UNIVERSIDAD MILITAR
NUEVA GRANADA

COMISION DE CONDUCTAS PUNIBLES EN LA INTERNET EN COLOMBIA

SANDRA ROCIO QUINTERO CHAPARRO

SANDRAPATRICIA SUAREZ LEON

Leyenda del trabajo como:
Clase del trabajo realizado, tesis, monografía, pasantía, etc.
(Centrado)

Doctor JAIME ALBERTO SANDOVAL
Docente Universidad Militar Nueva Granada

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE DERECHO
MAESTRIA PROCEDIMIENTO PENAL
BOGOTA, D,C.
2012

COMISION DE CONDUCTAS PUNIBLES EN LA INTERNET EN COLOMBIA*

SANDRA ROCIO QUINTERO CHAPARRO*
SANDRAPATRICIA SUAREZ LEON*

Fecha de Recepción:
Fecha de aceptación:
Artículo Resultado de Proyecto de Investigación.

RESUMEN

Los delitos informáticos son considerados como crímenes electrónicos y de acuerdo a ello se relacionan como un problema que obstaculiza el avance de la sistematización. A partir de ello, es posible encontrar que en este tipo de delitos se observan conductas como el robo, la falsificación de documentos, los fraudes, los chantajesy la alteración de caudales públicos; por mencionar algunos.

Lo anterior tiene su origen en el uso que se le da en la actualidad a las computadoras, ya que se utilizan no solo como herramientas de apoyo para la ejecución de actividades educativas, de oficina, y en general en todos los ámbitos de orden legal, sino además porque estas se constituyen como medio eficaz para obtener todo tipo de información, gracias a los avances presentados por las redes de comunicación en coherencia con el desarrollo de las Tecnologías de la Información y Comunicación. Esto también admite la incursión de nuevas e impensables posibilidades de delincuencia a través de la manipulación fraudulenta de los computadores con ánimo lucrativo, generando la destrucción de programas o datos y la utilización indebida de la información que puede afectar la privacidad.

PALABRAS CLAVE: La Internet, Fraude, Tecnología, Conductas Penales.

PUNISHABLE CONDUCT COMMISSION ON THE INTERNET IN COLOMBIA

Abstract:
Computer crimes are considered crimes electronic classified as a problem for the advancement of systematization of them are seen as crimes theft, forgery, fraud, blackmail and altered public funds.

Today computers are used not only as ancillary support tools, but as an effective means to obtain and get all kinds of information, because they are present in almost all fields of modern life, which also supports new and unexpected possibilities of crime using computer tampering for profit, causing the destruction of programs or data and misuse of information that may affect privacy.

Key Words: the Internet, Fraud, Technology, Criminal Behavior

INTRODUCCIÓN

El presente artículo busca caracterizar las posibles líneas de investigación para el desarrollo de procedimientos judiciales partiendo de la delimitación del delito informático y su evolución, en la necesidad de identificar nuevas conductas que permitan proteger el alcance y límites de la delincuencia en el ciberespacio. Se fundamenta igualmente, en la prioridad por amparar los derechos vinculados a este campo entre los que se pueden incluir la protección de datos, el derecho a la intimidad, el análisis del Convenio del Consejo de Europa sobre el cibercrimen,

efectuado el 8 de noviembre de 2001[1] y tomando en cuenta las tendencias procesales en la lucha contra la delincuencia informática. Para finalizar se realiza el examen de la legislación interna, desde el Decreto 1748 de 1995[2] hasta la ley 1273 de 2009[3], junto con el estudio de algunas doctrinas polémicas planteadas por los juristas especializados en este tema.

El método de investigación seleccionado para el desarrollo del presente artículo se clasifica como analítico ya que se pretende mediante la observación y examen de un hecho en particular sobre los delitos informáticos, emitir un análisis en el cual se incluyan las causas, la naturaleza y los efectos de este nuevo tipo penal de acuerdo a lo descrito en la problemática propuesta.

Del mismo modo es importante anotar que se reseñaron los posibles campos de investigación, enfatizando en la comisión de conductas en el ciberespacio en aspectos como el juzgamiento y desde los principios de territorialidad y extraterritorialidad de la ley.

---

* SANDRA ROCIO QUINTERO CHAPARRO, Abogada, Especialista en Procedimiento Constitucional y Justicia Penal Militar, Docencia Universitaria, Derecho Internacional Aplicable a los Conflictos Armados (DICA), Instituciones Jurídico Penales, Candidata a Magister en Derecho Procesal Penal de la Universidad Militar Nueva Granada. SANDRA PATRICIA SUAREZ LEON, especialista en derecho penal, constitucional y justicia militar

[1]SANCHEZ BRAVO, A. "El Convenio del Consejo de Europa sobre cibercrimen: control vs. Libertadespúblicas", en Diario La Ley, núm.5528, 22 de abril de 2002.

[2] COLOMBIA, MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO. Decreto 1748 (12, octubre ,1995). Por el cual se dictan normas para la emisión, cálculo, redención y demás condiciones de los bonos pensionales y se reglamentan los Decretos leyes 656, 1299 y 1314 de 1994, y los artículos 115, siguientes y concordantes de la Ley 100 de 1993. Bogotá D.C.: El Ministerio, 1995. hasta la ley 1273 de 2009

[3] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009). 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. Bogotá, D.C., 2009. no.47.223.

1 LA INFORMÁTICA: UNA BREVE DEFINICIÓN

Según PLEIN[4] "la informática es la disciplina que se dedica a estudiar la información y sus componentes, así como la tecnología para manejarla, conservarla y utilizarla de manera eficiente y económica, con miras a facilitar su acceso a otras personas para producir mayores beneficios".

Por otra parte, JORDÁN FLOREZ[5] la define como la Ciencia que tiene como objeto propio de su conocimiento la información como método, la teoría de sistemas como instrumento operativo, la computación como ámbito de desarrollo, la organización como objetivo, racionalización, eficacia y eficiencia en la acción, a partir del control del proceso de producción y circulación de información como misión de contribuir a la libertad del ser humano y a la consolidación de la democracia como valor de un bien económico.

Esta ciencia, que procesa la información mediante el empleo de microprocesadores y redes de telecomunicaciones, concebida con criterios de eficiencia, es probablemente la de mayor desarrollo en los últimos años. Todos los días las grandes compañías fabricantes trabajan afanosamente en conseguir la tecnología que les permita crear supercomputadores con un grado de sofisticación tal, que en el algún momento de su desarrollo lograrán igualar la capacidad del cerebro humano. Cuando ello ocurra, la informática será la herramienta indispensable para la realización de todas las actividades humanas y el nivel de dependencia será tan alto en un mundo interconectado que una simple falla podrá ser suficiente para amenazar la existencia de la humanidad entera.

[4] PLEIN. Temática Didáctica Educativa, Grupo Editorial Norma, 1998, pág. 592

[5] JORDÁN FLOREZ, Fernando, La Informática Jurídica (Teoría y Práctica), primera edición, Universidad Piloto de Colombia, Centro de Investigaciones Interdisciplinarias, 1983, pág. 40

2 EL DELITO INFORMÁTICO Y SUS ANTECEDENTES EN COLOMBIA

Uno de los antecedentes que marcaron la comisión de delitos informáticos en el país fue el caso en el cual se cometió un robo de US$13.5 millones de dólares y que sucedió el 11 de mayo de 1983. Este fue planeado y ejecutado por Roberto Soto Prieto, quien solo necesitó interceptar las líneas de télex del Banco de la República, enviar un mensaje al Chase Manhattan Bank de Londres y transferir los fondos a su cuenta en el Morgan Guaranty Trust de Nueva York. Luego realizó una transferencia al Hapoalin de Zurich, y posteriormente a tres cuentas cifradas en Panamá y para finalmente cubrir cualquier rastro del dinero; el cual se desapareció en las Islas Azores y en la Isla Caimán[6].

Aunque el hecho fue impactante, su investigación culminó con éxito, registrándola en la sentencia No. 29188[7] de la Sala de Casación Penal de la Corte Suprema de Justicia. En ese fallo se condenó al abogado Guillermo Luis Vélez Murillo por el delito de violación de derechos de autor previsto en el artículo 51-4 de la Ley 44 de 1993[8], a la pena de 24 meses de prisión, multa de cinco salarios mínimos legales mensuales vigentes e inhabilitación para el ejercicio de derechos y funciones públicas por igual tiempo al de la pena privativa de la libertad. La Corte resume los hechos de la siguiente manera:

> El 8 de octubre de 1999, se practicó diligencia de allanamiento al inmueble ubicado en la carrera 19 No. 24-94 al sur de esta ciudad, toda vez que, según queja presentada por la Asociación Colombiana de Productores de Fonogramas – ASINCOL- se estaban duplicando de manera ilegal discos compactos, ofreciendo

[6]EL TIEMPO.COM. Doce secretos del robo de US 13.5 millones. [En línea]. [Recuperado el 20 de agosto de 2011]. Disponible en internet: <http://www.eltiempo.com/archivo/documento/MAM-140569>

[7]COLOMBIA, CORTE SUPREMA DE JUSTICIA. Sentencia de Casación No. 29188. M. P. Dr. José Leónidas Bustos Martínez

[8] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 44. (05, febrero, 1993). Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. Diario Oficial. Bogotá, D.C., 1993. no.40.740.

tal servicio con el respectivo anuncio en el diario El Tiempo y fueron halladas cuatro (4) computadoras que tenían instalado el sistema operativo WINDOWS 98, OFFICE 97 y 2000, programas antivirus marca NORTON, enciclopedia ENCARTA 99, sin la respectiva licencia de funcionamiento; estableciéndose que tenían tarjeta de sonido, unidad ZIP, con una capacidad mayor que los CDs normales, además se instalaron programas de diferentes casas productoras de SOFTWARE que permitían copiar el DC RW y que podían ser grabados o reproducidos, sin que contaran con la licencia de utilización[9].

Lo anterior llama la atención sobre el uso de las tecnologías que se emplean para mejorar los sistemas de comunicación y resalta el valor que tiene la red de internet dentro de un sistema global de comunicaciones, además de su incidencia en la posible vulneración de los derechos y libertades de las personas, lo cual tampoco ha pasado desapercibido para la Corte Constitucional que en reiterados fallos plantea que los avances de la sociedad en campos como el científico y tecnológico conllevan siempre nuevos retos para el derecho, en el entendido en que *"*El desarrollo de nuevas técnicas de producción y el desenvolvimiento de complejas formas de comunicación, por citar tan sólo dos ejemplos, tienen efectos directos en la estructura política y económica de la sociedad, que de acuerdo con su grado de incidencia en el tráfico jurídico, en la distribución de bienes y servicios escasos y en el ejercicio de los derechos fundamentales de las personas, demandan diferentes respuestas del ordenamiento jurídico"[10], por lo tanto hoy se debe discutir sobre una política pública criminal que se encamine en proteger y salvaguardar los bienes jurídicamente protegidos por el Estado en una creciente y

[9] Ibíd. Ley 44. (05, febrero, 1993).

[10] La relación entre el derecho y las nuevas formas de comunicación que supone Internet es una materia que ya ha sido objeto de estudio por parte de esta Corporación al revisar tratados internacionales que han incorporado dentro de sus disposiciones elementos específicos que aluden a la utilización de la red, así como las disposiciones que en el derecho interno se han expedido con el propósito de regular la materia. Cfr., *e.g.*, Corte Constitucional Sentencia C-622 de 2000 M.P. Fabio Morón Díaz. Acción pública de inconstitucionalidad contra la Ley 527 de 1999 y, particularmente sus artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45, "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

cada vez mas un desarrollo protector de nuevas formas de delincuencia en lo que tiene que ver con la comisión de conductas punibles en la internet.

Consecuencia de lo anterior se destacan, entre otras muchas decisiones de la Corte Constitucional, con respecto al tema, la Sentencia C-831 de agosto 8 de 2001[11], que trata sobre el mensaje de datos, firmas digitales y entidades de Certificación, en ese sentido también se enfatiza en la Sentencia C-1147 de octubre 31 de 2001[12], que abordó el tema del Registro Mercantil de Páginas Web, Intimidad y habeas data, y facultades de la administración tributaria-transacciones en Internet.

La Sentencia C-662 de junio 8 de 2000[13], que se pronunció sobre la constitucionalidad de algunos artículos de la Ley 527 de 1999 relacionados con los mensajes electrónicos de datos y comercio electrónico; las firmas digitales; las entidades de certificación y, la admisibilidad y fuerza probatoria de los mensajes de datos y la Sentencia T- 414 de junio 16 de 1992, que abarca temas tan sensibles como el derecho a la intimidad, el derecho a la información son otros ejemplos. La libertad informática, el derecho a la información, la irrupción de nuevas tecnologías, la libertad personal, la intimidad, el dato y su "propiedad", perfiles de datos, derecho constitucional informático, informatización social e insuficiente protección jurídica también se inscribem en esta dinámica[14].

Llama la atención que en muchos de estos fallos, la Corte denunció "la inexistencia de mecanismos ordinarios de protección de los derechos relacionados con la libertad informática[15], y la ausencia de una ley estatutaria que regule con

[11] COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C- 381/01 M. P. Álvaro Tafur Galvis.
[12] COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C- 1147/01 M. P. Manuel José Cepeda Espinosa
[13] COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-662/00 M. P. Fabio Morón Díaz
[14] SENTENCIA. Expediente RE. 125. M.P. Rodrigo Escobar Gil. Mayo de 2003.
[15] Sobre la inexistencia de una regulación comprensiva del poder informático, y la insuficiencia de los mecanismos de protección actualmente vigentes, la Corte se ha pronunciado en repetidas

amplitud esta materia"[16] por considerar que esta cuestión es de suma gravedad, tomó la iniciativa de invitar al Congreso de la República a la Procuraduría General de la Nación y a la Defensoría del Pueblo, "para que en la medida de sus posibilidades presenten e impulsen respectivamente, un proyecto de ley estatutaria que ofrezca una regulación amplia, consistente e integral en la materia"[17], teniendo en cuanta el articulo 2 del código penal (ley 599 de 2000) con el fin de proteger el derecho a la autodeterminación informática, salvaguardar la información contenida en las bases de datos y establecer sanciones para las entidades administradoras de bases de datos y para desestimular y castigar prácticas indebidas en ejercicio del poder informático con fundamento jurídico, las normas internas sobre el particular y sobre todo los tratados y convenios internacionales ratificados por Colombia.

Por consiguiente la preocupación de la Corte no es infundada. El crecimiento que siguen teniendo las redes sociales y herramientas asociadas, lleva a que los usuarios consignen datos personales, algunos que no comparten, y otros que sólo comparten con ciertos grupos de amigos o contactos, hace urgente la implementación de nuevas estrategias tecnológicas y legales para proteger los datos privados, asegurar su no divulgación sin el consentimiento del titular e imponer sanciones a quienes contravengan estas disposiciones.

El problema va más allá de los niveles de confianza que ofrecen las redes sociales de no exponer información reservada de sus usuarios, y pasa por las amenazas serias y reales de que estas redes pueden ser objeto de ataques para apoderarse

---

ocasiones. Así, en las sentencias T-414 de 1992, SU-082 de 1995, T-307 de 1999 entre otras. En esta última, frente al problema de la insuficiencia de los mecanismos de protección, afirmó: "estos mecanismos resultan algunas veces insuficientes para la garantía plena, pronta y efectiva de los derechos comprometidos en el proceso informático. En efecto, no sólo se trata de garantías *ex post*, que no establecen *ab initio* reglas claras para todas las partes comprometidas en este proceso, sino que muchas veces no tienen el alcance técnico que se requiere para lograr la verdadera protección de todos los bienes e intereses que se encuentran en juego."

[16] Así en sentencias T-414 de 1992, SU-082 de 1995, SU-089 de 1995 y T-307 de 1999.

[17] Sentencia T-729 de 2002. Magistrado Ponente: Dr. Eduardo Montealegre Lynett.

ilícitamente de las bases de datos. Ataques que pueden provenir de las mismas entidades oficiales del Estado, al estilo de las interceptaciones telefónicas no autorizadas efectuadas por el DAS, popularmente conocidas como “chuzadas”, o por piratas informáticos que buscan apoderarse de información sensible con los más disímiles propósitos.

Si no se legisla urgentemente sobre la materia y se promulgan normas que protejan eficazmente a los ciudadanos que permanecen indefensos frente al abuso del “poder informático” ejercido por las autoridades públicas o los particulares que, de un modo o de otro, recopilan, sistematizan y utilizan sus datos personales y eventualmente pueden vulnerar derechos fundamentales como la intimidad y la libre autodeterminación reconocidos por la Constitución Política a todas las personas.

3 EL DERECHO INFORMATICO EN COLOMBIA ANTES DE LA CONSTITUCIÓN DE 1991

En Colombia, el derecho de acceso a la información general antes de la Constitución de 1991[18] aparece reglamentado en normas como el artículo 252del Código de Procedimiento Civil[19] que trata sobre los documentos u otros instrumentos que se asimilen (los discos electromagnéticos, planos, fotografías, etc.); la Ley 57 de 1985[20] (que amplía el derecho ya formado en la Ley 4 de 1913, (artículo 342)[21] para los documentos públicos; la Ley 16 de 1972 del 20 de diciembre[22] (regula el derecho a la información y en forma especial el derecho a

[18] CONSTITUCIÓN POLÍTICA DE 1991
[19]COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1400. (21, septiembre, 1970). Por los cuales se expide el Código de Procedimiento Civil. Diario Oficial. Bogotá, D.C., 1970. no.33.150.Art. 252.
[20] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 57 (12, Julio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. Diario Oficial. Bogotá, D.C., 1985. no.37.056.
[21] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 4 (22, Agosto, 1913). Sobre régimen político y municipal. Diario Oficial. Bogotá, D.C., 1913. no.14.974.Art. 342
[22]La ley 16 de 1972, de 20 de diciembre

rectificación y respuesta) y el Código Contencioso Administrativo (C.C.A de 1984-89)[23] para el acceso a los documentos por origen o asimilación (incluidos los documentos informáticos, electrónicos y telemáticos) o cualquiera otro que contenga información pública o de carácter particular, (artículo 14 Ley 16/72)[24].

No obstante, es obvio que el auge del Comercio Electrónico y su desarrollo lo que ha llevado a plantear la necesidad de contar con instrumentos eficaces que regulen y controlen el tráfico electrónico en el objetivo de proteger las actividades comerciales teniendo en cuenta que en la actualidad se efectúan constantemente por este medio, no solo en beneficio de quienes integran la actividad comercial; es decir, tanto compradores como comerciantes de bienes y servicios, sino de parte de quienes conforman el sector oficial en el recaudo de impuestos a este sector.

4 LA CONSTITUCIÓN DE 1991 FRENTE AL DERECHO INFORMÁTICO

La Constitución Política mostró un nuevo panorama en cuanto a la actualización de las normas y entre ellas se contempla las que se relacionan con los avances tecnológicos y científicos y su injerencia dentro de la vulneración de las libertades fundamentales de los colombianos. Con esta nueva reglamentación se protegen de esta forma, los derechos a la integridad personal, intimidad, imagen y buen nombre, el derecho de rectificación y el derecho de información que plasma la visión *ius*-informática de los derechos fundamentales, aplicable también al derecho a la intimidad.

Esta disposición se justifica históricamente en el surgimiento de lo que se denomina “el poder informático” conjugado con las infinitas posibilidades del manejo indiscriminado de los datos personales, frente a lo cual la jurisprudencia constitucional ha reconocido y protegido el derecho a la autodeterminación

[23] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 01(02, enero, 1984). Por el cual se reforma el Código Contencioso Administrativo. Diario Oficial. Bogotá, D.C., 1984.
[24] Articulo 14. Ley 16 de 1972 óp. Cit.

informática y el derecho al *habeas data*, que abarca desde el derecho a la libertad de información hasta el acceso, actualización, rectificación, bloqueo y cancelación de datos informáticos, electrónicos o telemáticos.

Para ilustrar mejor la panorámica nacional contemplada por los constituyentes, se presenta el ejemplo de DataCrédito, una institución privada que opera como central de información y maneja los datos financieros de todos los ciudadanos que de algún modo han estado vinculados con las entidades bancarias, sea porque han abierto una cuenta o porque han conseguido o tramitado un préstamo. Esta entidad recibe, procesa, almacena y suministra información sobre el historial crediticio, manifestando la forma como las personas y las empresas han cumplido sus obligaciones con los bancos, cooperativas, almacenes o cualquiera otra empresa que presta dinero o vende a crédito. De la información positiva o negativa que brinde sobre los clientes de cada entidad afiliada, depende el tratamiento que ellos reciban en sus operaciones comerciales y no son pocas las ocasiones en que Datacrédito o las entidades financieras han usado discrecionalmente la información consignada en su poder, sin que los directamente afectados se enteren o puedan oponerse, ya sea negando la expedición de certificaciones sobre sus datos personales a quienes lo solicitan; no rectificando a tiempo los reportes negativos, aunque los clientes se encuentren a paz y salvo; o suministrando datos no autorizados a otras corporaciones o empresas para que les nieguen servicios financieros a determinadas personas o los recluten como potenciales clientes.

La Constitución de 1991 buscó frenar el abuso de ese “poder informático” estableciendo mecanismos de protección; siendo la acción de tutela y la autorregulación los más conocidos. Mediante la primera se salvaguardan unas garantías mínimas del ser humano cuando se ve expuesto a la violación del derecho a la intimidad por revelación de datos suyos no autorizados y que no pueden ser de conocimiento de otros, sin su consentimiento. La autorregulación,

por su parte, impone a las mismas entidades la protección de los derechos ciudadanos en el funcionamiento de sus bases de datos, entre los cuales se destaca la posibilidad que tiene el titular de la información de consultar la historia de crédito, conocer qué usuarios han consultado su historia de crédito en un periodo determinado, presentar las reclamaciones del caso cuando se ha suministrado información incorrecta, exigir el cumplimiento del plazo legal para mantener la información negativa y que la información que se reporte respete la finalidad para la que fue solicitada. Igual ocurre en otros contextos como el de la salud o el judicial, en los que se maneja información de las personas.

De este modo, hoy por hoy, toda información que le pertenezca a una persona y esté bajo el control de los poderes públicos o de particulares, podrá ser actualizada, rectificada o cancelada, sea cual fuere el formato en que esté recogida, almacenada, transmitida o difundida, es decir, en referencia a mecanismos manuales o informáticos.

5 NORMAS EXPEDIDAS EN VIGENCIA DE LA CONSTITUCIÓN POLÍTICA DE 1991

Entre las normas reguladoras del procedimiento informatizado de datos personales de carácter económico, financiero y bancario privado, expedidas al amparo de la nueva Constitución, se destaca la Ley 1266 de 2008[25] que se ajusta a los artículos 15 y 20 Constitucional en lo que concierne a las facultades inherentes al derecho de *habeas data*.

[25] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266 (31, Diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no.47.219.

También existen otras normas contempladas en leyes, decretos, resoluciones y circulares que incluyen igualmente disposiciones relativas a la informática tales como el Decreto 1105 de 1992[26] que normalizó los procedimientos aduaneros a través del sistema informático de aduanas y los requisitos para la conexión directa al sistema informático de la aduana. La Ley 98 de 1993[27] para cuyos fines considera libros, revistas, folletos, coleccionables seriados o publicaciones de carácter científico o cultural, los editados, producidos e impresos en la República de Colombia, de autor nacional o extranjero, en base papel o publicados en medios electro-magnéticos.

En el Decreto 1748 de 1995[28] se define el concepto de Archivo informático: como toda información almacenada en un medio magnético, óptico o similar, a la cual sólo se puede tener acceso, mediante un soporte lógico adecuado, a través de un computador electrónico. Además en la Resolución 3316 de 1997(junio 3)[29] se reglamenta el uso de software aplicativo para la facturación. La Ley 383 de julio 10 de 1997[30] por la cual se expiden normas tendientes a fortalecer la lucha contra la evasión y el contrabando, donde se implementa la tarjeta fiscal en programa de computador. Y el artículo 34 de la Ley 365 de 1997[31] que regula las transacciones electrónicas.

---

[26] COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 1105(01, Julio, 1992). Por el cual se modifica parcialmente el régimen de aduanas. Diario Oficial. Bogotá, D.C., 1992. no.03.

[27] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 98 (22, Diciembre, 1998). Por medio de la cual se dictan normas sobre democratización y fomento del libro colombiano. Diario Oficial. Bogotá, D.C., 1993. no.41.151.

[28] COLOMBIA. MINISTERIO DE HACIENDA Y CRÉDITO PÙBLICO. Decreto 1748 (13, Octubre, 1995). Por el cual se dictan normas para la emisión, cálculo, redención y demás condiciones de los bonos pensiónales y se reglamentan los Decretos leyes 656, 1299 y 1314 de 1994, y los artículos 115, siguientes y concordantes de la Ley 100 de 1993. Diario Oficial. Bogotá, D.C., 1995. no.42. 049.

[29] RESOLUCIÓN NÚMERO 3316 DE 1997.

[30] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 383 (10, Julio, 1997). Por la cual se expiden normas tendientes a fortalecer la lucha contra la evasión y el contrabando, y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1997. no.43. 083.

[31] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 365 (21, Febrero, 1997). Por la cual se establecen normas tendientes a combatir la delincuencia organizada y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1997. no.42. 987. Art.34

También cobra importancia el Decreto 2150 de 1995[32] en el cual se suprimen y reforman las regulaciones, procedimientos o trámites innecesarios establecidos en la Administración Pública, y además se autoriza la cancelación de cuentas monetarias a través de transferencias electrónicas de fondos previendo que el envío de información por fax o cualquier otro medio de transmisión electrónica proveniente de una entidad pública prestará mérito suficiente y servirá de prueba en la actuación de que se trate siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite.

De igual modo le impone a las entidades de la Administración Pública el deber de facilitar la recepción y envío de documentos, propuestas o solicitudes y sus respectivas respuestas por medio de correo certificado y por correo electrónico; las obliga a habilitar sistemas de transmisión electrónica de datos para que los usuarios envíen o reciban información requerida en sus actuaciones frente a la administración; exigiendo que en ningún caso puedan limitar el uso de tecnologías para el archivo documental por parte de los particulares, sin perjuicio de los estándares tecnológicos que adopten para el cumplimiento de algunas de las obligaciones legales a cargo de los particulares.

Por último se incluyen la Ley 527 de 1999[33] que define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones y el Decreto 1747 de 2000[34] que reglamenta parcialmente la Ley 527 de 1999, en lo

[32] COLOMBIA. Ministerio y de justicia. Decreto 2150 (06, Diciembre, 1995). Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.. Diario Oficial. Bogotá, D.C., 1995. no.42. 137.
[33] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 (18, Agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999. no.43.673.
[34] COLOMBIA. MINISTERIO DE DESARROLLO ECONÓMICO. Decreto 1747 (14, Septiembre, 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las

relacionado con las entidades de certificación, los certificados y las firmas digitales.

Estas normas procuran otorgarle reconocimiento jurídico al intercambio de datos electrónicos que se impone cada vez con mayor fuerza en el mundo. Para nadie es un secreto que las personas utilizan los sistemas de comunicación electrónico para muchas de sus operaciones cotidianas, tales como las transferencias de dinero entre cuentas bancarias, el pago de facturas, la adquisición de todo tipo de bienes y servicios, peticiones y reclamos a las autoridades o particulares encargados de determinadas actividades, o simplemente para conocer personas y mantener una comunicación constante con sus relacionados.

Es un hecho inevitable que el papel y la tinta utilizados en las comunicaciones de antaño son hoy remplazadospor un soporte material, que es la memoria de masa sobre la que se graban los datos y los impulsos electromagnéticos que fijan su contenido. Sin embargo es necesario garantizar desde las leyes del Estado la autenticidad e integridad de esos productos informáticos, al igual que su confidencialidad o reserva, en los mismos términos en que se garantiza la de los documentos originales, porque de no ser así este mundo de relaciones interconectadas electrónicamente se convierte en un caos imposible de controlar.

6 EL DELITO INFORMÁTICO COMO UNA NUEVA MODALIDAD DE CONDUCTA DELICTIVA

A medida que el mundo avanza y se crean nuevos desarrollos tecnológicos, el Derecho Penal ha tenido que introducir nuevas conductas penales con el ánimo de reprimir los atentados contra la vida, la integridad personal, los crímenes contra el

---

entidades de certificación, los certificados y las firmas digitales. Diario Oficial. Bogotá, D.C., 2000. no.44.160.

patrimonio económico, las defraudaciones y demás conductas que atentan contra la supervivencia en sociedad.

En la aplicación de la Ley penal los diferentes países van estableciendo normas de convivencia y de restricción con las cuales se pretende evitar que se realicen ilícitos. Con el surgimiento de las nuevas tecnologías los criminales ampliaron sus acciones cometiendo diferentes delitos en los cuales se utilizan ese tipo de mecanismos evidenciando la necesidad de producir reformas urgentes y adiciones a las leyes penales para lidiar contra estos nuevos delitos y proteger la vida, honra y bienes de las personas.

En este frente, Colombia ha logrado un avance muy importante, pues ahora está castigando el robo de información personal con cárcel entre cuatro y ocho años. Y los delincuentes son procesados por dos delitos: robo de datos personales y hurto, con lo que las penas se hacen más duras[35].

Aun así, las noticias sobre la incidencia de estos nuevos delitos son alarmantes, según las autoridades colombianas, las bandas criminales ya no se concentran en robar dinero. Ahora su objetivo es la información sobre los clientes bancarios y para ese propósito usan técnicas más complejas que la simple clonación de una tarjeta. Se valen de lo que los expertos llaman “ingeniería social”, que consiste en reconstruir el perfil de una persona para obtener información clave como cuentas de correo, el nombre de los bancos donde la potencial víctima tiene sus cuentas, números telefónicos, actividades que realizan a diario, y todo lo que les sirva para perpetrar el delito. Las técnicas más empleadas incluyen llamadas por celular,

[35]COLOMBIA. Ley 1273 de 2009.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 47223. Enero 2009

envío de correos electrónicos con virus, acceso a redes sociales como Facebook y Twitter y otras[36].

Es precisamente en este contexto en el cual se desarrolla la presente línea de investigación, fundamentada en la conceptualización más aceptada por los penalistas para el delito informático, y complementada con la descripción de las conductas típicas informáticas que tienen características punibles, así como con el estudio del Convenio del Consejo de Europa sobre el Cibercrimen, efectuado el 8 de noviembre de 2001[37], y que se establece como la principal herramienta supranacional creada hasta el momento para el combate de estos delitos que no respetan fronteras, países ni nacionalidades. Finalmente se realiza un resumen de las últimas disposiciones en legislación interna dentro de las cuales se incluyen las nuevas conductas punibles derivadas del uso criminal de los medios informáticos.

Como objeto final también se reseñan los posibles campos de investigación principalmente lo relacionado con la comisión de conductas en el ciberespacio que tienen que ver con el juzgamiento basado en los principios de territorialidad y extraterritorialidad de la ley.

Como punto de partida se encuentra que el delito informático es definido y clasificado por los penalistas de la siguiente manera, como "todo comportamiento ilegal o contrario a la ética o aquel que no está autorizado y que conlleva un tratamiento automático de datos o de trasmisión de los mismos"[38].

[36] COLOMBIA, CORTE SUPREMA DE JUSTICIA. Sentencia de Casación No. 29188. M. P. Dr. José Leónidas Bustos Martínez
[37] Óp. Cit., Convenio del Consejo de Europa sobre el cibercrimen,
[38] ACURIO DEL PINO, Santiago. Delitos informáticos: Generalidades. [En línea]. [Consultado el 18 de noviembre de 2011] Disponible. En: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>

Igualmente TELLEZ VALDÉS[39] clasifica a los delitos informáticos según dos pautas fundamentales; el uso del "computador" como instrumento o medio, y el computador como fin u objetivo. Así, cuando se clasifican los delitos como instrumento o medio, dice que se consideran como tales los que contienen conductas criminógenas que se valen de la computadora como "método, medio, o símbolo en la comisión del ilícito"[40].

DE LA LUZ LIMA[41] propone una clasificación basada en tres criterios de calificación de la conducta. Dice que hay quienes "utilizan la tecnología electrónica como método, los que utilizan la tecnología electrónica como medio y los que utilizan la tecnología electrónica como fin".

Como método el delito informático es aquel en el cual los sujetos utilizan métodos electrónicos para cometer el ilícito, como medio son consideradas aquellas conductas criminales en donde, para realizar un delito, se usa una computadora como elemento por el cual se lleva a cabo. Y como fin, son las conductas criminales en contra de *la "entidad física del objeto o máquina electrónica o su material con objeto de dañarla"*.[42]

PÉREZ LUÑO[43] hace la clasificación a partir del criterio objetivo, subjetivo y funcional, así:

- Desde el punto de vista subjetivo, distinguiendo el tipo de los delincuentes informáticos, pues observa a los sujetos y a sus características, como por ejemplo en el caso de un delito de cuello blanco (es decir que tiene una relación de poder

[39] TELLEZ VALDÉS, J. Derecho Informático, Editorial McGraw Hill, México, 1997, pág. 105
[40] Ibíd. Derecho Informático
[41] Ibíd. Derecho Informático
[42] Ibíd. Derecho Informático
[43] Citado por Cuervo Álvarez, José, Delitos informáticos: protección penal de la intimidad.[En línea]. [Consultado el 18 de noviembre de 2011] Disponible en internet: <http://publicaciones .derecho.org/redi/No._06_-_Enero_de_1999/cuervo>

frente al sistema), o si es un delito realizado por personas del común, (no se tiene una posición favorable).

- Desde el punto de vista objetivo. Examina los daños que las conductas han ocasionado, definiendo al delito y su *modus operandi* según el tipo de delito, así:

1. Los fraudes (manipulaciones contra los sistemas de procesamiento de datos)
2. El sabotaje informático: (bombas lógicas, virus informáticos)
3. El espionaje informático y el robo o hurto de software
4. El robo de servicios
5. El acceso no autorizado a servicios informáticos

- Desde el punto de vista funcional, considera el proceso informático o de procesamiento de datos y, a partir de éste, propone una nueva clasificación de delitos que van desde atentados contra la fase de entrada del sistema, atentados contra la fase de salida del sistema, atentados contra los programas del sistema y atentados contra la elaboración, procesamiento de datos y comunicación telemática[44].

BAÓN RAMÍREZ establece que "dentro de la criminalidad informática se pueden distinguir dos grandes grupos de delitos" [45]:

- Un primer grupo se refiere a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática. Así, distinguen los delitos en: Relativos a la destrucción o sustracción de programas o de material; relativos a la alteración,

[44]http://www.alfa-redi.org/rdi-articulo.shtml?x=207
[45] BAÓN RAMÍREZ, ROGELIO. Visión general de la informática en el nuevo Código Penal, en ámbito Jurídico de las tecnologías de la información, cuadernos de Derecho Judicial, Escuela Judicial/ Consejo General de Poder Judicial, Madrid, 1996, págs. 79 a 112

destrucción o reproducción de datos almacenados y los referidos a la utilización indebida de ordenadores.

- En un segundo grupo se encuadraría la comisión de los delitos más tradicionales que van contra bienes jurídicos protegidos como: la intimidad, la propiedad, la propiedad industrial o intelectual, la fe pública, el buen funcionamiento de la administración y la seguridad exterior en interior del Estado.

  ROMERO CASABONA[46] analiza las distintas facetas de lo que llama "la repercusiones de las nuevas tecnologías de la información en el Derecho Penal" y de esta forma, divide su análisis en diferentes apartados bajo los títulos de: La protección Penal de la intimidad informática, la informática como factor criminógeno en el tráfico económico, el fraude informático, implicaciones penales de las manipulaciones en cajeros automáticos, mediante tarjeas provistas de bandas magnéticas, y las agresiones a los sistemas o elementos informáticos.

Los conceptos incluidos evidencian una amenaza en contra de la seguridad de la sociedad, la cual depende cada vez más de los avances de las comunicaciones y la informática como apoyo en las diferentes actividades de las personas, no solo profesionales sino en general en todas las dimensiones, mostrada a partir de situaciones como el pago de una factura por una compra cualquiera y llegando hasta los sofisticados sistemas que emplean las naciones para preservar la confidencialidad de su información más sensible, cuya vulneración sin duda, deja en riesgo su seguridad interna e incluso la paz mundial, como lo demostró el reciente escándalo desatado por el portal *WikiLeacks*, al filtrar cerca de 250.000 cables diplomáticos de embajadas y misiones estadounidenses, obtenidos ilegalmente.

[46] Citado por Cuervo Álvarez, José. Op. Cit., pág. 2

En cualquier caso queda demostrado que a partir de las nuevas dinámicas que dependen o se apoyan casi totalmente en la tecnologías, aparece igualmente una modalidad delincuencial frente a la cual tanto las organizaciones estatales como privadas no tienen los elementos sustanciales que le permitan enfrentar las intrusiones en los sistemas de seguridad informáticos y que a su vez, otorguen los mecanismos que ofrezcan los medios para sancionar el extenso listado de conductas punibles que se posibilitan desde el empleo de las plataformas informáticas y el acceso a computadores y redes como internet, representando un reto de grandes dimensiones para los organismos de investigación y los tribunales que deberán disponer de todos sus recursos y hacer uso de mecanismos de cooperación para prevenir los delitos e impedir que estos se lleven a cabo, advertir oportunamente los indicios que permitan controlar el trabajo de los delincuentes, tomar el control, recoger y analizar las evidencias, generar los reportes sobre lo ocurrido, judicializar y castigar a los autores.

Es innegable también que este fenómeno provocó preocupación en el mundo, a lo que se suma ventaja evidente que tienen los delincuentes informáticos ya que llevan la iniciativa, poseen la tecnología y manipulan la ciencia. Por ello, medidas como incrementar la seguridad informática, investigar y mejorar los mecanismos de encriptación estándar, educar a los usuarios y revisar o formular legislaciones referentes al caso resultan insuficientes cuando las redes son constantemente vulneradas.

En Colombia, el delito informático se incluye en la noción de la protección de la información y de los datos, las cuales se dividen entre las conductas típicas informáticas que podrían atentar contra la confidencialidad, la integridad la disponibilidad de los datos y de los sistemas informáticos y en los atentados informáticos que comprenden el hurto de medios informáticos y la transferencia no

consentida de activos que pueden ser incluidos en los diferentes estatutos penales, a saber:

- Manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información. fraude informático; que se realiza a través de la uso de un sistema o programa que manipula la conexión via modem de un computador[47].

- Introducción de datos falsos, falsear, logrando movimientos artificiales en transacciones de una empresa o sociedad con el fin de otorgarle solvencia económica a una persona jurídica o natural que no la tiene. “También puede ocurrir de publicar datos sensibles, como los referentes a las convicciones religiosas, políticas o a la vida íntima de las personas”[48].

- Caballo de Troya: Virus Informático que crea rutas distintas en un programa para que actúen en forma distinta a como estaba previsto[49].

- Técnica de salami: consiste en ejecutar un programa el cual remite instrucciones para que transfiera dineros de una varias cuentas a una en particular el dinero que se saca de estas cuentas es en una cantidad mínima para que los titulares de las mismas no se detecte de forma fácil. Es una manera ingeniosa de redondear cuentas que consiste en dar una “instrucción al sistema informático para que transfiera a una determinada cuenta, los dineros que se descuenten por el redondeo”[50].

---

[47] ACURIO DEL PINIO, Santiago. Delitos informáticos: Generalidades. [En línea]. [Recuperado el 25 de agosto de 2011]. Disponible. En: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf>

[48]DELITOS INFORMÁTICOS. [En línea]. [Recuperado el 25 de agosto de 2011]. Disponible en internet: <http://wwwmiderecho.blogspot.com/2008_04_01_archive.html

[49]Ibíd. DELITOS INFORMÁTICOS

[50]Ibíd. DELITOS INFORMÁTICOS

- Llave no autorizada: ingresa ha cualquier archivo la computadora por muy protegido que esté, con el fin de alterar, borrar, copiar o utilizar, en cualquier forma no permitida, datos almacenados en el ordenador[51].

- Bombas lógicas o cronológicas: se ingresa el virus a la computadora para que este tiempo después produzca daños en los sistemas operativos con el fin de que pareciere ser un sabotaje, estas bombas lógicas ocasionan destrucción de archivos paraliza el funcionamiento del sistema debido a la difícil forma de detectarlos es utilizado para extorsionar pidiendo dinero para no destruir información toda vez que la persona que instala este programa es el que determina a que momento va ha estallar el virus en la computadora[52].

- Divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa[53].

- Planificación y simulación de un delito informático antes de realizarlo, para ver qué repercusión va a tener en los asientos contables de una empresa[54].

- Hurto calificado por transacciones electrónicas de fondos: cuando se utiliza el sistema de transferencias de fondos o cuando se viola el empleo de claves secretas[55].

- Gusanos: Se infiltra en programas originales para modificar o destruir los datos pero es diferente del virus, es menos dañino que el virus pero las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus, es decir, un programa gusano que posteriormente se

[51]Ibíd. DELITOS INFORMÁTICOS
[52]Ibíd. DELITOS INFORMÁTICOS
[53]Ibíd. DELITOS INFORMÁTICOS
[54]Ibíd. DELITOS INFORMÁTICOS
[55]Ibíd. EL DELITO INFORMÁTICO

destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego destruirse[56].

- Homicidio: “El homicidio informático” sirve para alterar historias clínicas digitalizadas ingresando a la computadora del médico que formula a su paciente determinado medicamento alterando la correspondiente formula y en relación a esta se produce la muerte.

7 CONDUCTAS QUE ATENTAN CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS

En los últimos años son comunes las noticias sobre virus informáticos, gusanos maliciosos, ataques cibernéticos o fraudes en línea, todas estas palabras se han convertido en elementos familiares, a medida que el internet se extiende y la seguridad tecnológica se convierte en una constante preocupación, pues las amenazas virtuales como el robo de datos, ciberataques e infiltraciones son un lugar común en la era digital.

Las siguientes son algunas de las prácticas más habituales empleadas por los delincuentes informáticos:

a. Interceptación de los datos informáticos

Tiene relación con interceptar datos informáticos, en su origen o destino, o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes

[56]http://junisita.galeon.com/#gusano

de un sistema informático que los trasporte, sin que medie orden judicial previa, es conducta que tipifica la presente modalidad.

Así en este contexto se trata de sancionar la interceptación ilícita de los datos informáticos pero asumiendo esta ilegalidad desde la separación de una formalidad, orden judicial previa o la detección de la información contenida en el sistema o de sus emisiones electromagnéticas.

La interceptación del correo electrónico o *e-mail* también se constituye en una acción ilegal ya que este al igual que el correo tradicional está protegido puesto que se encuadra dentro de la definición de comunicación, pero con el agravante que la interceptación telemática de correo electrónico implica necesariamente acceso al sistema informático[57].

b. Daño informático

Esta conducta es originada por todas las personas que no se encuentren facultadas para ello o que destruyan, dañen, borren, deterioren, alteren o supriman datos informáticos, con un comportamiento intencional, perdiendo la integridad del sistema, del dato informático o de sus partes o componentes lógicos. Cualquiera de estas conductas puede recaer sobre los elementos informáticos mencionados. Sin embargo, se introduce la expresión Componentes lógicos que se constituyen específicamente desde lo que en informática se denomina como hardware y que se refiere al conjunto de componentes que conforman la parte material o física de una computadora, a diferencia del software que se refiere a los componentes lógicos o intangibles[58].

[57]MÁRQUEZ ESCOBAR, Carlos Pablo. El delito informático. Leyer Editorial. Pág. 122.

[58]ARBOLEDA VALLEJO, Mario, RUIZ SALAZAR, José Armando. Manual de Derecho Penal. 10ª Ed.2010. Leyer Editorial. Pág. 1000.

7.3 Uso de software malicioso

Este delito se presenta cuando sin estar facultado para ello, se produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos. El software se refiere a los componentes lógicos (intangibles) de una computadora, que tienen por objeto infiltrarse en el sistema y dañar la computadora sin el previo consentimiento del propietario. En la informática se le conoce con el nombre de malware[59].

Por definición se trata de programas no deseados y pueden incluir códigos para instalar barras de herramientas en los navegadores, anuncios publicitarios, o para descargar programas sin que el usuario lo sepa.

Los programas suelen ser utilizados también por quienes operan redes criminales en internet. Según la empresa de seguridad Symantec, cerca del 30% de los programas maliciosos provienen de China, seguidos de Rumania[60].

7.4 Violación de datos personales

Se produce a partir de que una persona buscando el provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales, contenidos en ficheros, archivos, bases de datos o medios semejantes.

[59]ARBOLEDA VALLEJO, Mario, RUIZ SALAZAR, José Armando. Op. Cit. Pág. 1001.
[60]BBC MUNDO. Todo lo que usted quería saber sobre seguridad informática. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://www.bbc.co.uk/mundo/noticias/2011/03/110324_1458_guia_preguntas_seguridad_informatica_virus_tlquqssynsaap_dc.shtml>

El objeto jurídico de la conducta parece ser la información genéricamente considerada, otros mencionan que es la intimidad[61]. Pero como ya se ha mencionado anteriormente, la intimidad tiene como objeto la información privada.

La conducta es antijurídica debido a que accede a un conjunto de datos almacenados por el titular de la base de datos, o por aquél que ha generado dicho registro de datos para su uso personal o para el uso autorizado de terceros. Así, toda la información contenida en ésta, y protegida en éste, es en un principio lo que el derecho busca proteger[62].

7.5 Suplantación de sitios web para capturar datos personales

Esta es la última de las modalidades delictivas que atenta contra la confidencialidad, integridad y la disponibilidad de datos y de los sistemas informáticos, suplantando sitios web para capturar datos personales, conducta a la cual incurre quien, obrando ilícitamente y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlace o ventanas emergentes, al igual que quien modifique el sistema de resolución de nombres de dominio.

A ésta figura se le conoce en el mundo informático como el phishing (pescar en inglés), que no significa otra cosa que la suplantación de identidad, la cual se apropia de datos confidenciales de los usuarios. En la red se utiliza el envío masivo de correos electrónicos que simulan proceder de entidades reconocidas que incentivan al internauta a realizar actualización de datos personales a través de una página que imita a la original, para posteriormente utilizarlos ilícitamente

[61] LEÓN MONCALEANO, William F. De la comunicación a la informática jurídica penal y bancaria, Bogotá, ediciones Doctrina y Ley, 2001, pág. 153
[62] MÁRQUEZ ESCOBAR, Carlos Pablo. Óp. Cit., pág. 22

por los ciberdelincuentes o más reconocidos como “pescados” de manera fraudulenta, por medio de spam o correos electrónicos no deseados, los cuales se utilizan de forma perniciosa, poniendo en peligro la integridad de la información sensible del usuario por supuesto con graves consecuencias.

En consecuencia, el phishing es, junto a los programas espías, una de las técnicas más empleadas por la ciberdelincuencia para apropiarse de la información confidencial a través de internet Para que este tipo de conducta sea tipificado como punible, se hace necesario que el agente actúe con un objeto ilícito, ya que si no hay ilicitud no será catalogado como delito, empleándose en esta modalidad dos acepciones: Página electrónica y enlace o ventana emergente. La primera, conocida también como página de internet, el cual es un documento adoptado por la web, el cual forma parte de un sitio de la misma: está compuesta fundamentalmente de información (sólo texto o multimedia) e hiperenlaces, además asocia datos de estilo con el objeto de especificar su visualización, la segunda, emergentes, que da a significar las ventanas que emergen automáticamente mientras se accede a ciertas páginas web, generalmente son publicitarias[63].

7.6 Infracción de los derechos de autor

La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on-line o de un sysop (la persona que se encarga de la operación de un sistema) respecto a las copias ilegales introducidas en el sistema. Mientras un tribunal condenó a un sysop porque en su BBS había imágenes escaneadas de la revista Playboy, en el caso LaMacchia, el

[63]ARBOLEDA VALLEJO, Mario, RUIZ SALAZAR, José Armando. Op. Cit. Pág. 1002.

administrador del sistema fue hallado no responsable de las copias de programas que albergaba su BBS. El recurso de los propietarios de sistemas on-line y BBS ha sido incluir una advertencia o una cláusula contractual que los exonera de responsabilidad frente a un "upload"[64] de un programa o fichero que infrinja los derechos de autor de terceros[65].

7.7 Distribución de música por Internet (mp3)

Con relación a la música existe el conocido MP3, que se constituye como un formato digital de audio con el cual se puede comprimir el tamaño de una canción digitalizada en una relación de 10 a 1; es decir que 10 MB de sonido digitalizado ocuparía solo un MB. Esto ha permitido un intenso tráfico de música dentro de la red derivando inclusive en la venta ilegal de compactos sin intervención de las discográficas que optaron por generar movimientos y numerosas medidas para tratar de evitarlo[66].

Como ejemplo de estas medidas en España desde la Sociedad Digital de Autores y escritores (SDAE) se han puesto al servicio de la detección de esta actividad nuevas tecnologías las cuales incluyen a una especie de robot que da vueltas por Internet y se dedica a descubrir aquellos que distribuyen música sin pagar derechos como una forma de tratar de controlarlo y evitarlo[67].

[64]Enviar un archivo desde el computador a otro sistema.
[65]SURF & SKATE. ¿Qué delitos se cometen a través de internet? [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: http://surfskate7.blogspot.com/
[66]RAMÍREZ LÓPEZ, Ricardo Alberto. Inclusión de los delitos informáticos en el Código Penal. [En línea]. [Recuperado el 12 de septiembre de 2011] Disponible en internet:<http://www.ilustrados.com/tema/2736/Inclusion-delitos-informaticos-dentro-Codigo-Penal.html>

[67]DERECHO INFORMATICO U.N.A. Definición sintética de delitos informáticos ya catalogados. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://lopezmontiellmarlene.blogspot.com/2010_05_01_archive.html>

7.8 Estafas electrónicas

Acciones como las compras electrónicas son un atractivo que favorece el incremento de los casos de estafa mediante un engaño a la persona que compra al distribuidor, al banco y/o al equipo principal encargado de la operación. La propagación de las compras telemáticas también permite que aumenten los casos de estafa[68].

Una de las facilidades que proporciona la informática es la ventaja de realizar muchas tareas sin moverse de casa o la oficina. Esto supone que ya no existe un contacto directo entre las personas para ejecutar varias labores. Como consecuencia de ello se ha producido un gran cambio en el mundo empresarial y de negocios, que han abierto nuevas perspectivas de consumo mediante el uso de Internet. El navegante, conoce la venta de cientos de productos, de diferentes marcas y modelos a través de la red, el ciberespacio se ha convertido en un nuevo sector a tener en cuenta para las empresas; lo cual es adecuado ya que se ahorran muchos costos y amplían su potencial de mercado.

Se trataría en este caso de una dinámica que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el *"animus defraudandi"* existiría un ardid a la persona que compra. No obstante seguiría existiendo una laguna legal en países que como Colombia en donde la legislación no provee los casos en los que la operación se hace engañando al computador.

Con todo lo anterior es posible definir la estafa informática como la *"manipulación o alteración del proceso de elaboración electrónica de cualquier clase y en*

[68]BALMACEDA HOYOS, Gustavo. El delito de estafa informática. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://es.scribd.com/doc/73056898/Estafa-informatica-Gustavo-Balmaceda>

cualquier momento de éste, realizada con ánimo de lucro y causando un perjuicio económico a un tercero"[69].

7.9 Transferencias de fondos

Este es el típico caso en el que no se produce engaño a una persona determinada, sino a un sistema informático, ya sea por el mal uso de contraseñas, tarjetas electrónicas falsificadas, llaves falsas o adulterando el contenido de la información externamente cometiendo un robo.

7.10 Delitos Convencionales

Se definen así a todos los delitos que se dan sin el empleo de medios informáticos y que con la aparición de las rutas virtuales se están reproduciendo también en el ciberespacio. Asimismo dentro de los actos que no son propiamente delitos, sino infracciones administrativas o ilícitas civiles predominan:

7.10.1 Espionaje: Se trata de casos de acceso no autorizado a sistemas informáticos e intercepción de correo electrónico de entidades gubernamentales, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera, evidenciándose una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales pro personas especializadas. Entre los casos más famosos es posible citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994, respecto a campos de pruebas de misiles. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha

[69]VIVES ANTÓN – GONZÁLEZ CUSSACpresentación de datos falsos relativos al estado contable en las insolvencias punibles (art. 261 cp). En: <http://www.uclm.es/aidp/pdf/barbero2/7.pdf>

evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales[70].

7.10.2 Espionaje Industrial: Son casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales y fórmulas que posteriormente son utilizadas por otras empresas de la competencia que se divulgan sin autorización[71].

7.10.3 Terrorismo: Se efectúa mediante el uso de equipos que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo. Esto puede realizarse desde los servidores que ofrecen servicio de correos gratis en donde se pueden ingresar datos personales y direcciones ficticias para crear cuentas de correo que posteriormente pueden aprovechar personas o grupos terroristas para enviar amenazas, remitir consignas y planes de actuación ilícitos[72].

7.10.4 Narcotráfico: Se presenta a través del envío de mensajes encriptados que sirven para que los integrantes de grupos delincuenciales que se dedican a esta actividad puedan ponerse en contacto, incluso, se ha detectado el uso de la red para la transmisión de formulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

7.10.5 Difusión de pornografía: En la mayoría de países incluyendo a Colombia es ilegal la comercialización de pornografía infantil o cualquier acto de pederastia. Un ejemplo de conducta activa sería remitir una recopilación de imágenes

[70]PERALTA, Naty.. Ensayo sobre delitos informáticos. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://natyperalta.wordpress.com/2008/11/16/ensayo-sobre-delitos-informaticos>

[71]SISTEMAS Y TECNOLOGÍAS. Las dimensiones morales de los sistemas de información. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://rocky7cd.blogspot.com/2011/01/43-las-dimensiones-morales-de-los.html>

[72]Los delitos informáticos. Aproximación a los perfiles de personalidad de los sujetos que realizaron delitos informáticos. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://psicopsi.com/Los-delitos-informaticos-Aproximacion-a-los-perfiles-de-personalidad-de-los-sujetos-que-realizaron-delitos-informaticos.asp>

pornográficas escaneadas a los *mailbox* o buzones de correo de un país en donde estuvieran también prohibidos los actos de difusión o comercialización de las mismas.

7.10.6 Manipulación de programa. Este tipo de conducta es difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Su ejercicio consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Uno de los métodos utilizados por las personas que tienen conocimientos especializados en programación informática es el denominado "Caballo de Troya"[73], 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 normal[74].

7.10.7 Manipulación informática: es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, incluir datos en distinto momento o lugar, variar las instrucciones de elaboración. Se diferencia en las estafas informáticas de las cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del engaño que determina de disposición patrimonial[75].

[73] El "caballo de Troya" es un programa destructivo que se disfraza de juego, cuando se ejecuta, efectúa alguna clase de comportamiento dañino en el sistema informático, mientras parece estar ejecutando una acción útil (Confróntese sipra, intro)
[74] Ibíd. "caballo de Troya"
[75] Ibíd. "caballo de Troya"

7.10.8 Falsificaciones informáticas: Definidas como la alteración de datos de los documentos almacenados en forma computarizada, por personas no autorizadas que acceden en forma engañosa al equipo, aprovechando que éste comparte directorios y permite que usuarios remotos tengan acceso a la información[76].

8 CARACTERÍSTICAS DEL DELINCUENTE INFORMÁTICO:[77]

Entre las principales características pueden detallarse las siguientes:

- Poseen importantes conocimientos de informática
- Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se les denomina en este sentido delitos ocupacionales ya que se cometen por el trabajo que se tiene y la facilidad en el acceso al sistema).

- Es importante considerar que son personas diferentes las que incurren en este tipo de conductas, porque no es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

- Son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

- Estos delitos se han calificado de cuello blanco, porque el sujeto que comete el punible es una persona de cierto status socioeconómico.

[76] Ibíd. “caballo de Troya”
[77] Delitos Informáticos. Delitos informáticos en Colombia. [En línea]. [Recuperado el 25 de agosto de 2011] Disponible en internet: <http://betypilus.blogspot.com/2010_06_01_archive.html>

- Poseen el síndrome de Robín Hood, porque consideran que hacen justicia al defraudar las grandes organizaciones financieras y por ello no consideran inmoral sus actos delictuales, pues creen que no les han hecho daño a las personas. Obtienen cierta simpatía de la opinión pública.

Por lo general, el delincuente suele aprovechar la falta de medidas de seguridad de los sistemas computacionales o su vulnerabilidad, para obtener acceso a la información almacenada en los equipos. A menudo, los hackers se disfrazan como usuarios legítimos del sistema, actividad que se les facilita cuando los usuarios autorizados utilizan contraseñas comunes con bajos niveles de protección.

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los computadores con ánimo de lucro, 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 algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos[78].

> "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 cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos. A ello se suma que estos ataques son

[78] Causa 39779. Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal de Argentina.

> 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"[79].

Sin embargo determinar los métodos de destrucción y/o violación del hardware y el software, es sin lugar a dudas necesario para identificar cuál será el recorrido que se debe seguir para orientar una política pública que abarque la protección jurídica de los sistemas informáticos, ya que a partir del conocimiento de los mecanismos de estos métodos es viable encontrar las semejanzas y diferencias que existen entre ellos por lo que pueden conocer los problemas que es necesario precaver para conseguir una protección jurídica eficaz sin caer en practicas innecesarias en la protección de estos bienes jurídicamente tutelados[80].

> 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 bancarias, financieras, tributarias, provisionales y de identificación de las personas y 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 llegar a estarlo algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger[81].

---

[79] GARAVILLA MIGUEL, Estrada. DELITOS INFORMÁTICOS. En: Universidad Abierta http://www.universidadabierta.edu.mx

[80] FAZ SÁNCHEZ, Juan de Dios. Delitos electrónicos. Delitos Electrónicos. La necesidad que se legisle en el Código Penal de Baja California. En: Delitos electrónicos. http://www.poder-judicial-bc.gob.mx/admonjus/n29/AJ29_004.htm.

[81] Ibídem.,

En la actualidad se considera que una de las estrategias político criminales para la protección de los sistemas informáticos bajo la representación de proteger transacciones civiles o comercial e incluso de derecho administrativo por lo tanto la protección de estos bienes jurídicos debe enriquecerse con la integración o interdisciplinaria estrechamente vinculadas en la comisión de delitos informáticos. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

9. EL CONVENIO DEL CONSEJO DE EUROPA SOBRE EL CIBERCRIMEN

Éste convenio se presenta como modelo a nivel mundial para la forma en que los países deben enfrentar su lucha contra la delincuencia informática. Su realización surge como respuesta a los vacíos de las legislaciones nacionales internas para combatir los delitos informáticos que, como se ha dicho, fácilmente ignoran las fronteras y jurisdicciones territoriales de las naciones, convirtiéndose en problemas transnacionales.

Como antecedente del convenio se incluyen los tratados de asistencia legal suscritos por los gobiernos de los diferentes estados para suministrar apoyo mutuo en la investigación de actividades criminales trasnacionales como el tráfico de drogas, y como antecedente remoto, las cartas rogatorias emitidas para obtener evidencias desde el extranjero. Pero estas formas de cooperación tradicionales hoy son inadecuadas para la investigación y procesamiento de los delincuentes informáticos que operan con total impunidad desde cualquier lugar del mundo, con el agravante de que muchas legislaciones aún no incluyen los delitos informáticos[82].

[82]BAUTISTA, Norma, CASTRO MILANÉS, Heiromy. Aspectos Dogmáticos, Criminológicos y Procesales del Lavado de Activos. [En línea]. [Recuperado el 02 de septiembre de 2011]

En este escenario, la Convención sobre Cibercrimen, busca resolver los problemas que se acaban de mencionar y se establece como el resultado de un esfuerzo que comenzó en 1997 con un estudio de la Organización para la Cooperación y Desarrollo Económicos (OCDE) sobre la posibilidad de armonizar las legislaciones nacionales sobre cibercrimen; mostrando como punto fundamental la necesidad de modificar las leyes nacionales para mejorar la capacidad hacia el cumplimiento de la ley frente al cibercrimen. La OCDE emitió un reporte recomendando que los países penalizaran un conjunto de conductas como cibercrimen. Al mismo tiempo, el Consejo de Europa se ocupó del asunto en un esfuerzo que culminó con la Convención sobre Cibercrimen.[83]

Como punto inicial la Convención requiere de los Estados partes que incorporen en sus legislaciones internas la criminalización de ciertas actividades que se desarrollan alrededor de los sistemas informáticos y los datos para obtener accesos no autorizados y causar daños (Artículos 2 a 9), incluyendo: la falsificación informática; los fraudes informáticos; el uso de la tecnología computacional para crear, distribuir o procesar pornografía infantil; y el uso de la tecnología computacional para cometer infracciones a la propiedad intelectual.[84]

Disponible En: http://www.google.com.co/url?sa=t&rct=j&q=suscritos%20por%20los%20gobiernos%20de%20los%20diferentes%20estados%20para%20suministrar%20apoyo%20mutuo%20en%20la%20investigaci%C3%B3n%20de%20actividades%20criminales%20trasnacionales%20como%20el%20tr%C3%A1fico%20de%20drogas%2C%20y%20como%20antecedente%20remoto%2C%20las%20cartas%20rogatorias%20emitidas%20para%20obtener%20evidencias%20desde%20el%20extranjero&source=web&cd=1&ved=0CBsQFjAA&url=http%3A%2F%2Fenj.org%2Fportal%2Findex.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26Itemid%3D%26gid%3D70&ei=mbzjTuzcFdGltwel0OihBA&usg=AFQjCNEnbPpXaLh46fl9xbEDzfAfLO6FFA>

[83]Consejo de Europa, 583 reunión de Delegados Ministeriales, 4 de Febrero de 1997, Apéndice 13, disponible en <http://www.cm.coe.int/dec/1997/583/583.a13.html>

[84]Artículos 2 a 10, de la Convención sobre Cibercrimen del Consejo de Europa (CETS No. 185).

En cuanto al procedimiento, la Convención fija pautas para que cada uno de los Estados diseñen mecanismos que faciliten la investigación, permitiendo la preservación y producción de evidencia electrónica; solicitando búsqueda e incautación legal de los sistemas informáticos; y autorizando a la autoridad para recolectar datos de tráfico y de contenidos.[85] Esta colaboración puede ir más allá para incluir la extradición de los delincuentes, compartir información y preservar, acceder, interceptar y revelar datos de tráfico y contenido.[86] Y cada parte debe designar un punto de contacto que será responsable de asegurar "asistencia inmediata" en "investigaciones y procedimientos" relativos a cibercrimen.[87]

La investigación del cibercrimen se centra principalmente en evidencia digital, por ejemplo, en el contenido de mensajes de correo electrónico, en las direcciones empleadas para enviar los *e-mails*, en los archivos *logs* o ficheros de texto de actividad computacional, y en la data almacenada en los computadores personales o portátiles. Estas evidencias son muy frágiles, fáciles de destruir o alterar, con sólo programar rutinas para eliminar los archivos *logs* relativos a la actividad de los sistemas, los cuales pudieran contener evidencia para investigar un delito informático.

Frente a este problema la Convención busca mejorar los procesos usados para preservar, localizar y compartir evidencia digital, con el fin de que los investigadores puedan disponer de ella para su uso; implementando normas que requieren a los Estados partes para que incluyan dentro de los delitos informáticos cualquier delito que sea *"cometido mediante un sistema computacional"*, y que la evidencia digital recolectada pueda ser usada en un procedimiento relativo a *cualquier* otro delito[88].

[85]Id., Artículos 16 – 21.
[86]Id., Artículos 23 – 34.
[87]Id., Artículo 35.

[88]Artículo 14 Id.

De igual modo establece que la interceptación y recolección de datos, usuales en investigaciones sobre “delitos graves”, de acuerdo con la legislación interna de cada país, puede emplearsetambiénpara la investigación de delitos informáticos y, en general, para investigar cualquier delito que requieran evidencia digital[89]. En todos los casos se prevé que la “implementación y aplicación de las facultades y procedimientos” prescritos por la Convención “están sujetos a condiciones y salvaguardias… las cuales proveerán una adecuada protección de los derechos humanos y libertades”[90], con lo que se busca la protección de los derechos humanos y libertades fundamentales, relacionadas especialmente con la privacidad y la protección de los datos personales.

Estas normas buscan hallar el punto de equilibrio entre el respeto y protección del derecho a la privacidad de que gozan todas las personas en relación con sus datos personales y la persecución del cibercrimen, pues los delincuentes cometen sus fechorías escudándose en las restricciones que tienen las autoridades para penetrar la órbita de su intimidad.

Hace unos pocos meses la revista Semana publicó el caso de un ciudadano de Medellín que encontró en su casilla de correo electrónico un mensaje que supuso era de su banco, porque traía el logo y la tipografía de la entidad, en el que se le pedía que actualizara sus datos. Así lo hizo, a través de una página que lucía idéntica a la página oficial de la institución financiera. Fue víctima de un phishing o sitio web falso y en esa operación perdió nueve millones de pesos que era todo el dinero consignado en su cuenta, pues el banco no tiene ninguna responsabilidad en ese fraude y porque es imposible recuperarlo, ya que fue girado ese mismo día a una cuenta en Barranquilla y retirado por una persona que utilizó una identidad falsa.

[89]Artículos 21 y 22 Id.
[90]Artículo 15 Id.

El computador desde el que se despachó el correo está ubicado en una sala pública de la Universidad de Antioquia, pero las transferencias fueron ordenadas desde Canadá y Chile[91]. A eso se le suma el tiempo que debe esperar la Unidad de Delitos Informáticos de la Policía Nacional para obtener autorización de la Fiscalía para hacer interceptaciones de correos y datos informáticos, demora que los delincuentes aprovechan para esfumarse, luego de haber tenido espacio suficiente para borrar las huellas dejadas por su delito en la red.

10 EL DELITO INFORMÁTICO EN LA ACTUAL LEGISLACIÓN PENAL COLOMBIANA

En Colombia este delito no está tipificado claramente como conducta punible individual y autónoma. El nuevo Código Penal, próximo a entrar en vigencia, en su artículo 195 y bajo el rótulo de Acceso Abusivo a un Sistema Informático, (Hacking en otras legislaciones), establece una sanción de multa, sin especificar la cuantía, para quienes abusivamente se introduzcan en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, restándole la seriedad y gravedad que la conducta implica.

En ese sentido pudiera afirmarse que el Legislador no sanciona el comportamiento en forma más severa, por tratarse de actos cometidos generalmente por jóvenes adolescentes (por eso se le denomina también (“crímenes en pantalones cortos”) que acceden a sistemas protegidos para demostrar sus grandes capacidades informáticas u obtener satisfacciones de carácter intelectual cada vez que logran descifrar los códigos de acceso o passwords, sin causar daños inmediatos y tangibles en las víctimas, limitándose hasta ahí y no generando esta conducta

[91]SEMANA.COM. En manos del “cibercrimen”. [En línea]. [Recuperado el 02 de septiembre de 2011] Disponible en internet: <http://www.semana.com/especiales/manos-del-cibercrimen/102658-3.aspx>

otras consecuencias en la mayoría de los casos, de modo que el ánimo involucrado no resulta extremadamente riesgoso.

Esa es tal vez la razón por la que el mero hecho de penetrar sin autorización a computadores o sistemas informáticos protegidos con medidas de seguridad, para ver qué hay dentro - actividad que en el medio informático se conoce como *hacking* -, sólo acarree una sanción de multa, según el artículo 195 del Código Penal. Pero no ocurre lo mismo si este acceso indebido es utilizado como medio para la comisión de otros ilícitos que tienen como propósito dañar, defraudar, espiar, falsificar o alterar datos, pues en estos casos el *hacking* indirecto o acceso indebido no es tomado en cuenta por los investigadores como delito autónomo que debe ser objeto de una sanción, sino que le atribuyen el papel protagónico al delito principal que se cometió o se intentó cometer, el cual se torna en el único que es objeto de persecución penal.

Por lo anterior, se plantea como una urgente necesidad que el Legislador introduzca modificaciones en esta materia en el Código Penal, estableciendo sanciones más drásticas para el hacking indirecto, a fin de que se le investigue como una conducta típica, independiente de otros delitos conexos que puedan tipificarse por el *Hacking* o Acceso Abusivo a Sistemas Informáticos.

Consideración aparte merece el tratamiento que se debe dar a los *hackers* que usan el acceso abusivo como medio para la ejecución de delitos como falsedad, sabotaje, piratería, espionaje o fraude, entre otros, a quienes hay que distinguir en dos grupos perfectamente identificables. El primero es conformado por aquellas personas que por razones de su trabajo u otras tienen autorizado el acceso al sistema y se valen para la comisión de los ilícitos del conocimiento de los códigos de seguridad. En este escenario se ubica a los trabajadores del área de informática de bancos, empresas u organismos del Estado en los cuales se ha

depositado un nivel de confianza importante. En el segundo grupo se debe incluir a los extraños que tienen el acceso prohibido o cerrado e ingresan al sistema a través del descubrimiento fraudulento del *password*. Como es de suponerse, los comportamientos de estos últimos son los más graves, sin embargo el estatuto penal no lo contempla así e incluye todas las conductas en la misma categoría, sin hacer distinciones de ninguna índole.

A partir de estas premisas es urgente entonces que el Código Penal establezca normas autónomas que consagren las diferentes modalidades del delito informático y la mayor o menor penalización que debe imponerse a los delincuentes, dependiendo de la relevancia del bien jurídico que resulte vulnerado, entre los que pueden citarse la libertad individual, la fe pública, el patrimonio económico y la seguridad del Estado, por citar algunos de ellos. De modo que sea distinto el tratamiento punible que reciba el transgresor del sistema que lo hace por curiosidad y con un fin aparentemente no doloso, del que debe imponérsele a otro que ingresa con el propósito determinado de alterar documentos electrónicos o apropiárselos.

A propósito de documentos, el concepto mismo del término debe ser objeto de actualización para que acompase con los que han surgido como producto de las nuevas tecnologías. En efecto, el artículo 294 del Código Penal (Ley 599 de 2000) establece que para los efectos de la ley penal[92], *"es documento toda expresión de persona conocida o conocible recogida por escrito o por cualquier medio mecánico o técnicamente impreso, soporte material que exprese o incorpore datos o hechos, que tenga capacidad probatoria"*, pero omite la inclusión de los documentos electrónicos, craso error el del Legislador, que no se ha percatado de que la información almacenada en un disco duro o flexible no equivale a la recogida en un medio mecánico porque su ejecución no es mecánica.

[92]Ibíd.En manos del "cibercrimen"

En este breve recorrido por el Código Penal para identificar delitos que pueden cometerse mediante el empleo de medios electrónicos, se observa que el Título IX, el cual trata de los delitos contra la fe pública, no describe como punible la falsedad en documento electrónico, por ello es urgente adicionarle un artículo al Capítulo Tercero, que se ocupa de la falsedad documental, para incluir específicamente la "falsedad en documento electrónico", a fin de que la adecuación de la conducta punible no tropiece con dificultades, como acontece actualmente, por no contemplar con toda precisión ese punible en particular.

En las siguientes líneas se trata de sintetizar los avances más importantes que se obtienen con la expedición de la Ley 1273 de enero de 2009[93], por modificó el Código Penal creando un nuevo bien jurídico denominado *"De la protección de la información y de los datos"*.

De su texto se extrae que esta ley tipifica como delitos una serie de conductas que tienen que ver con el manejo de datos personales, con lo que se busca castigar con mayores penas el aprovechamiento de los avances tecnológicos para apropiarse ilícitamente del patrimonio de terceros, ya sea clonando tarjetas bancarias, vulnerando o alterando sistemas de cómputo para efectuar transferencias electrónicas de fondos mediante manipulaciones de programas y cajeros electrónicos, además de otras conductas que se tornan cada vez más usuales en el mundo y se repiten peligrosamente en el país, generándole inmensas pérdidas económicas a los ahorristas y entidades financieras.

La Ley 1273 de 2009 adiciona el Título VII BIS del Código Penal y a su vez se divide en dos capítulos que denomina: "De los atentados contra la

[93]Ley 1273. Óp. cit.

confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones".
El primero capítulo busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, mediante el establecimiento de las siguientes sanciones:

a) Pena de prisión de 48 a 96 meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, para quienes incurran en estas conductas: (1) Acceso abusivo a un sistema informático[94]. (2) Obstaculización ilegítima de sistema informático o red de telecomunicación[95]. (3) Daño informático[96]. (4) Uso de software malicioso[97]. Y (5) Violación de datos personales[98].

b) Pena de prisión de 36 a 72 meses para el que intercepte datos informáticos sin previa orden judicial[99].

El artículo 269G establece una pena de prisión entre 48 y 96 meses y multa entre 100 y 1000 salarios mínimos legales mensuales para quien suplante sitios web con el propósito de capturar datos personales, conducta que está muy en boga en Colombia, pues no es infrecuente que los titulares de cuentas bancarias reciban supuestos correos electrónicos de sus entidades en los que son re direccionados a páginas falsas en las que se les pide diligenciar formularios con sus datos personales, modalidad de estafa que se conoce como *"phishing"*; cuando algunos incautos caen en la trampa, los delincuentes usan la información obtenida para transferir todos los fondos a cuentas para luego ser retirados sin dejar rastros del crimen.

[94]Artículo 269A

[95]Artículo 269B
[96]Artículo 269D
[97]Artículo 269E
[98]Artículo 269F
[99]Artículo 269C

Y el artículo 269H incluye nuevas circunstancias de agravación punitiva que contemplan el aumento de la pena de la mitad a las tres cuartas partes cuando la conducta se comete sobre redes o sistemas informáticos o de comunicación estatales, o por servidor público en ejercicio de sus funciones, o abusando de la confianza depositada por el poseedor de la información, o revelando el contenido de la información en perjuicio de otro, u obteniendo provecho del ilícito, o con fines terroristas, o utilizando terceros de buena fe. Y si quien lo hace es responsable en cualquier forma de esa información, como pena accesoria establece la inhabilitación para el ejercicio de la profesión relacionada con sistemas de información procesada en equipos de cómputo.

CONCLUSIONES

1º. La primera observación que surge de esta investigación es que era necesaria una reglamentación más amplia de la temática, como sí se ha hecho en otras legislaciones del mundo, proporcionándole la debida y verdadera trascendencia normativa en sus países, ya que ese acceso al que se refiere la medida está introducido en el interés económico, pero también es importante porque vulnera la fe pública, como ejemplo se puede nombrar la modificación de una escritura pública electrónica, conducta punible que no tarda en consumarse, puesto que ya se legalizó el manejo del documento electrónico y solo faltaría reglamentar el trámite de esta clase de instrumentos con el registro civil.

2º. De la misma forma y mediante un análisis de las legislaciones que se han decretado en diversos países se demuestra que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras.

3º. También se establece que desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos, pero también es evidente que es difícil elaborar estadísticas sobre los diversos tipos de delitos.

4º. En relación con lo anterior, se puede afirmar que la cifra de delitos de esta naturaleza es elevada y es evidente que no es fácil descubrir sus autores y por lo tanto sancionarlos, en parte gracias al poder económico que tienen y que aprovechan para que a través de los actos que desarrollan mediante los delitos informáticos originar daños económicos incalculables, los cuales son indiferentes para la opinión pública.

5º. Se agrava además con el problema que quienes cometen este tipo de conductas no se asumen como delincuentes, no se les segrega, desprecia, ni desvalora, por el contrario, el autor o autores de este tipo de delitos se consideran a sí mismos como "respetables" y enfrentan castigos como " objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad"[100].

En síntesis, se puede afirmar que la delincuencia informática se apoya en el delito organizado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aclarando que este no es el único medio por el cual se desarrolla. Las ventajas y las necesidades del flujo nacional e internacional de datos, aumenta incluso en países latinoamericanos, favoreciendo también la posibilidad que se incrementen estos delitos. Por lo mismo se caracteriza que la criminalidad informática constituye un reto desmedido tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las

[100] www.delitosinformáticos.html

autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

BIBLIOGRAFÍA

COLOMBIA. MINISTERIO DE HACIENDA Y CRÉDITO PÙBLICO. Decreto 1748 (13, Octubre, 1995). Por el cual se dictan normas para la emisión, cálculo, redención y demás condiciones de los bonos pensiónales y se reglamentan los Decretos leyes 656, 1299 y 1314 de 1994, y los artículos 115, siguientes y concordantes de la Ley 100 de 1993. Diario Oficial. Bogotá, D.C., 1995. no.42. 049.

BAÓN RAMÍREZ, ROGELIO. Visión general de la informática en el nuevo Código Penal, en ámbito Jurídico de las tecnologías de la información, cuadernos de Derecho Judicial, Escuela Judicial/ Consejo General de Poder Judicial, Madrid, 1996.

COLOMBIA, CORTE CONSTITUCIONAL, Sentencia SU-082/1995.

COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C- 1147/01.

COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C- 381/01.

COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-356/03.

COLOMBIA, CORTE CONSTITUCIONAL. Sentencia C-662/00.

COLOMBIA, CORTE CONSTITUCIONAL. Sentencia T- 729/02.

COLOMBIA, CORTE CONSTITUCIONAL. Sentencia. T-080/93.

COLOMBIA, CORTE SUPREMA DE JUSTICIA. Sentencia de Casación No. 29188.

COLOMBIA, MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO. Decreto 1748 (12, octubre ,1995). Por el cual se dictan normas para la emisión, cálculo, redención y demás condiciones de los bonos pensionales y se reglamentan los Decretos leyes 656, 1299 y 1314 de 1994, y los artículos 115, siguientes y concordantes de la Ley 100 de 1993. Bogotá D.C.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Decreto 01(02, enero, 1984). Por el cual se reforma el Código Contencioso Administrativo. Diario Oficial. Bogotá, D.C., 1984.

COLOMBIA. EL PRESIDENTE DE LA REPUBLICA DE COLOMBIA. Decreto 1105 (01, Julio, 1992). Por el cual se modifica parcialmente el régimen de aduanas. Diario Oficial. Bogotá, D.C., 1992. no.03.

COLOMBIA. EL PRESIDENTE DE LA REPUBLICA DE COLOMBIA. Decreto 1400. (21, septiembre, 1970). Por los cuales se expide el Código de Procedimiento Civil. Diario Oficial. Bogotá, D.C., 1970. no.33.150.Art. 252.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1266 (31, Diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no.47.219.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 4 (22, Agosto, 1913). Sobre régimen político y municipal. Diario Oficial. Bogotá, D.C., 1913. no.14.974.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273 (05, Enero, 2009). 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. Bogotá, D.C., 2009. no.47.223.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (05, enero, 2009). 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. Bogotá, D.C., 2009. no.47.223.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 365 (21,Febrero, 1997). Por la cual se establecen normas tendientes a combatir la delincuencia organizada y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1997. no.42. 987.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 383 (10, Julio, 1997). Por la cual se expiden normas tendientes a fortalecer la lucha contra la evasión y el contrabando, y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1997. no.43. 083.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 44. (05, febrero, 1993). Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. Diario Oficial. Bogotá, D.C., 1993. no.40.740.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527 (18, Agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de

certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999. no.43.673.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 57 (12, Julio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. Diario Oficial. Bogotá, D.C., 1985. no.37.056.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 98 (22, Diciembre, 1998). Por medio de la cual se dictan normas sobre democratización y fomento del libro colombiano. Diario Oficial. Bogotá, D.C., 1993. no.41.151.

COLOMBIA. MINISTERIO DE DESARROLLO ECONÓMICO. Decreto 1747 (14, Septiembre, 2000). Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Diario Oficial. Bogotá, D.C., 2000. no.44.160.

COLOMBIA. MINISTERIO DE DESARROLLO ECONÓMICO. Ley 599 (24, Julio, 2000). Por la cual se expide el Código Penal. Diario Oficial. Bogotá, D.C., 2000. no.44.097.

COLOMBIA. Ministerio y de justicia. Decreto 2150 (06, Diciembre, 1995). Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.. Diario Oficial. Bogotá, D.C., 1995. no.42. 137.

CONSTITUCIÓN POLÍTICA DE 1991

ITC (Información TechnologyCrime)

JORDÁN FLOREZ, Fernando, La Informática Jurídica (Teoría y Práctica), primera edición, Universidad Piloto de Colombia, Centro de Investigaciones Interdisciplinarias, 1983.

La ley 16 de 1972, de 20 de diciembre

LEÓN MONCALEANO, William F. De la comunicación a la informática jurídica penal y bancaria, Bogotá, ediciones Doctrina y Ley, 2001.

National White Collar Crime Center, Centro de Delitos de Cuello Blanco

PLEIN. Temática Didáctica Educativa, Grupo Editorial Norma, 1998. públicas", en Diario La Ley, núm.5528, 22 de abril de 2002.

RESOLUCIÓN NÚMERO 3316 DE 1997.

SANCHEZ BRAVO, A. "El Convenio del Consejo de Europa sobre cibercrimen: control vs. Libertades

SENTENCIA. Expediente RE. 125. M.P. Rodrigo Escobar Gil. Mayo de 2003.

TELLEZ VALDÉS, J. Derecho Informático, Editorial McGraw Hill, México, 1997.

RAMÍREZ LÓPEZ, Ricardo Alberto. Principales delitos informáticos.Legislación nacional. Hackers y Crackers. Publicado en http://www.ilustrados.com/tema/2736/Inclusion-delitos-informaticos-dentro-Codigo-Penal.html

MÁRQUEZ ESCOBAR, Carlos Pablo. El delito informático. Leyer Editorial.

ARBOLEDA VALLEJO, Mario, RUIZ SALAZAR, José Armando. Manual de Derecho Penal. 10ª Ed.2010. Leyer Editorial.

TÉCNICAS

Citado por Cuervo Álvarez, José, Delitos informáticos: protección penal de la intimidad. En: http://publicaciones .derecho.org/redi/No._06_-_Enero_de_1999/cuervo

Vives Antón – González Cussac PRESENTACIÓN DE DATOS FALSOS RELATIVOS AL ESTADO CONTABLE EN LAS INSOLVENCIAS PUNIBLES (ART. 261 CP). En: http://www.uclm.es/aidp/pdf/barbero2/7.pdf
www.delitosinformáticos.html