Universidad Católica
Nuestra Señora de la Asunción

LEGISLACIÓN PARAGUAYA PARA EL DELITO INFORMÁTICO

Facultad de Ciencias y Tecnología
Ingeniería Informática

Teoría y Aplicación de la Informática 2

Adriana Aranda Centurión
Matricula: 54210

2010

Índice

1. Introducción

En la sociedad contemporánea, indudablemente la tecnología se ha introducido en diferentes aspectos de la vida cotidiana de la sociedad. Tanto a nivel personal, educativo, económico, laboral y cultural, se crea una cierta dependencia de la tecnología para la comunicación entre personas, la simplificación del trabajo, el acceso a la información, el desarrollo profesional y personal.

Es indiscutible el alcance que han tenido hoy los computadores, personas de todas las edades y culturas hacen uso de esta útil herramienta en el día a día. Es por esto que se da lugar a diferentes riesgos en el uso de las mismas, debido al desconocimiento, o bien a la mala intención de los usuarios al momento de su utilización.

En este sentido surgen los delitos informáticos, donde personas malintencionadas buscan obtener informaciones indebidas o privadas de personas u organizaciones, perjudicar a terceros u obtener beneficios con esto. Si bien no existe aún una medida exacta de la importancia de estas transgresiones, es probable que su incidencia se acentúe con la expansión del uso de computadoras y las telecomunicaciones.

Los tipos penales tradicionales resultan en países inadecuados para encuadrar las nuevas formas delictivas, tal como la interferencia en una red bancaria para obtener, mediante una orden electrónica, un libramiento ilegal de fondos o la destrucción de datos. El tema plantea, además, complejos perfiles para el Derecho Internacional cuando el delito afecta a más de una jurisdicción nacional.

Los avances tecnológicos, el acceso masivo a Internet, el aumento de la pobreza y la relación al cambio bursátil del peso de las monedas extranjeras son identificados como los principales factores que explican la profundización de este delito. Las cámaras digitales y los videos grabadoras son cada vez más accesibles para los cibernautas de clases media y alta. No obstante, a medida de que bajen los costos las conexiones de banda ancha se multiplicaran, lo que propicia aún más el cyberdelito.

El área del derecho en el cual se debe buscar regular este tipo de delitos es el Derecho Penal, ya que la gran mayoría de las trasgresiones informáticas resultan en estafas, fraudes y suplantación de identidad.

Por lo tanto, el Derecho Penal debe también prevenir la comisión de éste tipo de hechos que de ninguna manera pueden ser entendidos como errores involuntarios, ya que son realizados por personas que generalmente están se encuentran especializadas en el trabajo con computadoras y que pueden conocer como entrar en los archivos de datos de cualquier individuo.

Sin embargo, el Derecho Penal debe resguardar los intereses de la sociedad, evitando manipulaciones computarizadas habituales o no, basadas en conocimiento de los objetos, programas, así como de algunas informaciones que extiendan y hagan imposible la detección de estos ilícitos.

2. Influencia de la Tecnología en la Sociedad actual

La tecnología se ha introducido en las diferentes áreas de la vida cotidiana, facilitando el desarrollo y el progreso de las sociedades y de las personas. En este aspecto, ha llegando a revolucionar las siguientes áreas principalmente:

- Personal: Hoy día el desarrollo de las personas, en sus diferentes niveles se ven respaldadas por las nuevas tecnologías que le sirven de herramientas para alcanzar sus metas en el nivel educativo, laboral, etc.

- Educacional: El uso de las computadoras y las redes como Internet, permiten contar con herramientas que le facilitan el acceso a la información, al acceso a nuevas metodologías de aprendizaje (E-Learning) y a nuevas herramientas de entrenamiento del saber adquirido.

- Laboral: En el ámbito laboral, hoy se cuenta con nuevas maneras de de desarrollo y testeo de productos, así como herramientas de informatización de la información y facilidades de gestión de la

misma y por tanto de las industrias o empresas. También se tienen nuevos sistemas de control y comunicación del personal y los gerentes, así como nuevos mecanismos de capacitación para los diferentes tipos de empleo.

- Económico: En cuanto a la Economía, los avances tecnológicos han facilitado el desarrollo de las industrias y los métodos de análisis económicos a nivel global, con lo que se impulsa a un progresivo avance en esta área y a un mayor progreso a nivel social.

- Trámites y Transacciones: Gracias a los avances tecnológicos, surgen facilidades en las transacciones monetarias y agilización de trámites, por medio de Internet y los sistemas avanzados en la comunicación. Referente a esto, hoy día ya no es requerida la presencia en las organizaciones para realizar compras, cobros o trámites, lo que favorece y agiliza los trámites o transacciones a realizar. De este modo, se apoya además al avance de la Economía en este aspecto.

- Salud: Actualmente, la gran mayoría de los estudios e intervenciones medicas son realizaras apoyadas por las nuevas tecnologías. Con el paso del tiempo, las tecnologías nuevas van mejorando y simplificando los métodos y maquinarias utilizados para este fin. La dependencia tecnológica en esta área es importante y, considerando los continuos avances de la tecnología, la dependencia de esta será aun mayor con el paso del tiempo.

- Investigación: En el ámbito de la investigación, las tecnologías no solo han servido de apoyo, sino que han permitido una mayor profundización en las diversas áreas. Además permiten el acceso y la diseminación de información de manera más rápida, así como el trabajo colaborativo entre investigadores de diversos lugares físicos. Esto ha sido de gran importancia en esta área, ya que ha permitido además un mayor desarrollo del conocimiento y de las sociedades en general.

- Desarrollo y Avance Tecnológico: La utilización de tecnologías existentes ha permitido la creación de nuevas tecnologías que fusionan y/o mejoran tecnologías anteriores, permitiendo así la evolución progresiva de las mismas. Este continuo desarrollo da lugar a nuevas maneras de encarar las diversas áreas de la vida cotidiana, ayudando al hombre en su actuar y desarrollo progresivo.

- Entretenimiento: En el ámbito del entretenimiento, cada vez han surgido nuevas maneras de encarar los juegos de consola y computadora, hacia juegos que no requieran controles o cables, buscando además adecuar el movimiento natural de las personas a los movimientos de los personajes dentro de los juegos. Se busca que los juegos sean lo más naturales posible para quien lo está jugando, generando así cada vez un mayor interés por parte de personas de diferentes edades; apoyando también, en ciertos casos, al entrenamiento físico de quien lo juega. Sin duda alguna, es un área de gran interés para los desarrolladores de nuevas tecnologías, por lo que su continuo progreso es indiscutible.

3. Delito Informático o Cyberdelito

Conforme han avanzado las tecnologías y se ha volcado hacia ellas la actividad del hombre, se ha dado lugar a una nueva forma de actividad delictiva que tiene como herramienta o medio a las actividades informáticas del hombre de hoy.

En este aspecto, se han generado vulnerabilidades frente a ciertas personas que buscar sacar provecho indebido con informaciones o actividades de otros; y es por esto que se necesita hacer frente a este tipo de actividades desde el punto de vista legal.

3.1. Definición General

Delito informático, crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. 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.

Existen actividades delictivas que se realizan por medio de estructuras electrónicas 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 datacredito), mal uso de artefactos, chantajes, fraude electrónico, ataques a sistemas, robo de bancos, ataques realizados por hackers, violación de los derechos de autor, violación de información confidencial y muchos otros.[1]

3.2. Clasificación de los Delitos Informáticos [2]

3.2.1. Según la Actividad Informática

Sabotaje informático

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección. Básicamente, se puede diferenciar dos grupos de casos: por un lado, las conductas dirigidas a causar destrozos físicos y, por el otro, los métodos dirigidos a causar daños lógicos.

- *Conductas dirigidas a causar daños físicos*

El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

- *Conductas dirigidas a causar daños lógicos*

El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se está trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo.

Fraude a través de computadoras

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho.

---

[1] Fuente: http://es.wikipedia.org/wiki/Delito_informático
[2] Fuente base: http://www.monografias.com/trabajos6/delin/delin.shtml

Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado» por el autor.

- *Estafas electrónicas*: La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el "animus defraudandi" existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

- *"Pesca" u "olfateo" de claves secretas*: Los delincuentes suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los "sabuesos" utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otros delitos, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

- *Estratagemas*: Los estafadores utilizan diversas técnicas para ocultar computadoras que se "parecen" electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos.

- *Juegos de azar*: El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la Red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

- *Fraude*: Ya se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en regiones donde existe el comercio electrónico.

- *Blanqueo de dinero*: Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones.

<u>Copia ilegal de software y espionaje informático</u>

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

- *Infracción de los derechos de autor*: La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

- *Infracción del Copyright de bases de datos*: No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan "downloads" de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

Uso ilegítimo de sistemas informáticos ajenos

Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometido por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo. En estos supuestos, sólo se produce un perjuicio económico importante para las empresas en los casos de abuso en el ámbito del teleproceso o en los casos en que las empresas deben pagar alquiler por el tiempo de uso del sistema.

- *Acceso no autorizado*: La corriente reguladora sostiene que el uso ilegítimo de *passwords* y la entrada en un sistema informático sin la autorización del propietario debe quedar tipificado como un delito, puesto que el bien jurídico que acostumbra a protegerse con la contraseña es lo suficientemente importante para que el daño producido sea grave.

Delitos informáticos contra la privacidad

Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos

Esta tipificación se refiere a quién, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

- *Interceptación de e-mail*: En este caso se propone una ampliación de los preceptos que castigan la violación de correspondencia, y la interceptación de telecomunicaciones, de forma que la lectura de un mensaje electrónico ajeno revista la misma gravedad.

3.2.2. Según el Instrumento, Medio o Fin u Objetivo

Como instrumento o medio

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.

- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

Como fin u objetivo

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos
- computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

3.2.3. Según Actividades Delictivas Graves

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- *Terrorismo*: Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. De hecho, se han detectado mensajes con instrucciones para la fabricación de material explosivo.

- *Narcotráfico*: Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

- *Espionaje*: El acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto de los Estados Unidos, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera. Aunque no parece que en este caso haya existido en realidad un acto de espionaje, se ha evidenciado una vez más la vulnerabilidad de los sistemas de seguridad gubernamentales.

- *Espionaje industrial*: También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y know how estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada.

- *Otros delitos*: Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

3.3. Delitos Reconocidos en Paraguay

Entre los delitos mencionados y clasificados anteriormente, en el Paraguay se tienen en consideración en el Código Penal y en el Código Procesal Penal, aunque algunas no directamente como delitos informáticos, los siguientes actos:

- Lesión del derecho a la comunicación y a la imagen

- Violación del secreto de la comunicación
- Alteración de datos
- Sabotaje de computadoras
- Operaciones fraudulentas por computadora
- Aprovechamiento clandestino de una prestación
- Perturbación de instalaciones de telecomunicaciones
- Pornografía infantil
- Intercepción, secuestro, apertura y examen de correspondencia
- Intervención de comunicaciones
- Derechos de Autor

4. Legislación Paraguaya para el Delito Informático

Existen diversas leyes y artículos que sancionan los delitos informáticos planteados en la sección anterior, que buscan regular las actividades que hacen uso de las tecnologías y las comunicaciones para fines maliciosos o dañinos.

A continuación se presentaran algunas de estas leyes obtenidas del Código Penal, del Código Procesal Penal y que son sancionadas por el Poder Legislativo.

4.1. Código Penal, LEY Nº. 1.160/97 [3]

Artículo 144°.- Lesión del derecho a la comunicación y a la imagen

1º El que sin consentimiento del afectado:
1. escuchara mediante instrumentos técnicos;
2. grabara o almacenara técnicamente; o
3. hiciera, mediante instalaciones técnicas, inmediatamente accesible a un tercero, la palabra de otro, no destinada al conocimiento del autor y no públicamente dicha, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º La misma pena se aplicará a quien, sin consentimiento del afectado, produjera o transmitiera imágenes:
1. de otra persona dentro de su recinto privado;
2. del recinto privado ajeno;
3. de otra persona fuera de su recinto, violando su derecho al respeto del ámbito de su vida íntima.

3º La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme a los incisos 1º y 2º.
4º En los casos señalados en los incisos 1º y 2º será castigada también la tentativa.

5º La persecución penal del hecho dependerá de la instancia de la víctima, salvo que el interés público requiera una persecución de oficio. Si la víctima muriera antes del vencimiento del plazo para la instancia sin haber renunciado a su derecho de interponerla, éste pasará a sus parientes.

Artículo 146°.- Violación del secreto de la comunicación

1º El que, sin consentimiento del titular:
1. abriera una carta cerrada no destinada a su conocimiento;
2. abriera una publicación, en los términos del artículo 14, inciso 3º, que se encontrara cerrada o depositada en un recipiente cerrado destinado especialmente a guardar de su conocimiento

[3] Fuente: http://www.oas.org/juridico/spanish/cyb_par_cod_penal.pdf

dicha publicación, o que procurara, para sí o para un tercero, el conocimiento del contenido de la publicación;

3. lograra mediante medios técnicos, sin apertura del cierre, conocimiento del contenido de tal publicación para sí o para un tercero, será castigado con pena privativa de libertad de hasta un año o con multa.

2º La misma pena se aplicará a quien hiciera accesible a un tercero una grabación o reproducción realizada conforme al inciso anterior.

Artículo 173°.- Sustracción de energía eléctrica

1º El que lesionando el derecho de disposición de otro sobre energía eléctrica, y con la intención de utilizarla, la sustrajera de una instalación otro dispositivo empleado para su transmisión o almacenaje, mediante conductor no autorizado ni destinado a la toma regular de la energía de la instalación o del dispositivo, será castigado con pena privativa de libertad de hasta tres años o con multa.

2º En estos casos, será castigada también la tentativa.

3º En lo pertinente, se aplicará lo dispuesto en los artículos 171 y 172.

4º El que lesionando el derecho de disposición de otro sobre energía eléctrica y con el fin de causarle un daño por la pérdida de ella, la sustrajera de una instalación u otro dispositivo empleado para su transmisión o almacenaje, mediante conductor no autorizado ni destinado a la toma regular de la energía de la instalación o del dispositivo, será castigado con pena privativa de libertad de hasta dos años o con multa.

La persecución penal dependerá de la instancia de la víctima.

Artículo 174°.- Alteración de datos

1º El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa.

2º En estos casos, será castigada también la tentativa.

3º Como datos, en el sentido del inciso 1º, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.

Artículo 175°.- Sabotaje de computadoras

1º El que obstaculizara un procesamiento de datos de importancia vital para una empresa o establecimiento ajenos, o una entidad de la administración pública mediante:

1. un hecho punible según el artículo 174, inciso 1º, o
2. la destrucción, inutilización sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra parte accesoria vital, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos, será castigada también la tentativa.

Artículo 188°.- Operaciones fraudulentas por computadora

1º El que con la intención de obtener para sí o para otro un beneficio patrimonial indebido, influyera sobre el resultado de un procesamiento de datos mediante:

1. programación falsa;
2. utilización de datos falsos o incompletos;
3. utilización indebida de datos; o

4. otras influencias indebidas sobre el procesamiento, y con ello, perjudicara el patrimonio de otro, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos, se aplicará también lo dispuesto en el artículo 187, incisos 2º al 4º.

Artículo 189°.- Aprovechamiento clandestino de una prestación

1º El que con la intención de evitar el pago de la prestación, clandestinamente:

1. se aprovechara del servicio de un aparato automático, de una red de telecomunicaciones destinada al público, o de un medio de transporte; o
2. accediera a un evento o a una instalación, será castigado con pena privativa de libertad de hasta un año o con multa, siempre que no estén previstas penas mayores en otro artículo.

2º En estos casos, será castigada también la tentativa.

3º En lo pertinente se aplicará lo dispuesto en los artículos 171 y 172.

Artículo 220°.- Perturbación de instalaciones de telecomunicaciones

1º El que:

1. destruyera, dañara, removiera, alterara o inutilizara una cosa destinada al funcionamiento de una instalación de telecomunicaciones para el servicio público; o
2. sustrajera la energía que la alimenta, y con ello impidiera o pusiera en peligro su funcionamiento, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos será castigada también la tentativa.

3º El que realizara el hecho mediante una conducta culposa será castigado con pena privativa de libertad de hasta dos años o con multa.

Artículo 239°.- Asociación criminal

1º El que:

1. creara una asociación estructurada jerárquicamente u organizada de algún modo, dirigida a la comisión de hechos punibles;
2. fuera miembro de la misma o participara de ella;
3. la sostuviera económicamente o la proveyera de apoyo logístico;
4. prestara servicios a ella; o
5. la promoviera. Será castigado con pena privativa de libertad hasta cinco años.

2º En estos casos, será castigada también la tentativa.

3º Cuando el reproche al participante sea ínfimo o su contribución fuera secundaria, el tribunal podrá prescindir de la pena.

4º El tribunal también podrá atenuar la pena con arreglo al artículo 67, o prescindir de ella, cuando el autor:

1. se esforzara, voluntaria y diligentemente, en impedir la continuación de la asociación o la comisión de un hecho punible correspondiente a sus objetivos;

2. comunicara a la autoridad competente su conocimiento de los hechos punibles o de la planificación de los mismos, en tiempo oportuno para evitar su realización.

Artículo 248°.- Alteración de datos relevantes para la prueba

1º El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en

caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa.

2º En estos casos será castigada también la tentativa.

3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º.

Artículo 249°.- Equiparación para el procesamiento de datos

La manipulación que perturbe un procesamiento de datos conforme al artículo 174, inciso 3º, será equiparada a la inducción al error en las relaciones jurídicas.

4.2. Código Procesal Penal de Paraguay [4]

Artículo 198°.- Intercepción y secuestro de correspondencia.

Siempre que sea útil para la averiguación de la verdad, el juez ordenará, por resolución fundada, bajo pena de nulidad, la intercepción o el secuestro de la correspondencia epistolar, telegráfica o de cualquier otra clase, remitida por el imputado o destinada a él, aunque sea bajo nombre supuesto.
Regirán las limitaciones del secuestro de documentos u objetos.

Artículo 199°.- Apertura y examen de correspondencia.

Recibida la correspondencia o los objetos interceptados, el juez procederá a su apertura haciéndolo constar en acta. Examinará los objetos y leerá para sí el contenido de la correspondencia. Si guardan relación con el procedimiento ordenará el secuestro; en caso contrario, mantendrá en reserva su contenido y dispondrá la entrega al destinatario.

Artículo 200°.- Intervención de comunicaciones.

El juez podrá ordenar por resolución fundada, bajo pena de nulidad, la intervención de las comunicaciones del imputado, cualquiera sea el medio técnico utilizado para conocerlas.
El resultado sólo podrá ser entregado al juez que lo ordenó, quien procederá según lo indicado en el artículo anterior; podrá ordenar la versión escrita de la grabación o de aquellas partes que considere útiles y ordenará la destrucción de toda la grabación o de las partes que no tengan relación con el procedimiento, previo acceso a ellas del Ministerio Público, del imputado y su defensor.
La intervención de comunicaciones será excepcional.

Artículo 228°.- Informes.

El juez y el Ministerio Público podrán requerir informes a cualquier persona o entidad pública o privada.
Los informes se solicitarán verbalmente o por escrito, indicando el procedimiento en el cual se requieren, el nombre del imputado, el lugar donde debe ser entregado el informe, el plazo para su presentación y las consecuencias previstas para el incumplimiento del deber de informar.

4.3. Poder Legislativo - LEY N° 2861/2006 [5]

Que reprime el comercio y la difusión comercial o no comercial de Material pornográfico, utilizando la imagen u otra representación de menores o incapaces.
El congreso de la nación paraguaya sanciona con fuerza de Ley:

Artículo 1°.- Utilización de niños, niñas y adolescentes en pornografía.

[4] Fuente: http://www.oas.org/juridico/spanish/cyb_par_cod_procesal.pdf
[5] Fuente: http://www.oas.org/juridico/spanish/cyb_par_ley_2861_2006.pdf

El que, por cualquier medio produjese o reprodujese un material conteniendo la imagen de una persona menor de dieciocho años de edad en acciones eróticas o actos sexuales que busquen excitar el apetito sexual, así como la exhibición de sus partes genitales con fines pornográficos, será castigado con pena privativa de libertad de cinco a diez años.

Artículo 2°.- Difusión o Comercialización de pornografía infantil.

El que distribuyese, importase, exportase, ofertase, canjease, exhibiese, difundiese, promocionase o financiase la producción o reproducción de la imagen de que trata el Artículo 1°, será castigado con pena privativa de libertad de tres a ocho años.

Artículo 3°.- Exhibición de niños, niñas y adolescentes en actos sexuales.

El que participase en la organización, financiación o promoción de espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años de edad en acciones eróticas de contenido sexual, será castigado con pena privativa de libertad de cinco a diez años.

Artículo 4°.- Agravantes.

La pena privativa de libertad establecida en los artículos anteriores, será aumentada hasta quince años, cuando:

1.- La víctima fuere menor de quince años de edad; o,

2.- El autor:

1. tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo;
2. operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente; o,
3. hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie.

Artículo 5°.- Pena Complementaria y Comiso Especial.

Cuando el autor actuara comercialmente o como miembro de una banda que se ha formado para la realización de hechos señalados en los artículos anteriores, se aplicará lo dispuesto en los Artículos del Código Penal referentes a la pena patrimonial y el comiso especial extensivo.

Artículo 6°.- Consumo y posesión de pornografía infantil.

1.- El que adquiriese o, a cualquier otro título, poseyese la imagen con las características descriptas en el Artículo 1° de la presente Ley, será castigado con pena privativa de libertad de seis meses a tres años.

2.- Con la misma pena será castigado el que asistiese al espectáculo descripto en el Artículo 3° de la presente Ley, salvo cuando por las circunstancias del caso no haya podido prever la realización de lo descripto en dicho artículo y que, habiéndose percatado de ello, inmediatamente se hubiese retirado del lugar y denunciado el hecho.

Artículo 7°.- Obligación especial de denunciar. Persecución y ejecución penal.

Toda persona que presencie la realización de los hechos punibles descriptos en los Artículos 1°, 2° y 3° de la presente Ley, está obligada a:

1. Denunciar sin demora a la Policía o al Ministerio Público;
2. Aportar, en caso que posea, los datos para la ubicación, incautación y eventualmente, la destrucción de la imagen, así como para la individualización, aprehensión y sanción del o los autores.

El que incumpliese estas obligaciones será castigado con pena privativa de libertad de hasta tres años o con multa, salvo que razonablemente arriesgue su propia persecución penal.

Quienes detenten la patria potestad, o soporten un deber legal de guarda o tutela respecto del niño o adolescente directamente afectado por el hecho, no podrán invocar la exoneración prevista en el Código Procesal Penal para quienes arriesguen la propia persecución penal o de un pariente hasta el

cuarto grado de consanguinidad o segundo de afinidad, ni la eximición de pena prevista en el Código Penal.

Artículo 8°.- Prohibición de Medidas Sustitutivas y Alternativas a la Prisión Preventiva y de Libertad Condicional.

Los procesados por la comisión de hechos punibles descriptos en esta Ley, no podrán ser beneficiados con medidas sustitutivas o alternativas a la prisión preventiva.
Los condenados por la comisión de hechos punibles descriptos en esta Ley, no podrán ser beneficiados con el régimen de libertad condicional.

Artículo 9°.- Protección de Derechos y Garantías durante la persecución penal.

En la investigación y persecución de los hechos contemplados en los Artículos 1º, 2º, 3º y 6º de la presente Ley, se observarán las siguientes disposiciones de protección de los derechos y garantías del imputado y del interés superior del niño, niña y adolescente:

1.- Las imágenes que estén en poder del Ministerio Público, no serán entregadas a las partes ni exhibidas a terceros.
2.- Se labrará un Acta del contenido de las imágenes, el cual quedará a disposición de las partes y tendrá siempre carácter reservado.
3.- El imputado podrá estar presente en el momento de labrarse el Acta. Si no hubiese comparecido al acto por sí o por intermedio de su defensor, podrá solicitar al Juez de Garantías, que las imágenes le sean exhibidas en audiencia reservada a las partes. Sus observaciones se harán constar en Actas.
4.- Las imágenes no serán reproducidas, salvo cuando el Juzgado disponga lo contrario, mediante resolución que sólo podrá fundarse en la conservación del medio de prueba. La parte que solicitó la medida podrá recurrir la resolución que la rechace. El Ministerio Público y la víctima podrán recurrir la resolución que la otorgue.
5.- Las personas que accediesen a las imágenes, en razón a su función pública o actividad profesional, de acuerdo a las disposiciones de este artículo o de otras leyes, son personalmente responsables de evitar que su contenido sea total o parcialmente reproducido, difundido o divulgado.

Artículo 10°.- Violación de derechos con motivo del proceso.

El que incumpliese las disposiciones del artículo anterior, será castigado con pena privativa de libertad de cinco a diez años.

Aprobado el Proyecto de Ley por la Honorable Cámara de Senadores, a los veinticuatro días del mes de noviembre del año dos mil cinco, quedando sancionado el mismo, por la Honorable Cámara de Diputados a los quince días del mes de diciembre del año dos mil cinco, de conformidad a lo dispuesto en el Artículo 204 de la Constitución Nacional.

4.4. Ley N° 1328/98: De Derecho de Autor y Derechos Conexos [6]

De los Derechos Conexos al Derecho de Autor y otros Derechos Intelectuales

Artículo 120°.- La protección reconocida a los derechos conexos al derecho de autor, y a otros derechos intelectuales contemplados en el presente Título, no afectará en modo alguno la tutela del derecho de autor sobre las obras literarias o artísticas. En consecuencia, ninguna de las disposiciones contenidas en el presente Título podrá interpretarse en menoscabo de esa protección. En caso de duda o conflicto se estará a lo que más favorezca al autor.

Sin perjuicio de sus limitaciones específicas, todas las excepciones y límites establecidos en esta ley para el derecho de autor, serán también aplicables a los derechos reconocidos en el presente Título.

[6] Fuente: http://www.sice.oas.org/int_prop/nat_leg/Paraguay/L132898c.asp#capxiv2

Artículo 121°.- Los titulares de los derechos conexos y otros derechos intelectuales podrán invocar las disposiciones relativas a los autores y sus obras, en cuanto estén conformes con la naturaleza de sus respectivos derechos.

Artículo 134°.- La presente ley reconoce un derecho de explotación sobre las grabaciones de imágenes en movimiento, con o sin sonido, que no sean creaciones susceptibles de ser calificadas como obras audiovisuales. En estos casos, el productor gozará, respecto de sus grabaciones audiovisuales, del derecho exclusivo de autorizar o no su reproducción, distribución y comunicación pública, inclusive de las fotografías realizadas en el proceso de producción de las grabaciones audiovisuales.

La duración de los derechos reconocidos en este artículo será de cincuenta años, contados a partir del uno de enero del año siguiente al de la divulgación de la grabación o al de su realización, si no se hubiere divulgado.

Artículo 135°.- Quien realice una fotografía u otra fijación obtenida por un procedimiento análogo, que no tenga el carácter de obra de acuerdo a la definición contenida en el numeral 16 del Artículo 21 y de lo dispuesto en el Título II de esta ley, goza del derecho exclusivo de autorizar su reproducción, distribución y comunicación pública, en los mismos términos reconocidos a los autores fotográficos.

La duración de este derecho será de cincuenta años contados a partir del uno de enero del año siguiente a la realización de la fotografía.

Artículo 148°.- La Dirección Nacional del Derecho de Autor podrá imponer sanciones a las entidades de gestión que infrinjan sus propios estatutos o reglamentos, o que incurran en hechos que afecten los intereses de sus representados, sin perjuicio de las sanciones penales o las acciones civiles que correspondan.

Artículo 149°.- Las sanciones a que se refiere el artículo anterior podrán ser:

1. amonestación privada y escrita;
2. amonestación pública difundida a través de los medios de comunicación social que designe la Dirección, a costa de la infractora;
3. multa que no será menor de diez salarios mínimos ni mayor de cien salarios mínimos, de acuerdo a la gravedad de la falta;
4. suspensión de la autorización para su funcionamiento hasta por un año; y,
5. cancelación del permiso de funcionamiento en casos de particular gravedad.

Artículo 150°.- Las infracciones a esta ley o a sus reglamentos, serán sancionadas por la Dirección Nacional del Derecho de Autor, previa audiencia del infractor, con multa por el equivalente de diez a cien salarios mínimos.

En caso de reincidencia, que se considerará como tal la repetición de un acto de la misma naturaleza en un lapso de seis meses, se podrá imponer el doble de la multa.

Artículo 151°.- Contra las resoluciones emitidas por la Dirección Nacional del Derecho de Autor, se podrá apelar ante el Ministro de Industria y Comercio. El recurso será interpuesto ante el Director de la misma dentro de cinco días hábiles. El Ministro dictará resolución fundada y contra ella podrá interponerse recurso contencioso- administrativo dentro de diez días hábiles.

Transcurridos quince días hábiles sin que el Ministro dicte Resolución, el interesado podrá recurrir directamente a la vía contencioso-administrativa.

Artículo 166°.- Se impondrá una pena de seis meses a un año de prisión o multa de cinco a cincuenta salarios mínimos, a quien estando autorizado para publicar una obra, dolosamente lo hiciere en una de las formas siguientes:

1. sin mencionar en los ejemplares el nombre del autor, traductor, adaptador, compilador o arreglador;
2. estampe el nombre con adiciones o supresiones que afecten la reputación del autor como tal o, en su caso, del traductor, adaptador, compilador o arreglador;
3. publique la obra con abreviaturas, adiciones, supresiones o cualesquiera otras modificaciones, sin el consentimiento del titular del derecho;

4. publique separadamente varias obras, cuando la autorización se haya conferido para publicarlas en conjunto; o las publique en conjunto cuando solamente se le haya autorizado la publicación de ellas en forma separada.

Artículo 167°.- Se impondrá pena de prisión de seis meses a tres años o multa de cien a doscientos salarios mínimos, en los casos siguientes:

1. al que emplee indebidamente el título de una obra, con infracción del Artículo 61 de esta ley;
2. al que realice una modificación de la obra, en violación de lo dispuesto en el Artículo 30 de la presente ley;
3. al que comunique públicamente una obra, en violación de lo dispuesto en el Artículo 27; una grabación audiovisual, conforme al Artículo 134; o una imagen fotográfica, de acuerdo al Artículo 135 de esta ley;
4. al que distribuya ejemplares de la obra, con infracción del derecho establecido en el Artículo 28; de fonogramas, en violación del Artículo 127; de una grabación audiovisual conforme al Artículo 134; o de una imagen fotográfica de acuerdo al Artículo 135 de la presente ley;
5. al que importe ejemplares de la obra no destinados al territorio nacional, en violación de lo dispuesto en el Artículo 29; o de fonogramas, infringiendo lo dispuesto en el Artículo 127 de esta ley;
6. al que retransmita, por cualquier medio alámbrico o inalámbrico, una emisión de radiodifusión o una transmisión por hilo, cable, fibra óptica u otro procedimiento análogo, infringiendo las disposiciones de los Artículos 25, 26, 131 ó 132 de esta ley;
7. al que comunique públicamente interpretaciones o ejecuciones artísticas, o fonogramas, que estén destinados exclusivamente a su ejecución privada;
8. al que, siendo cesionario o licenciatario autorizado por el titular del respectivo derecho, reproduzca o distribuya un mayor número de ejemplares que el permitido por el contrato; o comunique, reproduzca o distribuya la obra, interpretación, producción o emisión, después de vencido el plazo de autorización que se haya convenido;
9. a quien dé a conocer a cualquier persona una obra inédita o no divulgada, que haya recibido en confianza del titular del derecho de autor o de alguien en su nombre, sin el consentimiento del titular; y,
10. a quien fabrique, importe, venda, arriende o ponga de cualquier otra manera en circulación, dispositivos o productos o preste cualquier servicio cuyo propósito o efecto sea impedir, burlar, eliminar, desactivar o eludir de cualquier forma, los dispositivos técnicos que los titulares hayan dispuesto para proteger sus respectivos derechos.

Artículo 168°.- Se impondrá pena de prisión de dos a tres años o multa de doscientos a mil salarios mínimos, en los casos siguientes:

1. al que se atribuya falsamente la cualidad de titular, originario o derivado, de cualquiera de los derechos reconocidos en esta ley, y con esa indebida atribución obtenga que la autoridad competente suspenda el acto de comunicación, reproducción, distribución o importación de la obra, interpretación, producción, emisión o de cualquiera otro de los bienes intelectuales protegidos por la presente ley;
2. al que presente declaraciones falsas en cuanto a certificaciones de ingresos, repertorio utilizado, identificación de los autores, autorización supuestamente obtenida, número de ejemplares o toda otra adulteración de datos susceptible de causar perjuicio a cualquiera de los titulares de derechos protegidos por esta ley;
3. a quien reproduzca, con infracción de lo dispuesto en el Artículo 26, en forma original o elaborada, íntegra o parcial, obras protegidas, salvo en los casos de reproducción lícita taxativamente indicados en el Capítulo I del Título V; o por lo que se refiera a los programas de ordenador, salvo en los casos de excepción mencionados en los Artículos 70 y 71 de esta ley;
4. al que introduzca en el país, almacene, distribuya mediante venta, renta o préstamo o ponga de cualquier otra manera en circulación, reproducciones ilícitas de las obras protegidas;

5. a quien reproduzca o copie, por cualquier medio, la actuación de un artista intérprete o ejecutante; o un fonograma; o una emisión de radiodifusión o transmisión por hilo, cable, fibra óptica u otro procedimiento análogo; o que introduzca en el país, almacene, distribuya, exporte, venda, alquile o ponga de cualquier otra manera en circulación dichas reproducciones ilícitas;
6. al que inscriba en el Registro del Derecho de Autor y Derechos Conexos, una obra, interpretación, producción, emisión ajenas o cualquiera otro de los bienes intelectuales protegidos por esta ley, como si fueran propios, o como de persona distinta del verdadero titular de los derechos; y,
7. a quien fabrique, importe, venda, arriende o ponga de cualquier otra manera en circulación, dispositivos o sistemas que sean de ayuda primordial para descifrar sin autorización una señal de satélite codificada portadora de programas o para fomentar la recepción no autorizada de un programa codificado, radiodifundido o comunicado en otra forma al público.

Artículo 170°.- Se impondrá pena de prisión de dos a tres años o multa de cien a doscientos salarios mínimos a quien posea, use, diseñe, fabrique, importe, exporte o distribuya ya sea por venta, arrendamiento, préstamo u otro, cualquier artefacto, programa de computación o contra quien haga la oferta de realizar o realice un servicio, cuyo objetivo sea el de permitir o facilitar la evasión de tecnología de codificación.

4.5. Limitaciones Legislativas

Las leyes sancionadas en Paraguay referentes a delitos informáticos, dejan lagunas jurídicas por analizar y buscar reglamentar como serian:

- La suplantación de identidad en transacciones o medidas de obtención de informaciones privadas.
- El desarrollo de Software incorrecto.
- La mala utilización de las herramientas tecnológicas en actos que atacan la integridad de los datos de las personas, buscando obtener provecho a través de esto.
- Divulgación de Información confidencial o errónea por medio de las telecomunicaciones o Internet.
- Modificaciones intencionales de ciertos artefactos tecnológicos para sacar provecho, a través del funcionamiento erróneo, que pueda ser de utilidad para cometer otro tipo de delitos.
- Espionaje o invasión de privacidad haciendo uso de la tecnología.
- Etc.

Aunque algunos delitos pueden ser atacados desde otras leyes que se relacionen en cierta medida con la naturaleza del delito, por lo que en caso de darse estas, se podría atacar haciendo uso de otras reglamentaciones existentes.

5. Comparación con otros países [7]

5.1. Argentina

La ley vigente

La Argentina sancionó el 4 de junio del 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones.

[7] Fuente: http://es.wikipedia.org/wiki/Delito_informático

Definiciones vinculadas a la informática

En el nuevo ordenamiento se establece que el término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión (art. 77 Código Penal).

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente (art. 77 Código Penal).

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente (art. 77 Código Penal).

Delitos contra menores

En el nuevo ordenamiento pasan a ser considerados delitos los siguientes hechos vinculados a la informática:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Protección de la privacidad

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

Delitos contra la propiedad

Artículo 173 inciso 16: (Incurre en el delito de defraudación)...El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

Artículo 183 del Código Penal: (Incurre en el delito de daño)...En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Artículo 184 del Código Penal: (Eleva la pena a tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes):

Inciso 5: Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

Inciso 6: Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

Delitos contra las comunicaciones

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

Delitos contra la administración de justicia

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

5.2. España

En España, los delitos informáticos son un hecho sancionable por el Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio informático. Estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de Noviembre en el BOE número 281, de 24 de Noviembre de 1.995. Estos tienen la misma sanción que sus homólogos no-informáticos. Por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso Nº 2249/2006; resolución Nº 533/2007) que confirmó las penas de prisión para un caso de estafa electrónica (phishing).

5.3. México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sean que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal Federal en el titulo noveno capítulo I y II.

El artículo 167 fr.VI del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos.

La reproducción no autorizada de programas informáticos o piratería está regulada en la Ley Federal del Derecho de Autor en el Título IV, capítulo IV.

También existen leyes locales en el código penal del Distrito Federal y el código penal del estado de Sinaloa.

5.4. Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

La ley tipifica cinco clases de delitos:

Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); favorecimiento culposos del sabotaje o daño. (Art. 8); acceso indebido o sabotaje a sistemas protegidos (Art. 9); posesión de equipos o prestación de servicios de sabotaje (Art. 10); espionaje informático (Art. 11); falsificación de documentos (Art. 12).

Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19);
Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22);
Contra niños y adolescentes: difusión o exhibición de material pornográfico (Art. 23); exhibición pornográfica de niños o adolescentes (Art. 24);
Contra el orden económico: apropiación de propiedad intelectual (Art. 25); oferta engañosa (Art. 26).

5.5. Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

6. Conclusión

En el Paraguay, como en diversos países, existen reglamentaciones para ciertos delitos en el área de la informática, aunque estos no llegan a prever muchos de los delitos existentes hoy en día.

Es importante tener en cuenta que, al igual que el avance tecnológico es continuo, nuevos delitos informáticos surgen con ellos, ya que las nuevas tecnologías pueden dar lugar a falencias en la seguridad.

Considerando esto, debería ser de gran importancia la pronta reglamentación de los huecos que existen en la legislación paraguaya; pues en caso contrario, los espacios que dan lugar a esta tipo de delitos crecerán cada vez más.

Si bien es cierto que existen diversas propuestas y proyectos en esta área, existen muchas trabas para la aprobación, que retrasan en cierta medida el progreso en la reglamentación de dichos delitos.

Para eliminar progresivamente las lagunas en las legislaciones, debe haber un trabajo cooperativo y continuo en esta área que cada vez toma mayor importancia en las vidas de las personas y que así mismo pone en un riesgo continuo la integridad de las personas.

7. Bibliografía

- Wikipedia Enciclopedia Libre. Artículo referente al Delito informático. Ultima modificación del artículo realizada el 6 Agosto 2010, a las 02:33. http://es.wikipedia.org/wiki/Delito_informático
- Trabajo de Investigación referente a Delitos Informáticos. Realizado por el usuario mlandav. http://www.monografias.com/trabajos6/delin/delin.shtml
- Investigación sobre las legislaciones nacionales para el Delito Informático y Delitos Relacionados. http://www.oas.org/juridico/spanish/cyb_par.htm

8. Anexos

Lunes 16 de noviembre de 2009 - 15:54:00

Paraguay: aprueban proyecto de firma digital

La Cámara de Senadores aprobó ayer en sesión el proyecto de ley "De validez jurídica de la firma digital, los mensajes de datos y los expedientes electrónicos", presentado por los diputados David Ocampos, Ariel Oviedo, Luis Gneiting y Justo Pastor Cárdenas.

La Comisión de Legislación modificó unos 15 artículos del proyecto original presentado, por lo que el texto vuelve a la Cámara de Diputados para ser revisado.

El documento tiene 45 artículos y permitirá, por ejemplo, validar jurídicamente un certificado médico enviado a través de un correo electrónico.

El senador Alfredo Jaeggli destacó de este proyecto que de él dependerá la digitalización de la Corte Suprema de Justicia para todos sus documentos, tal como se utiliza en otros países.

Con la nueva realidad global, las oportunidades comerciales para las empresas locales y las infinitas posibilidades de accesos que surgen diariamente en internet, a cualquier persona que cuente con una red electrónica de transmisión de datos le implicará innumerables facilidades la legalización de la firma electrónica.

El objetivo de esta ley es reconocer la validez de los mensajes de datos electrónicos, así como establecer mecanismos que hagan que una firma digital pueda ser utilizada para dar confianza a una transacción comercial electrónica, fue uno de los argumentos esgrimidos por el diputado David Ocampos cuando presentó el proyecto.

Asimismo, el legislador afirmó que las interacciones, en su nueva modalidad electrónica, deben ser reguladas, atendiendo los principios fundamentales que rigen todos los campos tecnológicos y que deben prioritariamente asegurar la neutralidad tecnológica.

La firma digital es una firma electrónica que permite detectar cualquier alteración producida en el mensaje de datos al cual está asociada. De acuerdo a algunos expertos, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

Fuente: Ultima hora

- **PROYECTO DE LEY: "QUE CREA LA LEY QUE REGULA LOS DELITOS INFORMÁTICOS"**
  El Dir. Nac. Abog. Mario Soto Estigarribia plantea un proyecto de ley que regula directamente delitos informáticos, que aun no fue aprobado.
  Adjunto al trabajo el proyecto mencionado.
  Obtenido en:
  http://www.slideshare.net/osmar211bc/proyecto2473-que-regula-los-delitos-informaticos-paraguay