

LEGISLACIÓN NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

BANCO INTERAMERICANO DE DESARROLLO
BANCO INTERAMERICANO DE DESENVOLVIMENTO



INTER-AMERICAN DEVELOPMENT BANK
BANQUE INTERAMERICAINE DE DEVELOPPMENT



**CORTE SUPREMA DE JUSTICIA
NICARAGUA**

Delitos Informáticos

Legislación y el Manejo de la Información en la era del conocimiento

Preparado por el grupo de trabajo:
GLIN-Nicaragua Corte Suprema de Justicia Nicaragua

MSc. Ana Rosa Chavarría, Directora
José Antonio Pereira Vega, Ing. en Sistema
Lenin Ernesto Dávila, Ing. en Sistemas;

Managua, Nicaragua
Noviembre, 2005

Este documento es preparado para presentar, desde un concepto tecnológico, las oportunidades de mejora y trabajo posibles en los poderes Legislativos de las Américas. El objetivo principal es proveer información básica que permita una mejor discusión y un marco conceptual para aplicar las propuestas necesarias a la realidad nacional. Las interpretaciones, alternativas y conclusiones expresadas en éste documento son enteramente responsabilidad de los autores y no deben ser atribuidas a la Corte Suprema de Justicia Nicaragua, al Banco Interamericano de Desarrollo, sus organizaciones afiliadas, miembros de su Directorio Ejecutivo o países que representan.

INDICE

INTRODUCCIÓN	1
I.- Concepto de "delito informático"	2
II.- Su perfil criminológico.....	3
III.- Sujeto activo en los delitos informáticos.....	5
IV.- Sujeto pasivo de los delitos informáticos	7
V.- ¿Qué son los delitos informáticos?	8
VI.- Tipificación de los delitos informáticos	9
VII.- Tipos de delitos informáticos reconocidos por Naciones Unidas.....	12
VIII.- Elementos sustantivos a considerar	13
IX.- Regulación jurídica.	16
ANEXOS	19

EL DELITO INFORMÁTICO

INTRODUCCIÓN

En la sociedad de la información, en que actualmente estamos sumergidos, todos los ámbitos del quehacer cotidiano del ser humano se ven invadidos, manejados o al menos afectados por el hecho tecnológico. Esta "tecodependencia" se observa con claridad en la industria, la banca, el comercio y más recientemente en casi toda actividad pública como en los sistemas tributarios y electorales. Las ventajas que ofrece el empleo de las nuevas tecnologías en la optimización de múltiples procesos, son incuestionables, pero como casi todo, tiene su lado oscuro. Esta dimensión transgresora y abusiva del empleo de las nuevas tecnologías debe ser enfrentada por el Derecho Penal, como disciplina garante de la convivencia pacífica e instrumento último de control social.

Con el creciente desarrollo y popularización de la tecnología en los años setenta, empiezan los problemas de seguridad en los sistemas. En efecto, con la creación de aplicaciones interactivas, de sistemas *on Line* y de tratamientos en tiempo real, comienzan a verse casos de uso fraudulento del aparato o del *software* sobre datos comunes. De aquí la necesidad de los *passwords* e identificativos de usuarios para controlar y restringir el acceso a los datos.

En los años ochenta, lo anterior se triplica dado el avance de las bases de datos, el aumento del número de usuarios distantes conectados a través de redes de comunicación y de ordenadores personales trabajando como terminales del computador central o en procesos locales *off Line*. Todo eso, hizo que los factores de riesgo de las empresas se incrementaran por pérdida de un activo tan importante como lo es la información.

En la delincuencia informática, el derecho penal es alcanzado por:

- ✓ Las maniobras fraudulentas que se puedan hacer por computador, como medio o circunstancia (robo de ficheros, alteraciones en el ordenador, etc).
- ✓ Los actos fraudulentos que sólo se producen en ocasión de una operación informática.

Lo cierto es que la realidad del fenómeno fraudulento por medio de, o con ocasión de la informática es preocupante, pese a la dificultad para obtener cifras reales lo que ha llevado a algunos a mitificar la criminalidad informática. No obstante, hay algo cierto: el fraude informático lesiona cualquier sector de la economía.

Las víctimas del fraude informático son de preferencia del sector bancario y del sector seguros, le siguen las grandes empresas. En piratería de *logiciel* son los distribuidores, editores o autores del mismo.

El descubrimiento de la infracción es difícil porque a veces se programa la destrucción de datos o del *logiciel* para que ocurra meses más tarde. Casi siempre el fraude se descubre por azar, falta de previsión, negligencia o imprudencia del delincuente.

La prueba del hecho dañoso es con frecuencia difícil, porque casi nunca se dejan huellas (la informática se caracteriza por su "inmaterialidad"). El número de indagaciones iniciales es ínfimo, tal vez por prevención y el temor a tener que pagar las costas del juicio.

La "informatización" de la sociedad contemporánea ha incidido en muchos comportamientos sociales: han creado nuevos valores económicos (los bienes informacionales), han cambiado varias relaciones comerciales y profesionales, públicas y privadas.

Todo esto ha hecho que el derecho penal tradicional se vea cuestionado en algunos puntos como: el problema de la norma y de la desviación en relación con el uso de una nueva tecnología, la llegada al mercado de una nueva categoría de bienes por proteger, etc.

La inseguridad de los sistemas pone en peligro aun la organización democrática de los países, al suscitar una nueva desviación de la conducta delictiva y multiplicar las consecuencias dañosas.

I.- Concepto de "delito informático"

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en muchos países aún no ha sido objeto de tipificación".

Para Carlos Sarzana, en su obra *Criminalista y Tecnología*, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático".¹

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

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador".

¹ Véase sección de Anexos pagina I

En este orden de ideas, se entenderán como "delitos informáticos" todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes, debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin embargo, deberá tenerse presente que nuestro objetivo principal es proveer la información básica que permita una mejor discusión, y un marco conceptual para la aplicación de propuestas, en materia de regulación penal de aquellas actitudes antijurídicas que estimamos graves, como último recurso para evitar su impunidad, esto de acuerdo con la realidad nacional de cada uno de los países.

II.- Su perfil criminológico

Una aproximación al perfil criminológico del delincuente informático apunta hacia un individuo normalmente del sexo masculino, en edades comprendidas entre los catorce y treinta años, experto en el manejo de nuevas tecnologías, con un altísimo potencial intelectual y en muchos casos empleado de confianza habituado a trabajar sobretiempo. El delincuente tecnológico comúnmente asume una actitud de reto con los sistemas a que se enfrenta, de modo tal que considera suficientemente justificado el lucro que obtiene, como recompensa a su pericia e inteligencia.

Las modalidades son ilimitadas, sin embargo apuntaremos brevemente algunas de las piezas estelares de este género: La técnica del Salami, que consiste en la reducción automatizada, sistemática y continua de pequeñas cantidades de dinero de un gran número de cuentas, que luego son abonadas a otra cuenta bancaria, controlada por el defraudador. Manipulación de datos, que permite efectuar transacciones falsas, emisión fraudulenta de documentos, etc. Sabotaje informático, entre los cuales se incluyen las bombas lógicas y los virus, que representan un grupo de programas capaces de causar daños inestimables en sistemas de información.

Los Hackers, son la última avanzada de la delincuencia informática de este final de siglo. Hackers, es un término en inglés con el que se define a las personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, y apenas constituyen una muestra de la nueva faceta de la criminalidad: El delincuente silencioso o tecnológico.

En un evento celebrado hace algún tiempo en Caracas, la Profesora Española Mariluz Gutiérrez Francés refería en su ponencia titulada "Incidencia de las Nuevas Tecnologías de la Información en el Derecho Penal", lo siguiente:

"El computador es un factor criminógeno de primera magnitud que aporta a la conducta criminal, unas veces, un nuevo objeto (la información misma, potenciada y revaluada por los nuevos sistemas de procesamiento de datos y los programas), y otras, un nuevo instrumento: ofreciendo un inmenso abanico de técnicas y estrategias que pueden ponerse al servicio del delito, enriqueciendo el repertorio criminal." Esta acertada distinción permite precisar cuando la tecnología es medio y cuando objeto del delito.

Es común la expresión "La información cuesta", lo que refleja la apetecibilidad y atractivo que en la actualidad representa el manejar datos claves, es la información como elemento de conocimiento, poder y fortuna. Cuando la información se convierte en objeto de apropiación y en blanco lucrativo del delincuente, se ven afectados valiosos bienes jurídicos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del estado, entre otros.

En el mismo sentido, debemos señalar que las nuevas tecnologías se convierten en instrumentos del delito, cuando sus técnicas y sofisticadas herramientas para el tratamiento automatizado de la información se utilizan como medio de comisión de acciones generadoras de importantes daños y lesiones, patrimoniales o no, a personas y organizaciones.

Esta emergente categoría criminal ha sido encuadrada usando los términos: Delitos computarizados o Informáticos, y en una acepción mas amplia, designados como Crimen silencioso o tecnológico.

El delito silencioso se caracteriza principalmente por la participación, bien como instrumento o como objeto, que en los sucesos relacionados con su comisión tienen las nuevas tecnologías. Pero existen otros elementos distintivos de donde se origina tan peculiar denominación de silenciosos. Estos hechos - a diferencia de los estruendosos delitos ordinarios como el secuestro, el homicidio o la violación - son absolutamente discretos, no ocupan grandes titulares en los medios de comunicación y en la mayoría de las ocasiones permanecen ocultos e ignorados. Esta peculiaridad se debe a la dificultad existente para descubrir su ocurrencia, a la creciente imposibilidad de lograr evidencias que permitan descubrir a los culpables y a la común inacción de los agraviados, que normalmente prefieren evitar la divulgación de estas acciones que demuestran una cuestionable vulnerabilidad de sus sistemas de información.

Son varios los elementos que hacen atractiva la comisión de estos delitos. El primero de estos elementos es la relativa facilidad con que un experto informático puede perpetrar estas acciones, las cuales requieren del manejo de conocimientos y herramientas especiales que, en la mayoría de los casos, son de dominio exclusivo de personal técnico.

Los montos de las operaciones delictivo-informáticas son considerablemente elevados, en comparación con los delitos comunes contra la propiedad. En cifras del FBI, mientras un robo puede alcanzar cifras de hasta 3,500 \$, los fraudes informáticos rondan, en promedio, cifras de hasta 500,000\$. La mayoría de estos delitos no están tipificados, es decir considerados expresamente en la ley, lo que contribuye a engrosar los crecientes índices de impunidad que tales conductas tienen en las estadísticas policiales y judiciales. Estos delitos pueden perpetrarse a distancia, programar en el tiempo la aparición de sus efectos, borrar los rastros dejados e incluso emplear datos que deliberadamente desvíen las investigaciones hacia otra persona, a quién pudiera incriminarse. Además, resulta casi imposible distinguir de manera objetiva las frágiles fronteras entre la intención, el error técnico o la impericia.

Se acentúa el hecho de que la delincuencia subcultural no aparece como una dinámica antisocial, sino disocial, donde el grupo tiene su sistema de valores, sus propias normas sus formas de Status, sus reglas de prestigio. Diríamos, en términos conductistas, que los miembros de grupo tienen sus propios impulsos, sus modelos y refuerzos, modo de satisfacerlos y gozan de la aprobación del grupo, ello refuerza la conducta criminogena.

A diferencia de las personalidades antisociales, los delincuentes Subculturales (dysocial) pueden desarrollar lazos interpersonales genuinos, compartiendo un continuado y significativo aprendizaje de evitación (de la detección o de la condena)

III.- Sujeto activo en los delitos informáticos

Las personas que pueden cometer "Delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Estas características nos remiten a:

- Operadores, que se pueden poner en relación con el Sistema para modificar, agregar, eliminar, sustituir información y/o programas, copiar archivos para venderlos a competidores.
- Programadores, que pueden violar o inutilizar controles protectores del programa y/o sistema; dar información a terceros ajenos a la empresa, atacar el sistema operativo, sabotear programas, modificar archivos, acceder a información confidencial.
- Analistas de sistemas, que pueden colusionarse con usuarios, programadores y/u operadores para revelarles la operación de un sistema completo.
- Analistas de comunicaciones, que enseñan a otras personas la forma de violar la seguridad del sistema de comunicaciones de una empresa, con fines de fraude.
- Supervisores, que pueden en razón de su oficio manipular los archivos de datos y los ingresos y salidas del sistema.
- Personal técnico y de servicio, que por su libertad de acceso al centro de cómputo puede dañar el sistema operativo.
- Ejecutivos de la computadora, que pueden actuar en situación de colusión con otras personas.
- Auditores, que pueden actuar como los anteriores.
- Bibliotecarios de preparación, que pueden vender la documentación.
- Bibliotecarios de operaciones, que pueden destruir información mediante errores o pueden venderla a competidores.
- Personal de limpieza, mantenimiento y custodia, que pueden vender el contenido de los costos de papeles, fotocopiar documentos, sabotear el sistema.
- Usuarios, que pueden modificar, omitir o agregar información con fines fraudulentos.

Aunque con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los

posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "delitos informáticos", estudiosos en la materia los han catalogado como "delitos de cuello blanco" término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros".

Asimismo, este criminológico estadounidense dice que tanto la definición de los "delitos informáticos" como las de los "delitos de cuello blanco" no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables" otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo, que dada la naturaleza de nuestro objeto de estudio nos vemos en la necesidad de limitar.

IV.- Sujeto pasivo de los delitos informáticos

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros. Los bienes jurídicos tutelados afectados pueden ser numerosos:

- Las personas.
- El honor de las personas.
- La intimidad de las personas.
- La propiedad (de hardware o software).
- Los Documentos, Archivos, Registros, Bases de Datos, y toda información concerniente al que hacer propio de la Entidad.
- La fe pública.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los "delitos informáticos", ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables" y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

Por lo anterior, se reconoce que "para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, una análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento".

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, debemos destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

V.- ¿Qué son los delitos informáticos?

A nivel mundial subsiste esta discusión, alrededor de la existencia del delito informático. Ciertas opiniones se vuelcan a la no existencia del delito informático:

“Estamos en presencia de delitos clásicos en los que su naturaleza no varía en gran medida por el hecho de que para su perpetración se haga uso de moderna tecnología relacionada con la computación. Por lo tanto no puede hablarse de delito informático sino más bien de una categoría criminológica como delincuencia o criminalidad informática dentro de la cual se agruparán los problemas del procesamiento de datos, relevantes para el derecho penal sin modificar los tipos penales y las conductas a ellos vinculadas. La gran mayoría de los ilícitos informáticos pueden encuadrarse en los tipos penales tradicionales, en la medida en que sistemas computarizados sean utilizados como medio, instrumento, herramienta u objeto de aquellos.” Doctora Silvina Laura Rinaldi, ponencia : “Delitos informáticos, perfil criminológico del hacker, especial referencia a los delitos de contenido económico y normativa aplicable”, Primeras Jornadas Latinoamericanas de Derecho Informático, Mar del Plata, 2001

Pero ya son muchos los autores que manifiestan su opinión a favor de la existencia del delito informático. Uno de ellos, destacado doctrinario en la materia, el doctor Julio Téllez Valdez, quien conceptualiza al delito informático en forma típica y atípica, entendiendo a la primera como a *“las conductas típicas, antijurídicas y culpables , en las que se tienen a las computadoras como instrumento o fin”* y a las segundas *“actitudes ilícitas en que se tienen a las computadoras como instrumento o fin”*. VIII Congreso Iberoamericano de Derecho e Informática, Cancún y Distrito Federal, Méjico, Noviembre 2000.

“El campo de los delitos informáticos aparece hoy por ante el legislador como un mundo que puede decirse no al alcance de la mayoría y más aún si nos adentramos específicamente en el punto de los delitos electrónicos ya que su aprehensión implica un mayor grado de compromiso con conocimientos tecnológicos que a la postre resultan sólo para algunos elegidos.” Doctor Gabriel A. Cámpoli, ponencia “El Elemento Subjetivo En Los Delitos Electrónicos - ¿El Dolo O La Culpa?”, Primer Congreso Mundial de Derecho Informático, Quito, Ecuador, Octubre 2001.

Interpretando la tendencia, entonces consideramos que sí, existe el delito informático, pero que muchos de ellos ya se encuentran tipificados en la legislación penal de cualquier país, y otros no; y más aún, tardarán mucho tiempo en ser tipificados, en el caso de Nicaragua ya existen Proyectos de Ley e incluso el nuevo Proyecto de Código Penal de la República de Nicaragua ² recoge los delitos mas importantes en materia informática.

Dentro de nuestro marco regulatorio, existe un proyecto de ley sobre delitos informáticos “LEY ESPECIAL SOBRE DELITOS INFORMATICOS”³ que será considerado más adelante, y en donde no se define específicamente que es un Delito Informático, aunque si define los tipos de Delitos Informáticos.

Las computadoras proporcionan nuevos métodos para cometer delitos tradicionales:

- Fraude.
- Hurto.
- Amenazas.
- Distribución de Pornografía Infantil.

² Véase sección de Anexos pagina XXIII

³ Véase sección de Anexos pagina II

Sin embargo las leyes existentes para corregir los delitos tradicionales pueden no ser adecuadas para cubrir de forma precisa los delitos cibernéticos.

En este sentido las computadoras pueden pasar de ser un recurso para agilizar el trabajo, a una herramienta para delinquir.

VI.- Tipificación de los delitos informáticos

Los delitos informáticos han sido clasificados en tres grandes bloques:

1. El fraude informático por uso indebido o por manipulación dolosa de documentos informáticos de cualquier clase que posibilite un beneficio ilícito.
2. El vandalismo o terrorismo que atente contra la integridad de los elementos informáticos con el fin de causar perjuicio por paralización de actividades.
3. La "piratería" de software por actos que atenten contra la propiedad intelectual sobre derechos informáticos que se encuentren debidamente protegidos por las leyes.

Los elementos del fraude informático son tres:

- a) Un sujeto actor o autores de la conducta dañosa que produce fraude.
- b) Un medio adecuado para cometer el acto ilícito, o sea el sistema informático por medio del cual se lleva a cabo la acción.
- c) Un objeto, o sea, el bien que produce el beneficio ilícito para el o los autores.

El American Institute of Certificial Public Accountants (ALCPA), ofrece la siguiente definición:

"Cualquier acto, o serie de actos, realizados para defraudar o engañar (creando situaciones que induzcan a error) y que tienen un impacto real o potencial en los estados financieros de una organización. En la realización o encubrimiento del acto, o serie de actos, deben estar necesariamente involucrados dispositivos informáticos". (Informe sobre fraude informático, 1984).

En esta definición se aporta la idea de delito continuado (algo frecuente), de acto repetitivo; se recaba sobre el concepto de daño como perjuicio económico directo, indirecto o intangible. El profesor chileno EDUARDO HAJNA R., ha elaborado esta lista de conductas informáticas fraudulentas:

3.1. Hurto de tiempo por computador

Ya que normalmente los computadores no funcionan a capacidad y siempre tienen un espacio libre, hay personas que pueden utilizar el sistema en forma personal durante un lapso, sin grave riesgo para el sistema.

3.2. Manipulaciones

Aquí encontramos diferentes actuaciones que se pueden considerar como manipulación en el computador:

- a. Entrada-salida: Es la modificación de los soportes de información con el fin de introducir datos en la memoria e informes de estados de cuentas y créditos de las personas.
- b. Programas: Son métodos de bloqueo que impiden el corte en ciertas cuentas, para percibir los intereses o pagos de cheques a beneficiarios ficticios, etc.
- c. Hardware: Conjunto de modificaciones realizadas a las características de un equipo.
- d. Sabotaje: Consiste en la alteración u omisión de los mismos datos.
- e. Divulgación o apropiación de datos informatizados, técnicos o nominados protegidos por la vía del secreto tales como el robo de programas, venta de ficheros, etc.

Para Do B. PARKER, la clasificación de los múltiples métodos que afectan el software es la siguiente:

1. Datos engañosos: Es el más seguro y eficaz método utilizado por los delincuentes informáticos, el cual consiste en la alteración de los datos de entrada al computador, a través de manipulaciones difíciles y casi imposibles de detectar; los datos son ingresados con omisiones o agregaciones que los alteran en su sentido y contenido.
2. Caballo de Troya: Es otro método de sabotaje muy utilizado, mediante el cual se introduce una serie de órdenes en la codificación de un programa con el propósito de que éste realice funciones no autorizadas.
3. La técnica salami: Es muy utilizada en las instituciones en que hay un continuo movimiento de dinero y consiste en la sustracción de pequeñas cantidades activas de diferentes procedencias, logrando a través de él un redondeo en las cuentas.
4. Superzapping: Es el manejo de programas de uso universal, la copia y la reproducción que evita el pago de los derechos de propiedad.
5. Bombas lógicas: Son programas ejecutados en momentos específicos o bajo determinadas condiciones; son rutinas a posteriori según circunstancias de tiempo, de fecha, pago, etc.
6. Recogida de residuos: Es la recogida de información residual impresa en papel o magnética en memoria, después de la ejecución de un trabajo, con ella se puede establecer la situación de una empresa, los niveles de renta, etc., en fin, todos los datos que se encuentren en el papel y que quedan como borradores.
7. Suplantación: Consiste en lograr el acceso a áreas que son controladas por medios electrónicos o mecánicos.
8. Simulaciones y modelos: Fundamentalmente consiste en utilizar el computador para planificar y controlar un delito, mediante el uso de técnicas de simulación y modelos.
9. Puertas con trampas: Es la utilización de interrupciones en la lógica del programa, en la fase de desarrollo para su depuración y uso posterior con fines delictivos.
10. Pinchar líneas de teleproceso: Es la intervención en las líneas de comunicación para lograr el acceso y posterior manipulación de los datos que son transmitidos.
11. Ataques asincrónicos: Es el aprovechamiento de funcionamientos asincrónicos de un sistema operativo, basado en los servicios que puede realizar para los distintos programas de ejecución.

12. Filtración de datos: Consiste en filtrar o sacar los datos de un sistema por sustracción o copia, como ocurre al duplicar una cinta.

ULRICH SIEBER ha creado dos grandes categorías de delitos cometidos con ordenadores:

- a) Aquellas modalidades delictivas tradicionales que han existido antes de la aparición del computador y que ahora, con la utilización de este medio, incrementaron sustancialmente su volumen al poderse cometer con más rapidez e impunidad. Dentro de este grupo se encuentra una amplia variedad de atentados contra los bienes (pagos a proveedores o empleados inexistentes, figuración de préstamos o cuentas por cobrar, apropiación indebida o hurto de informaciones, etc.); contra las personas (atentados a la intimidad, al honor, etc.) e inclusive contra la seguridad de las comunicaciones.
- b) Las modalidades delictivas que surgen con los ordenadores y a causa de su posible empleo irregular son:

Fraudes por manipulaciones de un computador contra un sistema de procesamiento de datos o banco de datos (operados con participación de control humano o automáticamente).

- Espionaje informático.
- Sabotaje informático.
- Acceso no autorizado a sistemas de procesamiento de datos.
- Apropiación indebida o hurto de programas (software) y desarrollos.
- Uso y venta no autorizada de servicios y equipos (conocido como hurto de tiempo de máquina).

Los tipos penales tradicionales parecen inadecuados en la mayoría de las legislaciones para encuadrar estas nuevas formas delictivas. Otras dificultades inherentes al problema son:

- Este tipo de delincuencia opera a menudo sobre los objetos intangibles como el activo de los bancos, know how y otras expresiones incorpóreas de difícil aprehensión legal.
- El tema suele plantear complejos perfiles para el derecho internacional cuando el delito afecta a más de una jurisdicción nacional (Ver: RAÚL.. CERWNI. Opus cit. p.p. 151-152).

Los fraudes informáticos por manipulaciones cubren una amplia gama de creciente complejidad en los ilícitos que va desde una simple maniobra en el computador, hasta aquellas sofisticadas manipulaciones contra sistemas de resolución final automática con prescindencia de todo control humano. Las técnicas de input (alimentación de datos falsos en la computadora), de output (modificación de resultados), o bien falseando el normal procesamiento tras una manipulación en el programa de computación o en la consola (“caballo de Troya”, “programa de virus”, “salami”).

También existen los delitos relacionados con los documentos: falsedad, destrucción y ocultamiento, violación de correspondencia, de comunicaciones, el uso ilegítimo de patentes, sabotaje, hurto, etc.

VII.- Tipos de delitos informáticos reconocidos por Naciones Unidas

A.- Fraudes cometidos mediante manipulación de computadoras

- **Manipulación de los datos de entrada.** Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.
- **La manipulación de programas.** Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tiene conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
- **Manipulación de los datos de salida.** Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente el equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

B.- Fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo.

Es una técnica especializada que se denomina "técnica de salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

C.- Falsificaciones informáticas

- a.- **Como objeto.** Cuando se alteran datos de los documentos almacenados en forma computarizada.
- b.- **Como instrumento.** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser, surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

VIII.- Elementos sustantivos a considerar

- ¿Quién es la víctima?
- ¿Qué es una conducta ilícita?
- ¿Qué estado mental se requiere?
- ¿Dónde se cometió el delito y dónde se encuentra el delincuente?
- ¿Cuál es la pena?

Las víctimas pueden ser cualquier sistema Gubernamental o no Gubernamentales, Empresas privadas y estatales, y personas particulares.

Las conductas ilícitas pueden consideradas desde el punto de vista informático:

- Obstrucción al acceso de una computadora
- Ataques de denegación de servicios.
- Daños a la información de una computadora.
- Hurto de la información.
- Tentativa de cometer fraude usando una computadora.
- Daños o amenazas a la seguridad pública.
- Transmisión o creación de un código para cometer un delito informático.
- Intercepción de datos en transmisión
- Trafico de contraseñas personales o dispositivos de acceso.

La criminalidad mediante el uso de computadores se realiza a través de conductas dañosas sobre un bien jurídico tutelado por la ley que hace parte de un patrimonio. El delito informático es toda acción dolosa que cause un perjuicio a personas naturales o jurídicas que puede producir o no un beneficio material para su autor, pudiendo o no perjudicar de forma directa o inmediata a la víctima, caracterizándose dicha acción por ser realizada mediante dispositivos habitualmente utilizados en actividades informáticas.

Los sistemas y métodos utilizados para defraudar, son inagotables. Lo importante es que se configure el tipo penal previsto en el respectivo Código Penal (Artos 195, 196, 197; 201, 202; 244-247-249; 251, 267 del Proyecto de Código Penal de la Republica de Nicaragua⁴), con el fin de que surja con claridad el objeto jurídico que el Estado busca proteger y que resulte vulnerado por la conducta del agente.

Generalmente, la literatura penal no ofrece definición alguna de la infracción informática. Para muchos autores lo mejor es aprehender lo que caracteriza a la infracción informática:

- Ensayando un inventario, una tipología, una manera de clasificación.

⁴ Véase sección de Anexos pagina XXIII

- Tratando de cernir sus particularidades: consecuencias dañosas específicas, personalidad del delincuente, métodos utilizados, etc.
- Refiriéndose únicamente a las infracciones específicas creadas por la respectiva ley de informática y libertades.

J. DEVEZE dice que para justificar efectivamente la etiqueta de fraude informático, debe estar necesariamente ligado al funcionamiento de un ordenador o que produzca un atentado a bienes informacionales. Lo cierto, es que el fraude informático tiene un carácter horizontal porque atraviesa todos los dominios del derecho pero, sobre todo, las categorías de infracciones contra los bienes y contra las personas. Contra los primeros serían el robo, la destrucción, el sabotaje y de ordenadores. Contra los segundos serían la recolección, conservación, divulgación ilícita de informaciones nominativas, desviación de finalidad.

El desafío de una nueva forma de criminalidad, como lo es la criminalidad informática, ha planteado estas dificultades: tutela legal de los instrumentos informáticos, protección de la intimidad y de los datos reservados, contratos informáticos, responsabilidad civil por los daños emergentes de la informática, derecho procesal informático, los delitos instrumentados mediante el uso del computador. En todas estas áreas, gira siempre el tema recurrente de las inmensas sumas de dinero que mueve la informática y, por ende, la proclividad hacia el delito del orden económico.

El hecho penal profesional es sofisticado, técnico y, sobre todo, computarizado. Los procedimientos técnicos más usuales son la alteración del contenido de los campos claves de los documentos fuentes y de los archivos, la introducción clandestina de modificaciones en las instrucciones de los programas, accesos no autorizados por "puertas trampas", intercepción de comunicaciones (técnica predilecta del delito financiero internacional). BRANDT ALLEN, luego de estudiar 150 casos conocidos de delitos por computador, señala que el 69% de los casos estudiados resultaron ser transacciones agregadas, alteradas o eliminadas, 9% cambios de programa, 8% cambios en archivos, 3% operación indebida y 11% fraudes varios. La daño social de la delincuencia informática, es de gran magnitud: el perjuicio promedio sufrido en cada fraude descubierto apoyado en ordenadores, es superior a los U.S.\$60.000, mientras que en el periodo de 1972- 1982, el promedio por cada estafa o fraude común se ubica en una suma cercana a los U.S.430.000 (datos del F.B.I.). Según el Stanford Research Institute, sobre 375 casos conocidos hasta 1975, cada fraude por ordenador produjo una pérdida de U.S.\$ 500.000, que afectó en primer lugar, a las instituciones financieras con un 24% del total. Para 1984, la Universidad de Lieja encontró que las pérdidas anuales por concepto de fraudes informáticos alcanzó la cifra de U.S.\$ 150 millones en USA y en más de US\$80 millones en Europa; a fines de 1987, el incremento del daño fue superior al 25% en ambas áreas. Durante el trienio 1986-1989, las instituciones financieras de Brasil, Argentina y Uruguay fueron víctimas de 26 formas de fraudes informáticos con una pérdida cercana a los tres millones de dólares (Ver: RAÚL CERVINI. Reflexiones sobre los fraudes informáticos por manipulación. En: Revista del Colegio de Abogados Penalistas del Valle. Vol. XV, números 25 y 26 p.p. 143.163).

Las cifras expuestas ponen de manifiesto la necesidad de precisar expresiones como "criminalidad mediante computadoras". En una primera aproximación, se podría aludir con ella a todos los comportamientos antijurídicos según la ley vigente (o socialmente perjudiciales, y por eso punibles en el futuro) realizados merced al empleo de un equipo automático de procesamiento de datos. En este concepto, según KLAUS TIEDEMANN, se aborda, por una parte, el problema de la amenaza a la esfera privada del ciudadano mediante la acumulación, archivo, asociación y divulgación de datos mediante computadoras; y por otra parte, el concepto aludido se refiere a los daños patrimoniales producidos por el uso abusivo de datos procesados automáticamente.

El medio empleado, ha dado lugar a una nueva categoría de comportamientos punibles que recaen sobre objetos intangibles como dinero en los bancos, secretos comerciales, tecnología y otras informaciones.

Pese al rápido deseo de muchos penalistas de crear en los respectivos códigos penales capítulos adicionales para los denominados delitos informáticos, otros se preguntan si es necesaria dicha creación. Tal es la posición del jurista colombiano JOSE CANCINO, quien pide andar con "pies de plomo" para no caer en la trampa de sentirse obligados, como penalistas a crear toda una infraestructura de carácter legislativo en aspectos que solamente tienen incidencia en el campo instrumental o, para ser más claros, agrega, en el ámbito de los "medios de comisión de los delitos". Lo esencial, continúa CANCINO, es estudiar en qué medida los instrumentos normativos existentes no pueden cobijar, por sí solos, o con modificaciones pertinentes, las conductas delictivas realizadas a través de las computadoras o restantes medios similares que nos ofrece el revolucionario momento histórico de la cibernética.

La primera dificultad, es la de establecer el objeto jurídico a tutelar pues, como se deduce de esto, mediante la utilización delictiva de los diversos servomecanismos o aparatos cibernéticos, son muchos los tipos que se pueden estructurar y muy diversos los bienes e intereses jurídicos que se pueden menoscabar. La sistematización, al menos alrededor del "objeto jurídico", no se lograría al menos dentro de los patrones dogmáticos.

Las nuevas formas de comportamientos criminales que exigen renovación normativa ante la aparición de la informática, no significa (concluye CANCINO) que aceptemos la tesis según la cual se deba crear un derecho penal informático, como islote separado del Código Penal. ¿Es necesario crear en el Código Penal un capítulo para los denominados delitos informáticos?.

En igual sentido al de CANCINO, parecen las tesis de FERNANDA GUERRERO MATEUS y JAIME EDUARDO MERA. En efecto, estos autores parten de un hecho innegable: sobre lo que debe entenderse por delito informático han sido muchas las opiniones encontradas y aun ligeras. Se ha girado entre dos posiciones la penalización apresurada o la despenalización irresponsable. Las posibilidades de adecuación se manifiestan como una atipicidad absoluta o como una atipicidad relativa.

La Argentina se encuentra desde hace varios años, estudiando la forma de determinar la adecuación de la legislación penal vigente a la prevención y represión de la delincuencia informática. Todo parece indicar que los expertos van a inclinarse a tipificar acciones delictivas informáticas que por sus especiales características, hoy por hoy están quedando en la absoluta impunidad. Claro que no faltan los que proponen una modificación de diversos tipos penales, antes que la elaboración de un nuevo título o de una ley especial.

Es notable el esfuerzo realizado por los autores mencionados para tratar de levantar un ademécum de las posibles conductas delictivas de naturaleza informática:

- ✓ Daño en bien ajeno(bienes documentales).
- ✓ Abuso de confianza.
- ✓ Defraudación.
- ✓ Falsedad.
- ✓ Acceso indebido.
- ✓ Estafa.
- ✓ Hurto.

Una conclusión cierta, es que el fraude informático se está cada día internacionalizando mucho más.

¿Qué estado mental se requiere?

¿Qué tan deliberada fue la conducta? ¿Intencional, irresponsable, o absolutamente sin intención?

Cuando se requiera la intención, debe ser la intención de realizar la acción, no la intención de causar las consecuencias.

¿Dónde se cometió el delito y dónde se encuentra el delincuente?

¿Se encuentra la persona en el territorio nacional?

¿Se cometió el “delito” en el territorio nacional?

Las leyes necesitan ser capaces de soportar el procesamiento de personas que usan recursos o computadoras que no se ubican en territorio nacional.

¿Cuál es la pena?

¿Qué tipo de pena es apropiada?

La pena debe ser lo suficientemente grave como para actuar como elemento disuasivo. Generalmente esto significa periodos significativos de encarcelamiento, restitución a la víctima y, algunas veces, multas.

La pena puede variar dependiendo de que tan grave sea el delito cometido y los daños causados por el mismo.

IX.- Regulación jurídica.

Una vez examinada tanto la realidad y la importancia del proceso de informatización de la sociedad como los peligros que del mismo derivan es necesario afrontar el estudio de las medidas jurídicas que la sociedad, a través del Estado, puede y debe utilizar para intentar que los citados delitos informáticos no implique una merma de los derechos y libertades de los ciudadanos o una “reestructuración regresiva” del sistema político al que sirven de fundamento.

Premisa fundamental para lograr un planteamiento jurídico adaptado al fenómeno constituido por la irrupción de las nuevas tecnologías de la información en la estructura social es el hecho de que las mismas no suponen exclusivamente la posibilidad de un conflicto con algún derecho o libertad en concreto, sino que dicho acontecimiento, que debe calificarse de histórico, afecta a los pilares básicos de nuestra sociedad. De aquí que, frente a este problema, no quepan acercamientos o intentos de solución parcial en relación con cuestiones puntuales: puesto que la informática, en su vertiente relativa a la información, puede suponer un reto global a una determinada concepción de la sociedad, la respuesta social a la misma ha de ser también necesariamente global, lo que no implica, evidentemente, que en dicha respuesta no se intente hacer frente a problemas concretos. Se trata de afrontar esos problemas con la conciencia de que los mismos son manifestación de una cuestión que, por la aparición de las nuevas tecnologías, se presenta con perfiles cualitativamente distintos a situaciones anteriores: la regulación del tráfico de la información en una estructura social en la que la posesión de información implica posesión de poder.

Ahora bien, el ordenamiento jurídico, ante la aparición de un fenómeno nuevo puede optar entre una de estas dos posturas: o bien regular jurídicamente antes de que los peligros que de tal fenómeno se derivan se materialicen, con el consiguiente riesgo de que dicha regulación padezca de insuficiencia, precipitación o excesiva juridificación de la materia; o bien esperar a que se produzca un desarrollo del fenómeno en el tiempo, para, de esta forma calibrar y aquilatar mucho mejor la

respuesta jurídica y evitar, por tanto, cualquier innecesaria y precipitada intervención legislativa que pudiera entorpecer el desarrollo social.

En relación con el fenómeno de las nuevas tecnologías de la información parece que el legislador debe optar por la primera decisión de la disyuntiva planteada y ello por los siguientes motivos:

En primer lugar, los peligros que el nuevo medio conlleva no sólo hace tiempo que son reconocibles sino que algunos ya se han materializado en las sociedades que han alcanzado un cierto grado de desarrollo en relación con esta materia.

En segundo lugar, y con razón, se han comparado las consecuencias de esta evolución tecnológica con las consecuencias que para el medio ambiente ha tenido la evolución industrial: cuando el legislador ha querido controlar un proceso evidentemente dañoso para la sociedad muchas de estas consecuencias ya eran irreversibles. Por ello, es imprescindible que lo antes posible exista una regulación del tema para que este desarrollo se mueva dentro de unos límites claros y la propia investigación en materia fundamentalmente de software atienda no sólo a la obtención de los mayores beneficios posibles, sino que desde ya sea consciente de que en dicha investigación han de barajarse otros parámetros de importancia tan vital para la sociedad como el anteriormente citado.

El progreso en materia de tecnologías de la información debe buscar siempre más importantes grados de efectividad pero con el límite constituido por el respeto a los derechos y libertades de los ciudadanos y, en caso de conflicto, optar claramente por la preferencia de estos últimos: al encauzamiento en este sentido del proceso contribuirá decisivamente la existencia de una normativa legal.

Parece claro tras la exposición anterior relativa a la realidad y posibilidades de la informática, que el arsenal de medios de que en la actualidad dispone el ordenamiento jurídico se muestran claramente insuficientes en relación con la problemática de la información en la sociedad, ya que está dirigido a una estructura cualitativamente distinta frente a la que cabían reacciones individuales del tipo de las indemnizaciones de daños y perjuicios, insuficientes en la actualidad.

Es necesario, pues, articular toda una serie de medidas jurídicas que vuelvan a colocar al ciudadano en el papel activo que le corresponde en el Estado de Derecho, medidas que han de dirigirse específicamente a esa nueva realidad que abarca todos los sectores de la estructura social para que los individuos no se vean convertidos en meros objetos de información, sino que sean sujetos que intervienen en los procesos que les afectan.

Una vez examinado el carácter necesariamente global de la respuesta jurídica ante el problema informático se puede pasar ya al examen en concreto de cuáles son los medios que el legislador ha de disponer para que el proceso en examen permanezca dentro de los límites del Estado de Derecho.

En efecto, los peligros de una mala utilización de las nuevas tecnologías se derivan no son monopolio exclusivo del Estado. Por otra parte, tampoco son menores las necesidades de información en este sector que en el sector estatal. Tampoco debe olvidarse, que la fuerza de penetración de la informática en el sector privado es, en la mayoría de los subsectores igual, e incluso superior, a la que se da en el sector estatal. Por todo ello parece evidente la necesidad de una regulación global, lo que, por supuesto, no implica una regulación uniforme. Esta regulación ha de tener en cuenta necesariamente las peculiaridades de los distintos sectores para, de esta forma, hacer frente a los específicos problemas que de cada uno de ellos se derivan.

Una vez examinado el alcance en cuanto a la materia de la regulación del problema de la información en la sociedad actual puede pasarse al estudio de las medidas que el legislador ha de adoptar para canalizar en el sentido expuesto este proceso. Estas medidas son fundamentalmente de tipo administrativo u organizativo y de carácter técnico, ya que su finalidad primordial, dados los

específicos peligros que de dicho proceso dimanar, es preventiva. Es decir, tienden a evitar la materialización de toda esa serie de posibles consecuencias negativas. Pero estas medidas técnicas y administrativas deben verse acompañadas del reconocimiento de una serie de derechos de los ciudadanos en relación con la información que les atañe, así como de las correspondientes sanciones penales, tal y como ya han hecho los legisladores de otros países que se han enfrentado al tema, previstas para aquellas conductas que supongan una quiebra, ya de las medidas técnicas u organizativas, ya de los derechos reconocidos en esta materia a los ciudadanos.

El recurso al Derecho penal y, por tanto, el carácter grave de las sanciones de que hace uso el legislador se halla justificado tanto por la clase de los bienes en juego en esta materia, ya que se trata de garantizar las condiciones necesarias para el ejercicio de la mayor parte de los derechos fundamentales y libertades públicas; como por el carácter también especialmente grave de estas formas de ataque a dichos bienes, ya que colocan al individuo en una situación de absoluta indefensión, pues la mayoría de las veces no llegará ni tan siquiera a conocer que ha sido lesionado en sus derechos, sin saber en la mayoría de los casos quien ocasiono los daños.

AÑEXOS

CONSTITUCIÓN POLÍTICA DE LA REPUBLICA DE NICARAGUA

Arto. 26. Toda persona tiene derecho:

- 1.- A su vida privada y a la de su familia.
- 2.- A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.
- 3.- Al respeto de su honra y reputación.
- 4.- A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información...

La ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos cuando sea indispensable para esclarecer asuntos sometidos al conocimiento de los tribunales de justicia o por motivos fiscales.

Las cartas, documentos y demás papeles privados sustraídos ilegalmente no producen efecto alguno en juicio o fuera de él.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

BORRADOR

ANTEPROYECTO

DE

LEY ESPECIAL SOBRE DELITOS INFORMATICOS

Abril 2005

Secretaría Ejecutiva

CONICYT

LEY ESPECIAL SOBRE DELITOS INFORMATICOS

LEY No. ---

EL PRESIDENTE DE LA REPUBLICA DE NICARAGUA

Hace Saber al pueblo Nicaragüense que:

LA ASAMBLEA NACIONAL DE LA REPUBLICA DE NICARAGUA

En uso de sus facultades:

HA DICTADO

La Siguiente:

LEY ESPECIAL SOBRE DELITOS INFORMATICOS

INDICE

Anteproyecto de Ley Especial sobre Delitos informáticos

CAPITULO I

Disposiciones Generales

CAPITULO II

De los delitos y las penas

CAPITULO III

Disposiciones Finales

Capitulo I

Disposiciones Generales

Arto. 1.- Objeto de la ley. La presente ley tiene por objeto prevenir y sancionar los delitos cometidos en contra de los sistemas informáticos integrados en equipos físicos o datos e información almacenada en archivos, registros, bases o bancos de datos automatizados.

Arto. 2.- Ámbito de aplicación. Las disposiciones de la presente ley serán aplicables en todo el territorio nacional a las personas naturales que utilizan equipos físicos con sistemas informáticos integrados.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

Arto. 3.- Definiciones. Para los efectos de la presente ley, se entiende por:

- a. Datos: símbolos o caracteres representados apropiadamente para que sean difundidos o procesados por equipos electrónicos a los cuales se les asigna un significado.
- b. Computador: dispositivo o unidad funcional que acepta datos, los procesa de acuerdo con un programa guardado y genera resultados.
- c. Hardware: componentes físicos de un sistema informática.
- d. Información: procesamiento de datos realizado por una persona a los cuales se les asigna un significado.
- e. Software: Registro de rutinas o secuencia de instrucciones, de carácter lógico que, codificados en sistema binario, residen o se archivan en forma electrónica e intangible, en soportes magnéticos u ópticos, decodificados, interpretados y reproducidos, de cualquier forma a través de un computador o sistema informático.
- f. Sistema informático: comprende al hardware local y remoto conectado o no por una red telemática y al software residente en soportes electrónicos u ópticos, fijos o móviles, que dependen de el para realizar un trabajo en particular o resolver un problema dado.
- g. Virus informático: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un software o componente del sistema.

Capítulo II De los Delitos y las penas

Arto. 4.- Acceso indebido de datos. Comete delito de acceso indebido de datos el que sin el debido consentimiento, accede, intercepta, interfiere, copia o desvía datos o información almacenada en archivos, registros, bases, bancos de datos o en equipos físicos que utilizan sistemas informáticos, será sancionado con la pena de seis meses a dos años de prisión.

El que revele o difunda los datos o información obtenida indebidamente descrita en el párrafo anterior del presente artículo, será sancionado con la pena de seis meses a tres años de prisión.

Cuando el autor sea funcionario público en ejercicio de sus funciones, será sancionado con inhabilitación especial para el desempeño de cargos públicos por el doble de tiempo que el de la condena.

Arto. 5.- Alteración de documentos. Comete delito de alteración de documentos, el que utilizando equipos físicos con sistemas informáticos integrados, altera, modifica, borra, suprime o lo sustituye con otro en parte o en su totalidad el contenido de un documento Público o privado almacenado o no en dicho sistema, será sancionado con la pena de tres a seis años de prisión.

Si de tal acto, resultare en perjuicio a un tercero, la pena se aumentará en un tercio de lo dispuesto en el presente artículo.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

Arto. 6.- Daño a datos o sistemas informáticos. Comete delito de daño a datos o sistemas informáticos, el que sin la debida autorización destruya, dañe, altere o inutilice los datos o funciones de los sistemas informáticos integrados en equipos físicos, será sancionado con la pena de uno a tres años de prisión.

Si los efectos indicados en el presente artículo se realizaren por medio de un virus informático o programa similar, será sancionado con la pena de cinco a diez años de prisión.

Arto. 7.- Sabotaje informático. Comete delito de sabotaje informático, cuando los hechos descritos en el artículo anterior recaigan sobre los datos o sistemas informáticos de los archivos, registros, bases, bancos de datos que almacenan datos o información de carácter destinada a las funciones publicas, será sancionado con la pena de hasta diez años de prisión.

Arto. 8.- Fraude informático. Comete delito de fraude informático el que con ánimo de lucro, para sí o para un tercero, mediante el uso de equipos físicos que utilizan sistemas informáticos, inserte información falsa, manipule o modifique los programas existentes, procurando el traslado no consentido de cualquier activo patrimonial en perjuicio de otro, será sancionado con la pena de tres a ocho años de prisión.

Arto. 9.- Hurto informático. Comete delito de Hurto informático el que mediante equipos físicos que utilizan sistemas informáticos o medios de comunicación, se apodere de bienes tangibles o intangibles de carácter patrimonial, con el fin de tener un beneficio económico para sí o para un tercero, será sancionado con la pena de tres a seis años de prisión.

Arto. 10.- Espionaje informático. Comete delito de espionaje informático el que sin la debida autorización acceda y obtenga datos o información almacenada en equipos físicos que utilizan sistemas informáticos, con o sin intención de divulgarla, será sancionado con la pena de tres a ocho años de prisión.

Si el delito cometido, se obtuviere datos o información considerada muy secreta, secreta y confidencial, relacionada a la seguridad nacional, defensa o a las relaciones exteriores de Nicaragua, almacenada en bases de datos o sistema informáticos, será sancionado con la pena establecida en el arto. 541 del Código Penal.

Si el autor del delito descrito en el párrafo anterior revelare o divulgare los datos o información obtenida, será sancionado con la pena establecida en el arto. 542 del Código Penal.

Arto. 11.- Difusión pornográfica de niños, niñas o adolescentes. Comete delito de difusión pornográfica de niños, niñas o adolescentes, el que utilizando equipos físicos con sistemas informáticos integrados, soportes electrónicos y digitales, accede, imprime, copia, exhibe, distribuye, comercializa y difunde a través de cualquier medio material pornográfico con imágenes de niños, niñas o adolescentes que tuviere su origen en el territorio nacional, extranjero o desconocido, será sancionado con la pena de cuatro a ocho años de prisión.

La pena del presente artículo se aumentará hasta diez años de prisión cuando el delito cometido sea con ánimo de lucro.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

El que facilite el acceso, impresión, copia, exhibición, distribución, comercialización y difusión, será sancionado con la pena de tres a seis años de prisión.

Arto. 12.- Creación y distribución de virus informáticos. Comete delito de creación y distribución de virus informáticos, el que maliciosamente cree o distribuya cualquier programa con el objeto de destruir, dañar, alterar o inutilizar el funcionamiento de los equipos físicos que utilizan sistemas informáticos, será sancionado con la pena de tres a ocho años de prisión.

Arto. 13.- Violación de las comunicaciones. Comete delito de violación de las comunicaciones, el que interfiere, intercepte, acceda, capture, desvíe o elimine señal de transmisión o mensajes de datos contenidos en equipos físicos electrónicos, sin la debida autorización de la persona o juez competente; será sancionado con la pena de dos a cuatro años de prisión.

Capitulo III Disposiciones Finales

Arto. 14.- Vigencia. Esta Ley entrará en vigencia a partir de su Publicación en La Gaceta, Diario Oficial.

Dado en la ciudad de Managua, en la Sala de Sesiones de la Asamblea Nacional, a los --- días del mes de --- del dos mil ---.-
---, Presidente de la Asamblea Nacional. ---, Secretario de la Asamblea Nacional.-

ANTEPROYECTO

DE

LEY DE PROTECCIÓN DE DATOS PERSONALES

Abril 2005.

Secretaría Ejecutiva

CONICYT

LEY DE PROTECCIÓN DE DATOS PERSONALES

LEY No. ---

EL PRESIDENTE DE LA REPUBLICA DE NICARAGUA

Hace Saber al pueblo Nicaragüense que:

LA ASAMBLEA NACIONAL DE LA REPUBLICA DE NICARAGUA

En uso de sus facultades:

HA DICTADO

La Siguiente:

LEY DE PROTECCIÓN DE DATOS PERSONALES

INDICE

CAPITULO I

Disposiciones Generales

CAPITULO II

De los titulares y responsables de los registros

CAPITULO III

Derechos de los titulares de datos

CAPITULO IV

Usuarios y responsables de archivos, registros, bases o banco de datos

CAPITULO V

De la Dirección de Protección de Datos Personales

CAPITULO VI

Infracciones y sanciones

CAPITULO VII

Acción de Protección de Datos Personales

CAPITULO VIII

Disposiciones Transitorias

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

CAPITULO IX Disposiciones Finales

CAPITULO I Disposiciones Generales

Arto. 1.- Objeto. La presente ley tiene por objeto la protección de los datos personales almacenados en archivos, registros, bases o bancos de datos, sean automatizados o no, públicos o privados.

Arto. 2.- Ámbito de aplicación. Las disposiciones de la presente ley serán aplicables en lo correspondiente a los datos relativos a personas naturales y Jurídicas.

Arto. 3.- Definiciones. Para la presente ley se entiende por:

- a. **Archivo, registro, base o banco de datos:** Indistintamente, designan al conjunto organizado de datos personales, tratados automatizadamente o no;
- b. **cesión:** Cesión, revelación de los datos a una persona distinta de su titular;
- c. **datos personales:** Información determinada de persona natural o Jurídica; siempre que sea identificable;
- d. **datos personales informáticos:** Los datos personales tratados a través de medios electrónicos o automatizados;
- e. **datos sensibles:** Aquellos que revelan el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros;
- f. **disociación de datos:** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada;
- g. **responsable de archivo, registro, base o banco de datos:** Persona Natural o Jurídica, pública o privada, que decide sobre la finalidad y contenido del tratamiento de los datos;
- h. **tercero:** Todo persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o banco de datos propios o a través de conexión con los mismos;
- i. **titular de datos:** Toda persona natural, viva o fallecida, y Jurídica a la que conciernen los datos personales;
- j. **tratamiento de datos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, consultas, interconexiones o transferencias.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

Arto. 4.- Creación de archivos. La creación de archivos, registros, bases o banco de datos será lícito cuando se encuentren debidamente registrados, mediante consentimiento del titular, salvo excepciones de ley, observando en su operación los principios que establecen la presente ley y su reglamento.

Los archivos, registros, bases o banco de datos no pueden tener fines contrarios a lo establecido en las leyes de la materia.

Arto. 5.- Requisitos para la obtención de datos. Para obtener los datos, se requiere lo siguiente:

- a. Que sean adecuados, proporcionales y necesarios en relación al ámbito y fin para el que se colecta;
- b. que se haga por medios lícitos que garanticen el principio constitucional de cada persona;
- c. los datos solo pueden ser utilizados para los fines que motivaron su obtención; y no podrán ser utilizados para otros fines;
- d. los datos inexactos, incompletos, o que estén en desacuerdo con la realidad de los que le corresponden a la persona, deben ser suprimidos, cancelados, sustituidos, completados, actualizados según corresponda;
- e. los datos deben ser almacenados de modo que permitan el derecho de acceso del titular de los mismos;
- f. los datos deben ser cancelados cuando hayan dejado de ser necesarios a los fines para los cuales hubiesen sido recolectados.

Arto. 6.- Consentimiento. El Consentimiento:

- a.- Es lícito obtener y tratar los datos personales cuando el titular hubiere otorgado su consentimiento de manera inequívoca, o por otro medio que permita se le equipare, de acuerdo a las circunstancias; salvo que la ley disponga lo contrario.

El referido consentimiento prestado con otras declaraciones, deberá constar en forma expresa, previa notificación al interesado, de la información descrita en el artículo 7° de la presente ley.

b.- No se requiere el consentimiento cuando:

1. Los datos se obtengan de fuentes de acceso público irrestricto;
2. se trate de listados cuyos datos se limiten a nombre, Cedula de identidad, profesión u oficio, fecha de nacimiento y domicilio;
3. deriven de una relación comercial, laboral, contractual, científica o profesional del titular de los datos, y resulten necesarios para su cumplimiento;
4. se trate de las operaciones que realicen las entidades Bancarias y de las informaciones que reciban de sus clientes conforme las disposiciones de la ley de la materia.

CAPITULO II

De los titulares y responsables de los Registros

Arto. 7.- Obligación de informar al obtener los datos personales. Cuando se obtengan datos personales el responsable de los archivos, registros, bases o banco de datos, deberá informar previamente a sus titulares en forma expresa y clara de lo siguiente:

- a. La finalidad para la que serán utilizados y quiénes pueden ser sus destinatarios o clase de destinatarios;
- b. la existencia del archivo, registro, base o banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
- c. el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
- d. las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
- e. la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

Arto. 8.- Categoría de los datos. Los datos tendrán la categoría siguiente:

- a. Datos Sensibles: sólo pueden ser obtenidos y tratados sean por razones de interés general en la ley, o con el consentimiento del titular de datos, u ordenadas por mandato judicial. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares; y
- b. queda prohibida la formación de archivos, bancos o registros que almacenen información de datos sensibles, salvo lo dispuesto en la ley.

Sin perjuicio de ello, las diferentes Sociedades Mercantiles, Asociaciones Civiles, religiosas y fundaciones sin fines de lucro, puede llevar lista de sus miembros.

- c. los datos personales relativos a antecedentes penales o faltas administrativas sólo pueden ser tratados por las autoridades públicas competentes, en la esfera de sus competencias.

Arto. 9.- Datos relativos a la salud. Los Hospitales, Clínicas, Centros y Puestos de salud, Públicos o Privados, y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquellos, respetando el secreto profesional.

Arto. 10.- Medidas de seguridad. Las medidas de seguridad serán las siguientes:

- a. El responsable o usuario del archivo, registro, bases o banco de datos debe adoptar las medidas técnicas y organizativas que resulten

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado;

- b. queda prohibido registrar datos personales en archivos, registros, bases o bancos que no reúnan condiciones técnicas de integridad o seguridad;
- c. el reglamento establecerá los requisitos y condiciones mínimas de seguridad y de organización, la naturaleza de los datos almacenados y los riesgos a que estén expuestos.

Arto. 11.- Confidencialidad en el tratamiento de los datos. Se requiere de confidencialidad en lo siguiente:

- a. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos;
- b. el obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Arto. 12.- Cesión de Derechos. Los datos personales se podrán ceder cuando:

- a. Los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario;
- b. el consentimiento para la cesión es revocable, mediante notificación por escrito al responsable del archivo, registro, bases o banco de datos;
- c. el consentimiento no es exigido cuando:
 - 1. Así lo disponga una ley;
 - 2. se realice entre instituciones del Estado en el ejercicio de sus atribuciones;
 - 3. se trate de razones de salud Pública, de interés social, o de seguridad nacional;
 - 4. se hubiera aplicado un procedimiento de disociación de datos, de modo que no se pueda atribuir a persona determinada.
- d. el cesionario quedará sujeto a las mismas obligaciones de la ley y reglamento del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

Arto. 13.- Prohibiciones. Prohibición de transferencia y excepciones:

- a. Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales, que no proporcionen niveles de seguridad y protección adecuados;
- b. la prohibición no regirá en los siguientes supuestos:
 - 1.- Colaboración judicial internacional;
 - 2.- intercambio de datos en materia de salud, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica;
 - 3.- transferencias bancarias o bursátiles, conforme la legislación de la materia;
 - 4.- cuando la transferencia se hubiera acordado en el marco de tratados internacionales vigentes en los cuales la República de Nicaragua sea parte vinculante;
 - 5.- cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Capítulo III Derechos de los Titulares de datos

Arto. 14.- Derecho a solicitar información. Toda persona puede solicitar información al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

El registro que se lleve al efecto será de consulta pública y gratuita.

Arto. 15.- Derechos del Titular de los datos. El titular de los datos tiene derecho a lo siguiente:

- a. A solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes;
- b. los informes que se otorguen conforme al inciso anterior, pueden consistir en la simple observación o la comunicación por cualquier medio fiable que garantice la comunicación íntegra, y la constancia de su envío y recepción.

El informe se debe proporcionar dentro de los diez días hábiles posteriores a la recepción de la solicitud; vencido el plazo sin que se haya rendido el informe, el interesado puede promover la acción de protección de datos personales prevista en esta ley.

- c. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a cuatro meses, salvo que se acredite un interés legítimo al efecto, y puede ejercerlo antes y cuantas veces sea necesario;

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

- d. el ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales, previa acreditación.
- e. A no ser obligada a proporcionar datos personales de carácter sensibles;

Arto. 16.- Requisitos de la información. La información debe llenar los requisitos siguientes:

- a. Ser clara y sencilla, accesible al conocimiento de la población y titular de los datos;
- b. ser amplia y perteneciente al titular, aun cuando lo solicitado sólo comprenda un aspecto de los datos personales. No se podrá revelar datos relacionados a terceros, aun cuando se vinculen con aquel;
- c. podrá suministrarse por escrito, medios electrónicos, telefónicos, de imagen, u por cualquier otro que determine el interesado, a opción del titular, y de acuerdo a la capacidad técnica del responsable de archivo, base de datos.

Arto. 17.- Derechos de modificación de los datos. Toda persona tiene los derechos siguientes en relación con sus datos:

- a. A solicitar y que le sean rectificadas, actualizadas y, cuando corresponda, suprimidos o sometidos a privacidad los datos personales de los que sea titular, que estén incluidos en un archivos, registros, bases o banco de datos;
- b. a que el responsable del archivo, registro, base o banco de datos, proceda a la rectificación, supresión, complementación, inclusión, actualización o cancelación de los datos personales del afectado, dentro de los cinco días hábiles de recibido la solicitud del titular de los datos, informándole por escrito de manera completa, clara y sencilla el tratamiento realizado;
- c. a que si el titular del archivo, registro, base o banco de datos no cumple con la obligación que le impone el inciso anterior, el titular de datos puede ejercitar la acción de protección de datos prevista en esta ley;
- d. en el caso que la información se haya cedido o transferido, el responsable del archivo, registro, base o banco de datos debe comunicar la inclusión, complementación, rectificación, actualización o cancelación de los datos al cesionario, dentro de los cinco días hábiles siguientes al en que se haya resuelto el tratamiento correspondiente;
- e. la cancelación de los datos no procede por razones de interés social, de seguridad nacional, de salud pública o por afectarse derechos de terceros, en los términos que lo disponga la ley.
- f. durante el procedimiento que se siga de verificación y rectificación del error o falsedad de los datos personales que conciernen al titular, el responsable del archivo, registro, base o banco de datos debe bloquear los

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

datos materia de la solicitud o consignar al proveer la información relativa que se tramita un procedimiento con determinado objeto;

- g. a que los datos personales deban ser conservados durante tiempo que determine la ley o las disposiciones contractuales entre las partes involucradas.

Arto. 18.- Excepcionalidad para la modificación de los datos.

- a. Los responsables de archivos, registros, bases o bancos de datos, pueden negar la inclusión, complementación, actualización, rectificación, reserva o cancelación de datos personales solicitada, por resolución debidamente fundada y motivada en ley, la cual debe ser notificada al interesado;
- b. se deberá brindar acceso al titular de los datos personales que les conciernen en los archivos, registros, bases o banco de datos, en el momento en que el afectado tenga que ejercer su derecho de defensa.

Arto. 19.- Gratuidad de modificación de los datos. La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en archivos, registros, bases o bancos de datos se llevará a cabo de manera gratuita para el titular.

Capítulo IV

Usuarios y responsables de archivos, registros, bases o bancos de datos

Arto. 20.- Obligatoriedad de inscripción en el Registro.

- a. Todo archivo, registro, base o banco de datos destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite la Dirección de control, la que se establecerá su procedimiento en el reglamento de la presente ley;
- b. el registro de archivos, registro, bases o banco de datos debe recabar del titular del archivo, registro, base o banco de datos la siguiente información:
 - 1.- Nombre y domicilio del responsable, ya sea persona natural o Jurídica con toda la descripción de la razón social, fecha de constitución, objeto y representante legal;
 - 2.- características y finalidad del archivo;
 - 3.- naturaleza de los datos personales contenidos en cada archivo, registro, bases o banco de datos;
 - 4.- forma, tiempo y lugar de recolección y actualización de datos;
 - 5.- destino de los datos y personas naturales o jurídicas a las que pueden ser transmitidos;
 - 6.- modo de interrelacionar la información registrada;
 - 7.- medios utilizados para garantizar la seguridad de los datos, debiendo detallar nombre y domicilio de las personas que intervienen en la colecta y tratamiento de los datos;

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

8.- tiempo de conservación de los datos;

9.- forma y procedimientos en que las personas pueden acceder a los datos referidos a ellas para realizar la rectificación o actualización de los datos.

d. Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el archivo, registro, base o banco de datos;

e. cualquier modificación a la información contenida en el registro debe ser comunicada por el responsable dentro de los cinco días hábiles siguientes al en que haya tenido lugar.

El incumplimiento de estos requisitos dará lugar a las sanciones previstas en la presente ley.

Arto. 21.- Archivos, registros, bases o bancos de datos de carácter publico. Los archivos, registros, bases o bancos de datos de carácter público sólo se pueden:

a. Crear, modificar o extinguir por medio de disposiciones de carácter general de conformidad con las normas jurídicas aplicables, que se deberán publicar en el *Diario Oficial La Gaceta*.

b. Las disposiciones del inciso anterior, deben indicar:

1. Características y finalidad del archivo;

2. personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

3. procedimiento de obtención y actualización de los datos;

4. estructura básica, característica y finalidad del archivo, registro, base o banco de datos,

5. las cesiones, transferencias o interconexiones previstas;

6. órganos responsables del archivo, registro, base o banco de datos, precisando dependencia jerárquica en su caso;

7. las oficinas ante las que el titular pueda efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

c. En las disposiciones que se dicten para la supresión de los archivos, registros, bases o banco de datos se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

Arto. 22.- Excepcionalidad en el uso de los datos personales.

a. Los archivos, registros, bancos o bases da datos personales que por ser colectados y tratados para fines administrativos, deben permanecer indefinidamente, estarán sujetos al régimen general de esta ley;

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

- b. la colecta y tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de los órganos de las fuerzas armadas, policiales o inteligencia militar, sin consentimiento de los afectados, queda limitado a lo necesario para el estricto cumplimiento de las misiones legalmente asignadas a aquellos para la defensa nacional, seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad;
- c. los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Arto. 23.- Archivos, registros, bases o banco de datos de carácter privado. Los particulares que formen archivos, registros o bancos de datos que no sean para uso exclusivamente personal deberán registrarse conforme lo previsto en el arto 21 de esta Ley.

Arto. 24.- Proveedores de servicios de datos personales.

- a. Los terceros que provean servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación;
- b. una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

Arto. 25.- Proveedores de servicios de información.

- a. Quienes se dediquen a proveer servicios de información sobre la solvencia fiscal, solvencia municipal y de crédito sólo podrán tratar automatizadamente datos de carácter personal obtenidos de fuentes accesibles al público, facilitados por el interesado o con su consentimiento previo;
- b. pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés;
- c. a solicitud del titular de los datos, el responsable del archivo, registro, base o banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos tres meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión;
- d. sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho;

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

- e. la prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

Arto. 26.- Datos relativos a la Publicidad.

- a. Los archivos, registros, bases o bancos de datos destinados al reparto de documentos, publicidad, venta directa u otras actividades análogas sólo pueden incorporar datos personales con el consentimiento de la persona a la cual concierne, cuando ésta los ha facilitado, o cuando los datos obren en fuentes accesibles al público;
- b. el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno;
- c. el titular podrá con una simple solicitud en cualquier momento solicitar el retiro o bloqueo de su nombre de los archivos, registros, bases o bancos de datos a los que se refiere el presente artículo.

Arto. 27.- Datos relativos a las encuestas. Las normas de la presente ley no se aplicarán a los siguientes casos:

- a. las encuestas de opinión;
- b. investigaciones científicas o médicas, y
- c. actividades análogas.

Lo anterior es aplicable cuando hayan sido con el consentimiento del titular o persona determinada, y destinarse exclusivamente al cumplimiento de la finalidad para la que fueron recabados y sólo se pueden ceder con el consentimiento previo del interesado.

Capítulo V De la Dirección de Protección de Datos Personales

Arto. 28.- Creación de la Dirección de Protección de Datos Personales. Crease la Dirección de Protección de Datos Personales, como un organismo desconcentrado autónomo administrativamente y funcional, que contara con un Director y subdirector designado por el Presidente de la Republica y una estructura administrativa que el Reglamento de la presente ley establecerá, y tiene por objeto el control, supervisión y protección de los archivos, registros, bases o bancos de datos personales, y sus responsables.

Arto. 29.- Funciones. Corresponde a esta Dirección las siguientes funciones:

- a. Asesorar a las personas naturales o Jurídicas que lo requieran acerca del contenido y alcance de la presente ley;
- b. dictar las normas y disposiciones administrativas necesarias para la realización de su objeto en el ámbito de su competencia;

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

- c. llevar un registro actualizado y completo de los archivos, registros, bases o bancos de datos personales;
- d. vigilar que las normas sobre integridad y seguridad de los datos personales se respeten y apliquen por los titulares de los archivos, registros, bases o bancos de datos correspondientes;
- e. con ese objeto, podrá solicitar a la autoridad judicial competente autorización para inspeccionar los inmuebles, equipos, herramientas y programas de captura y tratamiento de datos;
- f. solicitar la información que requiera para el cumplimiento de su objeto a las entidades públicas y privadas titulares de los archivos, registros, bases o bancos de datos personales, garantizando en todo caso la seguridad, la integridad y confidencialidad de la información;
- g. imponer las sanciones administrativas que correspondan a los infractores de esta ley;
- h. formular y presentar las denuncias por violaciones a lo dispuesto en esta ley; y,
- i. constatar de que los archivos, registros, bases o bancos de datos personales destinados a suministrar informes cuenten con los requisitos necesarios para que proceda su inscripción en el registro de archivos, registros, bases o bancos de datos.

Capítulo VI Infracciones y Sanciones

Arto. 30.- Infracciones leves. Son infracciones leves a esta ley, las siguientes:

- a. Omitir la inclusión, complementación, rectificación, actualización, suspensión o cancelación, de oficio o a petición del interesado, de los datos personales que obren en archivos, registros, bases o bancos de datos;
- b. incumplir las instrucciones dictadas por la Dirección de Protección de Datos Personales; y,
- c. cualquiera otra que no pueda ser catalogada como grave.

Arto. 31.- Infracciones graves. Son infracciones graves a esta ley, las siguientes:

- a. Colectar o tratar datos de carácter personal para constituir, o implementar archivos, registros, bases o bancos de datos de titularidad pública, sin la previa autorización de la normativa aplicable;
- b. colectar o tratar automatizadamente datos de carácter personal para constituir, o implementar archivos, registros, bases o bancos de datos de titularidad privada, sin el consentimiento del interesado o de quien legítimamente puede otorgarlo;

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

- c. coleccionar, tratar automatizadamente o administrar datos de carácter personal con violación de los principios que rigen esta ley o de las disposiciones que sobre protección y seguridad de datos sean vigentes;
- d. impedir u obstaculizar el ejercicio del derecho de acceso, así como negar injustificadamente la información solicitada;
- e. violentar el secreto profesional que debe guardar por disposición de esta ley;
- f. mantener archivos, registros, bases o bancos de datos, inmuebles, equipos o herramientas sin las condiciones mínimas de seguridad requeridas por las disposiciones aplicables; y,
- g. obstruir las inspecciones que realice la Dirección de Protección de Datos Personales.

Arto. 32.- Sanciones administrativas. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones administrativas de:

- a. Apercibimiento;
- b. Suspensión de operaciones;
- c. Multa desde UN MIL CORDOBAS (C\$1,000.00) hasta QUINIENTOS MIL CORDOBAS (C\$500,000.00) al momento de comisión de la infracción; y,
- d. Clausura o cancelación del archivo, registro o banco de datos de manera temporal o definitiva.

En el caso de infracciones leves a esta ley, se aplicarán al infractor, dependiendo de las circunstancias del caso, del daño causado y de las condiciones del propio infractor, la sanción que corresponda conforme a los incisos a, b, y c de este artículo.

En el caso de infracciones graves, se impondrán al infractor dependiendo de las circunstancias del caso, del daño causado y de las condiciones del propio infractor, la sanción que corresponda conforme a los incisos c y d de este artículo.

El reglamento establecerá el procedimiento para la aplicación de las sanciones previstas.

Capítulo VII

Acción de protección de los datos personales

Arto. 33.- La acción de protección de los datos personales. La acción de protección de los datos personales o de hábeas data procederá en los siguientes casos:

- a. para conocer de los datos personales almacenados en archivos, registros, bases o bancos de datos destinados a proporcionar informes, y de la finalidad de aquellos;
- b. en los casos en que se presuma la falsedad, inexactitud, desactualización, omisión, total o parcial, o ilicitud de la información de que se trata, para exigir su rectificación, actualización, inclusión, complementación, reserva, suspensión o cancelación.

Arto. 34.- Legitimación Activa. La acción de protección de los datos personales podrá ser ejercida por las siguientes personas:

- a. el afectado,
- b. sus tutores y los sucesores de las personas naturales,
- c. por sí o por intermedio de apoderado.

Cuando la acción sea ejercida por personas Jurídicas, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.

Arto. 35.- Legitimación Pasiva. La acción procederá respecto de los responsables y usuarios de archivos, registros, bases o bancos de datos públicos, y de los privados destinados a proveer informes.

Arto. 36.- Competencia Judicial. Es competente para conocer de esta acción el juez de distrito del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Arto. 37.- Contenido de la demanda. La demanda debe expresar lo siguiente:

- a. El Juzgado ante el cual se promueve;
- b. el nombre del actor y del demandado;
- c. el objeto de la acción;
- d. con la mayor precisión que sea posible, el nombre y domicilio del archivo, registro, banco o base de datos y, en su caso, el nombre y responsable del usuario del mismo;
- e. en el caso de archivos, registros, bases o banco de datos públicos, se procurará establecer la institución estatal del cual dependen;
- f. los hechos en que el actor funde su petición, narrando sucintamente, con claridad y precisión, los motivos en los que apoya su acción, y por los cuales considera que los registros, archivos, bancos o bases de datos son omisos, incompletos, incorrectos, falsos, inexactos, o por los cuales

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

considera que los datos deben reservarse, suspenderse, o cancelarse y destruirse;

- g. el titular o quien promueva en su nombre y representación pueden solicitar que se asiente mientras dure el proceso que la información cuestionada se encuentra sujeta a proceso judicial;
- h. el juez puede disponer de oficio, por causa fundada y motivada, la suspensión o reserva de los datos personales;
- i. el fundamento de derecho; y,
- j. lo que se pida, designándolo con toda exactitud, en términos claros y precisos.

Arto. 38.-

- a. Con la demanda, el actor debe presentar los documentos en que funde su acción, o señalar el archivo o lugar en donde se encuentren si no los tiene a su disposición;
- b. con la sola declaración que haga el actor, el juez mandará expedir a costa de aquél copia de los documentos correspondientes.

Arto. 39.-

- a. De la demanda admitida, se correrá traslado a la persona contra la que se proponga, emplazándola para que la conteste dentro de los tres días siguientes;
- b. las cuestiones de jurisdicción, competencia y personalidad, deberán promoverse en la contestación de demanda y se resolverán de plano en el auto en el que se provea sobre ella.
- c. en los procedimientos seguidos por el ejercicio de una acción de protección de datos personales no procede la contra demanda, ni la ampliación de la contestación.

Arto. 40.- El juez puede, en todo momento, y hasta antes de dictar sentencia, recabar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa.

Arto. 41.- Apertura a pruebas. Contestada o no la demanda, inmediatamente el juez de oficio abrirá el proceso a prueba por un término único de seis días comunes a las partes.

Arto. 42.- Sentencia.

- a. Vencido el plazo de prueba, de oficio el juez dictará sentencia dentro de los tres días siguientes.
- b. Si la acción se resuelve fundada, el juez determinará los datos que deben ser incluidos, complementados, actualizados, rectificados, reservados, suspendidos o cancelados y destruidos, estableciendo un plazo no superior

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

de quince días para su cumplimiento y acreditación y, en su caso, la forma de hacerlo.

- c. La improcedencia de la acción no presume responsabilidad alguna en la que pudiera incurrir el demandante.
- d. La sentencia, cualquiera que sea el sentido en que se pronuncie, se comunicará inmediatamente a la Dirección de Protección de Datos Personales, con el objeto de que lleve un registro al efecto.

Arto. 43.-

- a. Los responsables de los archivos, registros, bancos o bases de datos no puedan alegar confidencialidad de la información que se les requiera, salvo en el caso de que se afecten fuentes de información periodística o así corresponda conforme a esta ley;
- b. cuando la confidencialidad se alegue en los casos de excepción previstos en la ley, el juez puede tomar conocimiento personal y directo de los datos, asegurando el mantenimiento de su confidencialidad.

Arto. 44.- Tramitación de la acción de protección de datos. La acción de protección de datos o habeas data se tramitará según las disposiciones de la presente ley y su reglamento, y supletoriamente por las normas del Código de Procedimientos Civiles.

CAPITULO VIII Disposiciones Transitorias

Arto. 45.- Obligación de inscripción en el registro Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca el reglamento.

Arto. 46.- Obligación de los bancos de datos proveedores de servicios. Los bancos de datos proveedores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

CAPITULO IX Disposiciones Finales

Arto. 47.- La presente ley será reglamentada de conformidad a lo previsto en el numeral 10 del artículo 150 de la Constitución Política de Nicaragua, después de su entrada en vigencia.

Arto. 48.- La presente ley deroga cualquier otra ley o decreto que se le oponga a sus disposiciones.

Arto. 49.- Esta ley entrará en vigencia a partir de su Publicación en La Gaceta, Diario Oficial. Dado en la ciudad de Managua, en la Sala de Sesiones de la Asamblea Nacional, a los días --- del mes de --- del dos mil ---.-

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

---, Presidente de la Asamblea Nacional. ---, Secretario de la Asamblea Nacional.-

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

Proyecto de Código Penal de la República de Nicaragua Comisión de Justicia de la Asamblea Nacional

24 de noviembre de 1999

TITULO IV DELITOS CONTRA LA INTIMIDAD

Capítulo I Delitos vinculados a la información personal

Artículo 195. Descubrimiento de correspondencia.

1. Quien abra ilegalmente una carta, un pliego cerrado o un despacho telegráfico, telefónico o electrónico o de otra naturaleza que no le esté dirigido o el que, sin abrir la correspondencia, por medios técnicos se entere de su contenido, será penado con prisión de seis meses a un años y multa de doscientas a quinientas días.

2. Si la persona difundiere o revelare el contenido de la correspondencia, será sancionado con prisión de uno a dos años e inhabilitación especial de tres a cinco años si fuere autoridad, funcionario o empleado público.

Artículo 196. Sustracción de papeles y desvío o supresión de correspondencia.

Quien se apodere ilegalmente de una carta o de otro papel privado, aunque no esté cerrado, o el que suprima o desvíe de su destino una correspondencia que no le está dirigida, será penado con prisión de uno a dos años y con multa de cien a doscientos días.

Artículo 197. Captación indebida de manifestaciones verbales.

Quien grabe las palabras o conversaciones de otro no destinados al público, sin su consentimiento, o el que mediante procedimientos técnicos escuche manifestaciones privadas o telefónicas que no le estén dirigidas, será penado con prisión de un año a dos años y multa de cien a doscientos días.

Artículo 201. Registros prohibidos.

Quien cree un banco de datos o un registro informático con datos que puedan afectar la intimidad de las personas, será penada con prisión de dos a cuatro años y multa de trescientos a quinientos días.

Artículo 202. Uso de información.

Quien sin 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 multa de doscientos a quinientos días.

TÍTULO VII
DELITOS CONTRA EL PATRIMONIO Y CONTRA EL ORDEN SOCIOECONOMICO
Capítulo VIII
Daños

Artículo 244. Destrucción de registros informáticos.

1. Quien dolosamente destruya, borre o de cualquier modo inutilice registros informáticos, será penado con prisión de dos a tres años, y multa de trescientos a quinientos días.

2. La pena se elevará de tres a cinco años, cuando se trate de información necesaria para la prestación de un servicio público o se trate de un registro oficial.

Artículo 245. Programas destructivos.

Quien distribuya o ponga en circulación programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación, será penado con prisión de dos a cuatro años, y multa de trescientos a quinientos días.

Artículo 246. Alteración de programas.

La misma pena del artículo anterior se aplicará al que altere, borre o de cualquier modo inutilice las instrucciones o programas que utilizan las computadoras.

Artículo 247. Manipulación de información.

Quien utilice registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica, será penado con prisión de uno a cinco años y multa de quinientos a mil días.

Capítulo IX

Delitos contra la propiedad intelectual

Artículo 248. Reproducción ilícita.

1. Quien con ánimo de lucro y en perjuicio de terceros reproduzca, distribuya, plagie o comunique públicamente, total o parcialmente, una obra artística, literaria o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte material o comunicada a través de cualquier medio; sin la correspondiente autorización de los titulares de los derechos de propiedad intelectual o sucesionarios, será penado con prisión de seis meses a dos años y multa de cien a quinientos días.

2. La misma pena se aplicará a quien importe, exporte o almacene ejemplares de las obras, producciones o interpretaciones artísticas sin la autorización antes referida, lo mismo el que fabrique, ponga en circulación, o de otro modo detente cualquier medio específicamente destinado para facilitar la supresión

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

no autorizada, o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de computación.

Artículo 249. Protección del programa de computación.

1. Quien sin autorización del autor, copie o de cualquier modo reproduzca las instrucciones o programas de computación, será penado con prisión de uno a tres años y multa de doscientos a quinientos días.

2. Se aumentará la pena de dos a cuatro años de prisión si comercialice o distribuya la copia fraudulenta.

Capítulo XI Disposiciones Generales

Artículo 251. Exención de pena.

1. Están exentos de pena, sin perjuicio de la responsabilidad civil, por los delitos de hurto, estafa, estelionato, apropiación indebida, apropiación irregular, administración fraudulenta, daño, destrucción de registros informáticos, alteración de programas y uso de información que recíprocamente se causen:

- a) los cónyuges no separados y quienes convivan en unión de hecho estable;
- b) los ascendientes, descendientes, adoptantes y adoptados y afines en línea recta;
- c) los hermanos, si viven juntos con el autor.

2. La exención de pena no es aplicable a los extraños que participen en el delito.

Capítulo XVI Delitos vinculados al mercado

Artículo 267. Revelación de secretos de empresa.

1. Quien, para descubrir un secreto de empresa, se apodere por cualquier medio de datos, documentos escritos o electrónicos, registros informáticos u otros objetos que se refieran al secreto, será castigado con pena de dos a tres años y multa de doscientos a quinientos días.

LEGISLACION NICARAGUENSE ANTE LOS DELITOS INFORMATICOS

2. La pena se incrementará en un tercio del límite máximo si se difunde, revelan o ceden a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que puedan corresponder por el apoderamiento o destrucción de los registros informáticos.

TÍTULO XVI DELITOS CONTRA LA SEGURIDAD DEL ESTADO

Capítulo II Delitos que comprometen la Paz

Artículo 353. Intrusión.

Quien, para comprometer o poner en peligro la paz, levante plano, o tome, trace o reproduzca imágenes de fortificaciones, naves, establecimientos, vías u obras militares o se introduzca con tal fin, clandestina o engañosamente en dichos lugares, cuando su acceso estuviere prohibido al público, o se introduzca en los programas informáticos relativos a la defensa del Estado de Nicaragua, será penado con prisión de seis meses a dos años e inhabilitación especial por el mismo período de tiempo.