Caracterización de los delitos informáticos en Colombia

Characterization of cybercrime in Colombia

Cómo referenciar este artículo:
Manjarrés, I & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia.
Pensamiento Americano, 71-82

Iván Manjarrés Bolaño *
ivanmanjarres@gmail.com
Farid Jiménez Tarriba **
farithebad@hotmial.com

Resumen
Es evidente que los avances tecnológicos demuestran la evolución del hombre, y eso lo podemos comprobar a través de los medios que permiten el almacenamiento, la transmisión y la administración de la información. Avances que han modificado el vivir diario de las personas y de las organizaciones, las cuales reflejan el aumento de transacciones comerciales, comercio electrónico, comunicaciones en línea, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc., pero los sistemas de información que han permitido mejorar ostensiblemente los procesos al interior de las organizaciones, son los que al mismo tiempo han generado una serie de comportamientos ilícitos, que se les denomina "Delitos Informáticos", y es el tema a abordar en este articulo de investigación, que se enmarca dentro del proyecto interdisciplinar titulado La seguridad en los Delitos informáticos desarrollado por estudiantes y docentes de los programas de Derecho e Ingeniería de Sistemas de la Corporación Universitaria Americana.

Palabras Clave
Delitos, Tecnologías, Internet, Información, Seguridad.

Abstract
It is clear that technological advances shows the evolution of man , and we can check through the means for storage, transmission and information management . Advances that have changed the daily life of individuals and organizations , which reflect increased business transactions, electronic commerce , online communications , industrial processes , research , safety , health, etc. . , But systems information that allowed significantly improve processes within organizations are at the same time have created a series of unlawful conduct, which are called " Computer Crimes " and is the subject addressed in this research article, that is part of the interdisciplinary project entitled security in cybercrime developed by students and teachers of law programs and Systems Engineering of the American University Corporation.

Key Words
Crimes, Technology, Internet, Information, Security

Introducción

Es evidente que en Colombia, el uso de las nuevas tecnologías digitales y de la telefonía inalámbrica ya se ha generalizado. Estas tecnologías nos brindan la libertad para poder movernos y permanecer comunicados y conectados con miles de servicios construidos sobre redes de redes. Nos dan la posibilidad de participar; de enseñar y aprender, de jugar y trabajar juntos, y de intervenir en el proceso político. Pero también estas tecnologías de la información pueden utilizarse, y se utilizan, para perpetrar y facilitar diversas actividades delictivas, convirtiéndose en instrumentos para actividades que ponen en peligro o atentan contra la vida, la propiedad o la dignidad de los individuos o del interés público.

* Licenciado en Biología y Química de la Universidad del Atlántico, Estudiante de Noveno Semestre de Derecho e integrante del semillero de investigación del Grupo Derecho, Justicia y Estado Social de Derecho de la Corporación Universitaria Americana. Ponente en el VI Congreso del Nodo Caribe de Investigación y del XXXIV Congreso de Derecho Procesal.

** Estudiante de Octavo Semestre de Derecho e integrante del semillero de investigación del Grupo Derecho, Justicia y Estado Social de Derecho de la Corporación Universitaria Americana.

Artículo recibido: Diciembre 12/2011. Aceptado: Febrero 7/2012

Este artículo es producto de un proyecto de investigación interdisciplinar que lleva el nombre de seguridad en los Delitos Informáticos, la cual hemos desarrollamos desde junio de 2011 como miembros del semillero de investigación del grupo: Derecho, Justicia y Estado Social de Derecho, con la asesoría de la Directora del Grupo de investigación, la Dra. Cristina Montalvo y con el apoyo de integrantes del grupo de investigación de Ingeniería de Sistemas. Teniendo, en cuenta que algunos de los objetivos trazados en dicho proyecto eran el dar a conocer los diferentes tipos de delitos informáticos que se cometen en Colombia y la legislación existente hasta el momento sobre el tema, hemos elaborado el presente artículo para dar a conocer parte de los resultados de investigación obtenidos .

Hasta ahora el estudio por parte de la doctrina del fenómeno de la criminalidad o delincuencia informática y la búsqueda de una adecua¬da reacción legal frente a la misma, e incluso el análisis jurisprudencial de los escasos supuestos que han llegado a los Juzgados y Tribunales pe¬nales, sobre todo en nuestro país, se ha venido efectuando mayoritariamente desde una perspectiva clásica del Derecho Penal, en donde "lo informático", es decir, la vinculación con la informática de la ac¬ción abusiva o ilícita, ha venido tratándose como una complementación a la inicial perspectiva de protección de un bien jurídico tradicional en la correspondiente rama del Derecho penal, determinando consecuen¬temente su punibilidad o su impunidad legal penal a tenor de su posi¬ble subsunción o no en los tipos delictivos existentes.

Con la promulgación de la ley 1273 de 2009, el legislador, al introducir aspectos informáticos o vinculados a las nue¬vas tecnologías de la información, y al incorporar nuevas figuras delictivas en pretensión de una adecuada respuesta a la criminalidad informática, por lo demás en continua evolución y con novedosas ma¬nifestaciones, ha continuado guiándose por esquemas dogmáticos pe¬nales tradicionales. Así mismo, tanto la doctrina penal Colombiana, en el análisis de tales modificaciones o, en su caso, de los nuevos tipos delictivos, como los órganos jurisdiccionales penales, en la reso¬lución de los escasos casos significativos que han llegado a su enjuicia¬miento, han seguido las directrices clásicas de enfocar el análisis de los denominados delitos informáticos única y exclusivamente desde la citada perspectiva de vinculación e incidencia de las nuevas tecnologías en, la comisión de delitos clásicos y en relación a la protección de bienes jurídicos tradicionales.

La continua evolución de la criminalidad informática y de las nue¬vas tecnologías, tanto en los métodos utilizados, en los objetos sobre los que recaen sus acciones» como en la ampliación y extensión cualitativa y cuantitativa de las posibles víctimas de tales ataques, hacen que en los últimos años hayan aumentado considerablemente no sólo los perjui¬cios y daños efectivos en los ámbitos personal o de la intimidad, econó¬mico, patrimonial y de seguridad jurídica, sino la gravedad del peligro y riesgo de quebranto de los bienes jurídicos sociales o colectivos y no sólo individuales vinculados a la informática y las nuevas tecnologías.

Precisamente por ello, y por la relevancia social que esta problemá¬tica ha ido adquiriendo en años recientes, sobre todo en nuestro país, tanto a nivel de investigación y especialización por parte de los Jueces y Fiscales, como a nivel de la sociedad en general, incluso del ciudadano medio, a través de la difusión por los medios de comunicación social de los cada vez más frecuentes y graves casos descubiertos y sacados a la luz pública, así como, en algunos su¬puestos, la falta de una adecuada respuesta legal y judicial, o, al menos, que la misma fuera precisa, coherente y sistemática frente a los diversos tipos de conductas y acciones informáticas ilícitas, incluso simila¬res, es lo que nos motivó la elección del presente tema de investigación.

Por otro lado, en medio del conflicto armado que vive el país y la actitud violenta que se respira en muchos espacios es difícil suponer que un delito se pueda cometer sin empuñar un arma. Pero la realidad es bien distinta. Basta hacer un clic, acompañado de unos cuantos pasos más para que el 'atracador virtual' o 'ingeniero social' como se le empieza a llamar en la jerga tecnológica, atente contra la información, el bolsillo de la gente o las arcas empresariales, entre algunas de las modalidades reconocidas como delito informático.

A medida que las sociedades dependen cada vez más de estas tecnologías, será necesario utilizar

medios jurídicos y prácticos eficaces para prevenir los riesgos asociados. Garantizar infraestructuras de informaciones seguras y fiables no sólo exige la aplicación de diversas tecnologías, sino también su correcto despliegue y su uso efectivo. Algunas de estas tecnologías existen ya, pero a menudo los usuarios no son conscientes de su existencia, de la manera de utilizarlas, o de las razones por las que pueden ser necesarias, esta última circunstancia esta muy fuertemente arraigada en la cultura nacional, de no enfrentar esta situación con la debida anticipación, negándonos la oportunidad de tener una clara percepción sobre esta grave problemática. En nuestro país la delincuencia informática se comete en el ciberespacio, y no se detiene en las fronteras nacionales convencionales. En principio, puede perpetrarse desde cualquier lugar del país y contra cualquier usuario de ordenador del mundo. El fenómeno de la criminalidad informática o de los llamados delitos informáticos en Colombia, no han alcanzado todavía una importancia mayor, esto por cuanto no se conoce en el entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo. El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

Metodología

La metodología utilizada para este trabajo de investigación fue la descriptiva, atendiendo que nuestro proyecto se centró en analizar y estudiar las conductas informáticas consideradas delictivas o reprochables y que están tipificadas como delitos en nuestro código penal, utilizando las diferentes Tecnologías de la Información y Comunicación. Para el desarrollo de este tema la técnica utilizada ha sido el análisis bibliográfico de la temática aquí abordada.

Breve Antecedente y Definición de los Delitos Informáticos.

La introducción de los ordenadores en determinados ámbitos sociales tuvo lugar por la década de los años 50 construida la primera computadora digital la ENIAC (Electronic Numerical and Computer) diseñada y construida por los ingenieros John Presper Eckert y John William Maucly, que por aquella época se le denominaba computadora, pues era la traducción directa y textual del inglés "computer" que, no obstante, se sigue utilizando en el derecho com¬parado (Guerra). Ha habido algunos intentos en nuestra doctrina de cambios de terminología, e incluso de modificar el término actual de ordenador, como por ejemplo por el de elaborador electrónico.

Fue hasta los años 60 cuando aparecie¬ron, principalmente en Alemania y en Estados Unidos, los primeros ar¬tículos y publicaciones sobre casos conocidos de abusos informáticos (manipulaciones de ordenadores, de sabotaje de programas informáti¬cos, de espionaje de datos informáticos, e incluso de uso ilegal de siste¬mas informáticos), esto es, manifestaciones del nuevo fenómeno de la criminalidad informática, cuya sustantividad ha sido discutida por la doctrina en dichos países y traducidas algunas al español (Taber, 1980). Pero para el año de 1949, Norver Wiener, publicó una obra en cuyo capítulo IV, denominado el "Derecho y las Comunicaciones" el cual expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: El Jurídico (Wiener, 1980).

Por otra parte, señala Wiener que el juez estadounidense Lee Loevinger publicó para ese mismo año de 1949, un artículo de 38 hojas en la revista Minesota Law Review, titulado "the Next step Forward" en donde menciona que el próximo paso en el largo camino del progreso del hombre, debe ser el de la transición de la Teoría general del Derecho Hacia la Jurimetría, que es la investigación científica, acerca de los problemas jurídicos (Wiener, 1980).

Los primeros estudios empíricos del delito informático o delito vin¬culado a la informática se llevaron a cabo a partir de mediados de los años 70, aplicando métodos científicos de investigación criminológica (Division de Investigacion y Desarrollo del Consejo Nacional de la Prevencion del Delito, 1981), identificándose el primer caso de delito informático en dicho informe, el caso de Draper Jhon, en Septiembre de 1970, también conocido como el Captain Curnch, des-

cubre que los obsequios ofrecidos en la caja de cereal Captain Curnch duplica perfectamente la frecuencia del tono 2600 hz de una línea de WATS permitiéndole hacer llamadas telefónicas gratis y la gran víctima era AT & T.

Estos trabajos y estudios se centraban en el ámbito de la delincuencia económica, y principalmente referidos a la comisión de actos defraudatorios mediante la utilización o aprovechamiento de medios o sistemas informáticos. Los mismos mostraron la existencia de un número limita¬-do de casos verificados de ilícitos informáticos, analizando algunos de cierta espectacularidad y resonancia, por aquel entonces, en el ámbito económico y social internacional, como el caso de fraude en la Fundación American Equity que integró manipulaciones de 56.000 reclama¬ciones de seguros por un valor de al menos 30 millones de dólares, as¬cendiendo en 1973 las reclamaciones por compensación de seguros en¬tre el billón y los 2 billones de dólares, el caso del Banco alemán Herstatt, relativo a transacciones especulativas cambiarias exteriores to¬talizando varios miles de millones dólares, y que no fueron grabadas en los archivos de cuentas del citado banco, que quebró en 1974 y causó pérdidas a sus clientes por un importe cercano a los mil doscientos mi¬llones de marcos alemanes, o las manipulaciones informáticas en la empresa automovilística sueca Volvo; pero al mismo tiempo pusieron de manifiesto la existencia de un estimable y elevado número de casos no detectados o denunciados, hecho que se constituirá, como veremos, en una de las características principales de esta categoría delictual , conocida como la cifra negra de criminalidad (Soiarz, 1990).

Por lo anterior, las primeras conceptuaciones de la criminalidad informática venían enfocadas desde el ámbito penal eco¬nómico. Así inicialmente Tiedemann (1983), consideraba la criminalidad mediante computación como una de las formas de criminalidad económicas neutrales, es decir, aquellas que surgen en cualquier sistema eco¬nómico con independencia de la naturaleza del mismo, y por ello procede a su estudio corno reflejo de la criminalidad económica, aludiendo a la parte de aquélla que perjudica los intereses patrimoniales, y no refiriéndose en absoluto a otros aspectos de la misma, como el afectante a la intimidad. Hacia fines de los años sesenta, la difusión de aplicaciones informáticas en lo social, ya resultaba suficientemente representativa como para denunciar implicaciones sociales y jurídicas. Emerge, así, el llamado Derecho de Informática, se revelan como primeras preocupaciones, la acumulación y uso indebido de los llamados datos personales, con el posible conflicto de este hecho y el derecho de intimidad o privacidad. También los contratos de equipamiento informático y la protección a los autores de los programas de computación, en cuanto a los derechos morales y de explotación de su obra; aparecen entre estas primeras inquietudes desarrolladas y ampliadas rápidamente en los sucesivos años. En la misma época se dedican artículos al tema de la automatización de la gestión de los estudios profesionales y la actividad procesal de la justicia, con lo cual nace la llamada Informática Jurídica de Gestión. Estos ámbitos de acción de la Informática Jurídica, nacen en los países del Common Law y pasan luego a la Europa Occidental, constituyéndose en la fuente directa de los cultores del mundo latinoamericano. Se debe resaltar el impacto que tuvo en los Estados Unidos, en cuanto a su tendencia documentaria, porque se aplicaba, no solamente a las sentencias de los jueces, sino también a las otras dos fuentes principales de conocimiento y/o aplicación del Derecho en el sistema de “civil law”; la legislación y normatividad en general y la doctrina de autores.

La Informática Jurídica surge como suma de tres áreas, la jurimetría, informática jurídica y derecho de la informática. Según MacKaay la jurimetría es la aplicación de técnicas estadísticas y matemáticas que permiten verificar la regularidad de ciertas hipótesis interesantes en el acontecer jurídico; permite también resolver algunos problemas concretos y elabora, a partir de esos datos, una cierta teoría del derecho, Para el mismo autor, la Informática Jurídica es el tratamiento lógico y automático de la información jurídica, en tanto soporte del conocimiento y la comunicación humana; finalmente define que el Derecho Informático es el conjunto de problemas jurídicos producidos por la informática.

El término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica. Después de una reunión en Lyón, Francia, se fundó un sub-

grupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a Internet. El "Grupo de Lyón" utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos (Perrin, 2005).

Al mismo tiempo, y guiado por los participantes en el grupo de Lyon, el Consejo Europeo comenzó a diseñar el Tratado sobre Delito Informático. Este tratado, que fuera presentado a la opinión pública por primera vez en el año 2000, incorporó una nueva gama de técnicas de vigilancia que las agencias encargadas de la aplicación de la ley consideraban necesarias para combatir el "delito informático". ¿Cómo se definió el delito informático? La versión final de ese tratado, aprobada en noviembre de 2001 después de los acontecimientos del 11 de septiembre, no definió el término. Es un término muy amplio referido a los problemas que aumentaron el poder informático, abarataron las comunicaciones y provocaron que haya surgido el fenómeno de Internet para las agencias policiales y de inteligencia. El tratado describe de la siguiente manera las diferentes disposiciones y áreas temáticas en las que se requiere una nueva legislación:

- Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.
- Delitos relacionados con las computadoras [falsificación y fraude].
- Delitos relacionados con el contenido [pornografía].
- Delitos relacionados con la violación del derecho de autor y los derechos asociados.
- Responsabilidades secundarias y sanciones [cooperación delictiva, responsabilidad empresarial].

Sujetos de los Delitos Informáticos.

Los sujetos que actúan en el Delito Informático son:

Sujeto activo

De acuerdo al profesor chileno Mario Garrido Montt, (Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992).se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que "desvía fondos" de las cuentas de sus clientes.

Edwin Sutherland, criminólogo norteamericano, en el año de 1943 señala 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".

Sujeto pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo. En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que

muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más. Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

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, además de que en algunos países como el nuestro no existe legislación alguna sobre esta clase de conductas ilícitas lo que empeora más la situación de las víctimas de estas conductas ilícitas.

Características de Delitos Informáticos.

Según el abogado e investigador mexicano sobre el tema de los delitos informáticos TELLEZ VALDEZ, este tipo de acciones presenta 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) puede llegar a cometerlas.
b. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya 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 económicos " al hechor.
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 y algunos impunes de manera manifiesta ante la ley (Tellez, 2005).

Clasificación de los Delitos Informáticos en Colombia.

Según estadísticas de la Comisión de Regulación de Telecomunicaciones (CRT), en los tres primeros meses de 2008 el total de suscriptores de Internet aumentó 13,6%, llegando a 1.569.126, de los cuales el 55,7% cuenta con conexión de banda ancha. La masificación de acceso de usuarios a Internet ha permitido grandes avances en tecnología, así como la creación de nuevas modalidades de robo y prácticas delincuenciales con este tipo de herramientas de tecnología y telecomunicaciones.

A través de la información, se han podido identificar diferentes tipos de delitos informáticos que se cometen en nuestro país, entre los que se encuentran aquellos que:

• Afectan el patrimonio económico: banca virtual, phishing, key logers, falsas páginas, venta a través de portales de compra y venta, falsos premios.
• Buscan el abuso de menores: comercializan videos, fotografía, audio, texto, falsas agencias, salas de chat.
• Afectan la propiedad intelectual: descargas de programas y comercialización de obras sin pagar derechos de autor.
• Afectan la información como bien jurídico: como por ejemplo cuando algunos empleados usan sus privilegios o permisos para acceder a información que es secreto de la empresa y luego entregarla a la competencia, teniendo como base el desarrollo que han tenido. Robos de información privilegiada.

Según estadísticas del Grupo de Investigación de Delitos Informáticos de la Dirección Central de Policía Judicial (DIJIN), el cual se dedica a la investigación de conductas delictivas derivadas del uso de la tecnología y telecomunicaciones, el hurto a través de Internet es uno de los mayores delitos que se presentan en Colombia (Grupo Investigativo de Delitos Informaticos - GRIDI, 2009).

Para contrarrestar este tipo de delincuencia, la Dijin trabaja en tres aspectos:
• Preventivo: A través de la página en Internet: www.delitosinformaticos.gov.co, donde expertos en el cibercrimen atienden las inquietudes de los ciudadanos y dan recomendaciones para no ser víctima de los delincuentes.
• Investigativo: Coordinando todas las actividades con la Fiscalía y las autoridades competentes para recopilar el material probatorio.
• Político: Participando en la promulgación y elaboración de proyectos de ley que permitan tipificar estas prácticas y disminuir este tipo de delincuencia.

De acuerdo a investigaciones adelantadas por la Dijin, los delincuentes cuentan con mayores recursos técnicos actualmente, tienen un muy buen ancho de banda, un buen computador, acceden a programas para esconder su dirección IP de conexión y así generar anonimato, razón por la que se recomienda a toda la ciudadanía tomar todas las medidas necesarias para garantizar su seguridad física y económica. Es importante invertir en seguridad, no basta con tener un buen computador, hay que protegerse con antiespías, antivirus y todo tipo de programas especializados para la protección de la información. Las personas deben adquirir una cultura de higiene informática, que hagan contraseñas robustas, que cuando naveguen en Internet eviten dar datos que puedan vulnerar su bienestar, que si manejan dispositivos como USB, las protejan, las vacunen antes de ingresarlas al computador (Grupo Investigativo de Delitos Informaticos - GRIDI, 2009).

Cifras sobre delitos informáticos en Colombia

Sègun el Colegio Colombiano de Juristas Colombia es el tercer país latinoamericano en donde mas se cometen delitos informáticos, se calcula que unas 187 denuncias mensuales son interpuestas por fraudes a diferentes bancos que traducido a plata podrían representar pérdidas cercanas a los 11 millones de dólares (unos 20 mil millones de pesos). La lista la encabezan Brasil y Mexico. La Fisaclìa en su división para la investigación

de este tipo de delito ha encontrado que los delitos electrónicos que más se presentan en el país y que, según expertos de la Fiscalía, van en aumento son acceder a bases de datos de bancos u otras entidades sin permiso, sustraer archivos de computadores, ingresar a redes sociales y correos ajenos y clonar tarjetas bancarias.

Un informe de la compañía Norton, de Symantec, realizado en 23 países incluido Colombia, el cual publicó el diario El Tiempo, reveló que en el último año, cada segundo, 18 personas adultas son víctimas de alguna modalidad de delito informático en el mundo. Esto significa que más de 1,5 millones de usuarios de la Red caen al día en las trampas de los hackers.Son unos 556 millones de personas al año, que perdieron en total 110.000 millones de dólares en el mundo. El estudio se realizó entre julio del 2011 y julio de este año mediante 13.000 encuestas entre usuarios adultos de Internet. "Son casos efectivos, es decir, de personas que cayeron en alguna forma de cibercrimen y que perdieron dinero por ello", señaló Gonzalo Erroz, experto de Norton Latinoamérica (Redaccion Tecnologica de El Tiempo, 2011).

El 50 por ciento de los usuarios de redes sociales en Colombia han sido víctimas del cibercrimen, mientras que al 20 por ciento de los encuestados locales les vulneraron algún perfil digital y suplantaron su identidad, dice el estudio. "El 56 por ciento de los usuarios adultos de Internet en Colombia no saben que el malware o código malicioso opera de manera oculta y silenciosa en su computador cuando es infectado, tras descargar contenidos o acceder a enlaces desde correos sospechosos", dijo el experto de Norton (Redaccion Tecnologica de El Tiempo, 2011). Entre tanto, el 77 por ciento de los adultos colombianos encuestados reconocieron haber sido víctimas en algún momento de su vida de un delito informático.

Regulación Jurídica de los Delitos Informáticos en Colombia.

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones.

El primer capítulo de los dos en que está dividida la Ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo Capítulo se refiere a los atentados informáticos y otras infracciones. A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.

Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los "delitos informáticos", con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.

Con los desarrollos jurídicos hasta ahora logrados acerca de "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las organizaciones pueden amparar gran parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo (Davenport, 1999), de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral.
Retomando la estructura de la Ley 1273 de 2009,

el capítulo I está orientado especialmente a apoyar la labor de los grupos de Auditoría de Sistemas, al apuntar al propósito de aseguramiento de las condiciones de calidad y seguridad de la información en la organización, cuando se refiere a los "atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos". Corrobora la importancia de la información como activo de valor para las organizaciones (ISO/IEC 17799/2005), que es necesario proteger adecuadamente para garantizar la continuidad del negocio, la maximización del retorno de la inversión y el aprovechamiento de las oportunidades del entorno, así como para disminuir y contrarrestar los riesgos y delitos que la amenazan.

La gestión confiable de la seguridad de la información en las organizaciones parte del establecimiento de políticas, estándares, procedimiento y controles eficientes, en natural concordancia con las características del negocio y, en ese sentido, el capítulo I de la Ley 1273 de 2009 contribuye a tal propósito, de la misma manera que los estándares nacionales e internacionales sobre administración eficiente de la información. El artículo 1 de la Ley 1273 de 2009 incorpora al Código Penal el Artículo 269A y complementa el tema relacionado con el "acceso abusivo a un sistema informático", que se manifiesta cuando el pirata informático o hacker aprovecha la vulnerabilidad en el acceso a los sistemas de información, o las deficiencias en los procedimientos de seguridad informática establecidos por las organizaciones, para extraer beneficios económicos o para indagar o demostrar la capacidad y recursos que ofrece la tecnología de la información. Cuando se presenta este abuso, en muchos casos, se observa que proviene de los mismos usuarios del sistema, tal como se evidencia en los informes anuales de la Pricewaterhouse Coopers, The global state information security y en estudios realizados por Cisco (2008), en los cuales se señala que el 42% de los tres casos de abuso más frecuentes corresponde a los detectados entre los empleados.

El artículo 269B contempla como delito la "obstaculización ilegítima del sistema informático o red de telecomunicación", y se origina cuando el hacker informático bloquea en forma ilegal un sistema o impide su ingreso por un tiempo, hasta cuando obtiene un beneficio por lo general económico. Aquí también se enmarca el acceso a cuentas de correo electrónico sin el debido consentimiento de sus propietarios y el manejo o bloqueo de las claves obtenidas de distinta forma.

El artículo 269C plantea la infracción relacionada con la "interceptación ilícita de datos informáticos", también considerada en el Artículo 3 del Título 1 de la Convención de Budapest de 2001. Se presenta cuando una persona, valiéndose de los recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transporte.

El delito relacionado con los "daños informáticos" está contemplado en el Artículo 269D y se comete cuando una persona que sin estar autorizada, modifica, altera, daña, borra, destruye o suprime datos del programa o de documentos electrónicos, en los recursos de las TIC.

El artículo 269E contempla el delito vinculado con el "uso de software malicioso" técnicamente denominado malware, ya generalizado en internet. Se presenta cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los recursos de las TIC.

El delito sobre "violación de datos personales" (hacking) lo trata el artículo 269F y está orientado a proteger los derechos fundamentales de la persona (como dignidad humana y libertad ideológica). Se da cuando un individuo sin estar facultado, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros.

El artículo 269G trata de la "suplantación de sitios web para capturar datos personales".
Sucede cuando el suplantador (pisher) o delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un hosting (espacio en un servidor) desde donde envía correos spam o engañosos (por ejemplo, empleos). Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base

de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye.

Las "Circunstancias de agravación punitiva", o aquellas situaciones que por agravantes aumentan la pena del delito (Artículo 269H/Ley 1273 de 2009). Estas condiciones se dan cuando el delito se comete en redes, sistemas informáticos y de comunicaciones del Estado o del sector financiero nacional o extranjero; o cuando se origina o promueve por un funcionario público; o cuando se da a conocer información confidencial en perjuicio de otro para obtener provecho propio o de terceros; o cuando se actúa con fines terroristas para atentar contra la seguridad o defensa nacional, o cuando se usa como instrumento a un tercero de buena fe.

Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala "por quien tuviere un vínculo contractual con el poseedor de la información".

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

Si la conducta descrita en los incisos del artículos 269: 269I: hurto por medios informáticos y semejantes y Artículo 269J: transferencia no consentida de activos. tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos ó telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea. En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información. Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información. Asimismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean concientes del nuevo rol que les corresponde en el nuevo mundo de la informática. Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas. Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

Conclusiones

Del presente proyecto hemos sacado las siguientes conclusiones:

El continuo avance de las Tecnologías de la información, está ocasionando, además de múltiples beneficios para la sociedad, la proliferación de los denominados delitos informáticos.

La delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio.

Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aún en países latinoamericanos, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.
Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de éstos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

Referencias Bibliográficas.

División de Investigacion y Desarrollo del Consejo Nacional de la Prevencion del Delito. (1981). Informatica y Delito. Estados Unidos.

Grupo Investigativo de Delitos Informaticos - GRIDI. (2009). L Investigacion tecnologica de los Delitos Informaticos. Bogota.

Guerra, B. J. Consideraciones para la regulación penal del delito informático. Sexta Ponencia: Delitos Informáticos - Abogacia e Informatica (pág. 3). Colegio de Abogados.

Perrin, S. (2005). Palabras en Juego: Enfoques Multiculturales sobre las Sociedades de la Información. Estados Unidos: C & Editions.

Redaccion Tecnologica de El Tiempo. (2011). Cada segundo hay 18 victimas de Ciberdelitos. El Tiempo .

Soiarz. (1990). Tecnologia Informatica y la Transformacion de la Criminalidad. Informe Nacional Sueco Presentado al XIII Congreso Internacional de Derecho Comparado , (págs. 285, 292). Suecia.

Taber, J. (1980). Una encuesta de los estudios de delitos informáticos . Estados Unidos: Informatica y Derecho Journal.

Tellez, V. J. (2005). Derecho Informatico. Mexico: Universidad Nacional de Mexico.

Tiedemann, K. (1983). La criminalidad económica como objeto de investigación. Cuadernos de Politica Criminal , 173 - 196.

Wiener, N. (1980). Cibernetica y Sociedad. Mexico: Editorial Mexico.

Acurio, S. Delitos Informáticos: generalidades. Recuperado en www.colombiadigital.net

Cuervo, J. Delitos Informáticos y Protección Penal a la Intimidad. Recuperado en www.derecho.org

Salellas, L. Sr Hadden Security Consulting. Recuperado en http://www.sr-hadden.com.ar

Salt, M. Informática y Delito. Recuperado en http://www.derecho.org.ar

Ley 1273 de 2009.