
1. Los diseños, tanto generales como detallados, del flujo lógico de los datos en un sistema de computación.
2. Los programas de computadoras, tanto en versión "fuente", principalmente destinada al lector humano, como en su versión "objeto", principalmente destinada a ser ejecutada por la computadora.
3. La documentación técnica, con fines tales como explicación, soporte o entrenamiento, para el desarrollo, uso o mantenimiento de software.
De esta manera, la situación legal ante daños infligidos a la información es problemática:

El artículo 1072 del Código Civil argentino declara "el acto ilícito ejecutado a sabiendas y con intención de dañar la persona o los derechos del otro se llama, en este Código, delito", obligando a reparar los daños causados por tales delitos.
En caso de probarse la existencia de delito de daño por destrucción de la cosa ajena, "la indemnización consistirá en el pago de la cosa destruida; si la destrucción de la cosa fuera parcial, la indemnización consistirá en el pago de la diferencia de su valor y el valor primitivo" (Art. 1094).

Existe la posibilidad de reclamar indemnización cuando el hecho no pudiera ser considerado delictivo, en los casos en que "alguien por su culpa o negligencia ocasiona un daño a otro" (Art. 1109).

Pero "el hecho que no cause daño a la persona que lo sufre, sino por una falta imputable a ella, no impone responsabilidad alguna" (Art. 1111).

En todos los casos, el resarcimiento de daños consistirá en la reposición de las cosas a su estado anterior, excepto si fuera imposible, en cuyo caso la indemnización se fijará en dinero" (Art. 1083).

El mayor inconveniente es que no hay forma de determinar fehacientemente cuál era el estado anterior de los datos, puesto que la información en estado digital es fácilmente adulterable. Por otro lado, aunque fuera posible determinar el estado anterior, sería difícil determinar el valor que dicha información tenía, pues es sabido que el valor de la información es subjetivo, es decir, que depende de cada uno y del contexto.

Lo importante en este tema es determinar que por más que se aplique la sanción del artículo 72 de la ley 11723, la misma resulta insuficiente a efectos de proteger los programas de computación, los sistemas o la información en ellos contenidos de ciertas conductas delictivas tales como: el ingreso no autorizado, la violación de secretos, el espionaje, el uso indebido, el sabotaje, etc.

No obstante, existen en el Congreso Nacional diversos proyectos de ley que contemplan esta temática; aunque sólo dos de ellos cuentan actualmente con estado parlamentario. Los presentados por los Senadores nacionales Eduardo Bauza y Antonio Berhongaray, respectivamente.

5.1.1 Proyecto de Ley Penal y de Protección de la Informática (Senador Eduardo Bauza). El Senador Eduardo Bauza, señala en el artículo 24 de su proyecto, que "*la alteración, daño o destrucción de datos en una computadora, base de datos o sistema de redes, se realiza exclusivamente mediante el uso de virus u otros programas destinados a tal modalidad delictiva, y aunque existen otros medios de comisión del delito, estos no fueron incorporados al tipo legal por el legislador."*

En materia de Sabotaje y daños, este Proyecto, en el artículo 23, prevé prisión de uno a tres años para aquél que en forma maliciosa, destruya o inutilice una computadora o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Se agrava la pena en caso de afectarse los datos contenidos en la computadora o en el sistema de redes. Se resalta que el tipo legal propuesto requiere malicia en el actuar. El artículo 24 también incluye malicia (en el actuar) para alterar, dañar o destruir los datos contenidos en una computadora, base de datos, o sistemas de redes, con o si salida externa. El medio utilizado, según la propuesta, es mediante el uso de virus u otros programas destinados a tal modalidad delictiva.

5.1.2.Proyecto de Ley Régimen Penal del Uso Indebido de la Computación (Senador Antonio Berhongaray). Este Proyecto de Ley, es abarcativo de muchas conductas delictivas, agravando especialmente la pena, cuando la destrucción fuera cometida contra datos pertenecientes a organismos de defensa

nacional, seguridad interior o Inteligencia. (Art. 3º inc.2), contemplando específicamente el espionaje.

El Proyecto del Senador Berhongaray, en su artículo 2, requiere el acceso a una computadora o sistema de computación, o almacenamiento de datos que no le pertenezcan directamente o a través de otra computadora, sin autorización del propietario o de un tercero facultado para otorgarla o si estando autorizado, excediere los límites de la misma. Basta para que se configure el tipo legal el ingreso sin autorización o teniéndola, que se exceda del marco de la misma.

En materia de Sabotajes y daños, BERHONGARAY, introduce agravamiento cuando se afecte a organismos de la defensa nacional, seguridad interior e Inteligencia, coinciden en aplicar penas de prisión para este tipo de delitos.

En el artículo 5, pena a quien a través del acceso no autorizado, o de cualquier otro modo, voluntariamente y por cualquier medio, destruyere, alterare en cualquier forma, hiciere inutilizables o inaccesibles o produjera o diera lugar a la pérdida de datos informáticos. Aclara qué se entiende por acción voluntaria, expresando que es aquello que hubiera consistido en la introducción de programas de computación aptos para destruir, alterar, hacer inutilizables o inaccesibles datos, de cuya acción proviniera el daño, ya fuera por computadora o sistema de computación en lo que se hallaban los datos dañados, o en cualquier otro.

El artículo 6, pena la destrucción o inutilización intencional de los equipos de computación donde se encontraban los datos afectados. Agravando la pena, cuando la destrucción, alteración o pérdida de datos trajera aparejadas pérdidas económicas; o cuando fuera cometida contra datos pertenecientes a organismos de defensa nacional, seguridad interior o inteligencia.

Referente a usos indebidos, en el artículo 11, se propone como tipo legal el acceso no autorizado y el uso indebido, incorporando un móvil que es la ventaja económica.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España y Chile.

5.2 SITUACION EN ESTADOS UNIDOS

Este país adoptó en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que

no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. Definiendo dos niveles para el tratamiento de quienes crean virus:
Para los que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa.
Para los que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

La nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

5.3 SITUACION EN ALEMANIA

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:
Espionaje de datos.
Estafa informática.
Alteración de datos
Sabotaje informático.

De igual manera el artículo 303 a del StGB (Código Penal Alemán) establece que "1. Quien ilícitamente cancelare, ocultare, inutilizare o alterare datos de los previstos en el 202 a, par.2° será castigado con pena privativa de libertad de hasta dos años o con pena de multa".

5.4 SITUACION EN AUSTRIA

El art. 126 a del Código Penal de Austria (östStGB) dispone que "1. Quien perjudicare a otro a través de la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que

carezca en todo o en parte, de disponibilidad, será castigado con pena privativa de libertad de hasta seis meses o con pena de multa de hasta 360 días-multa".

Con la ley N°88-19 del 5 de enero de 1988 Francia incluyó en su Código Penal varios delitos informáticos. Entre ellos, destacamos la figura del art. 462-4 referida a la destrucción de datos que, establecía que "Quien, intencionalmente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una de los dos penas". Con la reforma penal de 1992, este artículo quedó ubicado en el art. 323-1 del Nouveau Code Pénal, con la siguiente modificación: Se penaliza a quien al acceder a un ordenador de manera fraudulenta, suprima o modifique los datos allí almacenados.

5.5 SITUACION EN ITALIA

El artículo 392 del Código Penal italiano incluye la alteración, modificación o destrucción total o parcial de programas de computación y el daño a la operación de un sistema telemático o informático. El artículo 420 del Código Penal, referido a atentados contra sistemas de instalaciones públicas, ha sido también modificado. Actualmente cualquiera que realice un acto con la intención de dañar o destruir sistemas informáticos o telemáticos de instalaciones públicas o sus datos, información o programas puede ser castigado con prisión de uno a cuatro años. En casos de consumación del delito (destrucción o daño a los datos) la pena se eleva de tres a ocho años.

5.6 ITUACION EN GRAN BRETAÑA

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas.

Esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría.
El liberar un virus tiene penas desde un mes a cinco años, dependiendo del daño que causen.

5.7 SITUACION EN HOLANDA

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.
La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.
Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

5.8 SITUACION EN FRANCIA

En enero de 1988, este país dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 462-4 también incluye en su tipo penal una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que éste contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje). Por último, esta ley en su artículo 462-2, sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

5.9 SITUACION EN ESPAÑA

En el Nuevo Código Penal de España, el art. 263 establece que el que causare daños en propiedad ajena. En tanto, el artículo 264-2) establece que se aplicará la

pena de prisión de uno a tres años y multa... a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El nuevo Código Penal de España sanciona en forma detallada esta categoría delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intensión dolosa y cuando el hecho es cometido por parte funcionarios públicos se penaliza con inhabilitación.

5.10 SITUACION EN CHILE

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio a cinco años de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.

Esta ley prevé en el Art. 1º, el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el Art. 3º tipifica la conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

5.11 SITUACION EN COSTA RICA

Se realizó una ley con el objeto de reprimir y sancionar los delitos informáticos adicionándose al Código Penal, Ley Nº 4573, del 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, cuyos textos dirán: "Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos. Artículo 217 bis.-Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un

tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema. Artículo 229 bis.-Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

6. CONCLUSIONES

Es importante recalcar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, o incluso proferir legislaciones unificadas , que permitan "*fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática*", puesto que esta clase de delitos podrá cometerse a través del sistema de internet a miles de kilómetros del destinatario final.

Así mismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar.

De esta manera, una vez estudiado el contexto sistemático de éstas modalidades delictivas y de acuerdo a nuestro ordenamiento jurídico vigente, será de muy importante ayuda esta investigación en un futuro, puesto que se trata de reunir los conceptos más relevantes de estas nuevas conductas punibles en aras del entendimiento y futura suscripción en nuestro país, de este modo, deberá tratarse de tipificar una nueva ley que castigue los delitos informáticos como tal, pues como ya lo vimos anteriormente, respecto a las conductas de daños o modificaciones a programas, estarían actualmente subsumidas en el umbral de la atipicidad, siendo Colombia un paraíso terrenal para todos aquellos que se dediquen a las intromisiones electrónicas de acuerdo a su modalidad hacker o cracker .

Entonces la finalidad de esta investigación , pretende brindar soluciones que permitan incorporar al ordenamiento jurídico vigente, nuevas figuras delictivas que dado nuestro atraso desarrollo legislativo en cuanto a las tecnologías de la información aun no han sido expedidas.
Pues este esquema ha sido practicado en países como Estados Unidos, en donde se tiene una alta conciencia de que la "*carrera tecnológica posibilita nuevas formas de cometer conductas verdaderamente disvaliosas y merecedores de un reproche penal."*

Es de advertir, que este anteproyecto de ley, no es general y omisapiente de todas las modalidades delictivas que pueden suscitarse a través de Internet. Es difícil y muy dispendioso el estudio y clasificación de todas éstas actividades , pues para

nuestra investigación hubiera sido lo ideal, pero ante la falta de tiempo, solo hemos hecho relación en nuestro análisis a lo atinente a los daños o modificaciones de programas computarizados.

Desde el primer momento, se decidió privilegiar la claridad expositiva, el equilibrio legislativo y apego al principio de legalidad evitando caer en una legislación errática que terminara meramente en un recogimiento de la casuística local o internacional.

Para lo anterior, se evito tratar de encasillarnos directamente en tomar figuras del derecho internacional y aplicarlas en nuestra legislación, pues fue necesario conocer a fondo la teoría de la información como bien jurídico a proteger, así como el sujeto activo y pasivo del delito , además de conocer mucho más los modus operandi de las actuaciones previamente estudiadas.

En este sentido, se busco plantear hipótesis jurídicas en relación a principios claros de hermeneutica, dando claridad a las definiciones con el fin de evitar vacíos e interpretaciones erróneas al momento de aplicar una determinada ley , tal y como sucede a diario en nuestro jurídico transcurrir.

Esta hipótesis se basa en el principio de la mínima intervención en materia penal, "*buscando incriminar únicamente las conductas que representen un disvalor de tal entidad que ameriten movilizar el aparato represivo del Estado"*.

Pues bien , como lo hemos expresado anteriormente , nuestro punto esencial en la presente investigación tiene que ver con los Daños o modificaciones a programas a través de internet, es decir se debe abarcar al sujeto activo del delito como un sujeto remoto, pues en la mayoría de los casos se encuentra a varios kilómetros de distancia de la información objeto del daño, alteración o modificación.

Se tiene en cuenta entonces a los sistemas y datos informáticos como objeto de delito de daño así:

El que destruya, dañe, modifique, o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de..... Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice los datos o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

Entendiendo por tecnología de la información:
a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.
b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

De esta manera se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Así mismo, la incriminación de realizar “cualquier acto que altere” , tiende a proteger a los usuarios contra los virus informáticos, caballos de troya, gusanos, cancer routines, bombas lógicas y otras amenazas similares.
c Información: significado que el ser humano le asigna a los datos utilizando las convenciones conocidas y generalmente aceptadas.
A pesar que el Código penal prevé el daño en bien ajeno, será menester la incursión de esta figura, con el fin de dejar clara y expresamente tipificado aquellas conducta que pretendan destruir bienes inmateriales que a la luz de nuestra legislación no podrían ser considerados como susceptibles de ser dañados.

De esta manera, pretenderíamos introducir agravantes en relación a los sistemas susceptibles de ser dañados, tales como el realizado a un sistema o dato informático concerniente a la seguridad, defensa nacional, salud publica o la prestación de servicios públicos esenciales y en general, pues la trascendencia pública, como uno de los presupuestos básicos de las obligaciones del Estado hacen prever al manejo de esta información como esencial en el desenvolvimiento normal del aparato estatal.

De igual manera se trataría como un agravante el daño o modificación que se pueda realizar a instituciones educativas, culturales y científicas en aras de proteger la información que éstas puedan poseer constituyéndose en los pilares de una sociedad.

Así mismo, se constituiría en un agravante el daño o modificación que se realice a las demás entidades de la administración pública, como a todos los establecimientos regulados por el derecho privado, en los cuales pueden manejar importante información dentro de sus sistemas informáticos.

Igualmente, podría agravarse la conducta si como resultado de la acción criminal perpetuada por el craker, se produzca una lesión, grave o gravísima, o la muerte de alguna persona, que pudiere ocurrir con motivo de un daño a un sistema o dato informático, elevándose la pena en función de la elevada jerarquía jurídica que reviste la integridad física de los seres humanos.
De igual manera, será menester castigar , a aquellos individuos que se encarguen de facilitar los equipos , programen o distribuyan programas atinentes a cumplir lo fines anteriores, de acuerdo a lo siguiente:

Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, incurrirá en prisión de .....
Lo cual nos permite abarcar las dos modalidades principales de delincuentes informáticos los crackers y los hackers.

Así entonces, estaríamos siguiendo los lineamientos de las legislaciones externas, sin sobrepasarnos los limites impuestos por nuestra propia legislación, de manera que dejamos un espacio en el cual podrá llenarse el vacio existente, dando nuevas pautas para el desarrollo de una legislación acorde a los nuevos lineamientos vigentes de la informática.

7. BIBLIOGRAFÍA

ARENAS, Vicente. Compendio de Derecho Penal. 3ª Ed. Bogotá; Editorial Temis,1982. 522 p.

BARRIUSO RUIZ, Carlos. Interacción del Derecho y la Informática. España; Editorial Dykinson, 1.996. 254 p.

CASTRO OSPINA, Sandra Jeannette. XXIII Jornadas Internacionales de Derecho Penal. Bogotá; Universidad Externado de Colombia, 2002.

DAVARA, Miguel Ángel. Derecho Informático. España; Editorial Aranzadi, 1.993. 215 p.

EL ALBA DE LA CIVILIZACIÓN. Historia Universal. Tomo I. Bogotá; Circulo de Lectores, 1984. 384 p.

EL MUNDO DE LA COMPUTACION. Tomo I. España; Grupo Editorial Océano, 1991. 84 p.

HUERTA, Marcelo y LIBANO Claudio. Delitos informáticos. Chile; Editorial Jurídica ConoSur, 1.996. 198 p.

INFORMATICA Y DERECHO. Revista Iberoamericana de Derecho Informático Varios. España; Publicaciones de la UNED - Centro Regional de Extremadura, 1.992. 120 p.

MARQUES CARDONA, Pablo. El delito informático. Bogotá; Editorial Leyer, 2002. 545 p.

NUEVO CÓDIGO PENAL COLOMBIANO. Ley 599 de 2000.

PEREZ LUÑO, Antonio Enrique. Manual de Informática y Derecho. España; Editorial Ariel, 1.996. 260 p.

PUIG, Mir. Delincuencia informática. España; Promociones y Publicaciones Universitarias, 1.992. 340 p.

RAYMOND, Ruyer. La Cibernética y el origen de la Información. México; Fondo de la Cultura, 1987. 546 p.

RIOS ESTAVILLO, J.J. Informática jurídica y Derecho de la Información. México; Derecho e Informática en México, 1.997. 312 p.

SOLER, José. El delito informático. España; Revista protección y seguridad Mayo-junio,1996. 124 p.

TÉLLEZ VALDEZ, Julio. Derecho Informático. México; Editorial Mc Graw Hill, 1.996. 435 p.