REVISTA CARIBEÑA DE CIENCIAS SOCIALES

Diciembre 2018 - ISSN: 2254-7630

# "EL DELITO INFORMATICO, SU TRATAMIENTO EN EL ORDENAMIENTO JURIDICO CUBANO"
# "THE INFORMATIC CRIME, ITS TREATMENT IN THE CUBAN LEGAL ORDER"

**Autores: MSc. Neise Calixto González Cadalso.**
1[1] neisec@uniss.edu.cu
**2 [2]MSc. Delvis Ignacio Denis Morales. ****
**3[3]. MSc. Ramona Moraima Águila Villa. *****
Universidad de Sancti Spíritus "José Martí Pérez. Cuba

Para citar este artículo puede utilizar el siguiente formato:

Neise Calixto González Cadalso, Delvis Ignacio Denis Morales y Ramona Moraima Águila Villa (2018):

"El delito informático, su tratamiento en el ordenamiento jurídico cubano", Revista Caribeña de Ciencias Sociales (diciembre 2018). En línea

//www.eumed.net/rev/caribe/2018/12/delito-informatico-cuba.html

**RESUMEN:** En el proceso de globalización está el uso de las tecnologías las informáticas y las comunicaciones. El desarrollo de tecnologías trae nuevas formas delictuales en el ordenamiento jurídico, teniendo por finalidad los sistemas informáticos e internet. Cuba enfrenta importantes desafíos de adaptación jurídica en pos de informatizar de la sociedad; constituye un reto el delito por computadora; pues se pueden invadir sistemas de seguridad, correos, se sabotaje a bases de datos de entidades e instituciones bancarias y financieras dando lugar a la sustracción de dinero o inhabilitar sus operaciones, viéndose afectado su patrimonio; incluso violación la privacidad de personas. Para enfrentar al ciberdelincuente se necesita conocer su conducta o modo de actuación que puede ser: Hackers persona que accede o interfiere sin autorización sistemas informáticos; Crackers persona que desde sistemas remotos destruyen datos y causan problemas a los procesadores o redes informáticos; Phreaker especialista en telefonía que utiliza las telecomunicaciones gratuitamente; el Virucker en la persona que introduce virus; el Pirata es el que reproduce, vende o utiliza software que no le pertenecen o grava música de internet para CD. El Código Penal Cubano los preceptos sancionadores utilizados

[1] Profesor Auxiliar, imparte las asignaturas Seguridad y Defensa Nacional, Máster en Educación Superior "Mención Derecho". Ha impartido posgrado de Seguridad y Defensa Nacional. Ha participado en talleres provinciales de Educación Patriótica Militar e internacionalista, así como en nacionales de Riesgos de Desastres. Participó en el X Congreso Internacional de Desastre y la VI Conferencia Internacional de Bomberos

[2] Profesor Asistente Máster en Ciencias de la Educación Superior, imparte las asignaturas Seguridad y Defensa Nacional. Ha impartido posgrado de Seguridad y Defensa Nacional. Ha participado en talleres provinciales de Educación Patriótica Militar e internacionalista.

[3] Profesor Asistente Máster en Ciencias de la Educación Superior, , imparte las asignaturas Seguridad y Defensa Nacional Ha impartido posgrado de Seguridad y Defensa Nacional. Ha participado en talleres provinciales de Educación Patriótica Militar e internacionalista.

contra el ciberdelincuente se limitan a: falsificación de documentos bancarios y de comercio; estafa; apropiación indebida, entre otros. Los códigos penales latinoamericanos, y la ley de delitos informáticos, se refieren a delitos tales como: acoso ilícito, atentado contra a la integridad de datos informáticos, atentados a la integridad de sistemas informáticos, entre otros.
**Palabras claves:** delito informático, tratamiento, ordenamiento jurídico cubano.

**SUMMARY**: In the process of globalization is the use of computer technologies and communications. The development of technologies brings new forms of crime in the legal system, with the purpose of computer systems and the Internet. Cuba faces important legal adaptation challenges in order to computerize society; computer crime is a challenge; then security systems, emails, sabotage to databases of banking and financial entities and institutions can be invaded, resulting in the theft of money or disable their operations, their assets being affected; even violation of people's privacy. To confront the cybercriminal you need to know their behavior or mode of action that can be: Hackers person who access or interfere with computer systems without authorization; Crackers who from remote systems destroy data and cause problems to processors or computer networks; Phreaker specialist in telephony that uses telecommunications free of charge; the Virucker in the person who introduces virus; the Pirate is the one who reproduces, sells or uses software that does not belong to him or graves music from the internet for CD. The Cuban Penal Code the sanctioning precepts used against the cybercriminal are limited to: falsification of bank and commercial documents; fraud; misappropriation, among others. The Latin American criminal codes, and the law of computer crimes, refer to crimes such as: unlawful harassment, attack against the integrity of computer data, attacks on the integrity of computer systems, among others.
**Keywords:** cybercrime, treatment, Cuban legal system.

**Introducción**

Se plantea que ante los retos de los procesos de integración económica, política, social y cultural derivada de la globalización, se acompañada de un desarrollo vertiginosos de las Tecnologías las Informáticas y las Comunicaciones (TIC), Las nuevas herramientas que ofrecen las TIC al servicio del hombre están relacionadas con la *transmisión, procesamiento y almacenamiento* digitalizado de información, así como un conjunto de procesos y productos que simplifican la comunicación y hacen más viables la interacción entre las personas.

Se indica que las aplicaciones de las TIC a partir de internet, entre ellos *"cibergobierno", "cibereducacion"* y *"cibersalud"* se consideran elementos habilitantes para el desarrollo social puesto que proporcionan un canal eficaz para distribuir una amplia gama de servicios básicos en zonas remotas y rurales, pues estas aplicaciones facilitan el logro de los objetivos de desarrollo prospectivo, mejoras en las condiciones, medioambientales y en los Sistemas de Alerta Temprana ante desastre naturales .tecnológicos y sanitarios.

Se expresa que en la era de la informática se incrementan los riesgos relacionados a las tecnologías informáticas y de comunicación. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet.

Son evidentes los beneficios de los adelantos tecnológicos que trae para la sociedad el pos de la tecnología informática y comunicación, estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y la distribución de pornografía infantil y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos *"pishing",* la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

## 1. ASPECTOS GENERALES DEL DELITOS INFORMÁTICOS

Se plantea que "*el creciente desarrollo de tecnologías que permiten el almacenamiento, procesamiento y transmisión de grandes cantidades de información virtual, no sólo ha revolucionado los hábitos de trabajo y comunicación de las personas, sino que ha traído consigo importantes desafíos de adaptación jurídica; para nuestro país que marcha hacia la informatización de la sociedad cubana, constituye un reto, el*

*delito por computadora, pues no existe una norma en el ordenamiento jurídico cubano que penalice tales acciones"*

Se agrega que *"así ha sucedido, por ejemplo, en el ámbito del reconocimiento jurídico de los documentos electrónicos o a partir del siempre mayor desarrollo del comercio electrónico a través de Internet."*

Se indica que *"en el ámbito específico del Derecho Penal, la experiencia ha demostrado que el avance tecnológico trae consigo también nuevos peligros, nuevas formas de ataque contra bienes jurídicos relevantes"*

Se expresa que "*los delitos informáticos6 se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etc.; sin embargo esta forma de criminalidad no solo se comete a través de estos medios, pues éstos son solo instrumentos que facilitan pero no determinan la comisión de estos delitos. Esta denominación, es poco usada en las legislaciones penales; no obstante bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática*"

En la doctrina no existe un acuerdo en cuanto al concepto de delito informático. "podemos definir el delito informático como: acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de máquinas- hardware- o de los programas software" (Dávara Rodríguez, 1993, citado en (Chinchilla Sandí, Delitos Informáticos. Elementos básicos para identificarlos y su aplicación, 2004))

*"Por nuestra parte, entendemos a la criminalidad informática como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidos a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que las TIC son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión"*

*"Sin embargo, los delitos de ingresar sin autorización a un sistema de datos, sabotear la base de datos si se clasifican dentro de los delitos informativos porque no es posible la comisión de estos delito sin la intervención de la informática"*

*"Respecto de los delitos informativos, Krutisch citado por Mazuelos, identifica tres tipos de categorías: manipulación informática, sabotaje informático y acceso no autorizado a datos o sistema computarizados; pero no son categorías de delitos, sino modos de cometer los delitos informativos"*

"La doctrina, conforme hemos visto en anteriores oportunidades, aun no se ha puesto de acuerdo sobre la existencia de un bien jurídico penal en los delitos informáticos, ni menos aún en su contenido, sin embargo , el análisis se identificara según lo que es acorde a la realidad tecnológica de nuestra legislación"

*"Analizando la problemática del bien jurídico desde la sistemática empleada en nuestro ordenamiento punitivo, resulta confuso determinar lo protegido penalmente en el delito informático, si consideramos que la descripción se encuentra situada en los delitos contra el Patrimonio. En dicho capítulo, se considera como bien jurídico-penal tutelado al Patrimonio, en consecuencia, si realizamos una interpretación sistematiza de nuestra norma la protección seria directamente, valga la redundancia, el Patrimonio"*

*"El bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero se encuentra la "información" de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etc. Respecto de la información, debe ser entendida como el contenido de las bases y/o banco de datas o el*

*producto de los procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico y es la importancia del "valor económico" de la información lo que ha hecho que se incorpore como bien jurídico tutelado"*

**"***Sin embargo, creemos que la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco de la persona por la fluidez y el trafico jurídico, y por los sistemas que lo procesan o automatizan los mismos que equiparan a los bienes protegidos tradicionales tales como el patrimonio (fraude informático), la reserva, la intimidad y confidencialidad de los datos (agresiones informáticas a la esfera de la intimidad), seguridad o fiabilidad del trafico jurídico probatorio (falsificación de datos o documentos probatorios), etc."*

***"****Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados18, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos*."

Se expresa que *"las principales características de vulnerabilidad que presenta el mundo informático son las siguientes:*

*a. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.*
*b. El creciente número de usuarios, y la facilidad de acceso al medio tecnológico.*
*c. El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.*
*d. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos."*

Se indica que "*El perfil del ciberdelincuente -sujeto activo- en esta modalidad delictual requiere ciertas habilidades y conocimientos en el manejo del sistema informático, por ello también se les ha calificado como delincuentes de "cuello blanco", que tienen como características:*
 *Poseer importantes conocimientos informáticos.*
 *Ocupar lugares estratégicos en su centro laboral, en los que se maneja información de carácter sensible (se denomina delitos ocupacionales, ya que se comenten por la ocupación que se tiene y el acceso al sistema)."*

Para Marcelo Manson, los infractores de la Ley penal en materia de Delitos Informáticos no son delincuentes comunes y corrientes sino que por el contrario, son personas especializadas en la materia informática. Agrega que "*las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es habilidades para el manejo de los sistemas informáticos y que por su situación laboran en puestos estratégicos donde se manejan información sensible*

"Por su parte, Camacho Losa considera que el perfil de estas personas no coincide con el de un delincuente marginal y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas. También, Vives Antón y Gonzales Cussac afirman que "sujeto activo puede ser tanto las personas legítimamente autorizadas para acceder y operar el sistema (*operadores, programadores u otros*), como terceros no autorizados que acceden a las terminales públicas o privadas"

"Se pueden identificar diferentes sujetos activos que se les denomina de diferente manera dependiendo del modo como actúan y que conductas son las que realizan:

*HACKERS.-* Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, conocido como "*delincuente silencioso o tecnológico*". Les gusta indagar por todas partes, conocer el funcionamiento de los sistemas informáticos; son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos. Para Sieber los hacker son "*personas que acceden sin autorización a un sistema de proceso de datos a través de un proceso de datos a distancia, no cometido con finalidades*

*manipuladoras, fraudulentas, de espionaje, ni sabotaje, sino sencillamente como paseo por placer no autorizado*". Morón Lerma define a los hacker como *"personas que acceden o interfieren sin autorización, de forma subrepticia, a un sistema informático o redes de comunicación electrónica de datos y utilizan los mismos sin autorización o más allá de lo autorizado""*

CRACKERS.- Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como "piratas electrónicos." A característica que los diferencia de los hacker es que los crackers usan programas ya creados que pueden adquirir, normalmente vía internet; mientras que los hackers crean sus propios programas, tiene mucho conocimiento sobre los programas y conocen muy bien los Lenguajes informáticos. Por otra parte, Morant Vidal define a estos sujetos como personas *que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas*". También, Alfonso Laso sostiene que el cracker "*es la persona que, de manera intencionada, se dedica a eliminar o borrar ficheros, a romper los sistemas informáticos, a introducir virus, etc.*".

Son captadores de contraseñas, es un programa que descripta las contraseña o elimina su contraseña

Según *"(Bismarck Rodríguez Madrigal, et al) en su monografía para optar por el título de Licenciatura en Derecho "Los delitos informáticos y la información como nuevo bien jurídico protegido" se consideran como conductas ilegales más comunes las siguientes: Hackers, Crackers, Phreaker, Virucker y el Pirata Informático."*

Se explica que "*Phreaker es el especialista en telefonía, empleando sus conocimientos para poder utilizar las telecomunicaciones gratuitamente; el Virucker, es el ingreso doloso de un tercero en sistema informático ajeno, con el objetivo de introducir "virus" y destruir, alterar y/o inutilizar la información contenida, que pueden ser benignos molestan pero no hacen daño y los malignos que destruyen información o impiden trabajar y el Pirata Informático es quien reproduce, vende o utiliza Software que no le pertenecen o que no tiene licencia de uso, así como grabar música de Internet para grabarla en CD"*

Se expresa que "*la persona jurídica sí puede ser considerada como sujeto pasivo, como por ejemplo, empresas públicas y privadas (bancos, instituciones públicas, industrias, seguros, etc.), aunque en ciertos casos, estas personas jurídicas no denuncien los delitos del que son víctimas por cierto temor al desprestigio o al impacto entre sus clientes y consecuentes efectos económicos desfavorables".*

Gutiérrez Francés señala que "*el sujeto pasivo por excelencia del ilícito informático es la persona jurídica, debido al tráfico económico en el que desarrollan sus actividades, por ello son los sectores más afectados por la criminalidad mediante computadoras, y entre ellos están: la banca, las instituciones públicas, industria de transformación, etc."*

Según *"(Bismarck Rodríguez Madrigal, et al) en su monografía para optar por el título de Licenciatura en Derecho "Los delitos informáticos y la información como nuevo bien jurídico protegido" se consideran como tipos de delitos más comunes: Fraude a través de computadoras; conductas dirigidas a causar daños lógicos; la sustracción de información clasificada; uso ilegítimo de sistemas informáticos ajenos; el espionaje informático que tiene como técnicas: dialers, adware, programas de acceso remoto, programa de espionaje o spyware; la estafa informática con sus variedades: rounding of utility (redondeo) data didling (falsificación de datos, piggy backing (suplantación de la personalidad del usuario; la falsificación informática (delito de cuello blanco); sabotaje informático con sus modalidades: virus informático, gusanos informáticos, bombas lógicas; la piratería informática con sus formas: usuario de empresa o usuario finales, licencias de sustracción, derecho al primesupport, piratería por internet, falsificación, carga en el disco duro; la pornografía infantil por internet y por último el terrorismo en internet."*

**1. EL CODIGO PENAL CUBANO**

Se realiza en nuestro país una Reforma Constitucional, el que debe incluirse el Delito Informático, ya que nuestra sociedad cubana marcha hacia la informatización de la sociedad en aspectos tales como el uso

de la Internet, las tarjetas de pago del salario de los trabajadores, operaciones bancarias, el uso de los cajeros automáticos, las salas de Joven Club de Computación, los laboratorios de computación en las universidades, el uso de la telefonía celular, el usos de los correos electrónicos, las transacciones comerciales entre entidades, entre otras. Se corre el riesgo de los delitos informáticos y las consecuentes pérdidas económicas en la población y al país con la proliferación de los Delitos de cuello blanco y otros fenómenos.

A la hora de sancionar por un delito informático hay que hacerlo por preceptos tales como: Falsificación de Documentos Bancarios y de Comercio**;** Estafa; Apropiación Indebida. Preceptos legales que serán mostrados a continuación

Falsificación de Documentos Bancarios y de Comercio**,** Articulo 251. 1.- El que cometa false-dad de alguno de los modos que determina el apartado 1 del artículo 250, en cheques, mandatos de pago o cualesquiera otros documentos bancarios o de comercio, incurre en sanción de privación de libertad de tres a ocho años. 2. El que, con conocimiento de su false-dad, haga uso de un documento de la clase expresada en el apartado anterior, o se aproveche de él en cualquier forma, o lo tenga en su poder para usarlo, es sancionado con privación de libertad de dos a cinco años. **3.** Si el delito lo comete un funcionario público, con abuso de sus funciones, incurre en sanción de privación de libertad de cinco a doce años. 4. Los actos preparatorios del delito pre-visto en este artículo se sancionan conforme a lo dispuesto en el artículo 12.5.

Estafa. Artículo 334.1.- El que, con el propósito de obtener para sí o para otro, una ventaja o un beneficio patrimonial ilegítimo, y empleando cualquier ardid o engaño que induzca a error a la víctima, determine a éste a realizar o abstenerse de realizar un acto en detrimento de sus bienes o de los de un tercero, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas.2. Si el culpable, para la ejecución del hecho, se aprovecha de las funciones inherentes al cargo, empleo, ocupación u oficio que desempeña en una entidad económica estatal, la sanción es de privación de libertad de dos a cinco años.3. Si por el delito el culpable obtiene un beneficio de considerable valor, o si la víctima sufre un grave perjuicio en sus bienes, o el hecho se realiza por uno o más individuos actuando como miembros de un grupo organizado, la sanción es de privación de libertad de cuatro a diez años.4. (Adicionado) Incurre en sanción de privación de libertad de dos a cinco años o multa de quinientas a mil cuotas o ambas, el que a sabiendas: a) libre un cheque sin provisión de fondos o con provisión insuficiente, o después de haber retirado dicha provisión; b) libre un cheque retirando la provisión de fondos antes de que el cheque pueda legalmente ser presentado al cobro o antes de haber anulado su expedición por cual-quiera de las formas que en derecho pro-ceda.**5.** (Adicionado) Si, en los hechos previstos en el apartado anterior, el culpable abona al perjudicado la cantidad correspondiente al cheque, antes de la celebración del juicio oral, queda exento de sanción. Los apartados 4 y 5 de este artículo fueron adicionados por el artículo 30 del Decreto-Ley No. 175 de 17 de junio de 1997 (G.O. Ext. No. 6 de 26 junio de 1997, pág. 37).

Apropiación Indebida. Articulo 335.1.- El que, con el propósito de obtener una ventaja o un beneficio patrimonial ilegítimo para sí o para otro, se apropie o consienta que otro se apropie de bienes que le hayan sido confiados, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas.2. Si los bienes apropiados son de considerable valor, la sanción es de privación de libertad de dos a cinco años o multa de trescientas a mil cuotas o ambas.3. Si el delito se comete por un conductor de vehículo de carga o de persona responsabilizada con la transportación de bienes, la sanción es de: a) privación de libertad de uno a tres años o multa de trescientas a mil cuotas o ambas, en el caso del apartado 1;b) privación de libertad de cuatro a diez años en el caso del apartado 2.4. Cuando los bienes apropiados sean de propiedad personal, sólo se procede si media denuncia del perjudicado. Si en este caso el denunciante desiste de su denuncia, por escrito y en forma expresa, antes del juicio, se archivarán las actuaciones.

Se comenta que todos los códigos penales latinoamericanos abordan en cierta forma el Delito Informaticen el sus preceptos, pero solo ejemplificaremos algunos y haremos referencias a algunos

países que tiene su Ley contra Delitos Informáticos, para que en nuestro código penal cubano se incluya en los delitos informáticos o se establezca un Ley al respecto

Se pudiese incluir un capítulo titulado "Delitos contra datos y sistemas informáticos" que pudiesen incluirse figuras delictivas tales como: *acceso ilícito*,; *atentando a la integridad de datos informáticos*; *atentando a la integridad de sistemas informáticos; los cuales se detallaran*

Esta figura penal de *Acceso ilícito* sanciona la violación de la confidencialidad, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad establecida para evitar que ajenos ingresen a un sistema informático

Por la característica que presenta este tipo penal –*atentado a la integridad de los datos informático*- es clasificado como un *delito de mera actividad,* porque esta figura exige el solo cumplimiento del tipo penal, la sola realización de la conducta de *introducir, borrar, deteriorar, alterar, suprimir y hacer inaccesible* los datos informáticos para que se pueda configurar el ilícito, sin importar el resultado posterior, por tanto el delito queda consumado al realizarse cualquiera de estos actos.

Está figura penal sanciona las conductas que están dirigidas a inutilizar *(hacer inútil, vano o nulo algo)* total o parcialmente un sistema informático, entorpecer *(retardar, dificultar)46*e imposibilitar *(quitar la posibilidad de ejecutar o conseguir algo)* su funcionamiento o la prestación de sus servicios utilizando las TIC; por la característica que presenta este tipo penal –*atentado contra la integridad de sistemas informáticos*- se clasifica como un *delito de resultado,* porque para la configuración de este injusto penal no basta con cumplir el tipo que es *(inutilizar o perturbar)*, sino además es necesario que la acción vaya seguida de un resultado *(impedir el acceso, imposibilitar su funcionamiento, o la prestación de sus servicios),* por tanto el delito se consuma cuando se impide el *acceso, imposibilita su funcionamiento*, *etc.,* del sistema informático, caso contrario el hecho solo dará lugar a la *tentativa.*

*Se indica que son ejemplos de atentando a la integridad de sistemas informáticos, los cuales no están plasmados en la norma jurídica penal y son los siguientes:*

*"DELITO DE DAÑO.- comportamiento consistente en dañar, destruir o inutilizar un bien, en este caso es el sistema informático, expresa Bramont- Arias que el delito de daños existirá si usuarios, carentes de autorización, alteran o destruyen archivos o bancos de datos a propósito; la destrucción total de programas y de datos ponen en peligro la estabilidad económica de una empresa. El modus operandi se viene perfeccionando con el tiempo: virus, cáncer rotudtine. Estos actos deben causar un perjuicio patrimonial."*

*"EL SABOTAJE INFORMÁTICO.- consiste, básicamente, en borrar, suprimir o modificar (alterar) sin autorización funciones o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema, que se conoce comúnmente como "virus informático". Marchena Gómez señala que el "sabotaje informático es la conducta que consiste en la destrucción o en la producción generalizada de daños"51. Morant Vidal señala que "el sabotaje informático se dirige a inutilizar los sistemas informáticos causando daños a los programas"*

Las técnicas que permiten cometer sabotaje informático son las siguientes:

*"BOMBA LÓGICA.- introducción de un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo"*

*"RUTINAS CANCER.- Son distorsiones al funcionamiento del programa, la característica es la auto reproducción"*

*"GUSANOS.- Se infiltran en los programas ya sea para modificar o destruir los datos, pero a diferencia de los virus estos no pueden regenerarse"*

*"VIRUS INFORMATICO Y MALWARE.- Elementos informáticos que destruyen el uso de ciertos antivirus Vgr. borrar los antecedentes policiales, judiciales y penales de una persona; alterar la deuda real de un cliente; cambiar la clave secreta o eliminar la cuenta electrónica (correo, twitter, facebook) para impedir al titular el acceso a su cuenta"*

Se pudiese incluirse un capitulo dos titulado: delitos informáticos contra la indemnidad y libertad sexuales, pues aunque la prostitución sexual no es fenómeno social , en los últimos tiempos se ha generalizado entre la población que oscila entre los 18 y 25 años, por la informatización de la sociedad y la existencia del "paquete de la semana" de edad, delitos tales como: *proposición a niños, niñas y adolescentes con fines sexuales por medios tecnológicos y solicitar u obtener material pornográfico, llevar a cabo actividades sexuales*

Se sanciona "*el contacto (establecer contacto o comunicación con alguien) realizado con un menor de edad con fines a obtener material pornográficos o con el propósito de llevar a cabo actividades sexuales que involucren el quebrantamiento de la indemnidad o libertad sexual del menor (violación sexual o actos contra el pudor)"*

*"DELITOS CONTRA LA LIBERTAD SEXUAL.- son acciones destinado a vulnerar tanto la indemnidad sexual como la libertad sexual del menor. Este delito se consuma con la sola proposición, a un menor de edad con fines sexuales, ya sea para obtener material pornográfico o para acceder a la actividad sexual, esta conducta es sancionable porque afecta la indemnidad del menor y la libertad sexual y el medio utilizado para facilitar el contacto es la informática"*

*"PORNOGRAFÍA INFANTIL.- en esta conducta tipificada se denota la intención del legislador de proteger penalmente varios bienes jurídicos, cuya titularidad corresponde a menores de edad, cuales son los adecuados procesos de formación y socialización de unos*
*y otros y, su intimidad. Lo que se busca sancionar con esta tipo penal es el acto de ofrecer, vender, distribuir, exhibir material pornográfico de menores de edad. Esta conducta está referida a un sujeto activo indiferenciado (delito de dominio), es de mencionar que esta modalidad es dolosa: el sujeto ha de conocer la naturaleza del material y ha de querer realizarlo, difundir o poseer con dichos fines siendo indiferente que lo haga con ánimo lubrico o de lucro"*

Se pudiese incluir el Capítulo 3 titulado Delitos informáticos contra el patrimonio, que contemple la figura delictiva del *fraude informático*), que sanciona la acción de *diseñar, introducir, alterar, borrar, suprimir y clonar datos informáticos* en perjuicio de tercero.

*"Se sanciona diversas conductas, entre ellos: diseñar (proyecto o plan), introducir (entrar en un lugar), alterar (estropear, dañar, descomponer), borrar (desvanecer, quitar, hacer que desaparezca algo), suprimir (hacer cesar, hacer desaparecer), clonar (producir clones)67 datos informáticos o cualquier interferencia, o manipular (operar con las manos o con cualquier instrumento) el funcionamiento de un sistema informático procurando (conseguir o adquirir algo) un beneficio para sí o para otro en perjuicio de tercero; Clonar tarjetas bancarias, el fraude informático afecta los programa social"*

Se pudiese incluir un capitulo cuatro titulado: Delitos informáticos contra la fe pública, que incluya el delito de *suplantación de identidad* sanciona la suplantación de identidad de una persona natural o jurídica, siempre que de esto resulte algún perjuicio.

**"**Este tipo penal sanciona el hecho se suplantar *(ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba)* la identidad de una persona natural o jurídica causando algún perjuicio."

"La *suplantación de identidad* se puede calificar como un delito de resultado porque no basta con realizar la conducta típica de "*suplantar*" la identidad, sino que además es necesario que esa acción vaya seguida de un resultado separado de la misma conducta que consiste en causar un perjuicio, caso contrario quedaría en tentativa. *Vgr. crear perfiles falsos en las redes sociales (correo electrónico, Facebook, Twitter) atribuidos a personas naturales y/o jurídicas para engañar y perjudicar a terceros*

Se pudiese incluir como disposición común, figuras como *abuso de mecanismos y dispositivos informáticos*

Se sanciona diversas conductas, entre ellas : "fabricar *(producir objetos en serie, generalmente por medios mecánicos),* diseñar *(hacer un diseño)*, desarrollar, vender *(traspasar a alguien por el precio convenido la propiedad de lo que uno posee*), facilitar *(proporcionar o* entregar), distribuir *(entregar una mercancía a los vendedores y consumidores)*, importa *(dicho de una mercancía: valer o llegar a cierta cantidad) y* obtener *(alcanzar, conseguir y lograr algo que se merece, solicita o pretende),* para la utilización de mecanismos, programas informáticos, contraseñas, etc., diseñados específicamente para la comisión de los delitos previstos en esta ley. Este artículo es una expresión del adelantamiento de las barreras punitivas porque se sanciona la participación y más aún el sólo hecho de ofrecer un servicio que facilite la comisión de algún delito previsto en la presente ley"

"Se sanciona actos preparatorios alegando la puesta en peligro de la seguridad informática. *Vgr. tráfico de datos de usuarios y contraseñas obtenidas ilícitamente para cometer fraudes informáticos, comercializar equipos especializados en capturar, interceptar información."*

**2. EL DELITO INFORMATICO EN EL ORDENAMIENTO JURIDICO LATINAMERICANO**
Se muestran a continuación como algunos códigos penales le dan tratamiento a los delitos informáticos en el mundo.

El **Código Penal panameño**, en el **Capítulo III** "Delitos contra la Inviolabilidad del Secreto y el Derecho a la Intimidad" articulo 162 y 163 hace referencia, mensaje de correo electrónico, el cual, será sancionado con prisión de uno a tres años o su equivalente en días-multa o arresto de fines de semana. *En el* ***Capítulo*** **IV** "Delitos contra la Libertad de Reunión y de Prensa" Quien fabrique, elabore por cualquier medio o produzca material pornográfico o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de Internet o de cualquier medio masivo de comunicación o información nacional o internacional, presentando o representando virtualmente a una o varias personas menores de edad en actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de cinco a diez años. **Capítulo III** Estafa y otros Fraudes Artículo 222. Quien, para procurarse para sí o para un tercero un provecho ilícito, altere, modifique o manipule programas, bases de datos, redes o sistemas informáticos, en perjuicio de un tercero, será sancionado con cuatro a seis años de prisión. La sanción será de cinco a ocho años de prisión cuando el hecho sea cometido por la persona encargada o responsable de la base de datos, redes o sistema informático o por la persona autorizada para acceder a estos, o cuando el hecho lo cometió la persona valiéndose de información privilegiada. **Capítulo III** Delitos Financieros **Artículo 239.** Quien, en beneficio propio o de un tercero, se apodere, ocasione la transferencia ilícita o haga uso indebido de dinero, valores u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que se le hayan confiado, o realice esas conductas a través de manipulación informática, fraudulenta o de medios tecnológicos, será sancionado con prisión de cuatro a seis años. **Capítulo I** Delitos contra la Seguridad Informática Artículo 285. Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.

El **Código Penal de Nicaragua** Título III delitos contra la vida privada y la inviolabilidad del domicilio. **Capítulo I** delitos contra la vida privada; **Art. 192** Apertura o interceptación ilegal de comunicaciones Quien ilegítimamente abra, intercepte o por cualquier otro medio se entere del contenido de una carta, un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido, será penado con prisión de seis meses a dos años. **Art. 197** Registros prohibidos El que sin autorización de ley promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que puedan afectar a las personas naturales o jurídicas, será penado con prisión de dos a cuatro años y de trescientos a quinientos días multa. **Art. 198** Acceso y uso no autorizado de información Quien, sin la debida autorización, utilice los registros informáticos de otro, o ingrese, por cualquier medio, a su banco de datos o archivos electrónicos, será penado con prisión de uno a dos años, y de doscientos a quinientos días multa.

**Código penal de Honduras Capítulo** VII violación y revelación de secretos **Articulo 214.** Quien sin la debida autorización judicial, con cualquier propósito, se apoderare de los papeles o correspondencia de otro, intercepta o hace interceptar sus comunicaciones telefónicas, telegráficas, soportes electrónicos o computadoras, facsimilares o de cualquier otra naturaleza, incluyendo las electrónicas, será sancionado con seis (6) a ocho (8) si fuere particular y de otro (8) a doce (12) años si se tratare de un funcionario o empleado público.

**Código penal de Costa Rica** Titulo VI delitos contra el ámbito de intimidad Sección I **Artículo 196** bis.- Violación de comunicaciones electrónicas Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accede, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos. **"Artículo 217** bis.- Fraude informático Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema**." Artículo 229 bis**.- Alteración de datos y sabotaje informático Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accede, *borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora. Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres* a seis años de prisión. Si el *programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años. (Así adicionado por Ley N° 8148 de 24 de octubre del 2001)* Artículo 229 bis.-

**Código penal Peruano, artículo 207**-D en el Código Penal peruano, mediante el que se tipifica el tráfico ilegal de datos, conforme al cual, "el que, crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

**Francia Ley número 88-19 de 5 de enero de 1988** sobre el fraude informático.-Acceso fraudulento a un sistema de elaboración de datos (462-2). Este artículo sanciona tanto el acceso al sistema como el que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.-Sabotaje informático (462-3). Este artículo sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.-Destrucción de datos (462-4). Este artículo sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.-Falsificación de documentos informatizados (462-5). Este artículo sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.-Uso de documentos informatizados falsos (462-6). Este artículo sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

**Ley de Delitos Informáticos de Perú "Artículo 2.** Acceso ilícito El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. **"Artículo 3.-** Atentado a la integridad de datos informáticos El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa." **"Artículo 4.** Atentado a la integridad de sistemas informáticos **"Artículo 5.-** Proposiciones a niños, niñas y adolescentes con fines sexuales por

medios tecnológicos **"Artículo 7-** Interceptación de datos informáticos El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. **"Artículo 8.** Fraude informático El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. **Artículo 9.-**Suplantación de identidad El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años. **"Artículo 10.** Abuso de mecanismos y dispositivos informáticos El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

*En* ***Venezuela existe un proyecto de Ley*** **sobre delitos informáticos Título II** De los delitos Capítulo I De los delitos contra los sistemas que utilizan tecnologías de información. **Artículo 6.-** Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. **Artículo 7.-** Sabotaje o daño a sistemas. El que destruya, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. **Artículo 10**.- Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas o seiscientas unidades tributarias. **Artículo 11.-** Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. **Capítulo II** De los delitos contra la propiedad **Artículo 13**. Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. **Artículo 14.**- Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información de ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias. **Artículo 15**.- Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice la tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer

su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias**. Artículo 18**.- Provisión indebida de bienes o servicios. El que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, han sido falsificados, alterados, se encuentran vencidos o revocados o han sido indebidamente obtenidos o retenidos, provea a quien los presente, de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. **Artículo 19.-** Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venta, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos unes o cualquier ,equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias. **Capítulo III** De los delitos contra la privacidad de las personas y de las comunicaciones **Artículo 20.-** Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero. **Capítulo IV** De los delitos contra niños y adolescentes **Artículo 23**.- Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias. **Capítulo V** De los delitos contra el orden económico **Artículo 25**.- Apropiación de propiedad intelectual. El que, sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

**2.1Tratados internacionales**

Se expresa por Egil Emilio Ramírez Bejerano* Ana Rosa Aguilera en la Gaceta Jurídica que *"En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifique los derechos penales nacionales"*

*"El GATT (Acuerdo General sobre Aranceles Aduaneros y Comercio) se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC); por consecuencia, todos los acuerdos que fueron suscritos en el marco del GATT siguen vigentes."*

*"En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifique los derechos penales nacionales"*

*"En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e, incluso, transnacional, cuyo principal problema es la falta de una legislación unificada que facilita la comisión de los delitos".*

*"En 1990, en el VIII Congreso sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas (ONU), celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los países y que, por ello, se había difundido la comisión de actos delictivos."*

*"La ONU ha publicado una descripción de "Tipos de delitos informáticos". En 1992, la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo, Alemania, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos si no basta con la adopción de otras medidas, por ejemplo, el "principio de subsidiariedad".*

*"Hay otros convenios realizados por la Organización Mundial de la Propiedad Intelectual (OMPI). En noviembre de 1997, en Mérida España, se realizaron las II Jornadas Internacionales sobre el Delito Cibernético, donde se desarrollaron temas tales como aplicaciones en la administración de las tecnologías informáticas/cibernéticas; blanqueo de capitales, contrabando y narcotráfico; hacia una policía Europea en la persecución del delito cibernético; internet: a la búsqueda de un entorno seguro y marco legal y deontológico de la informática."*

Cuba debe realizar sus ajustes en esta materia o instituir una "Ley de Delitos Informáticos.", pues el Código Penal no es preciso y debe acudir a preceptos análogos, lo que da lugar a lagunas del derecho en la materia penal.

**Conclusiones**

Se ha demostrado que en la era de la informática se incrementan los riesgos relacionados a las tecnologías informáticas y de comunicación.

Se ha dicho que los adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y la distribución de pornografía infantil y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos *"pishing",* la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales.

Urge a nuestra legislación cubana, incorporar estos delitos informáticos, sobre todo nuestro Código Penal y sus nuevas figuras delictivas de forma más diáfana, así como incorporar al ordenamiento legal una Ley sobre Delitos Informáticos, debido al auge de los mismos en el mundo y Cuba.

**Bibliografía**

Arocena, G. A. (2012); "*La regulación de los delitos informativos en el código penal argentino. Introducción a la ley nacional N° 26.388"*, en Boletín Mexicano de Derecho Comparado, nueva serie, año XLV, N° 135, México, pág. 945- 988.

Azaola C, L. (2010); "Delitos informáticos y Derecho penal", UBIJUS, México, pág. 69.

Azaola C, L. (2010); "*Delitos informáticos y Derecho penal*", UBIJUS, México, pág. 27.

Azaola C, L. (2010)"*Delitos informáticos y Derecho penal*", óp., cit., pág. 27- 28.

Bramont- Arias, L. A (2000).; "Delitos informáticos", en Revista Peruana de Derecho de la Empresa Derecho Informático Y Teleinformática jurídica, Nº 51, Asesorandina. Lima.

Camacho L, L.(1967) "El delito informático" Gráficas Cóndor, Madrid, pág. 83- 84

Cfr. Gutiérrez F., (2012) "*Atentados contra la información como valor económico de empresa" Mazuelos Coello/Reyna Alfaro, "Delitos informático"/Durand Valladares, "Los delitos informáticos en el Código Penal Peruano"* Urquizo Olaechea, Revista Peruana de Ciencias Penales. N° 11, Lima.

Convenio sobre la ciberdelincuencia – Budapest, 23.XI.(2001): Cap. II, sección 1º, titulo 2º, Art. 8º.- fraude informático.

De Alfonso Lazo, D (2001); “El hackerin blanco. Una conducta ¿punible o impune?”, en Internet y derecho penal, Cuadernos de Derecho Judicial, Consejo General del poder Judicial, Madrid, pág.110-111.

Decreto 144-83 (26 de septiembre de 1983).

Decreto Legislativo Nº 635 (21-02-98).

Gonzáles de Chaves Calamita, M, E. (2004); “*El llamado ´delito informático´”,* en Anales de la Facultad de Derecho de la Universidad de la Laguna N° 21, España, 2004, pág. 44 – 65.

La Gaceta Jurídica (2016) Los delitos informáticos. Tratamiento internacional por Egil Emilio Ramírez Bejerano* Ana Rosa Aguilera legislacioncomparada.pdf. [visto el 23 de diciembre 2018].

Manson, Marcelo; *“Legislación sobre delitos informáticos”*, en https://dl.dropbox.com/u//dl.

Marchena G, M (2001); “El sabotaje informático: entre los delitos de daños y desordenes públicos”, en Internet y Derecho Penal, Cuadernos de Derecho Judicial, Madrid, pág. 356.
Miró L, F. (2012); “*El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*”, Marcial Pons, Madrid, pág. 44.

Morant V, J. (2002); “protección penal de la intimidad frente a las nuevas tecnologías”, Ed. Practica de Derecho, valencia, 2002, pág. 44.

Morant V, J. (2003); “Protección penal de la intimidad frente a las nuevas tecnologías”, Ed. Practica de Derecho, Valencia 2003, pág. 46- 47.

Moron L, E. (2002); “Internet y Derecho Penal: hacking y otras conductas ilícitas en la red”, Ed. Aranzadi, Navarra,, 2° ed., pág. 51.

Ley Nº 62 Código Penal cubano (29 de diciembre, 1987)

Ley 14 de 2007, con las modificaciones y adiciones introducidas por la Ley 26 de 2008, la Ley 5 de 2009, la Ley 68 de 2009 y la Ley 14 de 2010.

Ley No. 641(13 de noviembre 2007)

Ley N° 4573 (4 de mayo de 1970)

Ley número 88-19 ( 5 de enero de 1988)

Ley de Delitos Informáticos Nº 30096 (21 de octubre de 2013)

Ley Especial contra los Delitos Informáticos (4 de septiembre de 2001)

Real Academia Española y Consejo General del Poder Judicial. Madrid: Espasa Libros, S. L. U., 2016. Tapa dura.

Vives A. y Gonzáles C. (1996), “Comentarios al código Penal 1995”, Ed. TIRONT BLANCH, Valencia, pág. 1238.