

BANCO INTERAMERICANO DE DESARROLLO
BANCO INTERAMERICANO DE DESENVOLVIMENTO



INTER-AMERICAN DEVELOPMENT BANK
BANQUE INTERAMERICAINE DE DEVELOPPMENT



CORTE SUPREMA DE JUSTICIA NICARAGUA

Delitos Informáticos

UN ENSAYO DE DERECHO COMPARADO

Legislación y el Manejo de Información en la era del conocimiento

Preparado por Ana Patricia Escorcía - patyescorcía@yahoo.com
GLIN-Nicaragua - Corte Suprema de Justicia

Con la colaboración de:
Guillermo S. Castillo G. guillermos@iadb.org
División de Tecnología de la información para el Desarrollo,
Departamento de Desarrollo Sostenible. Banco Interamericano de Desarrollo.

Managua, Nicaragua, Washington, DC.
Noviembre, 2005

Este documento tiene como objetivo principal proveer información básica que permita una mejor discusión y un marco conceptual para aplicar las propuestas necesarias relacionadas con el tema de delitos informáticos a la realidad nacional sin perder la perspectiva globalizada.

Las interpretaciones, alternativas y conclusiones expresadas en éste documento son enteramente responsabilidad de la autora y no deben ser atribuidas a la Corte Suprema de Nicaragua, al Banco Interamericano de Desarrollo, sus organizaciones afiliadas, miembros de su Directorio Ejecutivo o países que representan.

INDICE

GLOSARIO DE TERMINOS	3
AUTORES DE LOS DELITOS INFORMATICOS	5
EL DELITO INFORMÁTICO	7
LEGISLACION EXISTENTE	10
Alemania	10
Austria	10
Gran Bretaña	10
Holanda	10
Francia	10
Francia	11
Italia	11
España	11
Estados Unidos	15
Perú	15
Costa Rica	16
Argentina	16
Argentina	17
Chile	19
México	19
Venezuela	20
Venezuela	21
CONCLUSION	28

GLOSARIO DE TERMINOS

1

Computador	Dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.
Contraseña (password)	Secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.
Data	Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.
Documento	Registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.
Firmware	Programa o segmento de programa incorporado de manera permanente en algún componente de hardware.
Hardware	Equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.
Información	Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.
Mensaje de datos	Cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), reparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.
Procesamiento de data o de información	Realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.
Programa	Plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.
Sistema	Cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.
Seguridad	Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

¹ Tomados de las disposiciones generales del proyecto de ley de delitos informáticos de Venezuela

Software	Información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.
Tarjeta inteligente	Rótulo, cédula o carné que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.
Tecnología de Información	Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software".
Mensaje de datos	Cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), reparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.
Mensaje de datos	Cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), reparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.
Virus	Programa o segmento de programa indeseado que se desarrolla incontroladamente que genera efectos destructivos o perturbadores en un programa o componente del sistema.

AUTORES DE LOS DELITOS INFORMATICOS

Las personas que cometen los «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.

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 delitos cometidos. De esta forma, la persona que «ingresa» 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 informático es tema de controversia ya que para algunos 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.

Sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlos. Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando. Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

Los autores de estos delitos son llamados:

Hackers: Son programadores y suelen ser jóvenes deseosos de conocer el funcionamiento de los diferentes sistemas. El Hacker aprovecha los agujeros, los fallos de los sistemas de seguridad. Sus intereses se centran en el conocimiento del funcionamiento de los sistemas. Rigen su actividad por un código ético (netiquettes).

Crackers o Piratas: Es el que se cuela en un sistema informático y roba información o produce destrozos en el mismo. El término "Pirata" se utiliza, sin embargo, de forma muy vaga y para designar todo tipo de actuación ilícita. Se tiende a diferenciar del Hacker en la intención.

Phreaker: El que emplea sus conocimientos para poder utilizar las telecomunicaciones gratuitamente. Acceden a la red utilizando "vías" gratuitas de las que disfrutaban ilícitamente o de forma no autorizada.

A continuación dos ejemplos de autores de la jurisprudencia Alemana:

1. - Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga -cómplice en la maniobra- mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática.

2. - El autor, empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor. Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por

este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los «empleados ficticios» y los pagos realizados, no aparecieran en los listados de control.

Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de «manipulación del programa», la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active.

En el ejemplo jurisprudencial citado al hacer referencia a las manipulaciones en el programa, el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal. Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Otros Autores:

Zinn, Herbert, Shadowhack. (expulsado de la educación media superior), y que operaba bajo el seudónimo de «Shadowhawk», fue el primer sentenciado bajo el cargo de Fraude Computacional y Abuso en 1986. Zinn tenía 16 y 17 cuando violó el acceso a AT&T y los sistemas del Departamento de Defensa. Fue sentenciado el 23 de enero de 1989, por la destrucción del equivalente a US \$174,000 en archivos, copias de programas, los cuales estaban valuados en millones de dólares, además publicó contraseñas e instrucciones de cómo violar la seguridad de los sistemas computacionales. Zinn fue sentenciado a 9 meses de cárcel y a una fianza de US\$10,000. Se estima que Zinn hubiera podido alcanzar una sentencia de 13 años de prisión y una fianza de US\$800,000 si hubiera tenido 18 años en el momento del crimen.

Smith, David. Programador de 30 años, detenido por el FBI y acusado de crear y distribuir el virus que ha bloqueado miles de cuentas de correo, «Melissa». Entre los cargos presentados contra él, figuran el de «bloquear las comunicaciones públicas» y de «dañar los sistemas informáticos». Melissa en su «corta vida» había conseguido contaminar a más de 100,000 ordenadores de todo el mundo, incluyendo a empresas como Microsoft, Intel, Compaq, administraciones públicas estadounidenses como la del Gobierno del Estado de Dakota del Norte y el Departamento del Tesoro.

Poulsen Kevin, Dark Dante. Diciembre de 1992 Kevin Poulsen, un pirata infame que alguna vez utilizó el alias de «Dark Dante» en las redes de computadoras es acusado de robar órdenes de tarea relacionadas con un ejercicio de la fuerza aérea militar americana. Se acusa a Poulsen del robo de información nacional bajo una sección del estatuto de espionaje federal y encara hasta 10 años en la cárcel.

Murphy Ian, Captain Zap. de 23 años de edad, en julio de 1981 se autodenominaba «Captain Zap», entra a los sistemas en la Casa Blanca, el Pentágono, BellSouth Corp. TRW y deliberadamente deja su currículum.

Morris Robert. En noviembre de 1988, Morris lanzó un programa «gusano» diseñado por el mismo para navegar en Internet, buscando debilidades en sistemas de seguridad, y que pudiera correrse y multiplicarse por sí solo. La expansión exponencial de este programa causó el consumo de los recursos de muchísimas computadoras y que más de 6000 sistemas resultaron dañados o fueron seriamente perjudicados. Eliminar al gusano de sus computadoras causó a las víctimas muchos días de productividad perdidos, y millones de dólares.

EL DELITO INFORMÁTICO

Cuando hablamos del delito informático es necesario hacer un recuento de donde se encuentra la legislación de América Latina al respecto. La estación GLIN-Nicaragua, Corte Suprema de Justicia (CSJ) presentó un trabajo conceptual del Delito Informático² el cual puede utilizarse como un marco conceptual y complementarse con estudios adicionales en el tema. El presente es un primer ensayo en ese sentido.

Antes debemos de conceptuar lo que es derecho informático y delitos informáticos y sus consecuencias, que, aunque son temas relativamente nuevos, como ya se conoce en nuestros ordenamientos jurídicos, académicos y sociales latinoamericanos, también ya se tiene un poco de conocimiento sobre ello, por ejemplo, en Nicaragua universidades nacionales han incorporado a sus pensums académicos el Derecho informático en las Carreras de Derecho.

Como lo explican Chavarría, Pereira y Dávila, 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 'en línea' y de tratamientos en tiempo real, comienzan a verse casos de uso fraudulento de los aparatos (computadores) o del software (programas) sobre datos comunes. De aquí la necesidad de los passwords e identificativos de usuarios para controlar y restringir el acceso a los datos existentes en las bases de datos y sistemas automatizados de información.

En la sociedad de la información, como se ha empezado a llamar a las sociedades modernas que utilizan la información para crear mucho mayor conocimiento, tal como sucedió en la década pasada y en la década actual, la automatización tecnológica, el uso de las computadoras, el acceso inmediato a la información ha incidido sin lugar a dudas en el comportamiento; ha modificado radicalmente las relaciones comerciales y profesionales; las relaciones públicas - privadas, y en síntesis, llevado a 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 las nuevas tecnologías.

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, en ese sentido, es pertinente aclarar un par de definiciones:

Derecho informático: es el área del derecho que se encarga de normar las relaciones y efectos que nacen o surgen de la informática; regula los efectos, consecuencias y resoluciones de orden jurídico que surgen de la aplicación de la informática; es el conjunto de leyes, norma y principios aplicables a los hechos y actos derivados de la informática. El derecho informático debido a su naturaleza tecnología, evoluciona al paso de las necesidades que son necesarias satisfacer y que surgen día con día, con el desarrollo tecnológico. El derecho informático vive en constante renovación de sus figuras jurídicas debido a que surgen nuevas situaciones o efectos que deben ser normados para el correcto funcionamiento de la sociedad actual.

Delitos informáticos: son acciones típicas, antijurídicas y culpables, en las cuales media un ordenador o computador como medio (para cometer la acción) o como fin (cuando este o sus elementos son receptores del daño ocasionado)

Los Delitos informáticos, dañan el derecho a la comunicación, a la propiedad, a la privacidad y a la seguridad patrimonial. Los bienes jurídicos afectados de manera general son:

1. Derecho a la privacidad o a la intimidad (inviolabilidad del domicilio, la inviolabilidad de la correspondencia y la inviolabilidad de secretos)
2. Derecho a la protección de la honra, dignidad y reputación

² Chavarría, Ana Rosa; Pereira, José Antonio; Dávila, Lenin Ernesto; Delitos Informáticos - Legislación y el Manejo de la Información en la era del conocimiento, Taller GLIN-MERCOSUR GLIN-Centroamérica, Antigua Guatemala, Noviembre-Diciembre 2005

3. Derecho a la Propiedad
4. Propiedad Intelectual
5. Patrimonio
6. Fe publica (falsificación de documentos públicos)
7. La seguridad del Estado y la Nación
8. La integridad física o psíquica de una persona

El Derecho comparado en si, especialmente entre países o sub-regiones mundiales es un arma útil para cualquier legislador, porque de este se puede aprender los pro y los contra en la creación y reglamentación de cualquier nueva ley, por esto siempre es importante su estudio en toda nueva investigación en el ámbito jurídico que se haga.

A nivel mundial los países se han preocupado por la protección de los derechos que pueden ser violados tras la comisión de un delito informático.

Desde hace aproximadamente diez años la mayoría de los países europeos han hecho todo lo posible para incluir dentro de la ley, la conducta punible penalmente, como el acceso ilegal a sistemas de computo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

El objetivo de las leyes y regulaciones en estos países es simple y sencillamente el de aumentar la protección a los individuos, negocios y agencias gubernamentales, protegiéndoles legal y jurídicamente de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente.

En el caso específico de Nicaragua, debido al desarrollo de la tecnología, modernismo, avances científicos, económicos, políticos y sociales, a los cuales desde luego Nicaragua por el momento esta predispuesta a gozar, es que el ordenamiento jurídico debe estar acondicionado para tales cambios y preparado para todos los imprevistos que los avances tecnológicos puedan ocasionar a la seguridad jurídica.

Es imperioso que los delitos informáticos sean reconocidos en nuestra legislación y que cualquier individuo nicaragüense o no, reconozca las situaciones de delito, ya sea para protegerse de ellos o para evitar cometerlos. Debido a como se dan las innovaciones de la tecnología, el repertorio de los delitos informáticos aumenta y, consecuentemente, los bienes jurídicos afectados.

Nicaragua no ha quedado atrás en el avance tecnológico-jurídico, los cuales van de la mano. En las nuevas reformas al código penal, los legisladores han propuesto una serie de artículos vinculados con la informática. Estos se encuentran dispersos a través de sus diferentes capítulos y títulos.

Las reformas que a la fecha de preparar este ensayo, aun no han sido aprobadas por la Asamblea Nacional Nicaragüense, incluyen los siguientes articulo en su propuesta:

Delitos vinculados a la informática personal, como el descubrimiento de correspondencia, registros prohibidos, uso de información inapropiadamente; en el articulo de la estafa agravada, el factor informático en la comisión del delito de estafa; En el capítulo de los daños, encontramos la destrucción de registros informáticos, implantación de programas destructivos, la alteración de programas, la manipulación de la información; en los delitos contra la propiedad intelectual, se sanciona la reproducción ilícita, etc. etc.

También incluye delitos vinculados al mercado, como la revelación de secretos de empresa y el abuso de información privilegiada, siempre influyendo algún elemento informático.

En Nicaragua, la Constitución Política el artículo 26 señala, toda Persona tiene derecho a:

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.

También, se cuenta con dos anteproyectos de leyes:

1. Anteproyecto de Ley especial sobre Delitos Informáticos y
2. Ley de Protección de Datos Personales.

En el ámbito internacional, los gobiernos se han dado cuenta de la necesidad de frenar la comisión de estos delitos, y han creado leyes que penalizan a cualquier individuo que afecte los bienes jurídicos protegidos por estas leyes. Los pioneros en el ordenamiento jurídico de esta materia han sido los países europeos, quienes igualmente y como región, han sido los primeros en desarrollar y contar con los avances tecnológicos de punta.

Hacemos notar que el Derecho comparado ha seguido los mismos lineamientos, pues frente a la evolución de los sistemas informáticos, las legislaciones penales debieron adaptarse a los nuevos bienes inmateriales.

Como política de legislación criminal, observaremos a continuación que muchos países han optado por incluir estos delitos en leyes especiales y no solo mediante la introducción de enmiendas al Código Penal, fundamentalmente para no romper el equilibrio de su sistemática y por tratarse de un bien jurídico novedoso que amerita una especial protección jurídico-penal.



LEGISLACION EXISTENTE

Alemania

Este país sancionó en 1986 la **Ley contra la Criminalidad Económica**, que contempla los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Alteración de datos.
- Sabotaje informático.

El art. 303 a del Código Penal Alemán establece que "1. Quien ilícitamente cancelare, ocultare, inutilizare o alterare datos de los previstos en el 202 a, par.2° será castigado con pena privativa de libertad de hasta dos años o con pena de multa".

Austria

La Ley de reforma del Código Penal, sancionada el 22 DIC 87, en el artículo 148, sanciona a aquellos que con "*dolo*" causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procedimiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión de especialistas en sistemas.

El art. 126 a del Código Penal de Austria dispone que "1. Quien perjudicare a otro a través de la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que carezca en todo o en parte, de disponibilidad, será castigado con pena privativa de libertad de hasta seis meses o con pena de multa de hasta 360 días-multa".

Gran Bretaña

Debido a un caso de "*hacking*" en 1991, comenzó a regir en este país la Ley de Abusos Informáticos. Mediante esta ley, el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que especifica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes a cinco años de cárcel, dependiendo del daño que causen.

Holanda

El 1° de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza el *hacking*, el "*preacking*" (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus. La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño.

Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero, si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

Francia

En enero de 1988, este país dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Cuando el ejemplo de los países anteriores se ha optado por la introducción de leyes que contemplan directamente el delito informático, Alemania específicamente también lo identifica claramente en el código penal, y los otros países han tomado reformas o ampliaciones al código penal

Francia

Con la ley N°88-19 del 5 de enero de 1988 Francia incluyó en su Código Penal varios delitos informáticos. Entre ellos, se destaca la destrucción de datos, que, con la reforma penal de 1992, quedó modificado de la siguiente manera: Se penaliza a quien al acceder a un ordenador de manera fraudulenta suprima o modifique los datos allí almacenados.

Italia

El artículo 392 del Código Penal italiano incluye la alteración, modificación o destrucción total o parcial de programas de computación y el daño a la operación de un sistema telemático o informático. El artículo 420 del Código Penal, referido a atentados contra sistemas de instalaciones públicas, ha sido también modificado. Actualmente cualquiera que realice un acto con la intención de dañar o destruir sistemas informáticos o telemáticos de instalaciones públicas o sus datos, información o programas puede ser castigado con prisión de uno a cuatro años. En casos de consumación del delito (destrucción o daño a los datos) la pena se eleva de tres a ocho años.

España

En España, a partir de la reforma del Código penal, el nuevo artículo 264.2 reprime a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos

Artículos del Código Penal Español referentes a Delitos Informáticos (Ley-Orgánica 10/1995, de 23 de Noviembre/ BOE número 281, de 24 de Noviembre de 1.995)

Artículo 197

1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198. La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Artículo 199

1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Artículo 200 . Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código.

Artículo 201

1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Artículo 211. La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Artículo 212. En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.

Artículo 238. Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1º.- Escalamiento.

2º.- Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.

3º.- Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.

4º.- Uso de llaves falsas.

5º.- Inutilización de sistemas específicos de alarma o guarda.

Artículo 239. Se considerarán llaves falsas:

1º.- Las ganzúas u otros instrumentos análogos.

2º.- Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.

3º.- Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.

Artículo 248

1.- Cometan estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

Artículo 255. Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1º.- Valiéndose de mecanismos instalados para realizar la defraudación.

2º.- Alterando maliciosamente las indicaciones o aparatos contadores.

3º.- Empleando cualesquiera otros medios clandestinos.

Artículo 256. El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Artículo 263. El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Artículo 264. 1.- Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

1º.- Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2º.- Que se cause por cualquier medio infección o contagio de ganado.

3º.- Que se empleen sustancias venenosas o corrosivas.

4º.- Que afecten a bienes de dominio o uso público o comunal.

5º.- Que arruinen al perjudicado o se le coloque en grave situación económica.

2.- La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Artículo 270. Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Artículo 278 .

1.- El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2.- Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

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

Artículo 400. La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536. La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

Estados Unidos

Este país adoptó en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribire la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030 (a) (5) (A)). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Perú

Artículo único.- Incorporase al Código Penal, promulgado por Decreto Legislativo N° 635, el Capítulo XI, Delitos Informáticos, los artículos 208a y 208b; con los siguientes textos:

Artículo 208 a.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de la libertad no mayor de dos años, o con prestación de servicios comunitario de cincuenta y dos a ciento cuatro jornadas.

Artículo 209 b.- El que indebidamente, interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de la libertad no mayor de dos años.
Lima, 18 de agosto de 1999.



Costa Rica

Ley 7557 del 20 de octubre de 1995, Ley General de Aduanas. Ámbito de aplicación; división territorial de aduanas; objetivos; Sistema Nacional de Aduanas; personal aduanal; control y funciones aduanales; procedimientos de investigación de delitos y violaciones aduaneras; auxiliares de la función pública de aduanas; agentes aduaneros; carga y transporte; deberes y obligaciones; entrada y salida de personas y mercaderías; procedimientos comunes a todo sistema aduanero; sistemas aduaneros; sistemas temporales; sistemas aduaneros en zonas francas; mejoramiento de los sistemas; procedimiento ordinario; creación del Tribunal Aduanero Nacional; delitos aduaneros; obligaciones aduaneras y violaciones administrativas; **delitos informáticos**; definiciones y normas transitorias. El artículo 225 contiene la legislación derogada. (268 artículos, p.p. 1-23)

DELITOS INFORMÁTICOS (COSTA RICA) COSTA RICA: LEY No. 8148

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

Decreta:

ADICIÓN DE LOS ARTÍCULOS 196 BIS, 217 BIS Y 229 BIS AL CÓDIGO PENAL LEY N° 4573, PARA REPRIMIR Y SANCIONAR LOS DELITOS INFORMÁTICOS

Artículo único.-Adiciónense al Código Penal, Ley N° 4573, del 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, cuyos textos dirán:

"Artículo 196 bis.-Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"Artículo 217 bis.-Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"Artículo 229 bis.-Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años."

Dado en la Presidencia de la República.-San José, a los veinticuatro días del mes de octubre del dos mil uno.



Argentina

En Argentina, aún no existe legislación específica sobre los llamados *delitos informáticos*. Sólo están protegidas las obras de bases de datos y de software, agregados a la lista de ítems contemplados por la Ley 11.723 de propiedad intelectual gracias al Decreto N° 165/94 del 8 de febrero de 1994.

Resolución 476 de la Secretaría de Comunicaciones de fecha 21 de noviembre de 2001. Somete a consulta pública, en el marco del Reglamento General de Audiencias Públicas y Documentos de Consulta para las Comunicaciones (Resolución 57/23-08-1996 ex Secretaría de Comunicaciones de la Presidencia de la Nación) el Anteproyecto de Ley de Delitos Informáticos. (5 artículos; p. 15-19)

Resolución 62 de la Secretaría de Comunicaciones de fecha 11 de abril de 2002. Prorroga hasta el 31 de marzo de 2002 el plazo para el mecanismo de consulta pública aplicado al anteproyecto de ley de delitos informáticos. (2 artículos, p. 9)

(ARGENTINA)
ANTEPROYECTO DE LEY DE DELITOS INFORMÁTICOS
SOMETIDO A CONSULTA PUBLICA POR LA SECRETARIA DE COMUNICACIONES POR
RESOLUCIÓN No. 476/2001 DEL 21.11.2001

Acceso Ilegítimo Informático:

Artículo 1.-

Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido. La pena será de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

En el caso de los dos párrafos anteriores, si las conductas se dirigen a sistemas o datos informáticos concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, la pena de prisión será de seis meses a seis años.

Daño Informático

Artículo 2.- Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

Artículo 3.- En el caso del artículo 2º, la pena será de dos a ocho años de prisión, si mediara cualquiera de las circunstancias siguientes:

- 1) Ejecutarse el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
- 2) Si fuera cometido contra un sistema o dato informático de valor científico, artístico, cultural o financiero de cualquier administración pública, establecimiento público o de uso público de todo género;
- 3) Si fuera cometido contra un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Si del hecho resultaren, además, lesiones de las descritas en los artículos 90 o 91 del Código Penal, la pena será de tres a quince años de prisión, y si resultare la muerte se elevará hasta veinte años de prisión.

Fraude Informático

Artículo 5.- Será reprimido con prisión de un mes a seis años, el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

En el caso del párrafo anterior, si el perjuicio recae en alguna administración pública, o entidad financiera, la pena será de dos a ocho años de prisión.

Disposiciones Comunes

Artículo 6.-

1) A los fines de la presente ley se entenderá por sistema informático todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

2) A los fines de la presente ley se entenderá por dato informático o información, toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

3) En todos los casos de los artículos anteriores, si el autor de la conducta se tratare del responsable de la custodia, operación, mantenimiento o seguridad de un sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo, no pudiendo superar, en ninguno de los casos, los veinticinco años de prisión.



Chile

En 1993 Chile sancionó la ley 19.223 (Diario Oficial de la República de Chile, Lunes 7 de junio de 1993) por la que se tipifican figuras penales relativas a la informática. En su art.3° dispone: "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio". **(Cabe señalar que Chile fue el primer país latinoamericano en sancionar una ley relativa a Delitos Informáticos)**

(CHILE) LEY RELATIVA A DELITOS INFORMÁTICOS

Ley No.:19223

Artículo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

México

En la mayoría de los Códigos Penales de los Estados Unidos Mexicanos se ha tipificado una figura de destrucción de datos y sistemas informáticos. También la ley federal de delitos informáticos, denominada Computer Fraud and Abuse Act de 1986, contempla en la Sección (a) (5) la alteración, daño o destrucción de información como un delito autónomo.

Los artículos federales son los siguientes:

ARTICULO 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

ARTICULO 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

ARTICULO 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

ARTICULO 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

ARTICULO 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

ARTICULO 211 bis 6.- Para los efectos de los artículos 211 bis 4 y 211 bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis de este Código.

ARTICULO 211 bis 7.- Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.



Venezuela

PROYECTO DE LEY DE DELITOS INFORMÁTICOS DE VENEZUELA

Ley Especial Contra los Delitos Informáticos

Título I

Disposiciones Generales

Artículo 1.- Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2.- Definiciones. A los efectos de la presente ley y cumpliendo con lo previsto en el art. 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a. Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data.

b. Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c. Data: Hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado.

d. Información: Significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e. Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f. Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g. Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos,

de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h. Firmware: programa o segmento de programa incorporado de manera permanente en algún componente de hardware.

i. Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas.

j. Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador.

k. Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

l. Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

m. Virus: Programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

n. Tarjeta inteligente: rótulo, cédula o carné que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

o. Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

p. Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3. Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4.- Sanciones. Las sanciones por los delitos previstos en esta ley serán principales y accesorias.

Las sanciones principales concurrirán con las accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente ley

Artículo 5.- Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable.

La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente

Título II
De los delitos
Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información

Artículo 6.- Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias

Artículo 7.- Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus o programa análogo.

Artículo 8.- Sabotaje o daño culposos. Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9.- Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas

Artículo 10.- Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11.- Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12.- Falsificación de documentos. El que, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad. El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II

De los Delitos Contra la Propiedad

Artículo 13.- Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14.- Fraude. El que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15.- Obtención indebida de bienes o servicios. El que, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16.- Manejo fraudulento de tarjetas inteligentes o instrumentos análogos. El que por cualquier medio, cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o el que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penado con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de

intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17.-Apropiación de tarjetas inteligentes o instrumentos análogos. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18- Provisión indebida de bienes o servicios. El que a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado, alterado, provea a quien los presente de dinero, efectos, bienes o servicios o cualquier otra cosa de valor económico, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19.- Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Capítulo III

De los delitos contra la privacidad de las personas y de las comunicaciones

Artículo 20.- Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21.- Violación de la privacidad de las comunicaciones. El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22.- Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV

De los delitos contra niños, niñas o adolescentes

Artículo 23.- Difusión o exhibición de material pornográfico. El que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24.- Exhibición pornográfica de niños o adolescentes. El que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V

De los delitos contra el orden económico

Artículo 25.- Apropiación de propiedad intelectual. El que sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26.- Oferta engañosa. El que ofrezca, comercialice o provea de bienes o servicios mediante el uso de tecnologías de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta de modo que pueda resultar algún perjuicio para los consumidores, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

Título III

Disposiciones comunes

Artículo 27.-Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1° Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

2° Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.

Artículo 28.- Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29.- Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las accesorias siguientes:

1° El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos previstos en los artículos 10 y 19 de la presente ley.

2° El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3° La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión, arte o industria, o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o conmutada la sanción principal cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4° La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30.- Divulgación de la sentencia condenatoria. El Tribunal podrá disponer, además, la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31.- Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el Juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

Para la determinación del monto de la indemnización acordada, el Juez requerirá del auxilio de expertos.

Título IV

Disposiciones Finales

Artículo 32.- Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela

Artículo 33. -Derogatoria. Se deroga cualquier disposición que colida con la presente Ley.

Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los seis días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación.



CONCLUSION

Para concluir con esta aproximación a un tema de gran interés y preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, es conveniente establecer tratados de extradición o mínimamente acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional para contrarrestar eficazmente la incidencia de la criminalidad informática.

Resaltamos como un ejemplo apropiado en este tema, el Artículo 3: Extraterritorialidad de la ley Venezolana: **Ley Especial Contra los Delitos Informáticos, Título I, Disposiciones Generales...**

Artículo 3. Extraterritorialidad. Cuando alguno de los delitos previstos en la presente ley se cometa fuera del territorio de la República, el sujeto activo quedará sujeto a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Asimismo, la problemática jurídica de los sistemas informáticos debe considerar la tecnología de la información en su conjunto (chips, inteligencia artificial, nanotecnología, redes, etc.), evitando que la norma jurídica quede desfasada del contexto en el cual se debe aplicar, o en otras palabras, ser suficientemente amplia para que los cambios tecnológicos no la afecten y dejen desfasada.

Las dificultades que enfrentan las autoridades en todo el mundo ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, las técnicas de investigación, la asesoría jurídica y las leyes de extradición para poder alcanzar a los delincuentes. Ya se han iniciado algunos esfuerzos al respecto.

El nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Finalmente, la ocurrencia de delitos informáticos en las organizaciones alrededor del mundo no debe en ningún momento impedir que éstas se beneficien de todo lo que proveen las tecnologías de información (comunicación remota, Interconectividad, comercio electrónico, etc.); sino por el contrario dicha situación debe plantear un reto a los profesionales de la informática, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad, controles, integridad de la información, etc. en las organizaciones.

