NECESARIA REFORMA LEGISLATIVA DEL CÓDIGO PENAL VIGENTE.

MsC Isabel María Acosta Fernández[1], MsC. Marlene Oliva León[2], MsC. Angel Raudel Piñón Pérez [3,]

1. Universidad de Matanzas- FUM" Luis Crespo Castro", Calle 13 no 2224 % 22 y 24 Jovellanos, Matanzas, Cuba.

2. Centro Nacional de Capacitación Azucarera (CNCA) – Filial Matanzas "Antonio Mesa Hernández", Carretera Central Km.150, EPICA, Matanzas, Cuba.
filial.matanzas@epicamt.azcuba.cu.

3. Universidad de Matanzas – FUM"Luis Crespo Castro", Calle13 #2224 e/ 22 y 24 Jovellanos, Matanzas
angel.pinon@umcc.cu

CD de Monografías 2014

Resumen

Los autores pretenden demostrar que a pesar de las reformas plasmadas en nuestra legislación penal vigente, ha quedado un vacío jurídico en cuanto a la tipificación de los delitos informáticos, realidad que debe ser modificada ya que los perjuicios ocasionados por quienes dominan la tecnología son cada vez más comunes en el mundo actual y también en nuestro país de ahí que en las condiciones actuales de la sociedad es posible que la norma penal contemple aspectos que respondan cómo darle solución a los delitos informáticos no contemplados en la legislación actual, pues dicha protección legal debe materializarse en varios subsistemas jurídicos, a los que se integra la legislación Penal, que debe prever los tipos delictivos aplicables a las conductas antijurídicas que se generan en el uso de las modernas tecnologías de la información y las comunicaciones.

***Palabras claves**: Delito informático; sanción penal; fraude informático.*

Cuerpo de la monografía

Dar un concepto sobre Delitos Informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones tipificadas o contempladas en textos jurídico penales , se requiere de la expresión "Delitos Informáticos" esté consignada en los códigos penales.

Doctrinalmente los seguidores de la respuesta penal parten de la referencia de un concepto de delito así, los consultados para este trabajo parten de un concepto general y mayoritariamente aceptado. Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países.

Según el ilustre penalista CUELLO CALON, los elementos integrantes del delito son:

a) El delito es un acto humano, es una acción (acción u omisión)

b) Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

c) Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.

d) El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

e) La ejecución u omisión del acto debe estar sancionada por una pena.

Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Se podría definir entonces partiendo del análisis anterior el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificado por La Ley, que se realiza en el entorno informático y está sancionado con una pena.

De esta manera, el autor mexicano Julio Tellez Valdés señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto típico)".Por su parte el tratadista penal italiano Carlos Sarzana[3], sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

Otros autores como Rafael Fernández Calvo define al delito informático como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos o libertades de los ciudadanos.

Por su parte María de la Luz Lima dice que el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.

Finamente y en cuanto a esa postura, vemos una posición cubana, Yarina Amoroso Fernández, presidenta de la Sociedad de Derecho e Informática, considera que "…es el conjunto de las acciones u omisiones que se pueden desatar por sobre los medios informáticos utilizados para realizar conductas delictivas que tienen su incidencia en la naturaleza de los bienes atacados, la forma de realización y los daños que puedan provocar".

Los autores definen que el Delito Informático no es sólo la acción u omisión que se relice a través de computadoras; sino toda acción u omisión que se realice utilizando cualquier medio, por el cual se pueda acceder a la red donde se manipule la información o se pueda cometer cualquier acto antisocial, el cual perjudique las buenas prácticas de las ciencias informáticas.

La generalización del uso de la informática ha provocado también un cambio en las características de los comisores de estos delitos, pues requerirán de determinados conocimientos y posición ocupacional. Hoy cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático.

El sujeto activo de los delitos informáticos se caracteriza y a la vez se diferencia del delincuente común en sus habilidades y destrezas para el manejo de la tecnología de la información, se consideran personas inteligentes, audaces y motivadas, dispuestas a aceptar cualquier reto tecnológico.

Los Piratas informáticos o Hackers acceden a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios a los cuales serán expuestos: El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema; a menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema, esto suele suceder con frecuencia en los sistemas en que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema y además tenemos la reproducción no autorizada de programas informáticos de protección legal: Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

Habiendo estudiado estos tipos de delitos los autores consideran que se debe preceptuar estas conductas en el Ordenamiento Penal cubano ya que la legislación penal sustantiva no posee figuras delictivas que tipifiquen de modo particular las conductas conocidas como delitos informáticos, por lo que al momento de juzgar los hechos que versen sobre estos aspectos como delitos , los Tribunales sancionan estas acciones como delitos recogidos en el Código Penal ya que la forma de realizar la actividad ilícita persigue el mismo fin que las acciones habituales que se juzgan.

Además si estudiamos el Derecho Comparado nos percatamos que ya en algunos países se han tipificado algunas de estas conductas criminógenas.

Múltiples son los ejemplos que se encuentran dando al problema de la seguridad un tratamiento dentro del derecho penal como fuera de éste, atemperad a normas administrativas, incluso existen naciones que llevan esta situación paralelamente.

Dentro del área geográfica resaltan casos como el brasileño. En este país, a tono con el Derecho Penal Informático la Parte Especial del Código Penal vigente desde 1940, por lo que las normas vigentes solo pueden aplicarse a aquellas conductas que encuadren con las figuras tipificadas en el mencionado cuerpo legal. Dado lo anterior se tratan acciones como las copias ilícitas de programas y producciones informáticas como violaciones a los derechos de autor como se ven en los Artículos 35 y 37 de la Ley 7646 de 18 de diciembre de 1987 que establecen:

Artículo 35: Violar derechos de autor de programas de ordenador: Pena: Detención, 6(seis) meses a 2(dos) años y multa. (Protege los derechos de autor)

Artículo 37- Importar, exportar, mantener en depósito para fines de comercialización, programas de ordenador de origen externo no registrados: Pena: Detención, de 1(un) año a 4(cuatro) años y multa. (Tipifica el contrabando informático).

El llamado Derecho Penal Informático en Brasil no da respuesta total al aumento de las conductas ilícitas por ejemplo en la red. En esta nación se trata el Proyecto de una nueva Parte Especial del Código Penal que incluye en su propuesta un Capítulo dedicado a Los crímenes contra el Orden Socio Económico el cual consta de 8 artículos, tres de los cuales tratan específicamente de los delitos informáticos.

Otro país latinoamericano es México donde la tipificación de este tipo de conductas es casi inexistente. Hugo Leal, prefiere utilizar actualmente el término de evento antisocial relacionado con la informática para definir aquellos actos ilícitos particularmente graves que hacen de las computadoras(elementos tangibles o hardware), sistemas y programas informáticos (elementos intangibles o software) o que buscan provocar en estos o en información sensible un resultado de lesión o peligro partiendo del hecho de que para que se configure una acción delictiva deben estar presentes dos presupuestos:

Que la conducta constitutiva del mismo esté tipificada por la ley y que medie una sentencia condenatoria en la cual el juez penal haya declarado probada la existencia concreta de una conducta típica, antijurídica y culpable constitutiva de delito informático, formalidades que para el tipo de conducta que nos ocupa no están dadas aún en México ni en muchos otros países del mundo.

En la parte norte de nuestro continente encontramos a Canadá donde los delitos realizados por medio de computadoras fueron incorporados al Código Penal (Canadian Criminal Code) y básicamente están contempladas en las secciones 342 y 430. Las sanciones, están previstas para quien de forma fraudulenta e ilegítima tenga acceso, directa o indirectamente a una computadora, o intercepte o cause que se intercepte a un sistema. Asimismo, se prevén penas de hasta diez años de prisión para quienes alteren datos, intercepten u obstruyan su transmisión o imposibiliten el acceso a quienes están autorizados a hacerlo.

Uno de los aspectos a destacar de la legislación canadiense, es que otorga una jurisdicción especial para los delitos cometidos por medio de computadoras, que caen bajo la órbita de Royal Canadian Mountain Police y la Information Technology Security Branco, que son los organismos encargados de la seguridad en tecnología de la información en Canadá.

En Cuba ante el continuo avance y desarrollo de las Tecnologías de la Información se fue haciendo necesario la implementación de normas legales que regularan el uso seguro de éstas, a saber, controlando, desde el punto de vista físico, cuidado, uso y explotación de equipos hasta el acceso a los mismos y redes evitando además la creación y proliferación de programas y códigos malignos. Fruto de esta situación se promulga por el Ministerio de la Informática y las Comunicaciones la Resolución No 127/07 de fecha 30 de julio de 2007: Reglamento de Seguridad para as Tecnologías de la Información, en consonancia con el Acuerdo 6058 del Comité Ejecutivo del Consejo de Ministros de fecha 9 de julio de 2007 que estableció los lineamientos para el perfeccionamiento de la seguridad de las tecnologías de la información en el país.

Ha existido dentro de la doctrina jurídica cubana una posición que no se puede desconocer en el presente trabajo y que se origina temporalmente a fines del siglo pasado. Esta posición, en materia de seguridad informática, ha versado sobre el tratamiento contravencional del tema y otros lo han visto en la práctica penal internacional como los Delitos Informáticos. Esta última postura, contó detractores afiliados a la moderna corriente del Derecho Penal denominada Derecho Penal mínimo o Derecho Penal de mínima

intervención aspecto que en criterio de los autores no riñe con la necesidad de tipificación de los Delitos Informáticos.

En la actualidad la informatización se ha implantado en casi todos los países; tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

La criminalidad informática incluye una amplia variedad de categorías de crímenes. Generalmente este puede ser dividido en dos grupos:

1. Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, Spam, ataques masivos a servidores de Internet y generación de virus.

2. Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

Un ejemplo común es cuando una persona comienza a robar información de websites o causa daños a redes o servidores. Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra en forma digital y el daño aunque real no tiene consecuencias físicas distintas a los daños causados sobre los ordenadores o servidores. En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de pruebas y, aunque el ordenador no haya sido directamente utimarinalizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de prueba ante cualquier corte del mundo.

Los diferentes países suelen tener policía especializada en la investigación de estos complejos delitos que al ser cometidos a través de internet, en un gran porcentaje de casos excede las fronteras de un único país complicando su esclarecimiento viéndose dificultado por la diferente legislación de cada país o simplemente la inexistencia de esta.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores 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 de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En el caso de la experiencia internacional, aunque no exista diferenciación clara en la manera de abordar estos problemas, en estrecha correspondencia con el grado de desarrollo de los países y el objetivo de la protección de su legislación, si existe consenso en la necesidad del tratamiento, prevención y penalización de las conductas delictivas generadas por el uso de sistemas informáticos en la sociedad.

A medida que aumenta la delincuencia electrónica, numerosos países han promulgado leyes declarando ilegales nuevas prácticas como la piratería informática, o han actualizado leyes obsoletas para que delitos tradicionales, incluidos el fraude, el vandalismo o el sabotaje, se consideren ilegales en el mundo virtual.

En la legislación penal cubana no se preceptúa aún las figuras que lo tipifiquen de modo particular las conductas conocidas como delitos informáticos, por lo que a la hora de juzgar estos hechos como delitos los tribunales se ven obligados a adecuar estas acciones a aquellas similares que aparecen tipificados en el código penal.

Desde el punto de vista penal primeramente hay que entender el delito informático y prepararse para ello. Se necesita además de que se unifiquen esfuerzos y que se asuma el enfrentamiento de manera dual, en la que los profesionales de la ley y los especialistas en informática trabajen juntos.

“Los primeros necesitan saber mucho de ese “mundo” y además de conocer los métodos tradicionales de investigación del delito, conocer cómo recoger y preservar las evidencias digitales, así como aspectos técnicos relacionados con la comisión de estos delitos. Los informáticos, por su parte, sí conocen las computadoras, las redes y su funcionamiento, pero carecen de la preparación en relación con la investigación legal y sus cuestiones, por lo que el trabajo en conjunto es lo ideal para obtener resultados exitosos en el enfrentamiento al delito.

Muchas de las acciones generales producto al uso indebido de la informática y las comunicaciones están relacionadas con figuras convencionales tales como el hurto, el robo, el fraude, la estafa, el espionaje, pero al realizarse dichas acciones con el auxilio de medios informáticos, se precisa, en cada caso un reanálisis de los elementos de la descripción legal, de la tipicidad de la norma vigente que conlleve la modificación de esta, haciéndola apta para ser aplicada a esos actos humanos, que se incrementan de forma directamente proporcional al desarrollo científico y técnico de la sociedad. Llama la atención sobre este particular porque si nos atenemos a uno de los elementos del concepto de delito: la tipicidad, no podremos considerar como tal una conducta que no ha sido previamente recogida por la legislación penal en vigor, resulte evidente que el Derecho Penal tiene un carácter normativo, clasista, determinado y determinante y cumple funciones de prevención, pero para que cumpla esa función necesita estar contenida en una norma jurídica, razón por la cual uno de sus principios fundamentales es que nadie puede ser sancionado sin una norma previa que reprima tal actuación y salta a la vista de que muchas de las conductas descritas en las clasificaciones establecidas no se ajustan.

Los delitos pueden clasificarse por el objeto, es decir, por el bien jurídico tutelable se clasifican en delitos de daño y de peligro, en el primero se daña, destruye pulveriza el bien

jurídico y en el segundo solo se amenaza ese bien jurídico con un posible o potencial perjuicio, toda vez que se entiende por objeto del delito, lo que ataca o amenaza al sujeto, que no es otra cosa que la relación jurídica, por lo que es necesario crear una legislación que vele por la seguridad de los sistemas de información, cuyos rasgos fundamentales son tres: integralidad, confidencialidad de la información, categorías conformadoras de lo que ha dado en llamar Seguridad Informática; y que pasaría a ser el bien jurídico que se pretende tutelar.

La generalización del uso de la informática ha provocado también un cambio en las características de los comisores de estos delitos, pues requerirán de determinados conocimientos y posición ocupacional. Hoy cualquier persona con medianos conocimientos de informática puede llegar a ser un delincuente informático.

El sujeto activo de los delitos informáticos se caracteriza y a la vez se diferencia del delincuente común en sus habilidades y destrezas para el manejo de la tecnología de la información, se consideran personas inteligentes, audaces y motivadas, dispuestas a aceptar cualquier reto tecnológico

El sujeto pasivo en este tipo de delito puede ser cualquier persona u organización privada o pública que utilice sistemas automatizados de información en red generalmente conectados a otros equipos o sistemas externos al que se le ocasione daños o perjuicios.

Los delincuentes de la informática son tan diversos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado.

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

Por todas las razones antes expuestas se requieren serias modificaciones y en otros casos nuevas normas que garanticen el adecuado funcionamiento de los sistemas de información para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático.

Ante la aparición de estas conductas, en los países en los que ha legislado sobre la materia, se han puesto en práctica dos vías de solución legislativa: Dedicar un título en las leyes penales a los llamados delitos informáticos.

Agregar a las figuras delictivas existentes en el código, aquellas descriptivas de tales acciones, bien como figuras nuevas ubicadas a continuación de los delitos convencionales con los que pueden tener relación, o bien incluyéndolos como modalidades agravadas o atenuadas, según el caso, de las ya previstas, en la Ley.

El Derecho Informático en el mundo, y en particular el referente a la rama penal es aún muy incipiente a escala mundial, en el caso de Cuba, coincidimos con la colega cubana Mariana Gómez en que la vía más adecuada para enfrentar estas conductas es la revisión de los delitos convencionales previstos en el Código Penal Cubano y atemperar su formulación a las nuevas condiciones en que puede materializarse la acción a través de medios

informáticos y en los casos en que esto no sea posible, agruparlas dentro de un nuevo Título dedicado a tutelar como bien jurídico la Seguridad Informática.

Conclusiones

- Es necesario que en la norma penal sustantiva sea preceptuado un nuevo título "Delitos Informáticos", un capítulo relacionando los delitos de manipulación que posea como figuras básicas: la manipulación de los datos de entrada, la manipulación de programas, la manipulación de los datos de salida y fraude efectuado por manipulación informática además del sabotaje informático, todos encaminados a la protección de un bien jurídico tutelado por la Constitución de la República de Cuba" los derechos individuales y el derecho a la intimidad y los derechos patrimoniales".

- Además pueden ser creadas figuras derivadas de delitos como Hurto, Robo con Fuerza en las Cosas, Malversación y Falsificación de Monedas así como el daño a través de medios informáticos o mediante el uso de los mismos para adquirir mayor probabilidad de éxito o en la ejecución de los mismos.

- Debido a que el Derecho Penal progresa con el desarrollo de la sociedad y también los modos de perpetración de los delitos, el ordenamiento jurídico cubano debe atemperarse a estos cambios, donde conductas delictivas relacionadas con la informática no deben continuar desprotegidas.

Bibliografía

Arregoitia López, Lic. Siura L. "Protección contra los delitos informáticos en Cuba" Facultad de Derecho. La Habana. Cuba. 2014.

Piqueres Castellote, Francisco. Conocimientos básicos en internet y utilización para actividades ilícitas en Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad? Cuadernos de Derecho de Derecho Judicial. Consejo General del Poder Judicial. Editorial Madrid, 2006.

Balanta, Heidy. Aproximación legal a los delitos informáticos una visión de derecho comparado. Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal.La Habana. Cuba. 2009.

Arregoitía López, Siura L– Protección contra los delitos informáticos [on-line],2014[citado: septiembre 14 de 2014]. Disponible en http://www.informatica-juridica.com

Gómez, Mariana - Criminalidad Informática, un fenómeno de fin de siglo [on-line], 2014[citado: septiembre 22 de 2014]. Disponible en http://www.alfa-redi.org.com

Rodríguez Da Costa, Marco Aurelio -El Derecho Penal Informático vigente en Brasil [on-line],2014[citado: octubre 20 de 2014]. Disponible en http://www.alfa-redi.org.com

Fuentes Legales:

Reglamento sobre la Protección y Seguridad Técnica de los sistemas informáticos Ministerio de la Industria Sideromecánica.La Habana. Cuba. Noviembre del 1996.

Código Penal, Ley No 62 del 29 de diciembre de 1987, actualizado, Ed. Félix Varela, La Habana. 2007.

Constitución de la República de Cuba, impreso en la Empresa Gráficas de Granma. Junio de 2004.

Resolución No.127/2007. Reglamento de Seguridad para las tecnologías de la Información.2007.

Reglamento de Seguridad Informática emitido por el Ministerio del Interior. Noviembre de 1996.