DELITOS INFORMÁTICOS, ¿MITOS O REALIDAD?

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

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

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

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

.

CD de Monografías 2014

Resumen

Existe una aguda polémica en relación con la necesidad de inclusión o no de los delitos informáticos en la parte especial del Código Penal y no verlo como una mera sanción administrativa para lograr que las personas se contengan a la hora de cometer un delito informático. Con la siguiente investigación se pretende 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, se 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. 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

***Palabras claves**: Delito informático, Código Penal, Conducta antijurídica*

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 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.

1. Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
2. Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
3- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
4. Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
5. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Estas conductas antijurídicas dejan planteadas, en teoría y práctica, infinidad de interrogantes, al extralimitar los modos tradicionales de comisión de delitos, revelando nuevas formas de ejecución y dejando además abierta para Criminología, la necesidad de evaluar nuevos rasgos de los ambientes delictivos y de los sujetos comisores de los mismos.

Los progresos mundiales de las computadoras, el creciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia

artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto

Un delito informático o ciberdelincuencia es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática, sin embargo; las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Por medio de estructuras electrónicas se realizan actividades ilícitas que van ligadas a un sin número de herramientas delictivas que buscan infringir y dañar todo lo que encuentren en el ámbito informático: ingreso ilegal a sistemas, interceptado ilegal de redes, interferencias, daños en la información, borrado, dañado, alteración o supresión de datos, mal uso de artefactos, chantajes, fraude electrónico, ataque a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, pornografía infantil, pedofilia en Internet, violación de información confidencial y muchos otros.

En Cuba se han venido promulgando algunos textos legales que sin ser penales, establecen determinadas regulaciones dirigidas a garantizar la Seguridad Informática. En Noviembre de 1996, entró en vigor el Reglamento de Seguridad Informática emitido por Ministerio del Interior el cual establece la obligación por "parte de todos los Organismos de la Administración Central del Estado de analizar, elaborar y poner en práctica el Plan de Seguridad Informática y Contingencia. Por esa misma fecha el entonces Ministerio de la Sideromecánica y la Electrónica, actual Ministerio de la Industria Sideromecánica, dictó el Reglamento sobre la Protección y Seguridad Técnica de los sistemas informáticos. Más adelante entró en vigor la resolución 127 / 2007 que aprueba y pone en vigor el Reglamento de Seguridad para las Tecnologías de la información.

A partir de la aplicación de estos reglamentos se han desarrollado y asesorado varios estudios parciales de situación operativa en el ámbito informático a entidades y empresas que por interés operativo o por informaciones ha sido prioridad para identificar la raíz de determinadas irregularidades.

Las empresas como INFOMED, Ministerio del Comercio Exterior (MINCEX), Cámara de Comercio, Ministerio de Justicia (MINJUS), Cubarte, Universidad de la Habana, Corporación CIMEX, COPEXTEL y el propio Ministerio de Informática y Comunicaciones han sido objeto de ataques y blancos de manifestaciones delictivas.

Los estudios realizados permitieron identificar como principales vulnerabilidades favorecedoras de la ocurrencia de actividades ilícitas las siguientes:

1. Existencia de usuarios que no pertenecen al grupo de administración, con cuentas que poseen privilegios plenos intercambio de información sensible a través de redes inalámbricas convencionales o por los correos electrónicos internacionales.
2. Presencia de información sensible en los activos informáticos que presentan conexión a Internet.
3. La existencia de recursos compartidos en la red donde se albergan programas de gestión ejecutables, así como informaciones sensibles del ámbito financiero, comercial, jurídico, organizativo entre otros.

Otros estudios desarrollados relacionados con temas informáticos han permitido determinar una serie de modalidades delictivas que afectan las infraestructuras informáticas del país, entre las que podemos encontrar, como más representativos, los siguientes:

a) Adquisición, montaje e instalación de sistema de antena parabólica que tienen acceso al internet de forma directa con el satélite, con la capacidad de recibir y enviar información. Servicios que brinda una entidad del Departamento de Defensa de los EEUU, por lo tanto no hay forma de controlar de lo que esta persona accede en la Internet.

b) Venta ilegal de cuentas para acceso a Internet y al correo eléctrico internacional.

c) Montaje e Instalación de servidores clandestinos los que se utilizan para brindar diversos servicios de comunicación.

d) Pizarras Telefónicas para la exportación de tráfico telefónico al exterior.

e) Comercialización ilegal de equipos de cómputos a través de las páginas en Internet relacionadas con Cuba para la venta de disímiles artículos.

f) Clonación de tarjetas pre-pagadas en CUC para la comunicación, al exterior fundamentalmente, a través de la telefonía pública.

El total de los recargadores emplean conexiones a la Internet, algunos lo hacen sobre cuentas legales a través de extranjeros, su mayoría de forma ilegal con cuentas robadas o por diferentes entidades. Realizan tareas de carga de tarjetas magnéticas para activar los sistemas satelitales, modificaciones y/o alteraciones dentro de los equipos para garantizar a los clientes acceder a los equipos hacia los canales televisivos del satélite, utilizan los datos de cuentas de tarjetas de créditos robadas (en el exterior) para pagar sus deuda o servicios.

Otras modalidades delictivas que afectan la Infraestructura informática son las siguientes:

a) Personas que crean y desarrollan programas de computación malignos, aplicaciones desarrolladas para destruir, mutilar modificar o inutilizar sistemas informáticos, información digitalizada, entre otros.

b) Se agrupan en 4 tipos de programas: la Bomba Lógica, el Gusano, el Caballo de Trolla y los Virus Informáticos.

c) La Bomba Lógica constituye un conjunto de instrucciones que se autoejecuta en un momento determinado, dada determinadas condiciones.

d) El Gusano es un programa con identidad propia que una vez que ha sido abierto busca espacio libre en la memoria interna de la computadora y se autograba en dicha memoria hasta el desbordamiento físico de la misma.

e) Un Caballo de Trolla es un programa legítimo que contiene una sección de "código oculto" , y a primera vista parece un programa inofensivo identificado generalmente con un nombre provocativo.

f) El virus informático es un segmento de programa de computación con capacidad para autorreproducirse y que al ser ejecutado cambia la estructura del software del sistema y destruye o altera programas o datos o provoca otras acciones sin autorización ni conocimiento del operador, de esta forma se afectan terceros que por desconocimientos, negligencias o fallas en los sistemas, cargaron el programa maligno en sus sistemas y se les provocó un daño, que en la mayoría de las ocasiones es irreparable.

Es de tal importancia percibir el daño a tiempo, quizás este pueda solucionarse, pues en la actualidad ciertamente los reglamentos vigentes no son suficientes para el control de las ilegalidades en este sentido, los sistemas informáticos continúan siendo blancos de infracciones, por lo que se considera oportuno el análisis de la posibilidad de reprimir los actos contrarios al buen funcionamiento de la tecnología informática a través de nuestra ley penal sustantiva.

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.

Según las autoras un delincuente informático es aquella persona que comete en un delito informático con ayuda de la computadora, como se pudo observar en el desarrollo de la presente investigación se centró en analizar la tipificación de los delitos informáticos en el Código Penal, por el nivel de importancia que estos presentan en la sociedad deben ser tomadas en cuenta para evitar este tipo de infracciones.

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, coincido 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

Con el avance de los sistemas informáticos se han desarrollado delitos de tipo tradicional en formas no tradicionales, estos ofrecen oportunidades sumamente complicadas de infringir en la ley. También se hace necesario que se establezcan normas que garanticen un adecuado funcionamiento de los sistemas de información, pues se ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible de imaginar. En Cuba la vía más adecuada para enfrentar tales conductas es la investigación de los delitos convencionales previstos en el Código Penal Cubano y agregar a las figuras delictivas existentes en el código, aquellas descriptivas de tales acciones, bien como figuras nuevas ubicadas a continuación de los delitos tipificados con los que pueden tener relación, o bien incluyéndolos como modalidades agravadas o atenuadas, según el caso, de las ya previstas o agruparlas dentro de un nuevo título dedicado a tutelar como bien jurídico la Seguridad Informática.

Bibliografía

ARREGOITIA, S.L. Protección contra los delitos informáticos en Cuba, Facultad de Derecho.

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

BALANTA, H. Aproximación legal a los delitos informáticos una visión de derecho comparado, Ponencia presentada en el II Congreso Internacional de Criminología y Derecho Penal, 2009.

GÓMEZ, M. Criminalidad Informática, un fenómeno de fin de siglo [on-line], 2014[citado: Noviembre 16 de 2014]. Disponible en http://www.alfa-redi.org.com

PIQUERES, F. 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 Judicial, Consejo General del Poder Judicial, Editorial Madrid, 2006.

RODRÍGUEZ, M. A. 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.