Atelier de l'Afrique de l'ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection de l'infrastructure de l'information critique

Praia, 27 -29 novembre 2007

LES DÉLITS INFORMATIQUES, LES LOIS LES PUNISSANT ET LA PRATIQUE

Par María-Gabriela Sarmiento[1].

I. INTRODUCCION

1. Antecedentes….La Internet y la inseguridad.

El presente trabajo es el resultado de una reciente investigación en materia de delitos informáticos a nivel de las propuestas nacionales e internacionales. Asimismo, para comprender la situación actual que vivimos con respecto a la seguridad informática y a los actos criminales perpetrados a través de medios electrónicos, informáticos, telemático y a fines, hemos efectuado una revisión de las obras literarias sobre delitos informáticos desde la década de los ochenta, lo cual no ha permitido cubrir la información existente sobre la materia en un período de veinte (20) años, que permitió la transición de las nuevas tecnologías del siglo pasado al nuevo milenio.

Cuando las computadoras pasaron a formar parte de las herramientas de trabajo de uso cotidiano, aparecieron los delitos instrumentados mediante el uso de computadoras y autores latinoamericanos[2] ya se adelantaban a pensar que "es probable que su incidencia se acentúe con la expansión del uso de computadoras y redes telemáticas", lo cual obviamente sucedió con gran impacto desde el año de 1996 cuando el uso de la www se masificó.

Ya en aquellos años ochenta, estos autores nos decían que los tipos penales tradicionales resultaban en muchos países inadecuados para encuadrar las nuevas formas delictivas y que, en caso de ocasionarse perjuicios en diferentes países por la comisión de un mismo delito cometido en un territorio, era extremadamente complejo determinar la jurisdicción aplicable al caso concreto.

2. Vulnérabilité technologique (manque de contrôle informatique, manque de ressources humaines compétentes chez les utilisateurs, les entreprises, la police, les avocats et les juges)

Depuis la venue des nouvelles technologies à notre vie quotidienne nous avons pu constater qu'il existe un manque d'un contrôle effectif des systèmes d'interconnexion. D'ailleurs, les utilisateurs inexperts, tant les particuliers comme les PMEs et les techniciens informatiques amateurs ont contribué à l'existence de cette vulnérabilité. Le manque d'information, la contribution minimale des gouvernements dans la promotion de l'utilisation des TICs et de la sécurisation des échanges ont aussi permis la création d'une plateforme « cybernétique » non fiable.

---

[1] *Avocate, Consultante indépendante appartenant au Cabinet-conseil Sarmiento Núñez www.snconsult.com ; ex-fonctionnaire de l'unité e-Strategy-BDT-UIT ; D.E.S.S. en Droit des affaires internationales France-1998; IUSE-ILO Post-Graduate Course on International Trade Law 2003* ;

[2] Batto, Correa, Czar de Zalduendo y Nazar, "Derecho Informático", Ediciones Depalma, Buenos Aires 1987 pa. 295 y sig.

Cette faiblesse a été profitée par des malfaiteurs qui eux, connaissant très bien les outils informatiques, commettent des actes illicites rendant les échanges informatiques et/ou électroniques douteux, non fiables et non sécurisés.

3. Les actes criminels perpétrés au moyen d'outils informatiques

Como efecto de lo anterior surgió la figura del *computer crime o computer kriminalitat* definido por la OCDE como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos.

Autores como Ulhrich Sieber[3] clasificaban las conductas delictivas en categorías como:

- **Fraude** por manipulación de computadora contra un sistema de procesamiento de datos, mediante la introducción en la computadora de datos falsos, la colocación de un caballo de Troya dando instrucciones a la comp. para efectuar transacciones no autorizadas o la introducción de virus que dan instrucciones a determinados programas.
- **Espionaje informático**, mediante la copia y obtención de información sin previa autorización y robo de software
- **Sabotaje Informático**, mediante virus, caballos de Troya, hackeos u otros destinados a destruir total o parcialmente información, datos, programas o hasta todo un equipo.
- **Acceso no autorizado** a sistemas de procesamiento de datos, efectuado por hackers y/o crackers para robar información, data y/o destruirla.

Estas conductas delictivas perpetradas mediante el uso de medios informáticos son consideradas por algunos autores como conductas que materializan delitos tradicionales y preexistentes en el Código Penal de cada país, puesto que se trata de delitos contra las personas, las cosas y la Nación, ya debidamente tipificados en la normativa legal de cada país.

Para otros autores estos, son actos criminales que versan sobre nuevos intereses sociales no protegidos por el derecho penal, como veremos más adelante en la definición de delitos informáticos en *strictu sensu*.

4. Les stratégies privées pour sécuriser les échanges informatiques

Softwares Antivirus, Anti-spyware, PKI, biométrie, SSL, Codes, codes-source, etc.

5. La participation de l'État dans la sécurité informatique. Pouvoir exécutif (Plan d'action, Stratégie nationale)

Una vez que hubo suficiente conocimiento sobre la materia y voluntad política para promover mejoras en la seguridad y confiabilidad de las TIC, los países comenzaron a adoptar Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información, así como también Planes Nacionales para implementar los lineamientos pautados.

6. La participation de l'État dans la sécurité informatique. Pouvoir législatif (La pénalisation des actes criminels, la naissance de la figue des délits informatiques, la création de lois)

El derecho penal es muy estricto. Uno de sus principios básicos establece que "*nulla pene sine lege*". Es por esta razón que los legisladores de cada país debieron tomar medidas respecto de los nuevos tipos de hechos ilícitos no previamente tipificados por el derecho penal tradicional y es por esta razón que nuevas leyes penales especiales fueron creadas para penar hechos hoy calificados como delitos informáticos.

[3] Sieber, Ulrich. *"The international handbook on computer crime : Computer-Related Economic Crime and the Infringements of Privacy"*, John Wiley & Sons, 1986, p. 3

La evolución social, producto de la globalización y del surgimiento y masificación de las nuevas tecnologías de la información y de la comunicación, conllevó a la forzosa evolución del ordenamiento jurídico en los distintos países del globo. Los intereses protegidos sufrieron modificaciones, despenalizándose algunas conductas y penalizando otras nuevas.

A raíz de estos cambios, surgieron normas legales a nivel mundial tuvieron por objeto proteger las bases de datos, su contenido y sus creadores, estableciendo tipos penales para su acceso, modificación, destrucción y sustracción ilegales que fueron reforzados con los derechos de autor, y en algún caso, con los de propiedad industrial. Asimismo, se crearon normas para proteger los datos personales; al mismo tiempo que surgía el principio de la libertad de circulación de información, basado en el derecho a la información. Y además, el derecho de autor venía siendo aplicado para la protección del software, como una creación e invención, contra su robo, reproducción, destrucción, alteración y difusión no autorizados.

Crímenes cometidos por personas, grupos de personas y organizaciones criminales a través de la red, en sistemas operativos, computadoras, bases de datos en línea y off-line, archivos electrónicos, programas de computación, hardware, certificados digitales, y mensajes de datos, entre otros, han pasado a formar parte de nuestro día a día. La pornografía infantil (y adulta en determinados casos), los actos ilícitos contra el honor y reputación de personas y empresas, la violación de derechos de autor, la propaganda no deseada ni solicitada, la propaganda engañosa, el fraude electrónico, son todos hechos ilícitos que forman parte de los hoy llamados delitos informáticos que han sido debidamente tipificados y recogidos en nuevas Leyes independientes sobre delitos informáticos o en reformas del Código Penal vigente de una gran mayoría de países. Pérdidas millonarias se han registrado en compañías que han perdido reputación debido a delitos informáticos perpetrados en contra de ellas, a través de virus, caballos de Troya u otra intrusión ilegal por parte de hackers. La violación de la privacidad e intimidad, la falsificación y alteración de información, de datos o de documentos, la apropiación indebida de información, el robo de data, entre otros, forman parte de la gama de delitos informáticos tipificados en las legislaciones especiales y códigos penales reformados. Estas conductas son hoy en día penalizadas en muchas Naciones como “delitos informáticos”.

Para coadyuvar y armonizar la iniciativa nacional, nació en noviembre de 2001, un nuevo marco legal internacional para luchar contra los delitos informáticos: la Convención de Budapest sobre Cyber Crime, creada con el objeto de luchar contra la xenofobia, el racismo, y cualquier otro tipo d delito cometido vía Internet. Esta Convención entró en vigencia a partir de Julio de 2004.

7. **La participation de l’État dans la sécurité informatique. Pouvoir judiciaire (création de la police « informatique », application des lois par les juges)**

8. **Les apports des organisations et de la communauté internationales.**

II. DELITS, NORMES JURIDIQUES ET CAS PRATIQUES

1. Les délits informatiques

1.1. Définition générique

No es fácil obtener una definición clara y concisa de delitos informáticos. Las interpretaciones son vastas y variadas y como dice el Dr. Gabriel Campoli, abogado mexicano, inclusive la Convención Europea de Cibercrimen está equivocando el camino para la creación de un marco jurídico que tipifique los delitos informáticos por cuanto confunde el medio comisivo del delito con el objeto del delito y con el bien jurídico protegido. Este jurista manifiesta también que los textos de mayor difusión en el mercado tienen este mismo error de no separar los delitos informáticos de los cometidos a través de medios informáticos, que no son más que los mismos delitos de corte tradicional establecidos en los Códigos Penales de cada país.

Insiste el Dr. Campoli en expresar que "los delitos cometidos por medios informáticos son delitos comunes, ya tipificados hace años, pero el error es no perseguirlos por pensarse que no están tipificados porque se usa una computadora para cometer dichas acciones, reitero mi posición respecto a que el derecho penal sanciona conductas, no medios comisivos, por lo que si buscamos la conducta, nos encontraremos con muchos tipos penales que nos pueden dar soluciones al problema concreto, es más un asunto de argumentación y de trabajo de fiscales y abogados, que de tipos penales". No obstante, el mismo jurista recuerda, no sin razón, que se requieren legislaciones específicas para muchas de las conductas perpetradas hoy en día con uso de medios informáticos, "justamente para no quedar atados a la interpretación que los jueces" den a las normas penales tradicionales a fin de aplicarlas al novedoso caso. Ello lo afirma debido a que en los países de sistema de common law esto podrá funcionar a la perfección, "pero en América Latina es un desastre".[4]

Sin embargo y para no decepcionar a la audiencia, la siguiente es una definición general de delitos informáticos: "Conducta ilícita o criminal que se comete a través del uso de computadoras"[5].

El derecho penal con respecto a los asuntos relacionados con las TICs o Delito informático puede ser definido como el derecho sobre los crímenes cometidos vía la Internet y otras redes de computación. Tipifica acciones dirigidas contra la confidencialidad, la integridad y disponibilidad de sistemas de computación, redes y datos de computación, así como el mal uso de dichos sistemas, redes y datos. Sanciona principalmente conductas que se materializan en infracciones de derechos de autor, pornografía infantil, fraude vía computadora y en la violación de redes de seguridad. También cubre asuntos procedimentales en material penal como investigaciones y vigilancia de plataformas y redes electrónicas Ej. La intercepción de correos electrónicos. Delitos informáticos pueden también cometerse al abusar de códigos de acceso y claves, o manipulando o dañando programas de computación mediante la instalación de virus.[6]

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). Las computadoras proporcionan nuevos métodos para cometer delitos tradicionales: Fraude. Hurto. Amenazas o Distribución de Pornografía Infantil.
- Los actos fraudulentos que sólo se producen en ocasión de una operación informática.

---

[4] Correo electrónico [alfa-redi] Delios Informáticos. Mailing List de Alfa-Redi. Julio de 2007.

[5] Reyna, Luis Miguel, "Aproximación al Estudio de la criminalidad mediante computadoras", publicado en "Informática & Internet, Aspectos Legais Internacionais" (Una obra originaria da comunidade ALFA-REDI), ADCOAS, Editora Explanada, Rio de Janeiro. 2002, págs. 239 y sig.

[6] Legal IST. "STATE OF THE ART OF RESEARCH ON LEGAL ISSUES RELATED TO THE INFORMATION SOCIETY TECHNOLOGIES". Contribution of the LEGAL-IST proposal Consortium to the e-Business Summit, Dublin, 27-28 April 2004.

1.2. Identification et définition des comportements considérés délit informatique.[7]

Una vez obtenida una definición genérica sobre lo que son delitos informáticos y sin olvidar que existe discrepancias en la doctrina sobre cuál es el bien jurídico tutelado bajo la figura de delitos informáticos, pasaremos a citar algunas de las conductas que, materializadas a través del uso de medio informáticos, causan perjuicios a terceros y son identificadas como delitos informáticos.

Muchas conductas ilícitas que se verifican en la actividad informática han sido identificadas como posibles delitos informáticos, algunas de ellas son: Daños, Estafas, Hurto y Violación de secretos, Apertura indebida de comunicaciones, denegación de servicio (DDoS)[8], intrusionismo informático, hacking, cracking, la destrucción física de los medios de servicio.

Un **tipo de ataque y denegación de servicio** es aquel mediante el cual el atacante usa códigos maliciosos instalados en varias computadoras para atacar un objeto singular definido. El atacante puede usar este método para tener una mayor efecto sobre su mira que el que podría obtener de un ataque con uso de una sola máquina.[9] En Internet un ataque de ***Distributed Denial of Service (DDOS)*** o Denegación Distribuida de Servicios es aquel en el que una multitud de sistemas comprometidos ataca a un objeto singular identificado, causando denegación del servicio para los utilizadores del sistema identificado. El flujo de los mensajes entrantes al sistema identificado contra el cual se ejerce el ataque lo fuerza a cerrar, trayendo como consecuencia la denegación del servicio al sistema por parte de los legítimos utilizadores. Un ***hacker*** (o si se prefiere un cracker) inicia un ataque DDoS explotando la vulnerabilidad de un sistema de computación. Es desde el sistema master que el intruso identifica y comunica con los otros sistemas que podrían estar comprometidos. El intruso baja herramientas de cracking disponibles en Internet a múltiples sistemas comprometidos. Con un simple comando, el intruso da instrucciones a las máquinas controladas paa que lancen uno de los tantos flujos de ataques contra un target específico. La inundación de packets al target específico causa la denegación del servicio. En la **Denegación Distribuida de Servicio, DDoS,** así como en otros usos de las redes de **robots o botnets[10]**, el delincuente se apodera para su uso de un bien de un tercero sin su autorización, pero sin quitárselo al dueño.

Un ***ataque DoS (o de Negación de servicios)*** es cuando una tercera persona malintencionada hace que los servicios de comunicación de red de una entidad dejen de funcionar y para ello utiliza varias técnicas. En cambio "negar un servicio" es cuando una persona o institución niega sus servicios por X razones a sus afiliados.[11] En el caso de un proveedor privado de información tal como un sitio de comercio electrónico, la negación deliberada de servicio ocasiona pérdidas en bienes tangibles y demostrables - ventas - y en reputación. En el caso de un proveedor público, la negación deliberada de servicio puede tener efectos que van desde retrasar algún trámite que realiza un ciudadano administrado, hasta ocasionar pérdidas tanto a éste como al gobierno, pues por ejemplo, no se lograría hacer el pago de impuestos en plazo determinado.[12]

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.

[7] Algunas de las definiciones aquí reproducidas forman parte de la RESOLUCION No. 127/2007 contentivo del REGLAMENTO DE SEGURIDAD PARA LAS TECNOLOGIAS DE LA INFORMACION

[8] DDoS es una técnica particular para lograr una negación de servicio.

[9] Definición de Microsoft.

[10] Los ***botnet***, es decir, redes de ordenadores no protegidos, controladas por delincuentes informáticos, que pueden utilizarse para estimular la creación de códigos maliciosos o para usurpar identidades;

[11] Ingeniero y abogado Katherine Fudinaga (katherine.fudinaga@gmail.com). Miembro de la Mailing List Alfa-Redi. Correo electrónico de Julio de 2007.

[12] Dr. Alejandro Pisanty. Director General de Servicios de Computo Academico UNAM, Universidad Nacional Autónoma de México. México DF México. Mailing List Alfa-Redi. Correo electrónico de fecha 23 de Julio de 2007.

Cracker: Intruso; individuo que intenta penetrar en un ordenador o sistema informático ilegalmente con intenciones nocivas.

Gusanos: Programas que pueden provocar efectos tan dañinos como los causados por los virus, pero se diferencian de éstos en su forma de transmitirse, pues no infectan otros programas con una copia de sí mismos, ni son insertados en otros programas por sus autores. Suelen funcionar en grandes sistemas informáticos conectados en red, difundiéndose rápidamente a través de ésta.

Spyware: Un tipo de software que envía datos del sistema donde está instalado sin que el usuario dé su consentimiento o ni siquiera lo sepa. Este tipo de información puede ir desde los sitios Web que se visitan hasta algo más delicados como por ejemplo el nombre de usuario y la contraseña.

Virus Informáticos: Programas capaces de reproducirse a sí mismos sin que el usuario esté consciente de ello. Se adicionan a programas de aplicación así como a componentes ejecutables del sistema de forma tal que puedan tomar el control del mismo durante la ejecución del programa infectado.

Programas de detección de pulsaciones [keyloggers] que copian en silencio lo que teclean los usuarios del ordenador y envían la información a los estafadores. En la mayoría de los casos, un programa para la detección de pulsaciones o similar simplemente espera a que se visiten ciertos sitios, como la página de un banco, o una cuenta de crédito electrónica, o que se introduzcan ciertas claves -DNI por ejemplo- para activarse. Lo tecleado se guarda en un archivo, se copian los formularios, e incluso se pueden tomar silenciosamente fotos de la pantalla de un usuario. Después, la información se envía a un sitio de Internet o a un servidor de espera donde un programa diferente, o ladrón, repasa los datos en busca de información útil.

Spam: Práctica de envío indiscriminado de mensajes de correo electrónico no solicitados que embasuran nuestros correos electrónicos con publicidad, engañosa o no, en todo caso no solicitada. De acuerdo a una publicación de la Comisión Europea la siguiente es la lista de los doce países más contaminantes: Estados Unidos, China, Francia, Corea del Sur, España, Polonia, Brasil, Italia, Alemania, Taiwán, Israel y Japón.

Mensajes de ***phishing*** [pesca en sentido figurado] que fingen ser de un banco o una empresa, pero que en realidad son intentos de robar contraseñas u otra información personal. Ej. mensajes de *phishing* que fingen ser de un banco o una empresa, pero que en realidad son intentos de robar contraseñas u otra información personal.

Hoax (en español: rumor, falsedad, engaño): Mensajes de correo electrónico engañosos que se difunden por las redes con la ayuda de usuarios irresponsables que los reenvían formando largas cadenas, lo que consume un gran ancho de banda y congestiona los servidores. Su contenido generalmente se basa en temáticas religiosas o de solidaridad, alertas sobre virus muy dañinos, etc.

Data mining (minería de datos): usar técnicas matemáticas y estadísticas para detectar relaciones en flujos de datos digitales o en grandes bases de datos. Es una práctica desarrollada desde hace décadas por los gigantes informáticos en busca de mercados comerciales. La minería de datos ya se utiliza en toda una serie de aplicaciones comerciales, ya sean compañías de tarjetas de crédito que detectan y evitan el fraude en cuanto se producen, o aseguradoras que predicen riesgos sanitarios.

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. Los elementos del fraude informático son tres: Un sujeto actor o autores de la conducta dañosa que produce fraude; Un medio adecuado para cometer el acto ilícito, o sea el sistema

informático por medio del cual se lleva a cabo la acción y Un objeto, o sea, el bien que produce el beneficio ilícito para el o los autores.

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.

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.

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[13]:

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 dificiles 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. También se les define como programas malignos que se introducen de manera subrepticia en los medios de cómputo para adquirir privilegios de acceso al sistema atacado y manipularlo a su conveniencia.
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., que persiguen actuar contra un sistema informático cuando se cumplan ciertas condiciones.
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.

[13] GLIN-Nicaragua-CORTE SUPREMA DE JUSTICIA, NICARAGUA BANCO INTERAMERICANO DE DESARROLLO, BANCO INTERAMERICANO DE DESENVOLVIMENTO, "**LEGISLACIÓN NICARAGUENSE ANTE LOS DELITOS INFORMATICOS".** Noviembre, 2005. Managua, Nicaragua.

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.

Tipos de delitos informáticos reconocidos por Naciones Unidas[14]

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

[14] GLIN-Nicaragua-CORTE SUPREMA DE JUSTICIA, NICARAGUA BANCO INTERAMERICANO DE DESARROLLO, BANCO INTERAMERICANO DE DESENVOLVIMENTO, "**LEGISLACIÓN NICARAGUENSE ANTE LOS DELITOS INFORMATICOS".** Noviembre, 2005. Managua, Nicaragua.

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.

2. Normes juridiques des pays qui punissent les délits informatiques:

2.1. Les Amériques

ANTIGUA Y BARBUDA

- THE COMPUTER MISUSE ACT, 2006. Las ofensas o delitos previstos en esta Le son las siguientes: acceso no autorizado a un dato o programa de computación, el acceso con intención de cometer o facilitar la comisión de una ofensa o delito, la modificación no autorizada de datos o programas de computación, el uso no autorizado o intercepción de servicios de computación, la obstrucción no autorizada del uso de computadoras, la difusión no autorizada de un código de acceso, recibir de manera no autorizada o dar acceso no autorizado a datos o programas de computación, causar que una computadora cese de funcionar, ataques de denegación de servicios, robo de identidad y la pornografía infantil, entre otros. Asimismo, se estipulan penas para los delitos relacionados con computadoras protegidas.
- THE ELECTRONIC TRANSFER OF FUNDS CRIMES ACT, 2006. Las ofensas o delitos previstos en la presente Ley son, entre otros: el falso testimonio, robo tomando o poseyendo una tarjeta, el robo de tarjetas, utilizar la tarjeta de un tercero, comprar o vender la tarjeta de un tercero, forjar documentos, firmar la tarjeta de un tercero, usar una tarjeta fraudulentamente, fraude cometida por persona autorizada para prestar bienes, servicios, etc., recibir dinero obtenido mediante el uso fraudulento de tarjeta, obtener bienes usando una tarjeta falsa, expirada o revocada, poseer un equipo para hacer tarjetas, alteración de la factura de tarjetas, transferencia electrónica fraudulenta de fondos
- The Mutual Assistance in Criminal Matters Act de fecha 17 de Febrero de 1993.

ARGENTINA

- Están protegidas las obras de base de datos y de software, agregados a la lista de ítems contemplados por la Ley 11.723 de propiedad intelectual publicada mediante el Decreto N° 165/94 del 8 de febrero de 1994.
- Ley 25.326 de Habeas Data sancionada el 03 de Octubre de 2000 y de Registro Nacional de Bases de Datos. Gracias a esta Ley Argentina es país líder en la protección de datos personales en América Latina.
- Ley 25.763 mediante la cual se aprueba el Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño sancionada el 23 de Julio de 2003 y promulgada de Hecho: Agosto 22 de 2003. http://www.snconsult.com/leyes_detalle.php?idley=4&idioma=
- La Cámara de Diputados de la Nación aprobó el 11 de Octubre de 2006 un proyecto de Ley que incorpora varios artículos al Código Penal para sancionar los llamados delitos informáticos. La iniciativa equipara el correo electrónico a la correspondencia tradicional; tipifica como delitos el acceso no autorizado a los correos electrónicos privados; su publicación sin el consentimiento de su remitente; como la manipulación de las comunicaciones informáticas para perpetrar delitos económicos. Sumario del proyecto de modificación del Código Penal: modificación al articulo 128 (delitos contra la integridad sexual; pornografía infantil); sustitución del epígrafe del capitulo III del titulo v del libro II (delitos contra la privacidad); sustitución del articulo 153 y e incorporación de los artículos 153 bis, 153 ter y 153 quater (violación de secretos y de la privacidad, violación de sistemas informáticos o datos electrónicos; sustitución de los artículos 155 y 157; incorporación de inciso 16) del articulo 173 (fraude); incorporación de segundo y tercer párrafo al articulo 183, sustitución del inciso 5 del articulo 184 e incorporación del inciso 6) al articulo

184 (daño); sustitución del articulo 197 (interrupción de las comunicaciones); modificación a la primera parte del articulo 255 (alteración de las pruebas); incorporación de párrafo al articulo 77 (falsificación de documentos electrónicos o informáticos). Para esa fecha, la Comisión de Legislación Penal comentaba que los artículos podrían sufrir algunas modificaciones.[15] Fundamentos legales de esta reforma son los hechos ilícitos reconocidos por la ONU como delitos informáticos y las convenciones internacionales.
Para el 19 de octubre de 2006, Proveedores de software y servicios informáticos, usuarios de computadoras, estudiantes y académicos de informática hicieron llegar un pedido a los legisladores que actualmente tratan la modificación al Código Penal para incorporar en él una serie de delitos informáticos: "Debido a que entendemos que su redacción actual se presta a interpretaciones que penalizan actividades normales y necesarias en la ejecución de nuestras tareas habituales", explican el comienzo del texto[16].

- Comenta el abogado argentino Alberto Soto (asoto@ibero-americano.org) en correo a una *mailing list* sobre nuevas tecnologías de fecha 10 de Septiembre de 2005, que con relación a la seguridad en la información y la responsabilidad de los bancos respecto a los datos de sus clientes, desde mucho antes de la obligatoriedad de bancarización en materia laboral para el pago de sueldos, el Banco Central de la República Argentina dictó entre tantas otras, la Circular "A" 3198 que es el resumen ordenado del texto de las previas "A 2659, "A 3149" y "B6776", que se denomina “Requisitos operativos mínimos del área de sistemas de información”. Esa Circular establece las obligaciones de seguridad, inclusive obligando a las instituciones financieras a guardar la información por un plazo de diez (10) años. El Durante muchos años, el Banco Central ejerció el poder de policía que esta Circular le confería, y ello brindó confiabilidad en el sistema e-banking.

BARBADOS

- Acte No. 2 of 2003 TO MAKE PROVISIONS SECURING COMPUTER MATERIAL AGAINST UNAUTHORISED ACCESS OR MODIFICATION AND FOR CONNECTED PURPOSES. Fecha 11 de Abril de 2003. Esta Ley prevé el Acceso no autorizado a material de computación, el acceso con intención de cometer o facilitar la comisión de ofensas, la modificación no autorizada a materia de computación, el uso o intercepción no autorizado de servicios de computación, la obstrucción no autorizada del uso de computadoras y la difusión no autorizada de códigos de acceso. Son igualmente punibles la incitación a delinquir y la tentativa. También están previstas las agravantes por ofensas relacionadas con computadoras protegidas.

BOLIVIA

- Ley de Modificación del Código Penal número 1768, de 10 de marzo de 1.997.Delitos Informáticos Bolivia con disposiciones que protegen las obras literarias y las bases de datos.

- Ley de Documentos, Firmas y Comercio Electrónico, aprobada el 21 de agosto 2007, entrará en vigencia 18 meses después de su aprobación. El proyecto de ley que fuera aprobado en grande el 21 de agosto de 2007 tiene como objeto reconocer el valor jurídico y probatorio de los mensajes de datos, documento electrónico, firma electrónica, contratación electrónica, así como el comercio electrónico, incluyendo

[15] Diario Judicial. “Se vienen los delitos informáticos”, 12 de Octubre de 2006. Diariojudicial.com, Diario Judicial.com S.A. Buenos Aires, Argentina.
[16] Infobae.com “Piden cambios al proyecto sobre delitos informáticos”. Argentina.

modificaciones al Código Penal sobre la utilización de los medios electrónicos y a los delitos informáticos. Según los entendidos este proyecto de ley no cambia la estructura del Derecho existente, simplemente reconoce el valor jurídico y probatorio de un nuevo soporte el "soporte electrónico", es así que se respetan los Códigos Civil y Comercial y sólo se incluyen modificaciones al Código Penal, incluyendo al correo electrónico, documento electrónico, medios electrónicos y nuevos delitos informáticos[17]. http://www.adsib.gob.bo/home/p_ley.htm

BRASIL

- No Brasil temos uma lei específica, mas destinada a funcionários públicos (9983/00), que alterou alguns artigos do Código Penal, além da lei de interceptação telefônica, que alguns defendem a aplicabilidade também para a web, (9296/96), e pelo menos três projetos de lei importantes, que tramitam em conjunto no Senado Federal: 76/00, 137/00 e 89/03 (este, já aprovado na Câmara).[18]
- LEI No 9.983, Brasilia, 14 DE JULHO DE 2000 Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências.
  "Apropriação indébita previdenciária" (AC)*
  "Inserção de dados falsos em sistema de informações" (AC)
  "Modificação ou alteração não autorizada de sistema de informações" (AC)
  "§ 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:" (AC)
  "III – quem altera, falsifica ou faz uso indevido de marcas, logotipos, siglas ou quaisquer outros símbolos utilizados ou identificadores de órgãos ou entidades da Administração Pública." (AC)
  declaração falsa ou diversa da que deveria ter constado." (AC)
  "I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;" (AC)
  "II – se utiliza, indevidamente, do acesso restrito." (AC)
- Decreto 3.505 de 13/06/2000 (Segurança da Informação)
- Decreto 3.872, de 18/07/2001 (ICP-Brasil)
- Decreto 3.996, de 31/10/2001 (Certificação Digital)
- Decreto 4.414, de 07/10/2002 (Certificação Digital)
- Decreto 4.553 de 27/12/2002 (Classificação da Informação)
- Medida Provisória nº 2.200-2 (ICP-Brasil)
- Projeto de Lei nº 84 de 1999 (Projeto de Lei de Crimes de Informática)
- Resolução Nº 7 do e-gov de 30/07/2002 (Resolução sobre Sítios Governamentais - E-Gov)
- Decreto 5.772 de 08/05/2006 (Criação DSIC)
- 2001: Proyecto de ley No 5460/01
- Ley sobre la difusión de pornografía infantil y adolescente por Internet

CANADA

- Criminal Code, C-46, An Act respecting the Criminal Law. Algunos de los delitos pervistos en este Código son: el Voyeurism, la pornografía infantil[19], Intercepción de comunicaciones privadas, incitar el odio contra grupos identificados incluso por medios electrónicos, robo de servicios de comunicación, quien posea herramientas para

[17] El Mundo. "Aprobaron ley de Documentos Firmas y Comercio Electrónico". Sábado, 10 de noviembre de 2007. http://www.elmundo.com.bo/ Bolivia

[18] Abogado brasileño Omar Kaminski. Mailing List Alfa-Redi. Correo electrónico de fecha 29 de septiembre de 2005.

[19] a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means

obtener facilidades o servicios de telecomunicación, el uso no autorizado de computadoras, la posesión de instrumentos para obtener servicios de computación, entre otros.

- Première session, trente-septième législature, 49-50-51 Elizabeth II, 2001-2002, LOIS DU CANADA (2002), CHAPITRE 13, Loi modifiant le Code criminel et d'autres lois [*Sanctionnée le 4 juin 2002*], PROJET DE LOI C-15A SANCTIONNÉ LE 4 JUIN 2002, 49-50–51 ELIZABETH II CHAPITRE 13. SOMMAIRE Le texte modifie le *Code criminel* comme suit :
  a) il crée de nouvelles infractions et prévoit d'autres mesures pour protéger les enfants contre l'exploitation sexuelle, notamment l'exploitation sexuelle mettant en jeu l'utilisation d'Internet; *b*) il augmente la peine maximale dans les cas de harcèlement criminel; *c*) il fait de l'invasion de domicile une circonstance aggravante pour la détermination de la peine; *d*) il crée une infraction réprimant le fait de désarmer un agent de la paix ou de tenter de le faire; *e*) il codifie et clarifie le processus d'examen des demandes d'examen auprès du ministre de la Justice concernant les erreurs judiciaires; *f*) il réforme et modernise la procédure criminelle concernant :
  (i) les aspects procéduraux de l'enquête préliminaire, (ii) la divulgation de la preuve des experts, (iii) les règles de cour à l'égard de la gestion des instances et des enquêtes préliminaires, (iv) les documents électroniques et les comparutions à distance, (v) un système complet d'enquête sur les plaidoyers, (vi) les poursuites personnelles, (vii) la sélection des jurés suppléants, (viii) les limites à l'utilisation de représentants.
  This enactment also amends the following Acts: (*a*) the *National Capital Act*, by increasing the maximum fine available; and (*b*) the *National Defence Act*, by providing for fingerprinting.
  Le texte modifie également : *a*) la *Loi sur la capitale nationale*, pour augmenter la peine maximale qui peut être imposée; *b*) la *Loi sur la défense nationale*, pour prévoir des dispositions sur les empreintes digitales.
- Este país cuenta igualmente con Leyes de protección de documentos electrónicos e información personal, de Radiocomunicación, de Derecho de Autor y otras disposiciones del Código Penal.
- Specific anti-spam law. On May 17, 2005, Canada's Task Force on Spam issued a final report entitled Stopping Spam: Creating a Stronger, Safer Internet. The report includes a range of recommendations including more rigourous law enforcement, public education, policy development and legislation.

CHILE

- Ley 19.223 TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMATICA. Fecha de publicación 7 de junio de 1.993. Fecha de promulgación 28 de mayo de 1.993. Fecha de entrada en vigor junio de 1.993. Prevé penalización para los siguientes hechos ilícitos: quien maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento; quien 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; quien maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información; y quien maliciosamente revele o difunda los datos contenidos en un sistema de información.
- Chile cuenta con una Brigada Investigadora del Ciber Crimen creada el 16 de Octubre del año 2000. Es una unidad especializada en los delitos cometidos vía Internet, tales como, amenazas, estafas, falsificación, pornografía infantil en Internet, y delitos informáticos propiamente tal, entre otros.

COLOMBIA

- LEY 527 DE 1999, Acceso y uso de mensajes de datos, comercio electrónico, firmas digitales y entidades certificadoras.

- ESTATUTO PARA PREVENIR Y CONTRARRESTAR LA EXPLOTACIÓN, LA PORNOGRAFÍA Y EL TURISMO SEXUAL CON MENORES DE EDAD
- Ley Nº 599 DE 2000 (julio 24) por la cual se expide el Código Penal (artículo 195) Artículo 195. Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.
  Ley 890 de 2004 y mediante ley 1032 de 2006 mediante la cual se modifica el Código Penal Colombiano, Ley 599 de 2000, por medio de la cual se adiciono el Código Penal, principalmente el capitulo Noveno sobre delitos contra medio de prueba y otras infracciones. Ver por ejemplo Art. 195 del Código Penal. El Código Penal colombiano prevé sanciones para conductas ilícitas que encuandran dentro de la VIOLACIÓN A LA INTIMIDAD, RESERVA E INTERCEPTACIÓN DE COMUNICACIONES. Ellas son: la Violación ilícita de comunicaciones; el Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas; La Divulgación y empleo de documentos reservados; el Acceso abusivo a un sistema informático; la Violación ilícita de comunicaciones o correspondencia de carácter oficial; la Utilización ilícita de equipos transmisores o receptores y la Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.
- 2001: Ley Nº 679 por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución
- DECRETO NUMERO 1524 DE 2002 (julio 24) - Delitos informáticos - Colombia por el cual se reglamenta el articulo 5° de la Ley 679 de 2001
- Ley 603, Derechos de Autor y antipiratería.
- Existen otras normas sobre violación de comunicaciones y medidas tecnológicas para proteger derechos de autor.
- Ley 600 Código de Procedimiento Penal. Este prevé la Recuperación de información dejada al navegar por Internet u otros medios tecnológicos que produzcan efectos equivalentes y la Búsqueda selectiva en bases de datos.
- Colombia cuenta con una Unidad de Delitos Informáticos del DAS y Delitos contra la propiedad intelectual de la Fiscaliza General de la Nación sería de gran utilidad.

COSTA RICA

- Ley No 8148 de fecha 24 de Octubre de 2001 sobre delitos informáticos ADICIÓN DE LOS ARTÍCULOS 196 BIS, 217 BIS Y 229 BIS AL CÓDIGO PENAL LEY Nº 4573, PARA REPRIMIR Y SANCIONAR LOS DELITOS INFORMÁTICOS Artículo único.- Adiciónanse al Código Penal, Ley Nº 4573, del 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, cuyos textos preven sanciones por violación de comunicaciones electrónicas; fraude informático; y alteración de datos y sabotaje informático.
- 2001: Ley Nº 8131 de la administración financiera de Costa Rica (artículos 110 y 111)

CUBA

- RESOLUCION No. 127/2007 contentivo del REGLAMENTO DE SEGURIDAD PARA LAS TECNOLOGIAS DE LA INFORMACION

DOMINICANA, REPUBLICA

- 2007: Ley de Crímenes y Delitos de Alta Tecnología
- 2001: Decreto No 48, Ley especial de delitos informáticos

ECUADOR

Ley 2002-67 (Registro Oficial 557-S, 17-IV-2002) DE COMERCIO ELECTRÓNICO, MENSAJES DE DATOS y FIRMAS ELECTRÓNICAS hace la reforma al Código Penal Ecuatoriano y tipifica las llamadas Infracciones Informáticas. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada; así como la obtención y utilización no autorizada de información; la falsificación electrónica; los daños informáticos; la apropiación ilícita; y la violación del derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.".

EL SALVADOR

- Decreto legislativo No. 1030 de fecha 26 de Abril de 1997. Reforma (17) D.L. No. 883 de fecha 27 de Junio de 2002
  El CAPITULO sobre LOS DELITOS RELATIVOS A LA INTIMIDAD prevé sanciones por la VIOLACIÓN DE COMUNICACIONES PRIVADAS; la VIOLACIÓN AGRAVADA DE COMUNICACIONES; la CAPTACIÓN DE COMUNICACIONES, la ESTAFA AGRAVADA y los DAÑOS AGRAVADOS.
  El CAPITULO relativo a LOS DELITOS RELATIVOS A LA PROPIEDAD INTELECTUAL comprende penas por la VIOLACION DE DERECHOS DE AUTOR Y DERECHOS CONEXOS: la VIOLACION AGRAVADA DE DERECHOS DE AUTOR Y DE DERECHOS CONEXOS y el FRAUDE DE COMUNICACIONES.

ESTADOS UNIDOS DE AMERICA (E.E.U.U.)

- En Estados Unidos ustedes pueden ubicar, en algunas áreas con un nivel de exactitud apabullante, los predators y sexual offenders de menores que vivan en su misma área, incluyendo nombre, dirección y muchos datos, tal y como encontrarán abajo. No tienen ellos defensa legal contra la publicación de esta información, por cuanto se considera que, muy por encima de sus consideraciones de privacidad, la sociedad sí tiene el derecho de saber que estos delincuentes están cerca y tomar medidas para proteger a los menores, que son en realidad a quienes debemos proteger por encima de cualquiera otro.
- 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
- El UNITED STATES CODE comprende un CHAPTER 47 sobre FRAUD AND FALSE STATEMENTS
  Section 1030. Fraud and related activity in connection with computers.
  (a) Whoever-
  (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
  (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-
  (A) information contained in a financial record of a financial institution, or of a card

issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5.000 in any one-year period;
(5) (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least USD 5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defence, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States;
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
(c) The punishment for an offense under subsection (a) or (b) of this section is--
See http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State or of an intelligence agency of the United States.

- Leyes de Delitos Informáticos de los diferentes estados americanos:
  - Alabama
  - Alaska
  - Arizona
  - California
  - Colorado
  - Connecticut
  - Delaware
  - Florida
  - Georgia
  - Hawaii
  - Idaho
  - Illinois
  - Indiana
  - Iowa
  - Maryland
  - Minnesota
  - New Jersey
  - New Mexico
  - New York
  - North Carolina

- Oregon
- Texas
- Virginia
- Washington
- West Virginia
- Wisconsin

GUATEMALA

- 1993: Decreto No 17-73 del Código penal. Reformas al Decreto 17-73 del Congreso de la República mediante el cual se publicó el Código Penal.
- Decreto 33-96 (artículos 13 al 19)

JAMAICA

- THE INTERCEPTION OF COMMUNICATIONS ACT de fecha 15 de Marzo de 2002
  Este texto establece entre otros los casos en los cuales deben ser libradas órdenes judiciales para mostrar información protegida. Algunos ejemplos:
  E-(1) A person who, in an application or affidavit under mences.
  this Act, makes a statement which he knows to be false in any material particular commits an offence and is liable upon summary conviction in a Resident Magistrate's Court to a fine not exceeding three million dollars or to imprisonment for a
  term not exceeding three years or to both such fine and imprisonment.
  (2) A person who intentionally discloses the contents of any communication-
  (a) obtained by means of a warrant, to a person to whom he is not authorized to disclose the communication; or (b) obtained in contravention of this Act, commits an offence and is liable upon summary conviction in a Resident Magistrate's Court to a fine not exceeding five million dollars or to imprisonment for a term not exceeding five years, or to both such fine and imprisonment.
  (3) Subsection (2) shall not apply to the disclosure of the contents of any communication obtained by means of a warrant which is made, in any criminal proceedings, to a person charged with an offence or to the attorney-at-law representing that person in those proceedings.

MEXICO

- 1999: Código Penal Federal (reforma de 1999), arts del 211 bis 1 al 211 bis 7.
  LIBRO SEGUNDO. TÍTULO OCTAVO. DELITOS CONTRA EL LIBRE DESARROLLO DE LA PERSONALIDAD.
  - CAPÍTULO I. CORRUPCIÓN DE PERSONAS MENORES DE DIECIOCHO AÑOS DE EDAD O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA COMPRENDER EL SIGNIFICADO DEL HECHO O DE PERSONAS QUE NO TIENEN CAPACIDAD PARA RESISTIRLO.
  - CAPÍTULO II Pornografía de Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen Capacidad para Resistirlo.
  - Capitulo II Acceso ilícito a sistemas y equipos de informática.
- Legislaciones a nivel estadal:
  - **ESTADO DE NUEVO LEÓN**: Prevé penas para los siguientes delitos: falsificación de títulos al portador, documentos de crédito público y relativos al crédito, la alteración de los medios de identificación electrónica de cualquiera de los objetos a que se refiere la, el acceso indebido a los equipos electromagnéticos de las instituciones emisoras de cualquiera de los objetos (adicionado con los artículos que lo integran, P.O. 28 de julio de 2004) el mismo texto legal prevé un título sobre los delitos por medios electrónicos adicionado, P.O. 28 de julio de 2004) que comprende conductas típicas tales como el acceso indebido a un sistema de tratamiento o de transmisión automatizado de datos (adicionado, P.O. 28 de julio de 2004); la supresión o modificación indebida

de datos contenidos en el sistema, o alteración del funcionamiento del sistema de tratamiento o de transmisión automatizado de datos (adicionado, P.O. 28 de julio de 2004); y la afectación o falsificación del funcionamiento de un sistema de tratamiento o de transmisión automatizada de datos.

- **ESTADO DE JALISCO:** Prevé la penalización de conductas relacionadas con **p**ornografía infantil, tales como inducir, obligar o entregar a una persona menor de dieciocho años de edad o que no tenga capacidad para comprender el significado del hecho, con o sin su consentimiento, para que realice o simule actos de exhibicionismo corporal, de naturaleza sexual o lasciva, con el fin de producir imágenes o sonidos de dichos actos a través de fotografías, filmes, videos, revistas o cualquier otro medio impreso, electrónico o tecnológico, con o sin ánimo de lucro; realizar materialmente la toma de fotografías, filmación, grabación de imágenes o sonidos, o cualquier otra actividad relativa con la producción o reproducción de las imágenes o sonidos a que se refiere la fracción anterior; emplear, dirigir administrar o supervisar a título de dueño, propietario, director, empresario o cualquier otro que implique la autoría intelectual de los actos señalados supra; o reproducir, vender, comprar, rentar, exponer, publicar, difundir o enviar por cualquier medio con o sin ánimo de lucro, las imágenes o sonidos señalados en anteriormente. La posesión de una o más fotografías, filmes, grabaciones o cualquier otro material impreso o electrónico, que contenga las imágenes o sonidos señaladas, cuando sea de su conocimiento el hecho de la posesión y de la minoría de edad de las personas que aparecen en las imágenes será también penalizada. Asimismo, se prevén castigos por REVELACION DE SECRETOS Y LA OBTENCIÓN ILÍCITA DE INFORMACIÓN ELECTRÓNICA y por Obtención Ilícita de Información Electrónica.
- **ESTADO DE COLIMA**: (REFORMADO P.O. 28 DIC. 2002). Este texto comprende penas para delitos relacionados con pornografía infantil mediante viodegrabaciones y fotografías difundidas por medios impresos y electrónicos; (REFORMADO, dec 404 30 de septiembre de 2003) el fraude electrónico, el uso indebido de Tarjetas y documentos de pago electrónico; (Reformada mediante decreto No. 193, aprobado el 19 de abril del 2005); el acceso indebido a los equipos y sistemas de computo o electromagnéticos; el Uso indebido de información confidencial o reservada de tarjetas, títulos, documentos o instrumentos para el pago de bienes y servicios o para disposición en efectivo. A quien obtenga un lucro en perjuicio del titular de una tarjeta, título, documento o instrumento para el pago electrónico de bienes y servicios o para la disposición de efectivo, mediante la utilización de información confidencial o reservada de la institución o persona que legalmente esté facultada para emitir los mismos.
- **ESTADO DE SINALOA**: 1992 – Decreto No 539 (artículo 217) Código penal del Estado de Sinaloa, artículo 217

  ARTÍCULO 356. Se impondrán de cien a doscientos días multa y prisión de uno a cinco años al funcionario partidista, precandidato o candidato que: (Ref. por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007)....XI. Sin autorización del Consejo Estatal Electoral contrate en medios electrónicos o prensa, por sí o por interpósita persona, propaganda electoral en los procesos electorales. (Adic. por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007).

  ARTÍCULO 358. Se impondrán de diez a cien días multa y prisión de seis meses a tres años, a quien:...XVII. Contrate propaganda electoral en medios electrónicos o prensa a favor o en contra de algún partido político, coalición o candidato; (Adic. por Decreto número 504, de 27 de marzo del 2007, y publicado en el P.O. No. 039 de 30 de marzo de 2007).

  ARTÍCULO 217. Comete delito informático, la persona que dolosamente y sin derecho:

  Use o entre a una base de datos, sistema de computadores 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; o

  Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

- México cuenta con un Grupo de Combate a Delitos Cibernéticos (DC México) y la Policía Cibernética, adscrita a la Policía Federal Preventiva

NICARAGUA

- ANTEPROYECTO DE LEY ESPECIAL SOBRE DELITOS INFORMATICOS que comprende los siguientes delitos Acceso indebido de datos; Alteración de documentos; Daño a datos o sistemas informáticos; Fraude informático; Espionaje informático; Difusión pornográfica de niños, niñas o adolescentes; Creación y distribución de virus informáticos y Violación de las comunicaciones. Abril 2005
- ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS PERSONALES. Abril 2005. Proyecto de Código Penal de la República de Nicaragua. Comisión de Justicia de la Asamblea Nacional. 24 de noviembre de 1999. El Proyecto prevé los siguientes Delitos vinculados a la información personal: Descubrimiento de correspondencia; Sustracción de papeles y desvío o supresión de correspondencia; Captación indebida de manifestaciones verbales; Registros prohibidos; Uso de información sin autorización. Los delitos CONTRA EL PATRIMONIO Y CONTRA EL ORDEN SOCIOECONOMICO han sido tipificados como Destrucción de registros informáticos; Programas destructivos; y Alteración de programas. Los Delitos contra la propiedad intelectual son: la Reproducción ilícita; la Protección del programa de computación y la Manipulación de información. La Revelación de secretos de empresa ha sido catalogado por este proyecto como un delito vinculado al mercado y la intrusión ha sido clasificada como un delito que comprometen la Paz dentro del Título relacionado con los DELITOS CONTRA LA SEGURIDAD DEL ESTADO.[20]

PANAMA

- **Código Penal.**
  Trata Sexual, Turismo Sexual y Pornografía con Personas Menores de Edad
  Art. 231-D.: Quien fabrique, elabore o produzca material pornográfico o lo ofrezca, comercie, exhiba, publique, publicite, difunda o distribuya a través de Internet o cualquier medio masivo de comunicación o información nacional o internacional, presentando o representando visualmente a una o varias personas menores de edad en actividades de carácter sexual, sean reales o simuladas, será sancionado con prisión de 4 a 6 años y con 15O a 200 días — multa.
  Art. 231-E.: Quien utilice a una persona menor de edad en actos de exhibicionismo obsceno o en pornografía, sea o no fotografiada, filmada o grabada por cualquier medio, ante terceros o a solas, con otra u otras personas menores de edad o adultos, del mismo o de distinto sexo, o con animales, será sancionado con prisión de 4 a 6 años y con 150 a 200 días multas. Igual sanción será aplicada a quien se valga de correo electrónico, redes globales de información o cualquier otro medio de comunicación individual o masiva, para incitar o promover el sexo en línea en personas menores de edad, o para ofrecer sus servicios sexuales o hacer que lo simulen por este conducto, por teléfono o personalmente.
  Delitos Financieros Artículo 393-A. Quien en beneficio propio o de un tercero, mediante la utilización de medios tecnológicos u otras maniobras fraudulentas, se apodere, haga uso indebido u ocasione la transferencia ilícita de los dineros, valores,

[20] GLIN-Nicaragua-CORTE SUPREMA DE JUSTICIA, NICARAGUA BANCO INTERAMERICANO DE DESARROLLO, BANCO INTERAMERICANO DE DESENVOLVIMENTO, "**LEGISLACIÓN NICARAGUENSE ANTE LOS DELITOS INFORMATICOS".** Noviembre, 2005. Managua, Nicaragua.

bienes u otros recursos financieros de una entidad bancaria, empresa financiera u otra que capte o intermedie con recursos financieros del público o que le hayan sido confiados a ésta, será sancionado con prisión de 3 a *5* años.

PARAGUAY

- Ley Nº 1160/1997 contentiva del Código Penal de la República del Paraguay, Artículos 174, 175, 188, 249.
  http://www.leyes.com.py/todas_disposiciones/1997/leyes/ley_1160_97.htm

PERU

- Proyecto de Ley Nº 1318/2007/CR. La penalización de los delitos informáticos, cuya finalidad es proteger y privilegiar la confiabilidad puesta en la informática, fue propuesta mediante un proyecto de ley en el Congreso de la República. Se trata de reprimir cualquier comportamiento antisocial que amenace o atente contra sistemas que utilizan tecnología de la información, así como contra la propiedad, la privacidad de las personas y de las comunicaciones, y contra el orden económico. El proyecto propuesto por la Célula Parlamentaria Aprista busca llenar vacíos existentes en la penalización de los delitos informáticos para combatir conductas delictivas que se producen en el país. Por ello se propone sanciones que incluyen penas privativas de la libertad de entre uno y diez años, las cuales pueden ser incrementadas según los agravantes del caso. Entre los delitos por sancionarse en cuanto al uso de tecnología de la información están el acceso indebido, sabotaje o daño a sistemas protegidos y espionaje informático, entre otros. En cuanto a los atentados contra la propiedad están los delitos de hurto informativo, fraude informático, manejo fraudulento de tarjetas inteligentes, apropiación de tarjetas inteligentes, etc. Entre los delitos contra la privacidad de las personas y las comunicaciones están la violación de la privacidad de la data o información de carácter personal, violación de la privacidad de las comunicaciones, y revelación indebida de data o información personal. Respecto a los delitos contra el orden económico están la apropiación de propiedad intelectual y el de la oferta engañosa. El Proyecto contempla también la penalización de diversos delitos vinculados con la tecnología y la informática, como fraudes y hurtos electrónicos, y el uso indebido de tarjetas de crédito y medios de pagos virtuales. El proyecto pasó a las comisiones de Justicia y Derechos Humanos, y de Defensa del Consumidor y Organismos Reguladores de los Servicios Públicos, para su correspondiente dictamen.

- 2004: Ley No. 28.251 sobre Pornografía Infantil
- 2000: Ley Nº 27.309 sobre incorporación de los delitos informáticos en el Código penal
  "CAPÍTULO XDELITOS INFORMÁTICOS
  Artículo 207-A.- Delito Informático
  El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas.
  Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.
  Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras
  El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207-C.- Delito informático agravado
En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:
1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional." (*)
(*) Capítulo incorporado por el Artículo Unico de la Ley Nº 27309, publicado el 17-07-2000.

- 1996: Decreto legislativo No 681 modificado por Ley No 26.612 Norma sobre delitos informáticos
- Perú cuenta con una Brigada de Delitos Tecnológicos (BIT) de la Comisaría General de Policía Judicial

VENEZUELA

- 2001: Decreto No 48, Ley especial de delitos informáticos Norma sobre delitos informáticos publicada en Gaceta Oficial N° 37.313 del 30 de Octubre 2001
  La violación de la privacidad de la data o información de carácter personal tiene una pena que va desde los dos años de prisión, para quien incurra en ese delito, según aparece estipulado en la Ley Especial. El texto contempla que "toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o la información personales de otro, que estén incorporadas en un computador, será penada con prisión de dos años a seis años y multa de doscientas a seiscientas unidades tributarias". Como agregado aparece que "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. En cuanto a la revelación indebida de data o información de carácter personal, se indica que la pena estipulada en el artículo anterior aumentará a un tercio de la mitad "si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare en perjuicio para otro".
  El comisario Pedro Juárez, jefe del CICPC-Zulia, indicó que "en caso de encontrar los CD con las bases de datos en el mercado negro, tanto las personas que los vende, como el propietario del local de donde se logró la distribución, serán detenidos por la comisión de un delito".[21]
- Gaceta Oficial No. 38.529 de fecha 25 de septiembre de 2006 mediante la cual se publica la LEY PARA LA PROTECCIÓN DE NIÑOS, NIÑAS Y ADOLESCENTES EN SALAS DE USO DE INTERNET, VIDEOJUEGOS Y OTROS MULTIMEDIAS de fecha 1ro de Agosto de 2006, entró en vigencia en fecha 25 de marzo de 2007 y tiene por objeto Garantizar a todos los niños, niñas y adolescentes el ejercicio y disfrute pleno y efectivo de sus derechos humanos a una información adecuada que sea acorde con su desarrollo integral y a la salud, en el uso, alquiler, compra, venta y permuta de juegos computarizados, electrónicos o multimedia, especialmente en salas de Internet; Promover el uso adecuado de los servicios de Internet con fines educativos, recreativos y para la libre comunicación entre las personas y favorecer la participación de las familias, organizaciones sociales y personas en general en la protección integral de los niños, niñas y adolescentes.
  Artículo 8.—…Sin embargo, está prohibido el acceso a información y contenidos que promuevan, hagan apología o inciten a la violencia, a la guerra, a la comisión de hechos punibles, al racismo, a la desigualdad entre el hombre y la mujer, a la xenofobia, a la intolerancia religiosa y cualquier otro tipo de discriminación, a la esclavitud, a la servidumbre, a la explotación económica o social de las personas, al uso y consumo de cigarrillos y derivados del tabaco, de bebidas alcohólicas y demás especies previstas en la legislación sobre la materia y de sustancias estupefacientes y psicotrópicas, así como aquellos de carácter pornográfico, que atenten contra la seguridad de la Nación o que sean contrarios a los principios de una sociedad de democracia revolucionaria…Está prohibido que las personas en general tengan acceso

[21] Panorama. "Pena de seis años para el clonador". 04 de Diciembre de 2006.

a pornografía de niños, niñas o adolescentes, así como a información que promueva o permita su abuso o explotación sexual.

- En el caso de la "negación del servicio" (DoS), sería sin duda un ataque a los medios de telecomunicación, delito ya previsto y sancionado en la Ley Orgánica de Telecomunicaciones de Venezuela... es como varias veces han repetido en los diversos correos: "cortar un cable" o "tumbar un poste"... si alguien realiza eso y nos afecta la tv por cable o el teléfono, nadie alegaría un delito informático, ni se realizarían metáforas con objetos jurídicos tan antiguos como la "propiedad".... simplemente, con figuras como sabotaje o daños... Recuérdese que la Internet es la vía para realizar todos los servicios asociados a ese medio de comunicación (emailto; www; etc).... partiendo de la hipótesis que nadie niega dicha condición a la tecnología que estamos estudiando. Por ejemplo, en Venezuela, para poder ser un ISP, necesitas obtener una habilitación ante Conatel (Comisión Nacional de Telecomunicaciones)... si eso, es igual en otros países, la respuesta en la afección de estos medios, sería la legislación de telecomunicaciones.[22]

2.2. L'AFRIQUE

AFRICA DEL SUR

- **Firmó la Convención de Budapest**
- **South Africa – Computer Misuse Act, Proposed.** Michael Masters. June 14, 2001

BOTSWANA

NIGERIA

- In summary, the Draft Nigerian Cybercrime Act provides the legal framework for the establishment of an Independent Cybercrime Agency and for the legislation concerning Cybercrime and Cyber-Security. Basically, the Draft Nigerian Cybercrime Act was divided into eight different sections namely:
  - Preliminary,
  - Offenses,
  - Protection & Security of Critical Information And Communication Infrastructure,
  - Ancillary and General Provisions,
  - Cybercrime & Cybersecurity Agency Establishment Of The Cybercrime Agency, Etc,
  - Functions and Powers of The Agency,
  - Management and Staff Of The agency,
  - Financial Provisions.

ZAMBIA

- An Internet crime Bill has been enacted by the Parliament, and is expected to be signed by the President before the end of 2004.
  According to this Computer Misuse and Crimes Law, convictions of computer hackers

[22] Abogado venezolano Fernando Fuentes (ffve@yahoo.com). Miembro de la Mailing List Alfa-Redi. Correo electrónico de fecha 25 de Julio de 2007.

and other offenders may result in sentences ranging from 15 to 25 years.
http://www.cybercrimelaw.net/laws/countries/zambia.htm

3. La cooperación internacional

Observadas como han sido las legislaciones nacionales de diferentes países del continente americano, conviene llamar la atención sobre la Convención de Budapest sobre Cybercrimen[23].

La Convención de Budapest establece los puntos básicos necesarios que permite a los países avanzar armoniosamente en el mismo sentido: delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y los datos informáticos; delitos estrictamente informáticos; delitos relativos al contenido; y, delitos relativos a la violación de derechos de autor y sus derechos afines. Además prevé aspectos procesales que son fundamentales, como la retención de información de tráfico y el acceso en tiempo casi real a esa información.[24]

En Octubre de este año de 2007, jefes y expertos de las unidades nacionales de lucha contra la delincuencia informática de 15 países miembros europeos se reunieron en la Secretaría General de INTERPOL para debatir sobre la Delincuencia Relacionada con la Tecnología de la Información, y en particular, sobre el examen forense de datos dinámicos, que permite la recuperación de pruebas en ordenadores en funcionamiento; los *botnet*; y las herramientas y técnicas destinadas a la investigación de la delincuencia informática. Una de sus principales actividades de este grupo de trabajo es la redacción del *Information Technology Crime Investigation Manual* (manual para investigadores especializados en delincuencia relacionada con la tecnología de la información), una guía de buenas prácticas para uso de los investigadores.[25] El precitado Manual comprende disposiciones sobre los medios de pago electrónicos a través de transacciones electrónicas seguras; la manipulación de la red de comunicaciones pública, el fraude con uso de las telecomunicaciones y los esquemas de hacking; las amenazas criminales contra el comercio electrónico y cómo realizar transacciones seguras; herramientas y técnicas utilizadas para realizar investigaciones sobre delitos cometidos con uso de la tecnología de la información y el desarrollo de un manual de investigaciones en Internet basado sobre la experiencia práctica.[26] El proyecto dará explicaciones sobre la tecnología VoIP, servicios disponibles de VoIP, la comunicación entre computadoras vía VoIP, y cómo investigar casos criminales en los que esté envuelta esta tecnología.

La Organización de Estados Americanos (OEA) propuso a sus Estados Miembros evalúen la conveniencia de la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética (2001) y que consideren la posibilidad de adherirse a dicha Convención. Asimismo les sugirió examinen y, si corresponde, actualicen, la estructura y la labor de entidades u organismos internos encargados de hacer cumplir las leyes, de modo de adaptarse a las cambiantes características de los delitos cibernéticos, incluso examinando la relación entre los organismos que combaten ese tipo de delitos y los que proporcionan la asistencia policial o judicial mutua tradicional.[27]

La OEA cuenta con una La Red Hemisférica de Intercambio de Información para la Asistencia Mutua en Materia Penal y Extradición ("la Red") que se viene formando desde 2000, cuando la Tercera Reunión de Ministros de Justicia o Procuradores Generales de las Américas (REMJA-

---

[23] Les Ministres ou leurs représentants des 26 Etats membres suivants ont signé le traité : Albanie, Arménie, Autriche, Belgique, Bulgarie, Croatie, Chypre, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Italie, Moldova, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Espagne, Suède, Suisse, " l"ex-République yougoslave de Macédoine ", Ukraine et Royaume-Uni. En outre, le Canada, le Japon, l'Afrique du Sud et les Etats-Unis, qui ont participé à son élaboration, ont également signé la Convention.

[24] Abogado Carlos Alvarez (carlosalvarezc@gmail.com). Miembro de la Mailing List Alfa-Redi. Correo electrónico de fecha 23 de Julio de 2007.

[25] INTERPOL. "Especialistas europeos celebran la 50a reunión sobre la lucha contra la delincuencia informática". 02 de octubre de 2007

[26] Adduci, Massimo. "L'impegno dell' Interpol alla lotta contro IT-Crime". Cybercrimes. Computer Forensics & Crimine informatico. Cybercrimes.it

[27] AG/RES. 2040 (XXXIV-O/04). REUNIÓN DE MINISTROS DE JUSTICIA O DE MINISTROS O PROCURADORES GENERALES DE LAS AMÉRICAS. (Aprobada en la cuarta sesión plenaria, celebrada el 8 de junio de 2004). Organización de Estados Americanos.

III) decidió incrementar y mejorar el intercambio de información entre los Estados miembros de la OEA en la esfera de la asistencia mutua en materia penal. Esta Red viene siendo utilizada por extensión a la materia relacionada con los delitos informáticos.

En el seno de la OEA se continúa fortaleciendo la cooperación con el Consejo de Europa con el fin de facilitar que los Estados Miembros de la OEA consideren la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética y la adhesión a ésta, así como la adopción de las medidas legales y de otra naturaleza que sean necesarias para su implementación. Asimismo, se continúan fortaleciendo los mecanismos que permitan el intercambio de información y la cooperación con otras organizaciones e instancias internacionales en materia de delito cibernético, tales como las Naciones Unidas, la Unión Europea, el Foro de Cooperación Económica del Pacífico Asiático, la Organización para la Cooperación y el Desarrollo Económico (OCDE), el G-8, el Commonwealth y la INTERPOL, de manera que los Estados Miembros de la OEA puedan aprovechar los desarrollos dados en dichos ámbitos.[28]

Latin America Working Party on Information Technology Crime. The aims of this Working Party are: Cooperation, sharing of knowledge and practical experience among INTERPOL member countries and other International Organizations dealing with High-Tech Crime. Promotion of standardization of methods and working proceedings to combat efficiently cyber crime. Establishment of good practice guidelines

El Interpol Working Party on IT Crime – ASP (ASPWP) sostuvo en este mes de noviembre el 9th meeting in Bali, Indonesia
As for the Projects, participant agreed to begin the new projects such as 'Investigative Reference Project' for gathering the legislation information to mutual assistance on the field of investigation faster, '3G Project' to share the knowledge about the 3 Giga Hz technology and 'Mobile Phone Forensic Project' to find the method to do forensic for various types of Mobile Phone. As for the Projects, participant agreed to begin the new projects such as 'Investigative Reference Project' for gathering the legislation information to mutual assistance on the field of investigation faster, '3G Project' to share the knowledge about the 3 Giga Hz technology and 'Mobile Phone Forensic Project' to find the method to do forensic for various types of Mobile Phone.

Train-the-Trainer Workshop on Information Technology Crime Investigation for ASP (TTI) **o**bjectives: In October 2003, 5th Interpol Asia and South Pacific Working party on Information Technology crime agreed to hold the 'Train-the-Trainer Workshop on Information Technology Crime Investigation' annually, in order to provide a training opportunity cheaply to increase the number of Information Technology Crime investigators in Asia and South Pacific region.

INTERPOL Secretary General Ronald K. Noble highlighted the need for an active and dynamic partnership between national police forces in the region, INTERPOL's General Secretariat and its Sub-Regional Bureau for West Africa in Abidjan, Côte d'Ivoire, which also serves as West African Policy Chief Committee (WAPCCO)'s secretariat.[29]

Le African Regional Working Party on Information Technology Crime acordó trabajar en pro de los siguientes objetivos: desarrollar y poner a disposición experticia para combatir los delitos de tecnología de la información en la región; desarrollar y estrechas lazos con organizaciones que trabajan en materia de delitos IT y establecer, coordinar y promover el uso de las mejores prácticas de investigación y prevención del crimen IT. Lo anterior, acompañados del deber de incrementar el flujo de información em las Unidades de Delitos Informáticos de la región y promover procedimientos operacionales de armonización en la región. Siguiendo los pasos del grupo Interpol Working Party on Information Technology Crime – Africa, se acordó manejar

[28] AG/RES. 2228 (XXXVI-O/06). REUNIÓN DE MINISTROS DE JUSTICIA O DE MINISTROS O PROCURADORES GENERALES DE LAS AMÉRICAS (Aprobada en la cuarta sesión plenaria, celebrada el 6 de junio de 2006) Organización de Estados Americanos.
[29] INTERPOL MEDIA RELEASE. "West African police chiefs urged to adopt common approach to fight crime". 03 de Octubre de 2007

programas de concienciación para la alta gerencia de países africanos y organizaciones de policía regional.[30]

Dans le ICT Best Practices Forum organisé par l'African Development Bank à Ouagadougou, Burkina Faso le 7-9 June 2007 a été adopté le Draft Ouagadougou Declaration dans lequel l'adoption des lois pour lutter contre les delits informaitques est demandee.

Le Forum sur la gouvernance d'Internet abordant des sujets aussi variés comme les délits informatiques a été organisé par le Centre sur la politique internationales des TICs Afrique du Centre et de l'Ouest (CIPACO)

The ITU Secretary-General Dr Hamadoun Touré set out a comprehensive *Global Cybersecurity Agenda* to tackle the issue within a framework of international cooperation. "With more than one billion Internet users in the world today, not only is the number of crimes committed in cyberspace increasing at an alarming rate, but the sophistication in the way these crimes are committed keeps evolving," Dr Touré said.
The goal of the Agenda is to foster a common understanding of the importance of cybersecurity and bring together all relevant stakeholders (governments, intergovernmental organizations, the private sector, and civil society) to work on concrete solutions to deal with cybercrime.[31]

Five Pillars of the ITU Global Cybersecurity Agenda
1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structures
4. Capacity-Building
5. International Cooperation

Legal Measures, **Technical and Procedural Measures** and **Organizational Structures** need to be undertaken at the national and regional levels but also harmonized at the international level. The last two pillars, **Capacity-Building** and **International Cooperation**, are cross-cutting in all areas. In order to carry out its agenda, ITU will fully engage its Member states and all the world's players in its activities. It will collaborate closely with its partners to identify current challenges, consider emerging and future threats, and propose global strategies to meet the goals of the Agenda. The Global Cybersecurity Agenda will facilitate the implementation of activities aimed at meeting ITU Strategic Goal in this domain by developing and proposing forward-looking global strategies using a wide range of expertise and taking account of existing initiatives.[32]
The UN Economic Commission for Africa (UNECA), supported ECOWAS and UEMOA in West Africa to develop the following harmonized regulatory guidelines on ICT and electronic commerce for adoption by Member States: Guidelines on a harmonized ICT framework; Guidelines on e-commerce; Guidelines on personal data protection; and Guidelines on fighting against cybercrime at the Connect Africa Summit held in October 2007 in Kigali, Rwanda.[33]

SHARING INFORMATION FOR PROMOTING GLOBAL CYBERSECURITY[34]:

[30] INTERPOL Regional Working Parties

[31] ITU. "World Telecommunication and Information Society Day ceremony honours three laureates, Three Major announcements made to curb cybercrime, connect Africa and connect the young". Geneva, 17 May 2007

[32] Cybersecurity Gateway, an ITU's initiative.

[33] ITU. "Creating an Enabling Environment for Investment Background Paper – Session Five". Connect Africa Summit 29-30 October 2007 Kigali, Rwanda 17 October 2007 .

[34] ITU. Cybercrime Gateway website.

- Organización de Cooperación y Desarrollo Económico

Asia-Pacific Economic Cooperation

- Organización de Estados Americanos
- European Network and Information Security Agency
- League of Arab States
- Union Africaine
- Unión Internacional de Telecomunicación

3. Les cas pratiques

ARGENTINA

AÑO	CASO
2006	La investigación sobre el espionaje contra las cuentas de correo electrónico (e-mail) de políticos y periodistas realizado durante el último fin de semana puede quedar en la nada, al igual que muchas otras causas por hechos similares: ocurre que en la Argentina no existen penas específicas para los delitos informáticos ni técnicas adecuadas para perseguir esos crímenes, manifestaron especialistas en la materia –y, en forma reservada, jueces y fiscales, que alertaron sobre el riesgo de que la Argentina pueda transformarse en un virtual "paraíso informático". "En materia penal, la laguna jurídica es insalvable, toda vez que no hay norma que tipifique como delito la violación de la correspondencia electrónica y tampoco se permite aplicar de manera analógica otra norma parecida", consideró el vicepresidente de la Comisión de Sistemas, Medios de Comunicación y Libertad de Expresión del Senado.[35]
2003	El caso se produjo en la agencia Young & Rubicam entre mediados de 1999 y principios de 2000 cuando sus sistemas operativos fueron invadidos de virus Mail Bomber y Vaninna enviados por un exempleado. Enviar virus a través del correo electrónico y provocar, por ejemplo, que se caiga toda una red informática no es delito. Lo estableció un fallo de la Cámara Federal Argentina, al sobreseer a un ex creativo de una agencia de publicidad que hizo colapsar deliberadamente los sistemas de su empleador. La decisión judicial admite que su conducta ocasionó "pérdida de tiempo" y "perjuicios económicos"; pero puntualiza que la figura del daño, por la cual este empleado había sido procesado en un principio[36], sólo puede verificarse cuando alguien le "destruya o inutilice" a un tercero una cosa mueble, inmueble o un animal. La Sala I de la Cámara concluyó que "la afectación de un sistema informático no cae bajo ningún tipo de sanción penal".
2002	Tribunales de Comodoro Py. el juez federal Sergio Torres, había sobreseído a un hacker que se introdujo en el sitio Web de la Corte Suprema Argentina y reemplazó las sentencias del máximo Tribunal del país por consignas en favor de las Madres de Plaza de Mayo. En aquella resolución, Torres destacó que esa intrusión, además de no estar sancionada expresamente por ninguna norma legal, no había provocado ningún daño. Sostuvo además que un sitio de Internet es algo inmaterial. "Una página web no puede asimilarse al significado de cosa. Ello es así, en tanto y en cuanto por su naturaleza no es un objeto corpóreo ni puede ser detectado materialmente".
1999	"Existe un precedente jurisprudencial que equiparó la violación de un e-mail a la violación de una carta, pero es un caso aislado.
Desconocido	En un caso de escuchas telefónicas descubrieron que el espionaje se hacía desde el exterior, a través de satélites. Un Fiscal argentino explicó que "La justicia penal argentina no puede dar ninguna respuesta a este hecho".
Desconocido	En el caso de Jujuy.com el juez decidió que la página web si es una "cosa", bien jurídico protegido por el derecho, contrariamente a la decisión de 2002.

AUSTRALIA

[35] La Nación. "Espionaje a políticos y periodistas. No hay castigo para los delitos informáticos. Jueces y expertos advierten que existe un "vacío legal"" Mayo de 2006. Argentina

[36] En 2002 un magistrado procesó por daño a este ex empleado que había enviado un mail spam con virus a la Agencia de publicidad en la que trabajaba. La Sala II de la Cámara Federal confirmó el procesamiento.

2006 (March). *Seventy five percent of Australian CIOs who spoke to IBM perceive that threats originate internally compared to a global benchmark, based on a total of 17 countries, of 66%. According to the IT executives surveyed, 49% of local businesses now perceive cybercrime to be a greater threat than physical crime to their business. At the same time, the perception is that perpetrators of cybercrime are becoming increasingly sophisticated; 80% of Australian CIOs (84% globally) believe that lone hackers are increasingly being replaced by organised and technically proficient criminal groups. When it comes to relative costs, Australian CIOs think that cybercrime has a more detrimental financial impact on their business than physical crime. They are most concerned about the loss of current customers as a result of cybercrime (71%), followed by loss of revenue (68%) and loss of prospective customers (67%). Just 38% of their global peers identified loss of prospective customers as a major concern, possibly reflecting the smaller size of the Australian market and relative importance of each customer. Significant numbers of Australian CIOs also pointed out the 'administrative' losses from cybercrime such the costs of investigating the breach (41%), notifying customers and suppliers (31%), and legal fees (18%).*[37]

BRASIL

2006 (Feb.) La policía federal brasileña detuvo en la ciudad norteña de Campiña Grande y en varios Estados circundantes a 55 personas -nueve, menores- por insertar en los ordenadores de incautos brasileños detectores de pulsaciones que registraban lo que éstos tecleaban cuando visitaban sus bancos en Internet. Los diminutos programas devolvían los nombres de usuario y las contraseñas a la banda. Según la policía brasileña, el fraude ascendió a unos 4,7 millones de dólares procedentes de 200 cuentas diferentes en seis bancos desde mayo. El objetivo de estos delincuentes es infectar los ordenadores de la misma forma que los virus. La diferencia es que los programas detectores de pulsaciones explotan los fallos de seguridad y controlan la senda que envía los datos del teclado a otras partes del ordenador. Es un sistema más agresivo que la pesca, más basada en la impostura que en la infección, y que engaña a la gente para que dé su información a un sitio de Internet falso.[38]

CHILE

AÑO	CASO
2007 (Nov.)	Hackean GobiernodeChile.cl: Hasta esta hora (21:00) sigue modificado el Sitio web de la Presidencia de Chile. Según informes de Canal 13, la portada fue modificada con imágenes alusivas a Perú, mientras que el personero de Gobierno, director de Política Exterior, minimizó el hecho señalando que hasta el sitio de la White House de E.E.U.U. ha sido atacado, pero que a días de la Cumbre Iberoamericana se reforzará la seguridad de los sistemas informáticos del gobierno. A esta hora sólo existe un banner que señala “estamos trabajando para usted”.[39]
2007 (May)	Dos piratas informáticos chilenos que intervinieron de manera ilegal sitios web privados, estatales e incluso internacionales, como la de la agencia espacial de Estados Unidos (NASA) fueron condenados a una pena de tres años de cárcel, que cumplirán en sus casas actividades. Los acusados aprovechando sus conocimientos en materia de computación procedieron a interferir en diversos sistemas de tratamiento de información, específicamente páginas web. La sentencia emana del Tercer Tribunal de Juicio Oral en lo Penal de Santiago, donde enfrentaron cargos en el delito reiterado de sabotaje informático, tras acreditarse su responsabilidad en los hechos, de acuerdo a lo establecido en la Ley de Delitos Informáticos, además del pago de las costas del juicio y de una multa de 2.845 euros, por los daños

[37] iTWire. “Cybercrime worse than physical crime for Australian business”. 13 de Marzo de 2006.

[38] El País.com “Los ciberladrones copian en silencio todo lo que se teclea. Programas de rastreo fáciles de usar permiten a los ladrones informáticos robar contraseñas y números de cuentas bancarias”. TOM ZELLER Jr. para NYT 09/03/2006

[39] Posted by Rodrigo Guaiquil. Chile.

	causados a la cadena de televisión chilena privada.

COLOMBIA

Año 2000. Con la colaboración de la Universidad de los Andes, de la Dirección de Tecnologías de Información (DTI) y la Oficina Jurídica de la Universidad, tras una investigación iniciada por la Fiscalía y el CTI, se logró la captura de un estudiante que se encontraba extorsionando a un familiar cercano a través de correos electrónicos amenazantes.

E.E.U.U.

AÑO	CASO
2007 (Junio)	Robert Alan Soloway, de 27 años, está en prisión sin fianza tras haber comparecido esta semana ante un tribunal de distrito de Estados Unidos. Soloway ha sido acusado por un jurado federal de 35 cargos, entre los que están fraude en el correo, en las comunicaciones, en relación con el correo electrónico, robo de identidad agravado y blanqueo de dinero. Soloway es el primer 'spammer' -emisor de correos basura- acusado en Estados Unidos de robo de identidad agravado de acuerdo con la Ley CAN-SPAM, del 2003. Los fiscales federales lo llaman el "rey del spam" por haber enviado supuestamente cientos de millones de correos basura a través de redes secuestradas.[40]
2007 (Mayo)	Siete personas y las compañías CurrenC Ltd. de las Islas Vírgenes Británicas, Gateway Technologies y Hill Financial Services con sede en UTA y la canadiense que posee el sitio de apuestas BetUS fueron acusadas con cargos de conspiración por violar la prohibición estadounidense sobre apuestas en Internet, que hacían ocultando los cargos de las tarjetas de crédito. La acusación de 34 cargos emitida en Salt Lake City, Utah, establece que los acusados armaron un plan para burlar una ley aprobada el año pasado que prohíbe a los bancos de Estados Unidos y las compañías de tarjetas de crédito procesar apuestas en Internet. La acusación establece que los acusados facilitaron el pago de más de 150 millones de dólares (más de 110 millones de euros) a sitios de apuestas en Internet violando la prohibición estadounidense sobre apuestas online.[41]
2006 (Agosto)	The following are the key findings of a study on network attacks: Average financial loss was more than $3M per case; Individual attacks caused as much as $10M in damages to individual organizations; Organizations suffered the greatest financial loss and damage, more than $1.5M per occurrence, when attackers used stolen IDs and passwords; Largest damages to organizations caused by attackers logging onto privileged user or administrator accounts where a small number of authorized computers were sanctioned to perform work; Most crimes, 84 percent, could have been prevented if the identity of the computers connecting were checked in addition to user IDs and passwords; Losses from stolen IDs and passwords far exceeded damages from worms, viruses, and other attack methods not utilizing logon accounts; Vast majority of attackers, 78 percent, committed crimes from their home computers; and most often using unsanctioned computers with no relationship to the penetrated organization[42]
2006 (Marzo)	El fiscal de Nueva York demandó a Gratis Internet por de vender información personal, tal como sus correos electrónicos, obtenida de millones de consumidores a pesar de su promesa de confidencialidad, en violación de las normas de privacidad a tres empresas independientes. En este caso, Datran Media, de Nueva York, dedicada al mercadeo del correo electrónico, fue acusada de utilizar información

[40] Reuters. "Primer arresto podría frenar correo basura en internet: ejecutivo**". 1ero de Junio de 2007.**

[41] IBLNEWS, AGENCIAS. "Siete personas acusadas por apuestas ilegales en Internet en EEUU" . 12 de Mayo de 2007.

[42] Trusted Strategies LLC. "Network Attacks: Analysis of Department of Justice Prosecutions 1999 – 2006". www.trustedstrategies.com, California, USA. 28 August 2006.

	personal recopilada por otras empresas de unos seis millones de direcciones electrónicas de todo el país.[43]
2006 (Marzo)	La minería de datos ya se utiliza en toda una serie de aplicaciones comerciales, ya sean compañías de tarjetas de crédito que detectan y evitan el fraude en cuanto se producen, o aseguradoras que predicen riesgos sanitarios. Millones de estadounidenses forman parte de una extensa, y cada vez más, red de datos. Para detectar actividades ilícitas, es necesario activar centinelas informáticos que examinen todos los comportamientos digitales, inocentes o no. Pero "cada vez que una herramienta o un humano mira el contenido de tus comunicaciones, viola tu privacidad". La controversia sobre la búsqueda de datos gira en torno al uso, amplio y secreto, que el Gobierno hace de ellos. Después de los atentados contra las Torres Gemelas, el potencial para analizar inmensas bases de datos tuvo como consecuencia la creación de un programa llamado Total Information Awareness (Conocimiento Total de la Información), hoy en día utilizado únicamente para el procesamiento, análisis y colaboración del espionaje antiterrorista en el extranjero". La Agencia de Seguridad Nacional ha invertido miles de millones en herramientas informáticas para controlar llamadas en todo el mundo –registrando no sólo su existencia, sino también su contenido- y más recientemente en intentar diseñar métodos digitales para obtener información de la Red.[44]
2005	Rafael Núñez, hacker venezolano, empleado de una empresa de telecomunicaciones de su país, ex-miembro del grupo de hackers World of Hell que funcionó durante el año de 2001, fue arrestado en Estados Unidos por cargos contra la seguridad nacional de ese país (Fuerza Aérea). Estuvo en prisión durante nueve meses, tras casi tres años de juicio y se le dio una restricción de entrada a Estados Unidos por 10 años.
2005	Protección de datos versus Derecho a la Información. Yahoo estuvo en una batalla legal con el padre de un soldado americano, Justin Ellsworth, fallecido en Irak, quien solicitó a Yahoo le deira acceso a la cuenta de correos de su hijo. En este juicio se debatía a quién pertenecen los mensajes de correo electrónicos escritos, una vez que su autor ha fallecido. Yahoo alegaba que debía respetarse las cláusulas del servicio que se firman antes de abrir una cuenta de correo electrónico en Yahoo. El acuerdo dice que "la cuenta de Yahoo es intransferible y los derechos…a acceder sus contenidos...terminan con su muerte". El padre venció la batalla al obtener una orden judicial que obligaba a Yahoo a hacer entrega del contenido de la cuenta de correos de su hijo Justin para el momento de su fallecimiento.[45]
2004 (Agosto)	Según fuentes de la CNN el pasado jueves se detuvieron más de cien personas por delitos relacionados con Internet, desde la usurpación de identidad hasta ataques sobre ISPs. El detonante de esta operación han sido las más de 150.000 víctimas de fraude en Internet que en su conjunto sufrieron una pérdida de más de 218 millones de dólares. No obstante según otras fuentes procedentes de organismos norteamericanos se cree que el coste a los estadounidenses por los delitos informáticos se elevan a más de 50.000 millones de dólares anuales.
2001	*In the 2001 US v. Gorshkov case, the hackers employed a wide array of distributed Perl scripts that transcend across national boundaries to trigger massive numbers of coordinated online auctions, email confirmations, and other fake transactions to accomplish fraudulent electronic fund transfers on numerous stolen credit card records. Under such a reality, the foremost daunting challenge is the discovery and collection of voluminous and often globally distributed digital evidence.*[46]
Sin fecha	Derecho a la Información versus Protección de Datos personales. Si vive en USA y quiere chequear el tipo de vecinos que lo circundan visite www.familywatchdog.us.

[43] Libertad Digital. "El fiscal de Nueva York demanda a una empresa por vender millones de direcciones electrónicas de sus clientes" 24 de Marzo de 2006.

[44] El País. "La vigilancia electrónica pone en peligro las libertades civiles". JOHN MARKOFF - Palo Alto 09 de Marzo de 2006

[45] The Internet Patrol. "Yahoo Gives Slain Marine's Family Access to Their Son's Email", Website mantenido por el Institute for Spam and Internet Public Policy, 24 de Abril de 2005.

[46] Evonne & Ralph's Weblog, De "Digital Evidence Collector"… "Systematic Approaches to Digital Forensic Engineering…" September 7, 2005

	Ejemplo: en el área en la que están las oficinas principales de Google USA aparece en el mapa un cantidad de 165 offenders plenamente identificados y otros 102 que no pueden ser mapeados; al hacer click en cualquiera de los offenders se obtiene la información siguiente: foto del rostro a color, Nombre completo, Dirección de habitación, Distancia del punto de referencia, Motivos por los cuales ha sido sentenciado; Fuente de la información, Descripción del ofender y Señas especiales, Mapa Google que lleva exactamente a la ubicación del lugar donde vive.

ESPAÑA

AÑO	CASO
2007 (Oct.)	La Organización de Consumidores y Usuarios (OCU) ha detectado algunas irregularidades en las ventas por Internet, tales como el cobro de gastos inesperados, páginas no seguras, "roturas de stock" o facturas incorrectas. Seis de los 20 comercios on line más visitados por los españoles reciben un suspenso por no entregar la mercancía pedida o el importe de la devolución solicitada. Tras las irregularidades detectadas en se aconseja a los consumidores desconfiar de las tiendas que omiten las informaciones exigidas por la ley y comprobar la información relativa a las condiciones de venta, entrega y gastos de envío, asegurarse de que las páginas en las que se dejan datos son seguras, repasar siempre la cantidad a pagar, conservar toda la información contractual, revisar el paquete a la llegada y exigir siempre una factura detallada. Además, según la OCU la publicidad de las tiendas on line no se ajusta a la realidad ya que el plazo de entrega de cinco días no se respetó en ninguno de los casos, tardando más de 40 días en recibir los productos. El objetivo de la OCU es denunciar que quedan muchos aspectos por mejorar como cumplir los plazos de entrega, permitir un ejercicio normal de la garantía y ofrecer más información y de mayor de calidad.[47]
2007 (Mayo)	El Centro de Mando Antifraude (AFCC) de la compañía de seguridad RSA ha revelado que en abril de 2007 fueron 178 las entidades financieras atacadas por *phishing* en todo el mundo, con un incremento del 91,4 por ciento frente a las 93 entidades afectadas durante el mismo mes en 2006. Según el informe, en España -que ocupa el tercer lugar en ataques de este tipo-, un total de siete entidades financieras españolas fueron contabilizadas como "víctimas de *phishing*" con un total de 53 ataques, frente a los 109 ataques registrados en marzo, también contra siete bancos españoles. Reino Unido, con el 10 por ciento, ocupa el segundo lugar y España se mantiene en el tercer puesto con un 4 por ciento del total de los ataques, por delante de Canadá e Italia, con un 3 por ciento del total de los ataques, Sin embargo, en abril, se aprecia que España ha sido también emisor de dichos ataques, aunque continúa lejos de los principales países emisores de ataques tales como Estados Unidos, Hong Kong Corea del Sur y Alemania.[48]
2007 (Abril)	Un menor de edad estafó 3.000E copiando número tarjetas en restaurante chino donde trabajaba, según informó hoy la Jefatura Superior de Policía en Cantabria en una nota de prensa, la investigación se inició a partir de una denuncia que se realizó el 4 de octubre de 2006, en la que se daba cuenta de la utilización fraudulenta de una tarjeta de crédito asociada a un cuenta bancaria por un importe de unos 477 euros y realizada mediante adquisiciones por Internet. A través de las gestiones practicadas se lograron datos de identidad y financieros del autor, así como las direcciones desde donde se realizaban las conexiones, de forma que se supo el lugar en el que se encontraba el acceso a Internet para la utilización fraudulenta. Se tuvo conocimiento de cuatro denuncias más. En todas ellas, los denunciantes decían haber utilizado sus tarjetas para pagar en un restaurante chino.[49]

[47] Libertad Digital. "La OCU detecta irregularidades en las ventas por Internet". Gastos inesperados, Seguridad, Facturas…29 de Octubre de 2007

[48] Laflecha.net "ESPAÑA SIGUE SIENDO EL TERCER PAÍS CON MÁS AMENAZAS. Los ataques de phishing contra bancos han aumentado en un 91% a nivel mundial". 14 de Mayo de 2007.

2006 (Sept.)	Un empleado recibió en su correo electrónico un mensaje publicitario de otra empresa, a la que solicitó por teléfono la suspensión de estos envíos. Volvió a encontrar más correos no deseados y denunció los hechos ante la Agencia Española de Protección de Datos (AGPD). La AGPD, en resolución de 9 de mayo de 2006, dio la razón al demandante por considerar que la empresa denunciada cometió una infracción de la Ley de la Sociedad de Servicios de Información y le impuso una sanción de 1.000 euros, al considerarse el envío de spam una infracción leve.[50]
2006 (Abril)	Agentes de la Dirección General de la Policía adscritos a la Brigada de Investigación Tecnológica de la UDEF Central y al Grupo de delitos contra la Propiedad Intelectual de la Comisaría General de Policía Judicial han detenido a 15 personas en diez ciudades españolas y han bloqueado un total de 17 de páginas web que se dedicaban al intercambio ilegal de archivos P2P, ofreciendo descargas piratas de películas, música, juegos y aplicaciones informáticas. Según informó el Ministerio del Interior, la mayoría de los detenidos en esta operación, sin precedentes en Europa y que continúa abierta, son ingenieros informáticos y responsables de importantes empresas que intervienen en el mercado de las telecomunicaciones como proveedores de servicios en la red. Por primera vez en una operación de estas características, cinco de los detenidos son propietarios de empresas de hosting, que proporcionaban alojamiento gratuito a portales de ficheros P2P a cambio de insertar publicidad o gestionar las bases de datos de los visitantes de estos lugares. Las empresas que prestaban alojamiento a estas webs de Internet aprovechaban el elevado número de visitas de las páginas para promocionar sus productos (alojamientos de páginas web, registros de dominios, servicios publicitarios, etc.) en foros donde los usuarios son potenciales consumidores de servicios informáticos, con la consiguiente ventaja económica derivada de esta actividad. Uno de los responsables de una empresa de hosting ha sido además acusado de obstrucción a la justicia al negarse a facilitar una serie de datos requeridos en la investigación. Por primera vez en una operación de estas características, cinco de los detenidos son propietarios de empresas de hosting, que proporcionaban alojamiento gratuito a portales de ficheros P2P a cambio de insertar publicidad o gestionar las bases de datos de los visitantes de estos lugares.[51]

FRANCIA

2004 (Mayo) Un científico francés se enfrentó a un juicio en el que fue condenado a al pago de una multa elevada tras haber sido demandado por descubrir y publicar varias debilidades en un software antivirus que anunciaba detectar el 100% de virus conocidos y desconocidos elaborado por una empresa francesa. Fue condenado en base a normas que protegen el derecho de autor y normas del Código Penal.
La investigación fue liderada por el *Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (O.C.L.C.T.I.C.),* grupo de la policía que se encarga de los casos relacionados con las tecnologías de la información.

ITALIA

[49] Terra Actualidad. EFE. 04 de Abril de 2007. España.

[50] Consumer.es Eroski. "Spam: 1.000 euros por enviar correo electrónico publicitario sin consentimiento". Septiembre de 2006.

51 NOTICIASDOT, IBLNEWS "La policía detiene a 15 personas y bloquea el acceso a 17 portales de emule y bittorrent". 09 de Abril de 2006

AÑO	CASO
2007	El Gobierno italiano está preparando *un proyecto de Ley que obligaría a los bloggers a depender de un periodista acreditado como "editor responsable".* Este mecanismo de supervisión y control obligaría a los dueños de los blogs a pagar impuestos, aunque no generen beneficios e incluso se podrían enfrentar a penas de cárcel en caso de que lo publicado sea calificado como contenido difamatorio, según recoge la legislación italiana. Tras su aprobación por el Consejo de Ministro el 12 de octubre sólo queda que el Parlamento lo ratifique[52]. De aprobarse la ley, los responsables de una web o de un blog tendrán que someterse, entre otras, a estas condiciones: Deberán registrarse como empresas editoriales; un periodista colegiado deberá asumir el papel de director responsable de todo lo que se publique; Los contenidos difamatorios se pagarán con multas e incluso penas de cárcel según el caso; Estarán obligados a pagar impuestos, independientemente de que el blog tenga o no ánimo de lucro. Esta ley puede considerarse como un ataque directo a la libertad de expresión y podría suponer el cierre del 99% de los blogs italianos.

MEXICO

2007 (Abril). El Instituto Nacional de Antropología e Historia (INAH) no tolera más el tráfico de bienes culturales a través de subastas vía Internet; piezas que, de acuerdo con la Ley Federal sobre Monumentos y Zonas Arqueológicas, Artísticas e Históricas, no pueden ser objeto de comercio alguno. El INAH interpuso una denuncia ante la Procuraduría General de la República (PGR) en contra de los hechos que ocurren en los websites www.mercadolibre.com.mx y www.deremate.com.mx. En la denuncia se solicita que se cite a declarar a los involucrados por posible encubrimiento de hechos delictivos, debido a que su venta y exhibición representa una clara violación a los artículos 29, 49, 50 y 51 de la Ley de Patrimonio. Se pide además, se ordene a los proveedores de servicios de Internet de México el inmediato bloqueo y que se realicen las diligencias necesarias para detener a los responsables, además de asegurar de los equipos informáticos que existan en Mercado Libre y en De Remate.

PAISES BAJOS

2006 (March). Investigadores de la Free University de Ámsterdam han creado un chip de identidad por radio frecuencia (RFID) infectado con un virus para probar que los sistemas de RFID son vulnerables a pesar de la extremadamente baja capacidad de memoria de estos baratos chips. El problema es que una etiqueta de RFID infectada, que se lee cuando pasa a través de un escáner, pueda alterar la base de datos que procesa la información de las memorias, afirma el estudio desarrollado por Melanie Rieback, Bruno Crispo y Andrew Tanenbaum. "Una etiqueta RFID puede ser infectada con un virus y este virus puede infectar la base de datos de respaldo usada por el software RFID. Desde aquí se puede expandir a otras etiquetas RFID", declararon.[53]

PERU

AÑO	CASO
2007 (Junio)	La investigación de agentes de la Policía española ha permitido la detención en Perú de uno de los pederastas más activos de Internet, que conseguía que numerosas niñas, a las que chantajeaba, se desnudaran ante la «webcam» y realizaran actos de contenido sexual. Este individuo -residente en Lima e identificado como M. A. S. Q.- era investigado desde 2005 y tenía en su poder casi 90 vídeos de pornografía infantil. A través del «messenger», este hombre obtenía la confianza de las víctimas haciéndose pasar por una chica de su edad para, después, enviar imágenes de pornografía. También pedía a las menores que realizaran actos obscenos a través de la «webcam» o le enviaran

[52] Noticias24. "Italia quiere regular los Blogs", http://www.noticias24.com/, 25 de Octubre de 2007

[53] IBLNEWS, AGENCIAS. "Los chips baratos que están sustituyendo a los códigos de barras podrían portar virus". 15 March 2006.

	imágenes de ellas mismas. Si las menores se negaban, el individuo, que había infectado el ordenador de la víctima mediante un programa espía, obtenía el control de la dirección de correo de la menor y la amenazaba para obligarla a acceder a sus pretensiones. La investigación sobre esos ordenadores pudo determinar que habían sido infectados con virus de los denominados «troyanos». Identificadas las conexiones, los agentes determinaron que procedían de Lima, por lo que se facilitó toda la información a la Policía peruana.[54]
2004-2005	En el Perú se han venido reportando delitos informáticos como el falso mensaje que se propaló en la página web que simulaba pertenecer al Banco de Crédito, ocurrido en el 2004, y que llevó a que varias personas proporcionaran información financiera confidencial que afectó a algunas cuentas bancarias, informó el Centro de Comunicaciones del Parlamento. Según la División de Investigaciones de Delitos de Alta Tecnología (Divintad) de la Policía Nacional del Perú, en el año 2005 se registró un total de 456 denuncias de este tipo.[55]

RUSIA

2007 (Noviembre). Expertos en seguridad han detectado un sitio ruso que vende acceso a redes bot, que son redes de computadoras infectadas propiedad de usuarios inocentes en todo el mundo. Los hackers infectan las computadoras y las controlan a distancia para realizar ataques coordinados. Los dominios cc pertenecen a las Islas Cocos/Keeling en las afueras de Australia, pero el texto del sitio en cuestión está principalmente en ruso, exceptuando la lista de precios. En el sitio loads.cc se ofrecen “servicios" como intervenciones y sabotaje. Los responsables de loads.cc venden sus servicios como si estuvieran compitiendo en un mercado totalmente abierto. Compiten en servicio al cliente y cobran por sabotajes exitosos. Los compradores de los servicios pueden optar por infectar computadoras de sus víctimas con software de libre elección que les permita decidir por cuenta propia cómo controlar las máquinas infectadas posteriormente. El precio es de alrededor de 20 centavos de dólar estadounidense por máquina. Los compradores pueden especificar los países y las direcciones IP que les interesa atacar.[56]

VIETNAM

En Vietnam todas las páginas web pornográficas están censuradas. Sin embargo, el subdirector del Instituto para el Desarrollo Social vietnamita, ha declarado que una página web "ortodoxa" sobre sexo podría ayudar a las parejas a tener "relaciones sexuales saludables", por lo que planean ofrecer películas educativas descargables a través de la Red. Afirma que existen casos de parejas que no han mantenido relaciones sexuales durante años, que hay altas tasas de divorcio y de prostitución, y que estos problemas podrían mitigarse. Eso sí, el subdirector ha dejado claro que las imágenes que se ofrecerían serían sólo "educacionales".[57]

VIETNAM AND CAMBODIA, Presuntamente en

INTERPOL is making a public worldwide request for assistance in identifying a man photographed sexually abusing children in a series of images posted on the Internet, the first time the organization has made such an appeal. The Bundeskriminalamt (BKA) in Germany working with INTERPOL’s Trafficking in Human Beings unit has been able to produce an identifiable picture. 'For years images of this man sexually abusing children have been circulating on the Internet. The search for the individual has been codenamed Vico after

[54] La razón, “El pederasta más activo en Internet “cazado” por la Policía en Perú ”, 04 de Junio de 2007

[55] Agencia Peruana de Noticias ANDINA. “Proponen en el Congreso la penalización de los delitos informáticos”, 3 de Junio de 2007.

[56] DiarioTi.com. ““Tienda en línea" Sitio ruso vende abiertamente sabotajes e intrusiones” 2 de Noviembre de 2007

[57] Ibl news. “Vietnam: Web pornográficas sí son aceptables, pero solamente las oficiales ”. 20 de Julio de 2006.

analysis of the photographs, around 200 in total featuring 12 different young boys, established that the pictures were taken in Vietnam and Cambodia.[58]

III. CONCLUSIONS

Durante la investigación que precedió estas conclusiones, pudimos observar que los legisladores de cada país utilizan diferente vocablo y definiciones para las mismas cosas, delitos y figuras jurídicas, inclusive dentro de un mismo continente y con la misma lengua materna; lo cual interpretado por el Juez de cada región o país puede conducir a la creación de precedentes y jurisprudencia inesperada y poco armonizada.

Es lamentable que la mayoría de los precedentes resultantes de la aplicación de leyes relacionadas con nuevas tecnologías de la información y de la comunicación provengan de los países de la Unión Europea, de la región Asia-Pacífico y de los E.E.U.U. En América Latina hasta hace dos años, los poderes judiciales argentino y colombiano encabezaban la lista de jurisdicciones con mayor número de casos que versaban sobre estos temas tan novedosos.

ONU, APEC, UE, OEA, OCDE, están trabajando continuamente sobre el tema de la protección de datos. El Abogado peruano Erick Iriarte Ahon decía el 2 de octubre de 2007 que por América Latina: México, Perú y Chile son parte del APEC; se espera que pronto Costa Rica y Colombia se incorporen como miembros plenos. Siendo así, y teniendo en cuenta las prioridades de desarrollo de nuestros países, y además las implicancias políticas de tener a USA y Canadá, es claro que el enfoque primario ira hacia las propuestas APEC, aunque poseemos un acuerdo de la Comunidad Andina de Naciones con la Unión Europea…Ahora bien, si es mejor APEC o Europa, pues me queda claro que uno es mas fuerte que el otro, y hasta complementarios, a diferentes niveles, pero con fines distintos, y que pudieran ser contrapuestos. Nuestros países (en LAC) tienen diferentes perspectivas, e intereses, la regulación es un instrumento de la política, y como tal estamos supeditados a lograr que la política sea en el mismo sentido de la regulación que proponemos. El problema no es si Europa es mejor que APEC, es saber qué persiguen nuestros mandatarios con la regulación, pues las políticas de desarrollo divergentes plantean soluciones divergentes al mismo tema. Mientras que a nivel de la Red Iberoamericana de Protección de Datos se trabaja la temática, y los actores son activos, el mismo tema se trabaja en APEC, y diferente en CITEL, y diferente entre los SocInfo, y sin contar los GRULAC, todos ellos trabajando sin ningún tiempo de coordinación y relación. El problema no es que es lo mejor que se puede hacer, sino como lograr el nivel político para lograrlo.

Es mandatorio, aprobar Directrices y lineamientos sobre estrategias comunitarias en pro de la seguridad de las comunicaciones electrónicas e informatizadas, que incorpore el compromiso de cooperación interregional para la lucha contra quienes pongan en peligro la seguridad mediante las nuevas tecnologías de la información y de la comunicación. MERCOSUR, COMUNIDAD ANDINA DE NACIONES, ECOWAS, APEC, UE, OEA, COMESA, CARICOM y demás acuerdos de integración regional deberían unir fuerzas para alcanzar lineamientos internos sub-regionales que estén fundamentados en lineamientos internacionalmente reconocidos y recomendados, a fin implementar, con más eficacia y mejores resultados, un marco institucional regional que tenga un verdadero impacto en la seguridad infomática.

El entendimiento de la tecnología es condición sine-qua non para regular el contenido de los sistemas de información computarizados, el intercambio de data a través de la red y cualquier otra herramienta tecnológica: por lo tanto, los abogados deben ABSTENERSE de redactar Ante-proyectos de Ley sin la asistencia de ingenieros de computación o de cualquier otro profesional calificado en la materia que nos acontece.

Quisiera reproducir aquí una recomendación dirigida al Legislador de cada país efectuada por el abogado mexicano Gabriel Campoli, mencionado en este trabajo y que me pareció muy plausible. El jurista sostiene que sería muy productivo para quien aplica las normas penales, si el mismo pudiese contar con un Código Penal que comprenda en su artículo mención a una agravante genérica aplicable a todos los delitos allí tipificados que vaya en este sentido "si cualesquiera de las conductas descritas en este Código se realizare con el uso de equipos

[58] INTERPOL Media Release. "INTERPOL seeks public's help to identify man photographed sexually abusing children. Operation Vico". 08 de Octubre de 2007.

informáticos o redes (agregar otros considerandos…) la pena se elevará de un tercio a las mitad de la pena prevista". Quisiéramos sugerir a los Legisladores de países que todavía no han adoptado medidas para luchar contra los actos ilícitos perpetrados mediante el uso de redes, de equipo informáticos y afines, que tomen en consideración la posibilidad de incluir una reforma a su Código Penal vigente en este sentido, en lugar de ponerse a redactar complejas leyes especiales sobre delitos informáticos que en definitiva no sabemos exactamente qué es lo que estarán tutelando estas leyes especiales que sea diferente de lo que tutelan nuestro Códigos Penales.

Adicionalmente, recomendamos identificar los actos ilícitos perpetrados mediante redes y/o equipos informáticos y, luego de hacer un análisis exhaustivo de su Código Penal, identifique cuáles de esos actos ilícitos podrían equipararse a conductas tipificadas en dicho Código y cuales no. Los hechos ilícitos no descritos en ningún artículo del Código Penal deberán ser objeto de regulación especial a través de la llamada Ley de delitos informáticos. Esta ley no debería ser compleja, pues las conductas tipificadas en ella, serían solo aquellas no previstas en la norma penal tradicional.

Para finalizar recomendamos ampliamente establecer, ya sea en la reforma de un Código Penal o en la redacción de una nueva Ley especial de delitos informáticos, la necesaria cooperación judicial e investigativa que a nivel internacional deben mantener las autoridades que conforman el poder judicial en cada país, llámese, jueces, procurador o fiscal y policías especializada.

No puedo cerrar estas conclusiones y recomendaciones sin recordar la importancia para la seguridad en la transmisión de datos a través de las redes, del uso de certificados digitales emitidos por entidades de certificación debidamente acreditadas por la autoridad de cada país, a fin de preservar los siguientes cuatro elementos básicos en el intercambio de datos a través de redes informáticas: integridad, autenticidad, confidencialidad y disponibilidad.

Luc Poulin, consultor senior del Instituto de Seguridad de la Información de Québec, ISIQ, y chief security officer (CSO) del Computer Research Institute of Montreal, CRIM, señaló que la seguridad se basa en tres pilares fundamentales, las personas, los procesos y la tecnología. "Cada persona es importante y dependiendo de su especialidad sabrán qué privilegiar a la hora de proteger sus datos. Por eso el conocimiento y la capacitación son primordiales. Lo mismo pasa con los procesos, la organización debe definirlos de acuerdo a las mejores prácticas y analizando los riesgos, definiendo qué es lo más crítico que se quiere proteger y de qué forma". [59]

Las nuevas tecnologías son maravillosas, pero en manos de delincuentes y gobiernos corruptibles son extremadamente dañinas para las personas naturales y jurídicas, incluso para las Naciones.

[59] La Segunda Internet. "Internet: Experto canadiense entrega claves para la Seguridad de la Información" 4 de Abril de 2007