Influencia de los criterios del Consejo Nacional de Política Criminal en los delitos informáticos de hurto y estafa

INTEGRANTES
GINETH ANDREA LONDOÑO LIEVANO
C.C. 1030557869
MARIA DEL PILAR GARAY CARREÑO
C.C. 1026278100

Universidad La Gran Colombia
Facultad De Derecho
Diplomado Técnicas De Juicio Oral
Tutor. Daniel Barragán
Bogotá, 2016

Influencia de los Criterios del Consejo Nacional De Política Criminal en los Delitos informáticos de hurto y estafa

Resumen

Dentro de la presente investigación se comienza estudiando lo que es la política criminal del estado y su regulación en el Decreto 2055 de 2014, su función y la influencia que esta tiene para regular los delitos informáticos, igualmente se estudia la multidimensionalidad estratégica, el papel de prevención que cumple y los diferentes conceptos acerca de los delitos informáticos tanto doctrinal como legalmente hablando.

Posteriormente se centra la investigación en los delitos de hurto y estafa informática, explicándolos de acuerdo a la Ley 1273 de 2009 por la cual se adicionaron los Artículos 269A, 269B, 269C, 269D, 269E, 269F, 269G, 269H, 269I, 269J en donde se crea el bien jurídico tutelado "de la protección de la información y de los datos". Y posteriormente se realiza una comparación entre los avances frente al tema tanto en Colombia como en Estados Unidos, partiendo del hecho que Estados Unidos como país desarrollado tiene una evolución más rápida no solo en la normatividad sino también en la penalización.

Para finalizar el presente trabajo de la manera más clara se dará respuesta al objetivo que durante la exploración se determine y que es desarrollado en el trascurso de los avances,dicha respuesta será revelada mediante las conclusiones que resulten de la investigación.

Palabras Clave

Política; Delito; Constitucional; Prevención; Penas; Legislación.

Abstract

Within this investigation is begun studying what is the criminal policy of the state and its regulation in Decree 2055 of 2014, its role and the influence this has to regulate cybercrime, equally strategic multidimensionality is studied, the role of prevention meets and different concepts about both doctrinally and legally speaking cybercrime.

Later research focuses on the crimes of theft and computer fraud, explaining them according to the Law 1273 of 2009 by which the 269A items, 269B, 269C, 269D, 269E, 269F, 269g, 269H, 269I were added, 269J in where the protected "protection of information and data" legally created. and then a comparison between progress is made towards the subject both in Colombia and the United States, based on the fact that the United States as a developed country has faster not only regulations but also in the penalty evolution.

It will respond to finalize this work as clearly as the target for exploration is determined and is developed in the course of progress and that will be revealed by the conclusions resulting from the investigation.

Key Words

Politics; Crime; Constitutional; Prevention; Punishment; Legislation.

Introducción

En la presente investigación se busca dar respuesta a la pregunta problema planteada para el desarrollo de este ensayo, la cual es ¿Cuál es la influencia del Consejo Superior de Política Criminal frente a los delitos informáticos de hurto y estafa?

Es un tema interesante, toda vez que muestra el camino que está recorriendo el Consejo Superior de Política Criminal frente a la Política Criminal en los delitos informáticos y cómo ésta ha influido para la creación de un nuevo bien jurídico tutelado denominado de la Protección de la Información y de los Datos, su implementación en la ley 1273 del 2009 y el avance que tiene respecto de la ley 599 del 2000 en los artículo 269 A y s.s., enfocándose el presente trabajo en los delitos informáticos de hurto y estafa.

Con los tendientes avances tecnológicos han crecido también las prácticas delictivas y las sociedades a su vez se ve en la necesidad de regular estas, Colombia por ejemplo un país donde a diario se forman bandas organizadas que tienen como fin delinquir bajo diferentes escenarios no es ajeno a tener que combatir contra los novedosos pero existentes delitos informáticos.

Se puede hablar que hace unos años los delitos se cometían casi que de manera presencial o como máximo con coautoría, pero hoy en día también se pueden cometer delitos por medio de instrumentos electrónicos que si bien por un lado convierten en la manera más ágil las transacciones en que a diario se ve inmerso un ciudadano del común, también facilita la comisión de delitos de esta índole, es por eso que dentro del presente escrito se busca relacionar esas prácticas con que se ha tenido que familiarizar el estado y a su vez la manera con las que intenta coaccionar dichas conductas por medio de la política criminal del estado con el fin de generar seguridad a las personas que a diario utilizan los medios tecnológicos.

Definir lo que es un delito informático implica tener en cuenta varias interpretaciones que se han dado y que por ende no necesariamente afecta un bien jurídico sino que puede llegar a afectar varios bienes jurídicos, se hablara entonces que el delito se perpetre a través de redes informáticas, o que se trate de un delito usual como son las amenazas, pero que su comisión sea a través de medios digitales; también puede ocurrir que dicha comisión viole la privacidad de la víctima como por ejemplo que alguna persona entre a su correo o a sus redes sociales sin su

permiso o que alguien le intercepte sin permiso una comunicación electrónica suya; ahora bien también se puede hablar de fraude informático en el evento que sea enviado un mensaje donde el remitente se haga pasar por usted o incluso que por medios electrónicos o por aplicaciones entren a su cuenta y trasladen dinero; y así existen muchas otras como que por ejemplo alguien extraiga información desde su PC, que haya falsificación de identidad con el fin de cometer un delito y así muchos más, pero en el presente documento se enfoca la investigación en los delitos de hurto y estafa.

Teniendo en cuenta que la Política Criminal no es una ciencia autónoma, sino que necesita de otras áreas de conocimiento criminal para realizar un estudio sociológico real y establecer la problemática actual frente a los actos delictivos que afectan a la sociedad, dado el caso será necesario remitirse a alguna de éstas para dar una respuesta acertada a esta investigación; la búsqueda se basa en los conceptos de la Corte Constitucional acerca, del Consejo Superior de Política Criminal, documentos del Consejo Nacional de Política Económica y Social y doctrinantes que aborden el tema.

El Estado debe garantizar la protección de los bienes jurídicos importantes para él y por eso es necesario analizar las leyes 599 del 2000 en su artículo 269 A y s.s. (Código Penal) y la ley 1273 del 2009, estableciendo que cambios se produjeron. Esta investigación lleva a un claro entendimiento sobre la Política Criminal y la influencia que ésta ha tenido frente al tipo penal de los delitos informáticos de hurto y estafa y que cambios produce con los avances de la sociedad.

Se busca determinar si los procesos de la política criminal del estado que se han incorporado en la legislación colombiana son suficientes frente los delitos informáticos de hurto y estafa, al igual conocer si el estado colombiano esta actualizado frente al tema de delitos informáticos y la aceptación que ha tenido la política criminal del estado frente a la sociedad colombiana en los delitos informáticos anteriormente mencionados.

Discusión

Para dar inicio a esta discusión, se debe hablar de que es la Política Criminal y es por esto que se toma la definición de la Corte Constitucional sobre Política Criminal, como lo refiere la Sentencia C-646 de 2001; así:

> "Es ésta el conjunto de respuestas que un Estado estima necesario adoptar para hacerle frente a conductas consideradas reprochables o causantes de perjuicio social con el fin de garantizar la protección de los intereses esenciales del Estado y de los derechos de los residentes en el territorio bajo su jurisdicción. Dicho conjunto de respuestas puede ser de la más variada índole" (Corte Constitucional, Sentencia C-646 de 2001)

Con lo anterior se difiere que el Estado debe proteger a sus ciudadanos cuando ellos sienten que están siendo vulnerados de alguna manera por una persona indeterminada y bajo una conducta reprochable, la respuesta del Estado a dicha protección es mediante normas que buscan delimitar ciertas conductas, como una forma de control social y la solución de las discrepancias que surgen entre los ciudadanos, y como objetivo primordial de la Política Criminal es la prevención y sanción de los actos que lesionan a una sociedad.

Es decir que la política criminal es la encargada de estudiar el hilo que puede ser muy delgado entre un actuar que se convierta en delito y previa regulación el sujeto se ve inmerso en un proceso penal, una vez cumplida la investigación este es condenado y debe cumplir con la pena señalada; pero también es la encargada de crear estrategias que prevengan la comisión de la conducta punible.

El Decreto 2055 de 2014 en el cual se reglamenta el Consejo Superior de Política Criminal, su funcionamiento y todos los asuntos relacionados con las demás instancias técnicas que se requieran para su normal funcionamiento, documento que no solo se enfoca en el tema de los delitos informáticos, sino también que es el mecanismo creado para asesorar al gobierno nacional en la implementación de la política criminal y además cumple funciones que se adhieren a nuestra investigación tales como:

- "Recomendar al Ministerio Justicia y del Derecho la elaboración o contratación estudios para establecer causas y dinámicas la criminalidad y del cumplimiento de los fines de la pena.

- Anualmente evalúa las estadísticas en materia de criminalidad y revisa el estado del sistema penitenciario.
- Crea proyectos de ley para acomodar la normatividad a la política criminal.
- Presenta recomendaciones sobre la estructura de la justicia penal.
- Proporciona lineamientos para la coordinación con las demás instituciones en la elaboración y adopción de políticas públicas y de igual manera intercambiar con esta información diagnósticos y análisis estudios de política criminal y penitenciaria.
- Expide el Reglamento del Comité Técnico del Consejo Superior de Política Criminal, Diseñar y aprobar el Plan Nacional de Política Criminal." (Ministerio del Justicia y del Derecho, Decreto 2055 de 2014)

Estas entre muchas más pero para conceptualizar con estas pocas podemos determinar que el Consejo Nacional de Política Criminal tiene funciones específicas y puntales que buscan prevenir la comisión de estos nuevos delitos.

La prevención es un conjunto de políticas y mecanismos que son orientadores para evitar, de algún modo, el nacimiento o el desarrollo de un acto reprochable, esta se puede dar en tres momentos, la primera antes que se cometa el acto delictivo para evitar las consecuencias que conlleva una acción que es tenida en cuenta como delito, la segunda en el momento que se comete el acto delictivo para disminuir las consecuencias para la sociedad que finalmente es la directa perjudicada al realizarse la conducta, y por ultimo después de haberse cometido el acto delictivo para realizar un control social, demostrando que esa conducta no es aceptada por la sociedad y que tiene una sanción para quien la cometa. Esta prevención va encaminada a la identificación de los factores que intervienen en la realización de un delito y a la observación de las condiciones que son necesarias para evitar la actividad delictiva, para la aplicabilidad de la Política Criminal no solo es necesario el área penal sino que también debe haber una intervención de otros mecanismos alternativos.

Estos mecanismos se pueden dar en dos categorías la primera cuando es dirigida a una población especifica que se denomina particular y la segunda distinguida como general, porque

enmarca todos los delitos que pueden ser cometidos dentro de una sociedad y busca evitar que estos se cometan.

Existe una multidimensionalidad estratégica que es el estudio que se realiza en diversos campos y que de alguna manera influye en el desarrollo de la Política Criminal; para la presente investigación solo se tendrán en cuenta los de carácter jurídico, social y tecnológico.

La dimensión jurídica es vista como aquellas normas que regulan los comportamientos de una sociedad, el Código Penal regula la parte fundamental donde se establecen los comportamientos específicos, según la Corte Constitucional en la Sentencia C-646 de 2001:

> "En cuanto al Código Penal, su contenido no es nada diferente que la articulación de las decisiones fundamentales de dicha política. Por lo tanto, forma parte de la etapa de diseño de la política criminal. Sin embargo no agota dicha política. Al ser tan sólo la articulación de la política criminal en un conjunto normativo, no comprende otros aspectos del diseño de la misma." (Corte Constitucional, Sentencia C-646 de 2001).

Y el Código de Procedimiento Penal es la forma en que se aplican las sanciones para esos comportamientos y según la Corte Constitucional en la misma Sentencia C-646 de 2001, expresa:

> "En cuanto al Código de Procedimiento Penal, su contenido es en esencia una articulación de la manera como el Estado investigará, acusará y juzgará a los presuntos infractores de la ley penal. Por eso aunque regula un aspecto de la ejecución del Código Penal, al fijar las reglas para hacerlo respetar, el procedimiento penal regula las formas y los plazos a los cuales deben sujetarse de manera rigurosa quienes deben ejecutar la política criminal. Por lo tanto, forma parte del diseño de dicha política. El Código de Procedimiento Penal en realidad es un elemento constitutivo del diseño de la política en la medida en que regula las formas y pasos que deben ser seguidos por quienes vayan a implementarla" (Corte Constitucional, Sentencia C-646 de 2001).

La dimensión social va encaminada al progreso que tiene una sociedad, puesto que cuando ésta tiene un avance surgen nuevos tipos penales y para contrarrestar estos nuevos actos delictivos se debe crear una legislación que regule y sancione dichos actos.

Y la dimensión tecnológica tiene una gran influencia en la aplicación y sanción de la Política Criminal, ya que para la aplicación de esta se necesita nuevos medios tecnológicos que coadyuvan y coaccionan la forma de la ejecución de las penas y las sanciones, porque está relacionado con la dimensión social.

Se deben tener en cuenta las alternativas que permiten tener una estabilidad frente a los principios de necesidad, razonabilidad, proporcionalidad y utilidad, además debe buscar más mecanismos que mejoren los establecimientos donde se cumplen las penas y también la administración de las mismas.

Según el Documento CONPES 2797 de Política Criminal y Penitenciaria el diseño de la Política Criminal nace desde el punto de vista general, ya que una comunidad reprocha cierta conducta que lesiona y no le produce ningún beneficio ni garantía frente a sus derechos, a causa de este reproche se debe establecer la sanción pertinente para dicha conducta, y de esta forma se establece un precedente hacia la sociedad, que de forma directa le hace saber a ésta, si se cometen estos actos reprochables, que tienen una sanción que castiga y de esta manera busca evitar que sean delitos continuos creando una desconfianza a la sociedad. (1995).

Con el avance tecnológico y más aun con el avance cibernético, se evidencia la mayor probabilidad de la comisión de delitos de carácter informático y en pocas palabras obliga al legislador de regular ampliamente estas conductas para que no queden en la impunidad estos nuevos delitos; aunado a esto es muy difícil tener un rastreo de la información resultante de la internet, pues se convierte en un entorno muy atrayente para los delincuentes, ya que por este medio se puede hurtar, extorsionar, falsificar, entre otros delitos sin ser rastreado, dejando su acción punitiva impune, pero si llegado el caso se llega a identificar el autor del acceso abusivo al sistema informático la pena es simplemente una multa, la cual no protege de una manera adecuada la lesión del bien jurídico tutelado; con la antigua legislación, el artículo no protegía totalmente este bien jurídico y de cierta manera los ciudadanos sentían una desprotección en sus seguridad y tranquilidad en sus actos cibernéticos, cuya dimensión es enmarcada dentro de la confidencialidad, integridad y disponibilidad, previendo esto, el legislador se ve en la necesidad de derogar el artículo 195 del Código Penal por no ser suficiente para la protección de este bien jurídico y crea uno nuevo con la Ley 1273 de 2009 teniendo en cuenta los tres aspectos

nombrados precedentemente, creando circunstancias de agravación punitiva y ampliándoles el verbo rector.

Si bien en cierto que con la antigua legislación, se trataba de proteger la seguridad de la información cibernética, no era suficiente para garantizar una real protección y por este motivo, el Estado se vio en la necesidad de tener en cuenta la Dimensión Social y Tecnológica dentro de la Política Criminal del Estado para poder contrarrestar y dar respuestas más concretas a los hechos que se cometen y una sanción acorde con la lesión que se produce, de esta manera se amplía a la Dimensión Jurídica creando nuevos tipos penales con sanciones más fuertes para quienes cometiese dichos actos, que ahora son considerados como reprochables mediante la integración del Titulo VII BIS con la Ley 1273 de 2009 al Código Penal.

Con la Ley 1273 de 2009 se integra un nuevo bien jurídico tutelado al cual se le denomina De la Protección de la Información y de los Datos; es con esta ley que el estado pretende incluir e involucrar todos y cada uno de los delitos informáticos dando conceptos sobre que se trata cada uno de los delitos y la conexidad con las penas que se impondrán por llevar a cabo estos actos punibles.

Esto demuestra que la Política Criminal de un Estado es necesaria para contrarrestar el auge de nuevos delitos, conforme avanza la sociedad y de esta manera se protege y garantiza a los ciudadanos sus derechos y libertades con base en la intimidad personal y la autonomía de la voluntad.

Teniendo un concepto básico de que es la Política Criminal y cuál es su objetivo principal, es hora de centrar la investigación en los delitos informáticos de hurto y estafa, para poder entender de qué se trata cada uno de estos y poder evidenciar los avances normativos sobre estos actos delincuenciales.

Hurto Informático

Este delito está tipificado en la Ley 599 de 2000, Código Penal en el Artículo 269I como Hurto por medios informáticos y semejantes, y consagra lo siguiente:

> "El que superando medidas de seguridad informáticas, realice la conducta realizada en el Art. 239 C.P manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el Art 240 C.P" (Congreso de la Republica, Ley 599 de 2000)

El Articulo 269I, tiene conexidad con el Artículo 239 de la misma ley pero complementa en su parte final indicando que lo debe hacer por medio de un instrumento informático, lo consagrado en el Artículo 239 es lo siguiente:

> "El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para si o para otro, incurrirá en prisión de dos (2) a seis (6) años. La pena será de prisión de uno (1) a dos (2) años cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales vigentes" (Congreso de la Republica, Ley 599 de 2000)

El artículo 240 del Código Penal por su parte hace referencia a la penalización del delito codificado en el Artículo 239 del mismo código; y al igual que el articulo 239 tiene conexidad con el articulo 269I, y lo que determina es que:

> "Si los elementos hurtados están destinados a las comunicaciones (telegráficas, informáticas, telefónicas, telemáticas o satelitales) o a la generación, transmisión o distribución de gas domiciliario o energía eléctrica, o a la prestación de servicios de alcantarillado y acueducto, la pena será de 5 a 12 años de prisión" (Congreso de la Republica, Ley 599 de 2000)

El que cometiera dicha conducta punible debe hacerlo a través de redes de navegación y por medio de los Crakers quienes son los que sin previa autorización llevan a cabo trampas y de esta manera se apoderan de los bienes de las víctimas que finalmente quedan indefensos ante tal situación y que para dar un concepto son:

> "aquellas personas que con comportamiento apremiante, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un cracker es hábil conocedor de programación de software y hardware, diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos" (Paloma, Delitos Informáticos en el Ciberespacio,2012).

El legislador se ve en la necesidad de crear un ordenamiento que proteja la sociedad y que le permita sentirse más segura frente a estos ciber delincuentes que con sus conocimientos especializados realizan la conducta punible; esto no quiere decir que los sistemas sean inseguros todo lo contrario, estos son los que han permitido facilitar la vida de los ciudadanos, el problema radica en que existen personas que se aprovechan y con comportamientos desequilibrados perjudican a la mayoría de la colectividad, este delito se encuentra muy ligado a los delitos contra el patrimonio pues las transferencias que se realizan muchas veces son percibidas por el titular del bien días o incluso meses después.

Los ciber delincuentes son personas que sin valores y pensando en un bienestar propio, sin esfuerzo laboral alguno pero valiéndose de sus conocimientos perjudican económicamente a la presunta víctima que no tiene como defenderse ante tal atentado, pues mientras el ciberdelincuente se encuentra detrás de un computador o cualquier otro medio que le facilite la comisión del delito, este desconoce por completo de lo que está siendo víctima, y se puede decir que es más reprochable dicha conducta que incluso la cometida con un arma convencional pues se comete "asalto virtual" (Paloma, 2012, Pag. 156) ya que no existe una sola posibilidad de defensa.

Este delito cada vez es más progresivo a nivel interno en Colombia, ya que no solo se habla de una pérdida económica a la persona sino que también tiene afectaciones sobre los bancos e incluso en las buenas costumbres de la sociedad y adicionalmente esta actividad virtual genera grandes beneficios económicos ilícitos que finalmente terminan con afectar directamente al país.

Solo existe una manera de prevención que son las contraseñas prediseñadas para que el usuario este seguro, o más bien crea estar seguro, ya que para estos delincuentes esta no es un obstáculo y una vez realizado el hecho delictivo la victima queda desamparada y ante tal actividad adolece de defensa.

Al ser un delito reciente, históricamente no son muchos los casos que se han llevado a juicio ni tampoco muchos los condenados pero en septiembre de 2011 se sentencia a cibercriminales por violación a las conductas estipuladas en los Artículos 269-A, 269-F y 269-I; que corresponden a las conductas punibles de acceso abusivo al sistema informático, violación

de datos personales y hurto electrónico en concurso con falsedad en documento privado y concierto para delinquir.

El hecho factico en dicho caso comienza cuando los cibercriminales ingresan a bases de datos personales y con esta información recopilada crean las tarjetas de crédito y débito con las que a nivel territorial retiran diferentes sumas de dinero.

Estafa

Este delito no está tipificado literalmente como ESTAFA en la normatividad colombiana, pero en el artículo 269J de la Ley 599 de 2000 se tipifica lo siguiente:

> "El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave," (Congreso de la Republica, Ley 599 de 2000).

Para desglosar lo enunciado en el artículo 269J de la Ley 599 de 2000, la estafa electrónica está orientada a proteger el bien jurídico individual cuando es vulnerado utilizando medios electrónicos, ya que por estos medios electrónicos no se utiliza la persona como tal para inducir a transferir su patrimonio, hablando de activos representados en datos informáticos o activos que se transfieran por medio electrónico, sino que se utiliza a un elemento electrónico o un máquina para que haga esta acto automáticamente.

Por los diferentes actos delincuenciales que se han presentado, se habla de la estafa electrónica y el Phishing como las formas de realizar este acto punible, sin embargo en la Ley 599 de 2000 el Código Penal Colombiano en el Articulo 269J, se tipifica la Transferencia no consentida de activos y si se analiza los verbos rectores se podría tomar como un tipo de estafa.

Esta modalidad de estafa electrónica sugiere que se utilicen dos modalidades las cuales son la manipulación informática y un artificio semejante, pero siendo cierto se necesitan ejecutar estas dos modalidades para poder cometer el acto delincuencial en su totalidad; "la manipulación informática es la alteración o modificación de los datos a través de supresión o introducción de datos falsos y su modificación dentro del programa", (Suarez, 2009, Pag. 253); teniendo en cuenta lo anterior, la manipulación informática es cuando se incide en un sistema electrónico y

por el hecho anterior se induce a un mal funcionamiento y por esto se comete el acto punible; y el artificio semejante se abarca de manera más amplia todas las modalidades de estafa informática, sin tener certeza del elemento o la acción que se va a utilizar para cometer el acto delincuencial.

Aunque no obstante para la realización de la comisión del delito se requiere que se haga una transferencia de activos patrimoniales para dar por culminado y perpetrado en su totalidad el delito de estafa informática, ya sea utilizando una manipulación informática o un artificio semejante y por supuesto que en esto exista el no consentimiento de la persona propietaria de los activos patrimoniales informáticos.

En lo pertinente a la técnica de estafa conocida como "phishing" se entiende como un engaño por medio electrónico para poder obtener información confidencial haciendo creer que el usuario está utilizando el elemento electrónico original pero en realidad está manejando una copia casi exacta al original.

Regularmente el "phishing" se utiliza para obtener información personal bancaria de los usuarios para poder utilizarla en las paginas bancarias reales y extraer o transferir activos patrimoniales de las entidades bancarias; el ciberdelincuente que realiza estos actos delincuenciales se le conoce como "phisher" y debe poseer conocimientos amplios sobre informática ya que no es un método muy común ni habitual sobre estafa; o este método también lo han implementado configurando un sistema informático para que automáticamente realice las conductas.

Después de analizar la tipificación de los delitos informáticos de hurto y estafa, se realiza una comparación entre la legislación de Colombia y estados unidos frente al tema, esto con el fin de medir los avances que cada uno de ellas ha tenido.

Buscando similitudes y diferencias entre la regulación del delito informático en Estados Unidos y Colombia se evidencia que mientras en Colombia la legislación es bastante reciente en Estados Unidos desde 1976 el FBI dicta cursos de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes

por los cuales estados como Florida, Michigan, Colorado, Rhode Island y Arizona se fundaron como los primeros en contar con una legislación específica en el año de 1985.

Un año después la Computer Fraud y Abuse Act en 1986 regula los delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales y estipula penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords con el fin de delinquir; esta acta fue modificada por el Acta Federal de Abuso Computacional en 1994 y es aquí donde se empieza a regular el tema de los virus (computer contaminant) pero los determina solo como aquellos que contaminan otros programas o bases de datos.

Con los avances tecnológicos aumentaron también los casos de hacking que es realizado por un "hacker" quien se define como:

> "aquel que se considera como capaz de poder penetrar en Sistemas Informáticos protegidos, pudiendo acceder a una cantidad variable de Bases de Datos y poder acceder a información que lógicamente, no está disponible al público, pudiendo tener inclusive una sensibilidad confidencial y hasta poder causar un perjuicio de poder hacerse pública, teniendo acceso a ella mediante un Escritorio Remoto, aprovechando entonces la conexión de Redes para dicho acceso."(Master Magazine, S.F.)

Por ende la inseguridad dentro de los cibernautas, por lo cual cambió la percepción de las autoridades con respecto a los hackers y sus ataques. Uno de los casos que demostró ese cambio fue el del "Cóndor" Kevin Mitnicky quien fue acusado por delitos informáticos contra empresas como COSMOS, de Pacific Bell , Microcorp Systems, MCI Communications y Digital Equipment Corporation, Digital Equipment, Tsutomu Shimomura, finalmente es detenido en su apartamento y se le aprehenden discos, ordenador, teléfonos móviles, manuales, etc, los cuales fueron usados como elementos materiales probatorios para finalmente sentenciarlo.

Estados Unidos cuenta con una federación especial para los casos de delitos informáticos que es la FCIC (Federal Computers Investigation Commitee), constituida por investigadores estatales y locales, agentes federales, abogados, auditores financieros, programadores de seguridad y policías. El FCIC es la entrenadora del resto de las fuerzas

policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional y cuentan también con la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), encargada de investigar nuevas técnicas de investigación sin destruir evidencia. Sus integrantes son "forenses de las computadoras" y trabajan también en Canadá, Taiwán e Irlanda. (Crime Research, S.F.)

Conclusiones

Penalmente hablando se puede deducir que de la ley 599 de 2000 (código penal colombiano) promulgada el 24 de Julio de 2000 y Ley 1273 de 2009 promulgada de 5 de enero de 2009 tuvo un gran salto, pues mientras la primera solo propone un artículo que cobije las practicas informáticas con fines delictivos en el artículo 195 que reza "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" la segunda crea todo un articulado que se titula "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y que nos habla de temas como : El acceso abusivo a un sistema informático, La obstaculización ilegítima de sistema informático o red de telecomunicación, la Interceptación de datos informáticos, el daño Informático, el uso de software malicioso, la violación de datos personales, la suplantación de sitios web para capturar datos personales. Y otro titulado "De los atentados informáticos y otras infracciones" donde consagra temas como: El hurto por medios informáticos y semejantes, la transferencia no consentida de activos y adicionalmente regulan la competencia sobre dichos temas,

La regulación del delito informático nace de la necesidad de protección por parte del legislador a los bienes jurídicos tradicionales como son el patrimonio económico, ya que lo que cambia es el medio de comisión de este, pues tanto en la estafa como en el hurto el fin sigue siendo el mismo, la diferencia es que para el caso del delito informático se debe ejecutar con la ayuda de un instrumento virtual que facilite la comisión del mismo.

Si bien el estado colombiano mediante la ley 1273 de 2009 genero avances al regular los delitos informáticos, hoy día con los avances tecnológicos se está quedando atrás, pues sería importante generar programas de conciencia a la sociedad para que esta no solo conozca la regulación sino que de alguna manera se prepare y en el eventual caso de ser víctima tenga algún medio de protección.

Es decir que no solo con crear un nuevo bien jurídico tutelado en el Código Penal, dar conceptos y las penas a imponer, se logra la no ejecución del delito, se deben crear grupos especializados con amplios conocimientos en los temas informáticos que se encarguen de buscar nuevos métodos de estudio ante la comisión del delito y la prevención sobre estos.

En la comisión de los delitos informático se debe estudiar tanto la disposición patrimonial con que cuenta la persona jurídica o la persona natural, y el perjuicio patrimonial que sufre esta una vez es víctima del hecho punible.

Aunque poco a poco la legislación colombiana ha avanzado en la implementación de ordenamientos que regulen la práctica de delitos informáticos, aun no vamos a la vanguardia como por ejemplo Estados Unidos, pues ellos tienen un ordenamiento aplicado desde hace aproximadamente 40 años y nosotros si bien el estado colombiano creó un articulo dentro del código penal en el año 2000 lo desarrollo hasta el 2009 con la ley 1273.

Mientras que Estados unidos cuenta con un comité especializado que le permite el estudio, implementación, creación y demás que regulen la comisión de delitos informáticos, Colombia cuenta con la comisión de delitos de política criminal que no solo se encarga de realizar prácticas con el fin de regular los delitos informáticos sino toda clase de delitos.

Referencias Bibliográficas

Colombia. Congreso de la República. Ley 599 (2000). "Por la cual se expide el Código Penal" Diario Oficial No. 44.097 del 24 de julio del 2000.

Colombia. Congreso de la República Ley 1273 (2001). "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" Diario Oficial No. 47.223 del 5 de enero de 2009.

Colombia, Consejo Nacional de Política Económica y Social – CONPES 2797, (1995) "Política Penitenciaria y Carcelaria". Departamento Nacional de Planeación.

Colombia. Corte Constitucional. (2001). Sentencia No. C-646. Mg. Manuel José Cepeda Espinosa.

Colombia. Ministerio de Justicia y del Derecho (2014). Decreto 2055. Ministro de Justicia y del Derecho Yesid Reyes Alvarado.

Crime Researcho (S.F.) "Computer Crime" Recuperado de http://www.crime-research.org/library/Alex.htm, pagina traducida al español.

Master Magazine (S.F.) "Definición de hacker" Recuperado de http://www.mastermagazine.info/termino/5204.php

Paloma, L. O. (2012) "Delitos Informáticos (en el ciberespacio)" Ediciones Jurídicas Andrés Morales.

Seguridad de la Información (S.F.) "Legislación y Delitos Informáticos - Estados Unidos" Recuperado de http://www.segu-info.com.ar/delitos/estadosunidos.htm

Suarez, A. (2009) "La Estafa Informática" Grupo Editorial Ibañez. Bogotá, Colombia.